“FRAMEWORK OF PROVENANCE TRACKING OF DIGITAL INFORMATION USING BLOCKCHAIN”

A thesis submitted to the
University of Petroleum and Energy Studies

For the award of
Doctor of Philosophy
In Management

BY
Deepika Sachdev

June, 2021

SUPERVISOR(s):
DR S.K.Pokhriyal
Dr Subir Purkayastha

School of Business
University of Petroleum & Energy Studies
Dehradun-248007, Uttarakhand

Topic

FRAMEWORK OF PROVENANCE TRACKING OF DIGITAL INFORMATION USING BLOCKCHAIN

A thesis submitted to the
University of Petroleum and Energy Studies

For the award of
Doctor of Philosophy
In Management

BY
Deepika Sachdev
SAP ID: 500049525

June, 2021

Under the Guidance of

Internal Supervisor:
Dr. S. K. Pokhriyal
Professor (Oil & Gas),
Advisor, Vice Chancellor
UPES

External Supervisor:
Dr Subir Purkayastha
President, Neeha Consulting Services,
Texas

UPES
UNIVERSITY WITH A PURPOSE
School of Business
University of Petroleum & Energy Studies
Dehradun-248007, Uttarakhand

June-21

Declaration

I declare that the thesis entitled "Framework of Provenance Tracking of Digital Information using Blockchain" has been prepared by me under the guidance of Dr S.K.Pokhriyal Professor and Advisor to Vice Chancellor, School of Business, University of Petroleum and Energy Studies and external Supervisor Dr Subir Purkayastha, President, Neeha Consulting Services, Plano, Texas. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Deepika Sachdev
SAP ID: 500049525
Research Scholar (PhD Management)
CCE, UPES, Dehradun
Date: 6th September 2021

UPES
UNIVERSITY WITH A PURPOSE

Great Place To Work. Certified APR 2019–MAR 2020 INDIA

June-21

Declaration

I certify that Deepika Sachdev (SAP ID: 500049525) has prepared the thesis entitled "Framework of Provenance Tracking of Digital Information using Blockchain" for the award of PhD degree of the University of Petroleum & Energy Studies, under my guidance. She has carried out the work at the Department of School of Business, University of Petroleum & Energy Studies.

Signature of Supervisor

Dr S.K.Pokhriyal
Professor and Advisor to Vice Chancellor,
UPES, Dehradun
Date: 6th September 2021

June-21

Declaration

I certify that Deepika Sachdev (SAP ID: 500049525) has prepared the thesis entitled "Framework of Provenance Tracking of Digital Information using Blockchain" for the award of PhD degree of the University of Petroleum & Energy Studies, under my guidance. She has carried out the work at the Department of School of Business, University of Petroleum & Energy Studies.

Signature of Supervisor

Dr Subir Purkayastha
President,
Neeha Consulting Services
Plano, Texas
Date: 6th September 2021

Abstract

Digital Information is growing quicker than any time before and by 2020, approximately 1.7 megabytes[10] of new datasets will be created every second for every individual on earth. Sharing information brings both risks and benefits to an organization. Blockchain technology provides an immutable and decentralized based Trust Infrastrutcure. However, it is limited by the scalability Trilema for Transaction Volumes. There are different Blockchain Industry standard Models, each of which provides a varying degree of Reliability, Investment and Benefits.

This Research focusses on three Key Verticals to conduct an in-depth analysis of Information Sharing challenges namely Health Care (IoT Enabled), Education and Online Media. The objective of this research is to objectively analyse challenges in Information Sharing across all three verticals by analysing key use cases encompassing People, Process and Technological issues. Based on Blockchain Industry Model, and Trust Requirements of the Use Case the Research provides a Framework for Optimization.
The **Key Business Problem** addressed by the research is:

- Information Sharing across Industries is Constrained by lack of Trusted Provenance and Has Varying Trust Needs Based on Use Cases
- Blockchain Model Provides a Secure, Immutable and Decentralized Framework for enabling Provenance Tracking and Is currently constrained by Low TPS, High Energy Consumption and Limited Compute Power
- To create a Framework for analysis of Trust requirements of the Use Case with Blockchain capability Matrix

This Research is a Convergence of known limitations of Information Sharing in the Industry and Business Benefits derived from Blockchain. This will provide a Framework for Analysis to help optimize Blockchain implementations in Information Sharing based on Use Case Analysis.

The theoeritcal underpinning of the research is the transaction cost theory of the firm formulated in 1937 by Ronald Coase. As per Ronald Coase given the imperfect market information, when the transaction cost of coordinating production through the market exchange is greater than what exists within the firm, then people start to organize production of goods within the firm. The theory analyzes why certain buyers and sellers exchange more Information than others. The characteristics of the Transaction i.e. the Risk in the Transaction influences the amount of information shared between Partners. Moreover given the high risks of Information Sharing they cannot be fitted into a one size fit all approach. Based on the same**, research objectives** are:

- To identify the influence of Provenance Tracking Intensities based on the Organization Trust Needs for Immutability, Business Verification Rule and Volume of Information Share (TPS)
- To create an Industry framework of Blockchain Patterns based on Provenance Tracking Needs for Immutability, TPS Scalability and Business Logic Implementation using Smart Contracts

The Research uses Grounded Theory and Framework Analysis Technique. Framework Analysis is a Qualitative Technique to get qualitative feedback from the Users who are experts in the identified areas. To aid Qualitative Data Analysis Nvivo 12 was used. The researcher created an initial conceptual lens which is verified by successive rounds of Industry Expert interviews as well as Literature and White papers based reviews to have a final for the industry

The Interview Protocol for the Research is of semi structured format which is refined through Framework Analysis Technique. The target population of the Research is based on Judgmental sampling since it is a qualitative research. Semi-structured interviews were conducted to collect data and NVIVO software was used to analyze the interview transcript. The population is divided into two categories

a). Experts in Vertical Domain including Health Care, Education and Media who contribute to the Industry Challenges and

b). Blockchain Experts to provide inputs on the Blockchain Framework Capability and verify the outcomes of the Model Capability Mapping

Key observations by the Researcher across both the Research objectives across all Industry Verticals as well as Blockchain applications are:

Interoperability and standards:

Interoperability of data does not work seamlessly across various Institute across all the three verticals. There is no mechanism to verify the authenticity of data uploaded by the Institutes in the blockchain. Public blockchains have a deep understanding about how blockchain networks should operate. Hence they are intrinsically more interoperable. On the contrary, private blockchains are dependent on different entities within an ecosystem defining their own shared standards based on mutual agreements. Public Permissioned Blockchains do not inherit the same disadvantage as Private Blockchains since they are not owned by a Consortium.

Transaction Volumes:

Typical Industry data comprising of electronic imaging records or Content Media require large storage requirements and cannot be stored in its entirety on the blockchain In Public blockchains the speed at which transactions are inserted and read by the blockchain, is slower comparsed to private versions. This is attributed to polling to achieve consensus and limits on transactions or block sizes. Storing large amounts of data on the a public chain is not reccomended. Permissioned Blockchains have a significant advantage over Permissionless Blockchains since they have controlled access.

Access Control:

Industry Stakeholders do not have trust on other institutes that content not will be altered without the owners permission. In a public blockchain access is open to everybody while in Private Blockchain only invited and approved parties can participate. Hence Private Blockchains (both Permissioned and Permissionless) can grant User level access contro, including Read and Write

Permissions at an atomic level. Data stored in Public Blockchain is visible to all and hence has Privacy issues.

Decentralization:

In addition to an immutable database, a key requirement for all verticals from Blockchain is Decentralization. Public blockchains (Permissioned and Permissionless) are governed by no Central Authority and hence support decentralization intrinsically. Private Blockchains (Permissioned and Permissionless) are owned by a Central Authority and hence there is no True Decentralization.

Business Rules:

In Use Cases which have extensively documented rules sets Smart Contracts can be coded using Blockchain. Further, payments can be automated based on Smart Contract trigger rules. In Public Blockchains, the Smart Contracts have limitations since the rules need to be replicated on all Nodes which is Time Consuming. Hence Private Blockchains provide more flexibility on Smart Contract implementation compared to that from Public Blockchains.

Operaional Usage:

The trustworthiness of blockchain technology does not preclude the necessity of audits in the real world. External data needed for maintaining blockchains needs Oracles for data verification. In addition the Blockchain needs trained IT resources which is not frequently available currently across all Verticals. Public Blockchains due to limitation of every Node replication offer significantly more Operational overheads compared to Private Blockchains.

Contribution to Industry and and Research:

The research concludes by providing the following Industry standardization:

- A new “Trust Requirements Framework” created in Health Care, Education and Media verticals to enhance Information Sharing across Organizations
- A Blockchain Industry Framework mapping application capability with “Trust Requirements”. The framework will act as a source of reference for Industry to baseline their Trust Requirement. It will be also beneficial for Industry Blockchain Adoption by creating a Cross Metric analysis of Trust requirement with Blockchain Solution capability

The research contributes to the theory by providing a Trust Requirements Model which was absent in the Transaction Cost Theory of Firm. Subsequently, this will help the Organization to create an assessment matrix to optimize the Transaction Cost of Information Sharing.

Chapter Wise Thesis Illustration

Chapter 1- Introduction

Information Sharing in the Industry is constrained due to lack of Trust across Organizations. This results in Operational delays and overheads. Every Organization has varying Requirements of Trust based on Business Requirements, Traffic Volumetrics and Need for Immutability.

Blockchain provides an Immutable, Secure and Decentralized Architecture for Interaction between Non-Trusted Parties. In the ideal scenario if Blockchain is applied for Information Sharing across Organizations it should significantly remove Information Sharing Barriers. However, it Is currently constrained by Low TPS, High Energy Consumption and Limited Compute Power. This is called the Scalability Trilemma in Blockchain parlance. There are different Blockchain Industry standard Models, each of which provides a varying degree of Reliability, Investment and Benefits.

Hence the **Business Problem** is that there is a need for an Industry Framework for Blockchain Models Based on the Organizations Trust Needs for Sharing Information with Partners. This model will provide a Framework for Organizations to Define their Trust requirements. The Trust Framework will be used to identify the most appropriate Blockchain Industry Standard Model.

The **Research Objective** is to increase information sharing across Organizations which is currently constrained by lack of Trust. The Trust Requirements across Organizations vary based on Business Requirements, Need for Immutability and Volumetrics. Blockchain has multiple Industry standard Models which provide varying support for Trust. The researcher shall create a Model to define the Trust requirements for Industry Verticals based on varying levels of Trust Requirements between Organizations.

Research Gap	Research Question	Research Objective
Provenance Tracking Models for Information Sharing based on specific	What is the influence on Provenance Tracking Models of an	To identify the impact of Provenance Tracking Intensities based on the

Trust Needs of an Organization	Organization based on Specific Trust Needs of Information Sharing with Partner?	Organization Trust Needs for: • Immutability • Business Verification Rules • Volume of Information Share (TPS)
Blockchain Frameworks based on Information Provenance Propensity Not Identified	What are the applicable Blockchain Patterns when used for Information Provenance Tracking based on Specific Trust Needs?	To create an Industry framework of Blockchain Models based on Provenance Needs for: • Immutability • TPS Scalability • Business Logic Implementation using Smart Contracts

The Research has used Grounded Theory and Framework Analysis Technique for Verifying the objectives. The Researcher has used Strauss and Corbin's version of Grounded Theory which transitions from Open Coding to Axial and finally Selective Coding for identifying patterns of data in the underlying transcripts. The Dependent Variables used in the Research are Business Rules, Technical Barriers, Interoperability, Transaction Volumes, Access Control and Decentralization. The Interview Protocol for the Research is of semi structured format which is refined through Framework Analysis Technique.

Research Population: The target population of the Research is based on Judgmental sampling since it is a qualitative research. Semi-structured interviews were conducted to collect data and

Software: NVIVO software was used to analyze the interview transcript. Annex -5 captures NVivo Analysis done as part the research. Annex 6 has detail of survey responders based on profile and demographics. The population is divided into two categories

a). Experts in Vertical Domain including Health Care, Education and Media who contribute to the Industry Challenges and

b). Blockchain Experts to provide inputs on the Blockchain Framework Capability and verify the outcomes of the Model Capability Mapping

Chapter 2- Literature Survey

The second chapter focusses on Literature Survey carried out from sources such as research articles, published reports, manuscripts, company annual reports etc. The researcher's extensive literature review covered over two hundred published literatures They key themes are:

- Organization Information Sharing Risks and Barriers

- Cost Challenges of Information Sharing for Provenance Tracking
- Blockchain Models for Provenance Tracking for Information Sharing

Blockchain for Information Sharing is an extensively researched topic in the last four years. Research is focussed on Industry Applications of Blockchain and Case Studies where Blockchain has been successfully applied. Challenges of Blockchain are also document and technical proposals for overcoming the challenges are in proposal and verification stages. The key gaps identified based on the themes are:

- Research is focused on the value of Trust in Information Sharing and how it increases value for the Organization. However, there was no research found which shows an impact on Provenance Intensities in Information Sharing governed by Trust with a need for Immutability.
- Research is extensively focused on the Cost of Information Sharing for sectors. However, there is limited research that correlates various Use Case based requirements of a sector and compares them with Blockchain Cost Challenges.
- There is research in the areas of Industry Framework for Blockchain based on specific Use Cases. However, there is no existing research in the area of Blockchain Frameworks based on Provenance Needs of an Organization defined by the Trust Requirements of Information Sharing

Chapter 3 - Theoretical Premise - Theory of Firm

The third chapter focusses on the Theoretical Premise. Theory of firm is a set of Economic theories which was created around the first world war. Its purpose is to explain the theoretical framework of the nature and existence of the firm is what it explains. The theory explains that a firm will exists when the environment is such that it becomes efficient to produce in a Non-Market Environment. The term “Transaction” was added to the theory in 1931 to emphasize the role of Transactions and not Individuals in the Theory of Firm. This resulted in the Transaction Cost Theory of Firm in 1937 to segregate the Transactions done by Market and Firm based on the Cost of Transactions. In 2010, Ogan added the TCT Approach for Information Sharing with Key Suppliers which introduced the concept of Risk in Transformation. This brought the important concept that information exchange between buyers is influenced based on Trust requirements.

The theoretical gap will be covered by creating a framework to understand the influence of Information Sharing Transactions Costs based on Provenance Intensities governed by varying levels of Trust Requirements between Organizations.

Chapter 4 - Research Design & Methodology

The Research will use Grounded Theory and Framework Analysis Technique for Verifying the objectives. Framework Analysis is a Qualitative Technique which is used to get feedback from the Users who implement the Policies.
The Researcher has used Strauss and Corbin's version of Grounded Theory which transitions from Open Coding to Axial and finally Selective Coding. This is useful to identify patterns of data in the underlying transcripts. Using Framework Analysis, the charted data from various respondents has been compared for getting an in-depth understanding of the phenomenon/problem under study. Framework analysis provided a systematic review of different perspectives from the respondents. The Researcher analysed the patterns of underlying relationships from the row and columns of the matrix.

To aid Qualitative Data Analysis Nvivo 12 was used. The key reason for using Nvivo is the ability of NVIVO to make the analysis transparently available for review. The respondents who have deep expertise in their respective Verticals (More than 20 Years of Experience were selected as part the Framework Analysis technique. Annex 6 has detail of survey responders based on profile and demographics. "Principle of saturation" is used for determining the sample size. When the addition of one more respondent does not contribute any further information or dimension for the study saturation occurs.

Chapter 5 - Conceptual Lens Formation

As part of Framework Analysis Technique, the initial conceptual lens (CONCEPTUAL LENS - 1) is framed based on Literature Survey and is used to draft the interview protocol (INTERVIEW PROTOCOL – 1). All the research papers which were analysed for the literature review in the study were imported into Nvivo & using the tool identification of themes and classification of the literature data was done. Annex -5 captures NVivo Analysis done as part the research. The validity and reliability of the Interview Protocol has been verified using Framework Analysis technique. Annex 6 has detail of survey responders based on profile and demographics.

Variables Used for Research: 25 Independent and 6 Dependent Variable Categories were used as part the Research:

Business Rules: Complexity of Business Rules, Need for External Data to implement Rules, Existing Challenge of Rule Implementation, Business Rule process Document, Future Requirements of Business Rules
Technical Barrier: Complexity of Implementation, Technical Skills of staff, Graphical User Interface Availability, Maintenance Overheads
Interoperability: Trusted Need for Interoperability, Availability Uniform Protocols for Data Exchange, Interoperability feasibility across Data Sources, Business Benefits of Interoperability
Transaction Volume: Number of Transactions done by User, Number of Transactions done by User, Average growth rate of Transactions, Size of User Base, Average Volume of Transaction

Access Control: Trusted or Non-Trusted Consortium, Risk of Data Exposure, User Access Control Permission requirements
Decentralization: Availability Uniform Protocols for Data Exchange, Regulatory Compliance to enforce Decentralization, Cost of Implementing Decentralization, Business Benefits of Decentralization

The Initial Conceptual Lens was familiarized and analysed by Use case Analysis, Literature review and Preliminary Interview with Industry Professionals in Phase-1. The final verification was done by Interview with Industry Experts in Phase-2. Below is a summary of the Technique followed for One Vertical (Education). The same was repeated for Health Care and Media Vertical also. Data Analysis using NVivo has been done in each stage to refine, verify and review the Conceptual Lens and Interview Protocol. The output is a Trust and Blockchain Framework that can be applied for Industry Verticals for Information Sharing optimization

.

Chapter 6 - Study Findings

Based on the Research Objectives and Methodology, there are two categories of Study Findings

- Vertical Wise Use Case analysis of the requirements for Trust Framework
- Blockchain Industry Framework for Capability Analysis based on Trust Framework

The findings are based on Literature Survey and Industry expert's interview. The final output is a Use Case Based Framework for the Three Use Cases across the Industry verticals and a Blockchain capability matrix. The Researcher has also verified the study findings with existing Research. The conclusion is that previous studies are aligned with the current study.

Interoperability

Public blockchains are more interoperable since they are based on common understandings about how blockchain networks should operate. By contrast, private blockchains are dependent on different parties within a system coming together to agree on their own shared standards from scratch. Public Permissioned Blockchains do not inherit the same disadvantage as Private Blockchains since they are not owned by a Consortium.

Transaction Volumes:

- The speed at which transactions are written and supported by the blockchain, is slower in public blockchains than private versions. This is attributed to polling to achieve consensus and limits on transactions or block sizes.
- Storing large amounts of data on a public chain is not recommended.

Access Control:

- In a public blockchain access is open to everybody while in Private Blockchain only invited and approved parties can participate. Hence Private Blockchains (both Permissioned and Permission less) can grant User level access control, including Read

and Write Permissions at an atomic level. Data stored in Public Blockchain is visible to all and hence has Privacy issues.

- Permissioned Blockchains have a significant advantage over Permission less Blockchains since they have controlled access.

Decentralization:

Public blockchains (both Permissioned and Permission less) are governed by no Central Authority and hence support decentralization intrinsically. Private Blockchains (Permissioned and Permission less) are owned by a Central Authority and hence there is no True Decentralization.

Business Rules:

Business Rules are implemented in Blockchain through Smart Contracts. In Public Blockchains, the Smart Contracts have limitations since the rules need to be replicated on all Nodes which is Time Consuming. Private Blockchains give more flexibility on Smart Contract implementation compared to Public Blockchains.

Operational Usage:

- Operational Usage incurs Operating system upgrades and Ease of Data Entry. This is important is Use Cases where the Data Entry is to be done by unskilled Users and not trained IT staff. Public Blockchains due to limitation of every Node replication offer significantly more Operational overheads compared to Private Blockchains.

- Governance around Blockchains is in early stages and is expected to evolve rapidly over the next few years for mass adoption.

Chapter 7 - Contribution to Theory

Key contribution to Theory of this Research is identified in this chapter as:

- The research is proposing a Trust Framework comprising of six variables to analyze the Provenance Tracking Requirements of a Firm for Information sharing comprising of Access Control, Business Rules, Decentralization, Interoperability, Operational Usage and Transaction Volumes
- Trust Requirements Model which was absent in the Transaction Cost Theory of Firm, subsequently, this will help the Organization to create an assessment matrix to optimize the Transaction Cost of Information Sharing.

Chapter 8 - Contribution to Industry

Multiple challenges inhibit Information Sharing in the Industry. The Information sharing needs vary based on the Trust Requirements of the Industry. Blockchain provides a secure Trusted Solution for Information sharing. However, with the emergence of Technology, there are multiple Blockchain Frameworks providing varying degrees of Trust. The research provides six

key pillars for defining Trust requirement based on the Industry Use Cases. It goes further to analyze the Trust capabilities delivered by each Blockchain Framework. This will ensure that the Information sharing Industry is enabled by providing a structured methodology to analyze its Information Sharing requirements and also to analyze the Blockchain Framework that provides the optimum capability.

Chapter 9 - Conclusions and Recommendations:

This paper has identified a Trust Framework for Education, Health Care and Media Sector. It has also created a Conceptual Lens of the Four Blockchain Industry Standard Models against the of six identified Barriers in for Information sharing. All four Blockchain Models provide varying levels of Trust Capability which aligns with varying Trust needs of the Use Case. In conclusion, the research provides Conclusion and recommendations for the Research Questions.

Chapter 10: Limitations:

This chapter focusses on the limitation on the scope of the study including focussed Vertical Coverage as well as fast technological evolution of Blockchain.

Acknowledgements

First and Foremost – Prayers and Thanks to the Divine Mother for bestowing upon me her blessing throughout the research work.

I would like to express my wholehearted gratitude to my Supervisor – Dr. S. K. Pokhriyal, Professor and Advisor to Vice Chancellor for the motivation and guidance provided during the research work. Being a part-time student, there were times when I was on the verge of quitting research. It was only due to the motivation and guidance from Dr. S.K. Pokhriyal that I was able to pursue the research further. The most important message given – "There is only one short cut in research – that is, researching systematically – putting in hard, smart work."

I would like to convey to gratitude to my external Supervisor Dr Subir Purkayastha. Dr Subir has always fostered a culture of research and innovation in the organization which has motivated all of us to think systematically. There has always been a focus on Business Benefits in every aspect of research.

I would also like to convey my sincere gratitude to Mr Sylesh Nechulli, PhD scholar UPES 2015 batch. Even though, not being my Supervisor or co- Supervisor, he spent hours with me – at times, even after working hours, to illuminate me regarding the various concepts of Research Methodology.

Last but not the least, I would also like to thank – Ms. Rakhi Ruhal for the valuable administrative support provided during research – her swift replies to my emails and frequent reminders – helped me to be on track. I am also indebted to SRC members for their valuable suggestions and other non-teaching staffs whose friendly and helping nature made my residencies at UPES very memorable.

Table of Contents

List of Figures

List of Tables

List of Annexes

1. Introduction

1.1 Motivation

1.1.1 Challenges of Information Sharing in the Digital Age

Digital Information is growing quicker than any time before and by 2020, approximately 1.7 megabytes[10] of new datasets will be created every second for every individual on earth. Sharing information brings both risks and benefits to an organization. It is critical that risks arising from sharing information are well appreciated and implemented within global risk management strategies. With the advent of social media and online technologies, information is freely accessible to all, however it is important to understand the Source and Authencity of the information before it is used in an Organization.

This Research focusses on three Key Verticals to conduct an in-depth analysis of Information Sharing challenges namely Health Care (IoT Enabled), Education and Online Media. The objective of this research is to objectively analyse challenges in Information Sharing across all three verticals by analysing key use cases encompassing People, Process and Technological issues.

1.1.2 Quantification of Losses due to Challenges of Information Sharing:

There is widespread literature available on information sharing in research papers as well as Industry white papers. On the contrary, there is very limited literature that tries to quantify the benefits or studies and analyses the drivers and the magnitude of their impact on these benefits.

In recent years there is limited information published in the quantifying the value in the supply chain (between retailers and manufacturers), is starting to become visible. Numeriacl analysis based research that has been done till now does suggest that the total system will see significant benefits from information sharing, when the quantum of Information Sharing is large. When the volume of Information Sharing is increased, exponential growth in the Percentage of Cost Savings is seen by the Information Consumer.

To understand a quantitative magnitude of the savings that can be derived from Information sharing, we can take an example from the Supply chain industry. The use case here is the matching of supply with demand, with the objective of reduceing the costs of inventory and preventimng stock outs. Astronomical savings can potentially be seen. The can range from fourteen billion dollars for the food service vertical to as much as thirty billion dollars for the grocery online industry. These numbers provide an appreciation of the magnitude of savings which are possible based on Industry Sector and the quantum of Information shared between the various participants. As has already been discussed above, the Savings that can be derived from Information Sharing are an exponential factor of the quantum of Information shared.

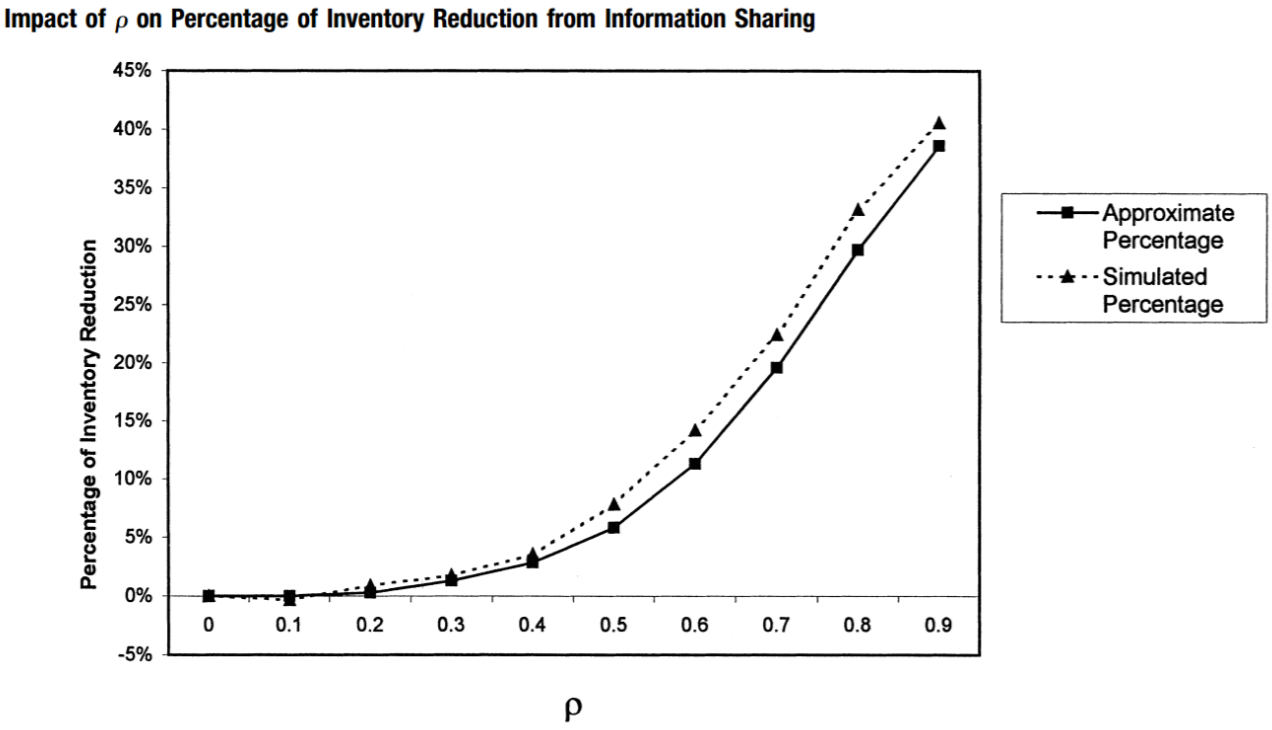


Figure 1: Source: The Value of Information Sharing in a Two-Level Supply Chain - Hau L. Lee • Kut C. So • Christopher S. Tang – May 2000

Education sector has seen significant and pervasive technology adoption in the recent years. Students have been empovered to access virtual learning due to lower data tariffs and cheaper access devices. Education 4.0 is aligning with the needs of Industry 4.0. This education revolutiuon comes with its own barriers & challenges. To analyze in a systematic manner the barriers in Sharing of Information in the Education vertical across some of the key use cases like MOOC Record Keeping, IPR, and centralized, unique Student identifiers is the objective of this research. Key challenges concerning the above scenarios, encompassing People, Process and Technological issues, and the ways in which Blockchain can help overcome the same with its key tenants of Immutability, Transparency, Disintermediation, Decentralisation and Trust are identified and analyzed by this research. In this research, we analyse the applicability of Industry Standardized Blockchain Types namely Public, Private and Permissioned across significant use cases and subsequently recommend Blockchain Roadmap features to enable trust and interoperability amongst educational institutions.

The research categorizes Industry standards based Blockchain Models.It creates and refines a conceptual lens which forms the basis for further analysis. The objective of this research is to identify challenges in industry adoption of these Use Cases and to objectively verify the effectiveness of Blockchain for these scenarios. This is augmented by Literature Survey as well as a detailed Framework Analysis methodology by expert verification in the Industry.

The research is concluded by defining a capability roadmap of Blockchain Models for Education Sector.

1.1.3 Blockchain as a Provenance Tracker for Information Sharing

Blockchain Functional Pillars

The Blockchain characteristics critical for any application are:

- **No Intermediary**: Based on the category of Blockchain identified, the consensus can be owned by public or by a central authority [3]. Decisions are made by consensus. They are not controlled by a single owner.
- **Transparency**: the information can be accessed by all owners [23]
- **Immutability**: once information is stored, it cannot be modified [85].
- **Decentralization**: Multiple participants have access to same information and so there is no central owner of information [2]
- **Transaction Speeds**: Blockchains offer low to high Transaction Speeds. This varies based on the type of Blockchain Framework [64]

Blockchain Schematic

The Blockchain protocol was created by Satoshi Nakamoto[94]. It is a ledger with append-only properties with very limited update or purge features. It does not store itemized transactions. It stores transaction blocks which are chained together cryptographically. Blockchain was originally started by Satoshi for Finance Sector. It is now rapidly spreading to other verticals. It holds the promise of True Decentralization [3] as well as removal of the intermediary. Blockchain has many applications for the Government Sector. As described in [50], Blockchain will help to enable Digital Autonomy in the Government Sector (DAG) [6].

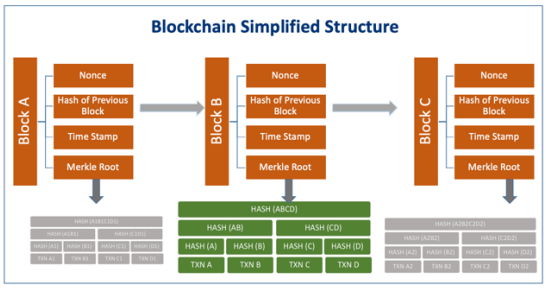


Figure 2: Blockchain Schematic

Blockchain as a Trust Enabler

Blockchain is a Decentralized Asset Managed Platform at its core. Its unique trait is that it empowers third parties who do not have any existing Relationship to exchange trusted Assets [36]. This could vary from, Currency Physical Assets or Digital assets in a highly secure environment. The below diagram demonstrated Data Exchange techniques used in Non Trusted Organizations versus Trusted:

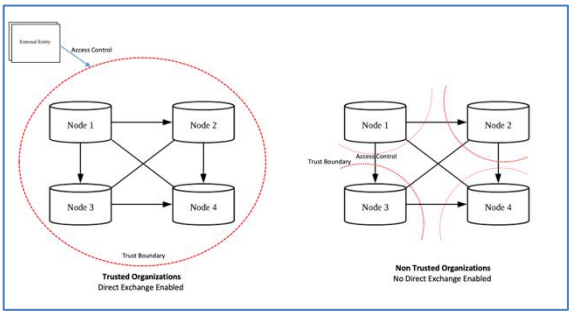


Figure 3: Data Exchange in Trusted and Non-Trusted Organizations

Blockchain technology is applicable for creation of trust in information especially in scenarios which involve heterogeneous stakeholders. In centralised traditional databases, which have a single entity responsible for securing collecting, and sharing information. However for blockchain platforms this is based on shared and decentralised databases which are verified and updated by the user community. In addition Business Logic [6] implemented using Smart Contracts can be truly automated in the Blockchain for verification by users. This will lead to substantial cost and time savings.

Data Integrity and Reliability

In "Decentralizing Privacy: Using Blockchain to Protect Personal Data"[117] it is explained by Oz Nathan et al. that in centralized organizations [118] such as Public Sector traditionally large quantities of personal and sensitive information is gathered. The users have restricted control over the data and how it is used in such scenarios [32]. Further, Nathan et al. proceed to create Blockchain based patterns where the consumers have full control of their data. This eliminates the need to trust third parties with their private information. A key advantage of the Blockchain is that it is tamper proof to fraud due to its Decentralized architecture. This is mentioned by Ahmed Alketbi et.al in [5]

Decentralized Access Control

Unexpectedly, blockchain make it relatively easy to keep data both easily shareable as well as private [44]. Based on how the underlying system is designed, owners can configure permission schemes to manage which user has access to what category of information, what can be shared by which user, and based on which validation rules. Contrary to a traditional database, Blockchain applications enable such capabilities among large, untrusted users without having the need to trust a single authority to do the access control. In the paper [117] Nathan et. have defined a unique Blockchain based Framework in which access-control configurations will be securely stored on the blockchain. Only the authorized users will be permitted to change it.

User Privacy

Blockchain is expected to significantly increase the reliability of information through the use of consensus mechanisms. This will ensure that information exchange happens upon receiving consent from all relevant stakeholders as mentioned in [84]. The Blockchain ensures prevention of the unauthorized change of data and data integrity by the use cryptographic techniques as

mentioned in [5]. Security in blockchain is ensured through decentralized Ledgers. Importantly these are controlled by a consortium and not by an Individual Owners. Blockchain is very reliable in the creation of audit trails of information [45] which are trustable. This makes it simple to create platforms to enable data tracking to audit data entry.

1.2 Business Problem

Information Sharing across Industries is:

- Constrained by lack of Trusted Provenance
- And Has Varying Trust Needs Based on Use Cases

Blockchain Model:

- Provides a Secure, Immutable and Decentralized Framework for enabling Provenance Tracking
- Is currently constrained by Low TPS, High Energy Consumption and Limited Compute Power

Scalability Trillema of Blockchain

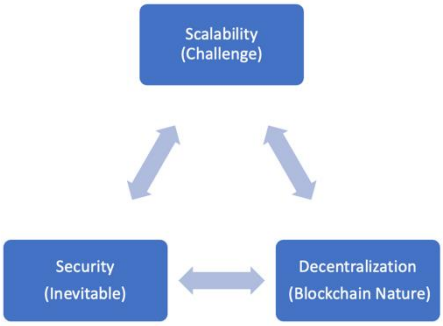


Figure 4: Scalability Trilemma

The scalability trilemma is well-known in blockchain [2]; which was forumlated by Vitalik Buterin, the cofounder of Ethereum. Due to the nature of Blockchain, there are inevitable trade-offs between three important properties: decentralization, scalability, and security.

- Decentralization is the core and the nature of blockchain,
- Security is an essential propriety,
- Scalability is the main challenge.

The number of transactions that can be processed per second is up to 7 for Bitcoin [54] and 15 for Ethereum. Most traditional operational systems need much larger processing power, for e.g. Visa handles an average of 1700 transactios per second [49].

Significance Of Problem Statement: This Research is a Convergence of known limitations of Information Sharing in the Industry and Business Benefits derived from Blockchain. This will provide a Framework for Analysis to help optimize Blockchain implementations in Information Sharing based on Use Case Analysis.

1.2.1 Quantification of Business Problem:

Access Control in Health Care: As per Accenture Analysis, Total Cost of Health Care Data Breaches [67] between 2015 and 2019 is expected to be **$305 Billions** of which $56 Million will be borne by Patients
As per Ponemon Institute 65 percent of victims who encountered medical identity theft had to pay from there pocket costs of approximately $13,500 per patient.

Pay4Performance: A large health care system functioning as a accountable care organization (ACO) for medicare [11] received a bonus of approximately $20 million. However, the health system was unable to quantify the amount, this was not recorded as revenue in its financial statements.

Decentralization in Health Care: Focussing on the benefits of decentralization Walker mentioned that based on review of the elements [85] of interoperability which we can be assigned dollar values, total savings from nation level implementation of complete interoperability across healthe providers and another five organizations could help to save $77.8 billion annually This constitues approximately 5 percent of the $1.661 trillion which is annually spent on U.S. health care.

Record Keeping. Universities frequently charge transaction fees to provide transcripts. Transcript issuance is constantly growing as explained by Tapascott & Kaplan in 2019 [101]. Sixty-two percent organizations have observed an increase in the official transcripts generated by their institution year on year. Average cost to students varies between $5.00 and $9.99.15 based on country and university.

In India, the current system of digital signatutes and digital certificates depends on pre-defined trusted third parties. Due to its nature this current process is susceptible to malicious fraudulent attacks. This is demonstrated in the 2018 case of CEO of CA Trustico which involved mailing private keys of approximately 23,000 certificates.

Data Piracy: Sony, which is one of the three big music labels, conducted a detailed study for identifying reasons for low profitability. The key reason identified was Data Piracy. In a period of three months it posted a loss of approximately 160 million dollars.

Allen Ezell highlights in “Degree Mills: The Billion-dollar Industry That Has Sold Over A Million Fake Diplomas” [98] that more than 1 million fraudulent degrees have been created in

the past ten years globally. As reported by The Star, on an average one in twenty job applicants enter companies using fake qualification in Malaysia.

Due to Covid, the Malaysian colleges, universities and polytechnics have moved to Massive Open Online Courses (MOOCs). In the forecast period of 2016–2023 the growth of online education industry is expected to be 16.4% annually.

Schools also face high costs due to data breaches. A recent study by the Ponemon Institute highlights that a data breach cost is $141 on average per record. However in education it typically peaks to $200 per student record. This has been increasing further, and in last the four-year price is averaging to $260 [102].

Business Problem: Need for an Industry Framework for Blockchain for Provenance Tracking Based on the Organizations Trust Needs for Sharing Information with Partners

1.3 Research Objectives

Key Research Objectives are:

1. To identify the influence of Provenance Tracking Intensities based on the Organization Trust Needs for:
   - Immutability
   - Business Verification Rules
   - Volume of Information Share (TPS)
2. To create an Industry framework of Blockchain Patterns based on Provenance Tracking Needs for:
   - Immutability
   - TPS Scalability
   - Business Logic Implementation using Smart Contracts

Based on the Research Gap, the Research Questions and Objectives are identified as follows:

Research Gap	Research Question	Research Objective
Provenance Tracking Models for Information Sharing based on specific Trust Needs of an Organization	What is the influence on Provenance Tracking Models of an Organization based on Specific Trust Needs of Information Sharing with Partner?	To identify the impact of Provenance Tracking Intensities based on the Organization Trust Needs for: • Immutability • Business Verification Rules

		• Volume of Information Share (TPS)
Blockchain Frameworks based on Information Provenance Propensity Not Identified	What are the applicable Blockchain Patterns when used for Information Provenance Tracking based on Specific Trust Needs?	To create an Industry framework of Blockchain Models based on Provenance Needs for: • Immutability • TPS Scalability • Business Logic Implementation using Smart Contracts

1.4 Research Methodology

.

The Research will use Grounded Theory and Framework Analysis Technique. Framework Analysis is a Qualitative Technique which is used to get feedback from the Users who are experts in the identified areas. The Research encompassed 6 Depenedent and 25 Independent Variables.

Business Rules: Complexity of Business Rules, Need for External Data to implement Rules, Existing Challenge of Rule Implementation, Business Rule process Document, Future Requirements of Business Rules
Technical Barrier: Complexity of Implementation, Technical Skills of staff, Graphical User Interface Availability, Maintenance Overheads
Interoperability: Trusted Need for Interoperability, Availability Uniform Protocols for Data Exchange, Interoperability feasibility across Data Sources, Business Benefits of Interoperability
Transaction Volume: Number of Transactions done by User, Number of Transactions done by User, Average growth rate of Transactions, Size of User Base, Average Volume of Transaction
Access Control: Trusted or Non-Trusted Consortium, Risk of Data Exposure, User Access Control Permission requirements
Decentralization: Availability Uniform Protocols for Data Exchange, Regulatory Compliance to enforce Decentralization, Cost of Implementing Decentralization, Business Benefits of Decentralization

Interview Protocol: The Interview Protocol for the Research is of semi structured format which is refined through Framework Analysis Technique.

Research Population: The target population of the Research is based on Judgmental sampling since it is a qualitative research. Semi-structured interviews were conducted to collect data and NVIVO software was used to analyze the interview transcript. Annex -5 captures NVivo

Analysis done as part the research. Annex 6 has detail of survey responders based on profile and demographics. The population is divided into two categories
a). Experts in Vertical Domain including Health Care, Education and Media who contribute to the Industry Challenges and
b). Blockchain Experts to provide inputs on the Blockchain Framework Capability and verify the outcomes of the Model Capability Mapping

1.5 Chapter Scheme

Chapter 1. Introduction
Chapter 2. Literature Survey
Chapter 3. Theoretical Premise
Chapter 4. Research Design & Methodology
Chapter 5. Conceptual Lens Formation
Chapter 6. Study Findings
Chapter 7. Contribution to Theory
Chapter 8. Contribution to Industry
Chapter 9. Conclusions and Recommendations
Chapter 10. Limitations of Study
Chapter 11. Bibliography
Annex -1 Literature Review Challenges of Provenance Tracking for Information Sharing
Annex -2 Literature Review for Blockchain Frameworks for Information Sharing
Annex -3 Literature Review for Organization Information Sharing Behaviours
Annex – 4 Literature Review for Theoretical Premise
Annex - 5 Glossary

2. Literature Survey

This chapter focusses on Literature Survey carried out from sources such as research articles, published reports, manuscripts, company annual reports etc. The researcher's extensive literature review covered over two hundred published literatures They key themes based on the Business Problem to conduct the Literature Survey are:

- Organization Information Sharing Risks and Barriers
- Cost Challenges of Information Sharing for Provenance Tracking
- Blockchain Models for Provenance Tracking for Information Sharing

The below table explains the justification of the Themes in relation to the Business problem and the Search outlook applied by the Researcher:

Table 1: Themes for Literature Review

Business Problem	Theme	Justification	Search Outlook
Need for an Industry Framework for Blockchain Adoption for Provenance Tracking Based on the Organizations Trust Needs for Sharing Information with Partners	Organization Information Sharing Behaviours	Understand research in Why, Why Not, How and Risks of Information Sharing	Information Sharing, Risks, Benefits, Trust
	Challenges of Provenance Tracking for Information Sharing	Understand Challenges and Standards for Provenance Tracking in Information Sharing	Provenance, Lineage Tracking, Trust, Standards
	Blockchain Models for Provenance Tracking or Information Sharing	Understand existing research done on Blockchain Patterns	Blockchain, Information Sharing, Provenance

2.1 Literature Review

2.1.1 Understanding Issues in Information Sharing

2.1.1.1 Education Sector

Key Use Cases in Education Section encompassing the Challenges for effective Digital Information Sharing include:

Record Keeping: Degree Mills is the term that is used for Institutions which are known to be awarding illegal or fraudulent degrees to candidates without making sure that they meet the educational standards solesly for the purpose of earning the a fees charged for awarding such degrees. These have been deined as "an epidemic of corruption worldwide"[24] by UNESCO's International Institute for Educational Planning (IIEP). Data is available from multiple sources to prove that the prevalence of such Fraudulent academic credentials and degree certificates from such Degree Mills is quite wide spread in organizations today:

- Allen Ezell [9] in "Degree Mills: The Billion-dollar Industry That Has Sold Over A Million Fake Diplomas" have mentioned that more than One Million fake illegal degrees have been generated in the past ten years.
- The Star newspaper in Malaysia reported that for every job application in Malaysia, on average one in every twenty applicant applied with credentials backed by a fake degree.
- Mohamedabad in [76]mentions that South Africa has been taking action against such fake programs & 42 institutes offering fake, unaccredited programs have been closed down.
- As per Giles in [42], currently there are two million fraudulent degree certificates in the United States alone. The US 300 universities issuing fraudulent certificated

- The unfortunate outcome of the acitvites of these Degree Mills is that less than 30 percent of US universities now accept the validity of credentials based on online education as explained by Lam et. al in [62]. The main reason for this is a persistent lack of implementation od Permissioned Access Control.

Hence we derive that a very important requirement in current Record Keeping by Universities is the generation of immutable decentralized [36] certificates. These would be certified once by the University or the Issuing authority and from these on the control will be with the student or reseacrher to publish their credentials to various parties be it their future employers or any higher education institutions.

Managing Education Intellectual Property: The evolution of MOOC's in the last decade has started new patterns related to online education as mentioned by Wahid et. al in [109]. There are interlinked copyright challenges associated with MOOCs. These copyright challenges get associated with the the inter relationship between students, faculty, the education institute, and the MOOC providers [62]. The author and the course content producer(s) in most cases, own the primary right while the secondary rights rest with the company or person(s) who have originally filed the IPRT. As explained by Mohammed et al in [77], trust has a very significant impact on an organizations behaviour and attitude towards sharing of information. Lack of copyright protection for the course material is a very critical problem in information sharing for education [99]. The course content which could include educational course, presentation and lectures is typically created by educators. Thes educators have limited knowledge about copyright management as explained by Mingaleva et al in [75]. The rewards expectation is another very important element of education Information Sharing, and it has a direct effect on the originators of the content as explained by Bock et al in [16]

Awareness about and managementof intellectual property rights, as part of the educational maturity process is now becoming a key mission for educational institutes, as explained by Mok et al in [78]. A European expert working group, ETAN, is focussing on the Education sectors need for training and inculcation of an IP culture as mentioned in [78]. The lecture recording processes is now being used by 71% of the major institutions. The recorded Lecture is a key asset for IPR as per UCISA [90], 2016. The key imperartive for IP in education sector is for the generated content to be associated to the original owner through the maintainance of an immutable record via a digital identity. The critical success factors will be:

- Content Access Control validation via an interoperable network generated for this purpose.
- Business process automation enabling micro-payments based access to Education Literature and automated sharing of Revenue the Creators of the Content[61]

Identity Management: Identity is defined as a linked attribute which is associated with an entity [29] as per ISO/IEC 24760-1. Normally computer use Digital identity to verify the uniqueness of a specific subjects. SSI is an addition, alternate identity solution. Here credentials are provided by a central authority and are in turn verified by a third party in order to review the identity of the holder [36]. The fact that Digital Identity Management [62] in the Education Sector is primarily

conducted by an institute or (in some cases) a country, is an important barrier in this sector. Digital Identity Management is not done globally and this causes gaps.

The known challenges with the prevailing SSI Platforms for Education, which cause decreased Trust can be summarized as below:

- Devices and Browser have Low Security. Result is a lack of Privacy [105]
- Use of weak Authentication Protocols. Result is Identity Hack by hackers
- Central Authority owned and hence lacking Global Interoperabilty [99]
- Not Immutable. Hence easy to perpetucate frauds related to the information identity of Companies [45]

2.1.1.2 Online Media

Hidden 'artist penalty'[71] has been a persistent problem on the internet. Fair recognition of for the creators of digital content and the correct compensation for their work becomes difficult on the internet. Mc Conaghy et al. in [71] has pointed out the problem of online attribution ows its origin to the unidirectional links in the 1989 design of the World Wide Web. The results is no built-in attribution or ownership. As mentioned in [110] one of the three big lables Sony has seen serious erosion of profits due to Digital piracy. An approximate loss of $160 million was reported by Sony for the quarter ending June 30, 2002

Content Distribution systems have had there generations of evolution as explained by Rinaldi [89]. These are on Centralization, Reliability, Scalability and Content Structure. All three generation have face the below mentioned challenges:

Multiplicity of Music Metadata

Each recorded music track has two copyrights

Copyright Category	Description	Meta Data Quality
Musical Composition	Includes the music and lyrics created by Songwriters	Was historically a B2B business, most settlements were based on Sampling or Blanket licensing hence not very detailed information is available
Recording Composition	Created by the recording artists and owned by the labels	Well documented since owned by recording Labels and required for Revenue Settlements

Figure 5: Music Metadata formats

Owners copyright information gets scattered avross the various databases of the record companies, the aggregator societies, and the publishers. These entities do not have any incentives to share or consolidate the copyright information as described by Savelyev et al. in [95]. The fact that artists end up releasing their albums with multiple labels across different countries proliferates the problem. The complexity of Metadata tracking is highlighted as per a 2017 study from Music Reports based on ASCAP [12] below. It shows that for each song, the numbers of Song Writers and Publishers has been continuously increasing over the last few decades:

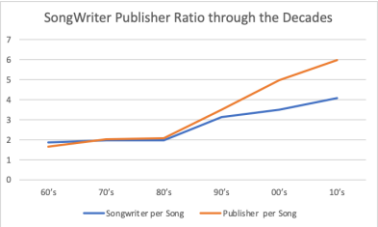


Figure 6: Song Writer Publisher Ratio through the decades

Lack of Metadata Standardization

The status of standardization based on Copyright Category can be seen as per [104], and is highlighted below:

Copyright Category	Standards	Utilization
Musical Composition	ISWCs - International Standard (Musical) Work Codes	Not so widely used since historically involved B2B settlements which were done in Wholesale and not based on Itemized Transaction Tracking
Recording Composition	ISRC - International Standard Recording Code	Widely Used since this is important for Revenue Settlements

Figure 7: Status of metadata standardization

No single source of truth exists, which can be used to correlate Copyright information of the Recordings with the underlying Composition. Some proprietary databases exist, for example the HFA and MRI, but these are neither standardized nor are they very comprehensive [12]. These databases have used different Label Fields for the Metadata attributes. As an example, say the label for identifying the Engineering team is “ProTools Engineers” but when defining the Label Metadata a sapcing is introduced between Pro and Tools ane the lable becomes “Pro Tools Engineers” the credits will end up getting lost.

Metadata Tampering

Almost All commercial-based digital content have DRM and CAS applied have for protection. These Content Super Distribution systems as explained by [54] are constantly targeted by pirates. They pirates hack them with the intent to steal the content or alter the Metadata without the due legal procedure.

CSS (Content Scramble System) which along with regional coding is still used to protect DVDs was hacked by a teenager in 1999. Lee [63] has explained the critical problem that the DRM systems in vogue today only focus on the Media Distributor and Consumer relationship. The complex chain of actors involved in creation of content and its processing gets completely ignored.

As explained by Bhowmik et. al in [14] MPEG formats were developed as a result of significant effort directed toward creating an efficient multimedia distribution systems. This end result is that the networking for Multimedia Delivery has become very content centric. However, the

indexes can be easily removed as explained by M. O'Dair, The networked record industry: How blockchain technology could transform the consumption and monetisation of recorded music [80] due to which content integrity [46] and security can still be compromised.

Human Error
Normally when a song is completed, the composer, artist or producer compiles the Metadata and publishes to the Distributors, Labels, and Digital Streaming Providers as explained by M. Zhaofeng, H. Weihua, G. Hongmin in A new blockchain-based trusted DRM scheme for built-in content protection [116]. The Metadata entry is complex. Mostly initial submission are rushed and this leads to incorrect or missing entries. These lead to human error in submissions.

International Regulations
Music is heard in all countries and languages. Music distribution has multiple challenges including different copyright laws per country, multiple languages and an overall hesitation to share Information. This results in siloed Meta Data which is fragemented for the same piece of Music Content as explained by by Taylor, Karen,[4] Sanghera, Amen, Steedman, Mark & Thaxter, Matthew. The US mandates that Creative Work is copyrighted as soon as it is created. In addition there is also a mandate in case of lawsuites to be registered with the UC Copyrights office. This is not sufficient to prevent piracy.

Transparency in Revenue Settlement
A primary trait and the key advantage of online channels being utilized for Digital Media Distribution is the direct nature of the medium. Critical for successful marketing and Revenue distribution [12] is the transparency, correctness and validity of Content Meta Data. This includes the identity of the artists, the content aggregator and the composer. This transparency with the Content owners is completely compromised due to the siloed pipelines which results in fragementation of Metadata.

2.1.1.3 Health Care (IoT Enabled)

The researcher analysed the Barriers observed in Information Sharing in Healthcare Sector. This was analysed in important use cases for Medical vertical. The following key Gaps were identified:

Aggregated Clinical/administrative data Availability for Research: While there is progress in digitization of paper records, enablement of the sharing of patient data across providers has still not happened. Patients medical records get created with multiple healthcare providers as patients visit different specialists, change healthcare plans or move to a new city [85]. The records typically reside in separate discrete data silos, which have their own storage structures, security mechanisms and descriptive semantics. This complicates secure data sharing between patients, providers and the payers.

A key factor for electronic medical record (EMR) global adoption is by ensuring interoperability in medical standards[17].

Interoperability in standards is a primary prerequistite for ensuring that EMR gives us the requisite economic, social and trust benefits. EMR adoption will further augment the challenges in information that are wide spread in the current manual based medical files as explained by [53] if we do not cross the barriers of interoperability. This will increase the control of patient information by some limited institutes and lack of global data availability. As explained by Tanesh (2019), The primary challenge is modification in current electronic healthrecords (EHR/EMR) is the maintainence of interoperability among various stakeholders who are involved in patient healthcare.

More than 500,000 different types of medical devices, including wearables, implanted and stationary medical devices are manufactured by Medical technology (Medtech) companies [105]. Big Data Analytics in Healthcare can take advantage of connected devices only with the improved availability of data structure standardization, access security, as well as storage and exchange as explained by [57] et. al.

With a 48% rate of annual increase as explained by Mehndi Hassan (2019), Halthcare data is expected to enter the yottabyte (one yottabyte ¼ 10008 bytes) range by 2020. Healthcare analytics industries are growing exponentially with a compounded annual growth rate (CAGR) of 27.3%. By 2022, this is anticipated to reach 29.84 Billion USD from 8.92 Billion USD in 2017.

Patient Data Security: HIPPA, Health Insurance Portability, and Accountability Act regul;ates and governs the privacy of a patient's data [51]. A key requirement of HIPPA is that PHI (Patient health information) has to be secure from breaches and modification. At the same time patient data cannot be restricted and the security regulations need to be manged to allow this. Healthcare is a complex system involving multiple entities and there is a requirement for patients to share their medical records and data across the ecosystem.

Malware attacks on Health Care records are quite common, as explained by [86] in May 2017 the treatement to thousands of British patients was delayed as GPs and other vital services across NHS were iimpacted by malicious software. US cyber-warfare agents had manually created a virus for hacking of data which caused this effect.Across the UK approximately 30 health service organizations had malware attacks, many more had to be temporarily shut down as a precautionary measure.

The data leakage and potential shortcoming in security mechanism has made the patients hesitant to share and store their personal medical information as mentioned by Tanesh Kumar (2018) [51].

The is also a trade-off between the availability of computing capabilities versus the quantum of medical transactions and this can potentially limit the scalability of healthcare systems.

The growth of data and Connected Devices is creating more difficulties in securing patient information at the hospitals and clinics. The factors critical for success will be:

- An interoperable network for validating Health Care Information Access Control [31]
- Automated Business processes that enables micro-payments for Revenue sharing and enables the access to Healthcare Literature, as explained by Bram et. al in [18]

Thhe data accuracy needs are different for regulated and non-regulated health data as mentioned by [37]. Unlike Marketeers, Health care providers require very accurate patient data. Hence Security and Provenance related requirements vary across Business Needs.

PayForPerformance: As explained by Roxanne J. Kovacs (2020) Pay for performance based incentive schemes have been developed globally including low income countries. This schemes ensures that health care workers are giving financial benefits for ensuring that good quality health care is provided to all segments of societ based on agreed KPI's.

Studies show there is a lot of variation in the effect of P4P schemes on outcomes based on Performance Plans and Information availability. Incentive design is being adequately reported is a key observation. Many studies fail to report key design features. Mehmet [11] explains that a key enabler for P4P based models will be the availability of Digital Health Information exchanges (HIE) which are able to accurately provide information tracking points. The validity of such HIE is subject to trust of the provider and the Health Care provider can manipulate data to tamper the results [13].

Counterfeit Drugs : The prevalence of counterfeit medicine is an increasingly acute and urgent worldwide issue, as explained by Matthias Mettler (2016) [74]. World Health Organization reports say that ten percent of drugs worldwide are counterfeit. In developing countries this number can rise up to 30 percent. The impact of counterfeit drugs is not limited to so-called lifestyle products but it also impacts drugs for the treatment of critical diseas like cardiovascular disorders and cancer and medicines like antibiotics, painkillers, contraceptives and other prescription drugs.

Siyad et. al (2019) have explained that during the drug manufacturing and manufacture, Blockchain could play a pivotal ro.w

Blockchain can be used for evaluation, monitoring, and managing the production processes of

The process of potential drugs [4] manufacturing, design, analysis, management and patient monitoring can be tracked and audited on Blockchain. Hyperledger one of the most popular private Blockchains has recently launched a project for fighting counterfeit drugs. In this drug traceability from creation to distribution is tracked over the private permissioned Blockchain platform for eliminiation of counterfeit drugs [97]. Since the Blockchain has an immutable audit trail, any changes in the Drug supply chain are effectively monitored and drug. This is extremely

useful for developing countries where fraud practises in drug manufacture can cause serious damage to patients health.

Provenance of Diamonds and other high value items is currently stored on paper. This can be easily tampered with or stolen, as mentioned by Deepika Sachdev (2019). In the health care sector counterfeit drugs which have been manufactured illegally can cause life long effects for patients (Mackey & Nayyar 2017) [43]. Illegal manufacture and supply of products is not limited to health care industry. It extends to high fashion handbags, expsnsive shoes, diamonds and watches. (Lomas 2015). The TE-Food research shows that even data which is generated from a third party like the inventoru systems, is not trusted by other members [44].

Smartcontract-enabled software in place at the point of sale as explained by Bajpai (2016) [15] can be used to alert the relevant authorities. This will prevent pharmaceutical fraud from impacting millions of unsuspecting victims.

2.1.1.4 Fintech

Fintech applications are driving innovation in Financial Technology and are helping to create more innovative & efficient solutions. Traditionally the Financial Institutions are extremely conservative businesses. They have transformed at a slow pace. In this sector, gaining trust & building reputation is a slow process, but loss of reputation can happen very quickly [55]. This can result from Technology issues like outages of critical systyems, security lapses and malicious activities like hacking and ransomware, insider fraud, financial fraud, non-traceability of funds and numerous other such issues [39]. The need for consumer protection, regulation and stability of financial markets, national financial governance & continuity of critical financial services mandate xtremely heavy regulation for this sector. Traditionally there is lack of Trust in the Regulatory Framework if the Financial sector is not well regulated [55].

The first layer of pressure on the speed at which technology in the Financial sector had to change was unleasehed by the mobile, digital era [2]. There was a need to bring financial services online, this in term required the integration of the various services offered to a customer by the bank. It also neccessiated the real time integration between intra-bank & inter-bank processes. The banks were working on making the customer interface more real-time and digiotal, in parallel alternat players started offering services for lending, mobile payments and online trading with little or no participation by the banks [50].

AI is driving the next wave of innovation in Fintech. This is enabled by the greater computing power of new dense computing infrastructure and with higher involvement and collaboration among among financial institutions and FinTech start-ups. Blockchain powered cryptocurrencies, digital advisory and trading systems powered by artificial intelligence (AI) and machine learning, equity crowdfunding, mobile payment systems, financial inclusion, and peer-to-peer (P2P) lending systems are examples of the new trend FinTech innovations [5].

Financial innovators are taking distinctly separate approaches in the developed & developing world. In the developed world the focus of the Fintech play is primarily around process simplification & speed. Alternate methods of credit rating, crowd funding, automated online investments, and cryptocurrencies have been the dominant areas of development [52]. In the developing world the focus has been Mobile Payments, Mobile Money or Mobile Wallets, Micro Payments & lending, and New Payment Banks.

Governments, Regulators and the the Financial Institutions continue to be the significant actors in the Fintech vertical. The new actors are the Fintech Innovators or the startups and the Fintech Investors who are providing the financial base to the Fintech Innovators. All of these players are services that "End User" who is progressively becoming more and more used to instantaneous responses & high quality of service on her digital screen be it the Mobile device or the Computer / Laptop [82].
Crowd funding is one of the better researched areas in the Fintech space and it has seen significant development. But lack of regulation in this space which does not have any consistent global standards. Crowdfunding disrupts the traditional financial fund raising model but replaces the old intermediaries with a set of new ones and the business has multiple issues of investment protection and ensuring that the lay investor does not get duped which has resulted in slower regulatory acceptance. Hence application of Blockchain in this space is currently unregulated [55].

At the broadest level Blockchain will be key catalyst in the Fintech space but is not a standalone technology to drive this vastly complex sector [111]. The use cases which Blockchain will actively enable to further drive Fintech would be around Smart Contracts, Digital Payments, Share Trading and Digital Identity among others [81].

Preliminary research in this space would the direction of regulatory support that the Innovators in the Fintech Space can get to thrive in a well structure financial market that takes care of the regulatory, needs for Federation of Identity, monetary controls, financial transparency etc.
Since this Research focuses on Information sharing Use Cases and Verticals, hence fintech shall not be included as part of this study. This shall form part of further research work.

The literature review was carried out from sources such as research articles, published reports, manuscripts, company annual reports etc. The researcher's extensive literature review covered over two hundred published literatures (referenced in Bibliography section) relevant on the subject. Based on the need for the research discussed earlier, the review of the existing literatures have been under three main themes namely:

- Organization Information Sharing Risks and Barriers
- Cost Challenges of Information Sharing for Provenance Tracking
- Blockchain Models for Provenance Tracking for Information Sharing

2.1.2 Theme: Organization Information Sharing Risks and Barriers

2.1.2.1 Information Sharing Risks and Barriers in Education:

Centralizated Data Storage Challenges

Efanov & Roschin , 2018 highlighted that centralized management and data-storage systems are susceptible to intrusion, hacking and data breaches.

[28], Eman Yasser, Yousef Awwad Daraghmi, & Yuan, Shyan Ming (2019) highlighted that over the last decade, the adoption of new technologies for the daily management of Electronic Academic Records (EARs) have started worldwide. But EARs are usually physically localized and institutes maintain separate EARs, which are not connected to each other. This creates problems for individuals who transfer from one institute to another, and when they search for jobs or scholarships. Moreover, the gap among various institutes makes the availability of data for newer institutes not available for predictive analysis.

Significantly, a student may have to visit more than one university in the period of his study, such as registering in one university while taking courses in another.

Degree Mills

Asiri, Layla [9](2020) suggested that typically, the certificates/diplomas are produced on paper have some limitations. Paper certificates and diplomas require manual issued and verification; this process becomes time-consuming. Moreover, counterfeit paper certificates/diplomas can be purchased from mill diploma websites. This indeed questions the credibility of academic degrees and fake certificates.

In 2018, BBC News had published an article based on a software company called *Axact* dealing in selling fake certificates and diplomas [9]. After selling around 215 fake diplomas, the company earned approximately 51 million. BBC found that there was a list of people in the UK who bought fake diplomas for different purposes from this Pakistan based company. Allen Ezell, former FBI agent mentioned that, “We live in a highly credential aware society globally [42]. As long as we rely on paper based documents, there is going to be scenarios where somebody counterfeits the papers and prints it and sells it” [9]. Also, a newspaper discovered that the LinkedIn network stores thousands of fake resumes and fake degrees [1]. Students traditionally modify their resumes to ensure they fit the requirement; just like some others filter pictures on social media.

Choudhury, Tanupriya (2020) in the US explained, owing to reputation created by existing Degree Mills, it is observed that less than thirty four percent of reputed universities recognize the value of online institutes. This is because Permissioned Access Control for university data has not been strictly implemented.

Grolleau, Gilles (2014) [42] shares evidence that refers that

diploma mills are not a new phenomenon. They have been in existense since the times of the American Civil War. Recently the increase in fraud degrees has reached gigantic proportions globally. In January 2005, Ezell and Bear 2005 , the two experts in the field defined the fake degree business a "billion-dollar industry that has sold more than a million fake college diplomas" [42].

As per Bahur (2003), Approximately 800 individual diploma mill operators ogrss well over $20,000,000 per year.

Gilles Grolkau, Tarik Lakhal and Naoufel Mzoughi explained that the internet has reversed the trend of geographical limitation of degree mills. The fake industry actually effects all countries. Anecdotal evidence supports that English speaking countries are larger education markets. These are more widely impacted by the fake diploma industry (Brown 2006) compered to smaller ones like the French.

According to Moore, Michael Grahame [79] (2009), the extent of the problematic situation is indicated by reference to an inventory maintained by the state authorities in Michigan. A staggering six hundred alleged diploma mill institutions (State of Michigan n.d.) are reported. Approximately 200 Million profit from this activity is estimated.

For the purpose of collecting data, the study International Journal (2017) identified the research department of Kenya National Examination Council [83]. Ten respondents were randomly selected in the department. For collection of qualitative and quantitative data, pre-defined questionnaire was used as the primary data collection tool. The results highlighted that 87% of the respondents highlighted that the pre-defined security features on the certificates were insufficient to avoid document fraud. In addition, another 98% stated that a computer-based system would help in recognition of illegitimate certificates. At the time of prototype testing approximately 78% students were convinced that an existing computer system was used for the existing methods of certificate authentication.

To ensure that these requirements are met is conducted through verification of certificates. Quite frequently, these institutions are victims of fake certificates (Muthoni, 2015). A very large number of students used fraud secondary school certificates to aquire admission into training institutions as well as institutions of higher learning[76] (UNMC, 2014). Success of using fake academic certificates inorder to get enrolled into these institutions is a validation that the procedure being used is to verify the authenticity of certificates is questionable.

In 2020, [92], Omar S, Ghazali, Osman & Rana, Muhammad Ehsan stated employees provide fake degrees to organizations to prove there academic qualifications. It is expected that there are about 2 Million fake degrees in circulation in the United States alone. In the US alone it is expected that there are about 300 fraudulent universities [7]. This is expected to be the highest number of fake Universities globally. This is followed by United Kingdom next with approximately 270 fake institutes. In addition, Healy (2015) states that more than thirty percent of the candidates in Australia shared faking academic degrees for the securing employment. [8] It is observed that majority of the candidates lay false claims educational credentials [9] about some part of the academic career. It is observed that academic fraud due to illegal certificates costs employers approximately $ 600 billion every year.

In 2018, Sun, Han, Wang,[99] Xiaoyue & Wang, Xinge referred that the current manual form based system of online education have many issues even though it is immensely popular. The learning results and processes of MOOCs do not get public recognition and public certification. The courses security entirely depend on the online and centralized education platform. Hence the students' privacy can be compromised easily.

In today's internet world where data is easily accessible and tamperable it is extremely hard to maintain the authenticity of intellectual property.

To make the learning process and results reliable, it is extremely critical to develop a distributed and trusted data storage mechanism to record the students learning records. In the current environment, since online education has just started to evolve there is lack of secure and mature online paltforms for sharing of academic information across institutes.

Access Control

In 2020, Lam,[62] Tsz Yiu & Dongol, Brijesh mentioned that assessment is the most critial process in the student education industry. It helps to convert the learning process into credentials ability as described by (Campbell, 2010, p. 160) while enforcing a learning culture. However, due to a lack of transparency in the evaluation process, there arises the option of mistrust and tension amongst the students and the educational provider. Brown (1999, p. 62) stated that there exists sufficient evidence to conclude that the current examination system makes it hard to provide a reliable, transparent and proven system to assess student results.

Suhre, Torenbeek, Jansen collected information from university students for six months to understand their goals to study, and found three main factors: personal motivations, inherent abilities (some examplses are the fear of failure or the need to achieve), and transparency in assessments. In 2006, Bryan and Clegg (p. 100) research indicated that under extreme pressure, the full potential of students is realized.

Mohamedbhai, Goolam [76] (2016) explained that even if there is different level of motivation amongst the students, there is an equal visibility of corruption in higher education in the developed and the developing nations. It is observed that in the West, corruption is more

frequently triggered in higher education since it is highly commercialized. Higher education is slowly getting converted into a corporate business or rather money-generating institution. Industry has strong linkages to higher education institutes and hence the level of control is increasing. Contararily, in the developing world, there is limited resources resulting in content of student admission. This is supplemented by need of faculty to raise additional income as well as publishing research papers to climb the academic ladder.

In April 2015, the Four Corners program of the Australian Broadcasting Corporation [76] clarified instances of how through the bad practices the principles of Australian colleges are being undermined, especially because of the tension on them to enroll unfamiliar understudies and to guarantee they finish the tests to get reserves. The models incorporated the inclusion of deceitful enrollment arbiters just as colleges graduating ineffectively qualified or unqualified medical caretakers, common copyright infringement, cheating and abuse. The program was [40] truly characterized as Degrees of Deception." In 2014, a diary on Australia migration administrations seemed exhibiting how the misrepresentation and defilement inside and outside the nation allowed a huge number of unfamiliar understudies to procure illicit perpetual residency visas in Australia. This had prompted work of Degree Mills. The offer of phony degree certificates of noticeable colleges and the activity of organizations that give degrees scarcely any time of study, regularly known as degree plants. There are accounted for cases 14 Number 84: Winter 2016 There were instances of bought counterfeit levels of global Higher Education by legislators, strict pioneers, and other senior officials in different created and agricultural nations. Greatest degree factories are situated in North America and Europe, while others are dissipated worldwide in secret areas. It is likewise notable that either advanced education associations work with no accreditation, or get licensed by sham accreditation bodies, called accreditation factories.

In 2005, Mohammed, M. A., Maroof,[77] E. Y., Thamer, Ali & Huda, I. mentioned that trust can affect the employee’s behaviour to share information. Besides, it can expand the efficiency and precision of their electronic information sharing with others [30]. Hence, the lack of trust between employees in public organizations can create problems to share the information electronically [40, 41]. Trust is measure of behavioural characteristics. Trusting each other at work and collaboration of information and knowledge efficiently among organization employees is extremely important. [31, 42]

In 2019, Tapscott, and Kaplan, state that students, guardians, and workers will begin asserting their privileges to learning institues: Schooling establishments and organizations should now basically place responsibility for information under the control of the actual students or to their guardians and representatives. It is important to ensure the security and network protection of researchers. As of late, inquiries of character, security, and protection of student information have faced questions from suppliers and clients of Eduction Technology. Notorieties of College have been brought to light and fraud frameworks have been hacked. To deal with students rights numerous discussions have approached. For example, innovation organizations like IBM, foundations like MIT, guidelines associations like IMS Worldwide Learning Consortium,

and blockchain schooling organizations like Learning Machines have started verification process for student degree certificated.

MOOC & IP Protection

E-learning credentials are still quite under objection and interrogation and considered as inferior in developed countries as well as developing. In the US, approximately 33% of college resources have been recognizing the significance and authenticity of online training. This rate has noticed a change over a time of nine years. Responsibility and transparency are fundamentally needed for advanced education. This advocates quality managing lifecycle based on multiple review cycles. Employers have deep motivation to understand in the real assessment of the candidates and there ability since it will in general impact the worker enlistment program.

Mingaleva, Zhanna & Mirskikh, Irina [75] (2013) mention that intellectual property can be generated by the lecturer whilst the process of education (on lectures, tutorials, etc.) seldom uses the employer's (university's) services or aid. These circumstances give assent to numerous problems the most serious of the lot being the making of decisions about whom intellectual property rights shall belong to. Russian Laws including Law on Education and Civil Code do not look after the copyright relations between the lecturer and the university in the ongoing educational process.

The gradual change in digital technologies and the internet led to the change of copyright ownership policies placed on the content of education courses and lectures. Thanks to the internet, the content of lectures, seminars and education courses, ideas and information belonging to the teachers, educators and universities have arrived into free access and public domain. Putting a halt on the dissemination of educational information is nearly impossible.

Rios-Amaya,[91] Juliana, Secker, Jane and Morrison, Chris (2016) directed an overview on the copyright and licensed innovation arrangements of higher instructive establishments of the UK to address the recording systems. The normal custom of utilizing institutional semi-robotized address recording frameworks is turning into a broad method with 71% of foundations purportedly utilizing it in 2016. However, these frameworks are dependent upon various inquiries concerning copyright and IPR that in certain cases are being reported in explicit approach archives. Issues that surface comprise of the content that is procured from the resources, the ownership of the resulting products and responsibility undertaking for utilizing the recorded material in the talks. These issues are likewise frequently related to with more extensive basic moral ascribes like character, protection and scholastic opportunity. The review discoveries are introduced alongside an investigation of strategy of IPR archives and strategies from 11 establishments. These are verified by the direction given by Jisc (2015) [90]. The review techniques uncover that a large portion of the organizations are still creating as far as their IPR strategy with recording addresses. The instructors gets consent of license from numerous foundations, yet addresses are noticing an expansion in recording rather than a reduction.

The review uncovered that in 94% of the cases the teachers or moderator is responsible for any instances of the outsider involved inside their talk. However organizations do give ideas with respect to taking care of outsider substance, a generous measure of it is conveyed in a generally manageable manner, through concurring after utilizing the framework or by information made effectively available online in guides. The discoveries from the strategy investigation portray that those bodies with an undeniable degree of institutional control regularly have a higher fluctuating scope of approach towards the use of talk recording. Also, the establishments that offer a higher help level for exhortation on copyright, have an inclination for coordinating open practice and more elevated levels of craving for hazard. A word of wisdom of training for organizations and insight for research ahead are introduced as a feature of this investigation.

Wahid,[109] Ratnaria, Mohd, S., Bakri, Subhan, Muhammad Azizuddin, Mat, & Saidin, Khaliza state that complex copyright issues are displayed by the MOOCs. This arises questions on the association among the higher education institution, its learners, facultyand MOOC providers.

Via copyright law, original works owners or authors have been provided with economic security in order to reproduce, publish, issue copies, rent out, lend, perform, broadcast, show, play, make adaptation or permit others to securely reproduce the original work. It is the responsibility of a copyright owner to have complete ownership to restrict or regulate the mechanisms by which the orignal work may be tampered or used by others.

Technology Barriers

In 2005, Mohammed, Thamer, Ali & Huda M. A., Maroof, E. Y., [77], I. referred to the different attitudes towards Technology. It can play significant roles in the acceptance and actual use of computers [43, 44]. On the other hand, older academic staff may be unskilled with ICT in their teaching structure, especially if they do not use it in their academics.

Tse, [107] By Emily & Education, International (2015) described a study conducted in 2010 which showed that 23 individuals on LinkedIn provided degrees from Almeda University which is a Degree Mill. The same study was conducted two years later in 2012 in which the number of students jumped to 2500 from the same institute by Ezell and Bear.

Subsequently a third study was conducted in 2015 In which the student number increased from 2500 to 4,000 from the same University (Neifer, 2015).

2.1.2.2 Information Sharing Risks and Barriers in Health Care:

HIE Benefits for Health Care

In 2017, Ayvaci, Mehmet, Cavusoglu, Huseyin, Kim, Yeongin & Raghunathan, Srinivasan reviewed that while mobilizing from “paying for volume” (fee-for-service) to “paying for value”

(some kind of performance-based payment), there will be stronger incentive for providers to produce high quality efficiently. To achieve this- coordination, elimination of duplication and outcome tracking is required. This will be facilitated by health information exchange. Logically, it will be good to rely on new payment systems to achieve the right outcome measures, so that they have strong quality side incentives.
In addition to that, while participating in an HIE, a provider is less likely to repeat diagnostic tests. Particularly, when test information from other providers is made available as part of electronic health records.

In 2019, Khezr, Seyednima, Moniruzzaman, Md, Yassine, Abdulsalam & Benlamri, Rachid mentioned that to improve the healthcare system quality it is required to share healthcare and medical data [59]. The sharing of health records could take place between individuals and also possible between an individual and a stakeholder. For example- during a doctor's visit for the very first time, a patient would like to share his medical history [66]. Along with sharing between individuals, sharing could also happen such as between a patient and an insurance company. Let us take the case of patient who wishes to share his medical history with a research centre or an insurance company. The data can be shared within or outisd the country [67]. But there are some evidences of limitations in operational mechanism of today's health-related systems. In case of health records, patients hardly have access to them. The patient is not informed about the process and privacy protection mechanisms implemented in sharing of their own health data with untrusted partners [68]. The blockchain based healthcare plays a very crucial role in improving the information sharing mechanism of electronic health data. This in turn, enables improved interactions and collaboration with the healthcare industry. [69].

It is observed that many institutions have undergone loss of reputation and capital. As the medical care organizations are information driven, and the volume of information produced is filling significantly in this period unlike any another time with the advent of IoT [74]. The information security and protection are constantly abused either inadvertently or by unlawful clients.Data access should be provided by properly allocating different roles to different users.

Challenges in Health Care

In 2016, Kruse, Clemens Scott, Raval, Yesha & Marawi, Goswamy, Rishi, Sarah researched that the EHR's sharing of data is intra-organizational i.e., they share data within the same organization, still it is observed that EHR platforms are fragmented. The absence of information normalization causes issues in transfer of information [5,25]. Information is implemented in design patterns that are not operable with all applications and advances [13,22]. This prompts confusion in information procurement as well as purging processes. The information is rarely normalized for data storage. Restricted interoperability represents an enormous test for large data sets of information to empower verification and worldwide sharing [12,13,16,22]. Such issues are caused in obtaining and purging of information into a normalized design [13,17,23,25,27].

Cost of Data generation is comparatively less compared with the transfer and storage of the data. Even though data is generated easily, the secondary costs associated with storing and securing

them are high [25]. Costs will also be rendered while transferring and analysing data across locations. [14,21,22].

There are some challenges associated with data collection. Self-reported data is extensively used in health care, so it is crucial that consistency of data collection is maintained [12]. Keeping information up to date and accurate is an important challenge.

SECURITY CONCERNS IN HEALTH CARE

Liang, X[65]ueping, Zhao, Juan, Shetty, Sachin, Liu, Jihong & Li, Danyi in 2018, raised that firstly, health data are privacy-sensitive, that too of a higher degree, and with the quantum of data storec in public cloud increasing exponentially the vulnerability of data exposure increases. Secondly, current systems use centralized architecture, and these require centralized trust. Moreover, a very challenging task that needs to be effectively tackled is the the integration of health data and the interoperability between different healthcare systems. The fact that users have little or no control over their personal health data is any key area of cioncern. User-centric access control and privacy preservation will have to be the key themes in the development of a new version of EHR systems that cater to the concept of self-sovereignty and incorporate security aspects required to managed the increasing adoption of the mobile platform and wearable devices.

Malware attacks on Health Care records are quite common. Pilkington details that [86] in May 2017 thousands of British patients had delayed treatment since GPs and other vital services across NHS were infected by malicious software with a virus based on hacking tools developed by US cyber-warfare agents. Approximately 30 health service organizations had malware attacks, and many more were temporarily shut down as a precautionary measure.

DATA STORAGE RISKS IN HEALTH CARE

In 2019, Onik, Md. Mehedi Hassan, [85] Aich, Satyabrata, Yang, Jinhong, Kim, Chul-Soo & Kim, Hee-Cheol– referred that data in healthcare system is exponentially increasing and with a 48% rate of annual increase, by 2020 it is expected to get into the yottabyte (one yottabyte ¼ 10008 bytes) range. Acoording to a survey the healthcare analytics industries are posting a healthy groth rate with a compound annual growth rate (CAGR) of 27.3%. In 2022 this industry is expected achieve a revenue of 29.84 Billion USD as against 8.92 Billion USD in 2017. The Guardian reported that 26% of consumer's medical records were tampered with in the United States. Ten of the largest healthcare data breach incidents were notified by the Department of Human and Health Services Office of the United States were for handling of civil rights cases. Anthem Blue Cross, a health insurance gaint, suffered a breach which impacted 80 million healthcare data records, on January 29, 2015.

INTEROPERABILITY ISSUES IN HEALTH CARE

As mentioned by Taylor, Karen,[4] Sanghera, Amen, Steedman, Mark & Thaxter, Matthew in 2018 interoperabilit along witht the need to adhere to the various different standards and protocols for data exchange and utilization at the national and international level is arguably the largest issue that MedTech faces today. Technical challenges such as the creation of a unified governance methodology and the obtaining permission for access to medical data continue to persist. Open platforms which are based on open data standards is the direction that the industry needs to head towards if it wants to make interoperability work to its utmost potential. With this the payers, the providers and the technology vendors will be able to unite in the effort to make data more available to each another.

In 2018, Zhang, [100]Peng, Walker, Michael A, White, Jules, Schmidt, Douglas C & Lenz, Gunther noticed that the HIPAA privacy regulations would be requiring the confidentiality and security of individually identifiable health information. This information is transferred, received, handled, or shared by healthcare professionals and organizations. Also, only the required health information can be used or shared, which is vital to carry out business. All systems and apps created to share personally identifiable information (PII) must be complying to HIPAA. Therefore, any PII accessed by the DApp or written to a public blockchain needs to be encrypted and securely managed by parties, that are interacting with this app.

2.1.2.3 Information Sharing Risks and Barriers in Media:

Immutable

Bhowmik, [14]Deepayan & Feng, Tian in their paper in 2017 say that the present multimedia distribution does not provide self-retrievable trails of information or history of modified content. Things like soft copies of important works of art, archives such as books, creative work in entertainment or media are often distributed digitally for the purpose of exhibition, library archival, gallery collections and such.

At times, original media in forms of documents, images, audio or video are edited for content creation or may even be repurposed for self-interest or even false propaganda over social media platforms, however in the current times there is no means to trail the translation history of such modifications.

Access Control

Caress,Stephanie [20] in their work in 2017 claimed that our current copyright laws for the digital music industry are outdated and that the major problems killing the industry are piracy and in accuracy of ownership information. They also point out that understanding the how ownership of songs is determined under the copyright laws of the US is essential to be able to gauge the true potential of these conditions and their outcomes. In the aftermath of several failed attempts to arrest the problems through means of litigation, education programmes, technological advancements, the Global Repertoire Database was created with the idea to create a single international song owners database was created. Unfortunatekly by 2014 this too was declared a failure. The need to create a sounder program has become increasingly more urgent with the emergence & pervasive popularity of platforms like Spotify, YouTube and Instagram.

Some of the challenges faced by the digital media industry today are fake news and propaganda, copyright infringement, forensic media. JPEG claims that blockchain and DLT have the potential to overcome these challenges through their technology components in transparency-oriented media transactions.

- **Trust, privacy & security in the media consumption chain:** Media blockchain has emerged as an efficient solution to issues in these areas with the following requirements:
- **Digital rights management (DRM):** A media asset management tool on blockchain which has universal acceptance and accessibility.
- **Copyright protection:** In the era of fake news and tampered media specimen, it is of paramount importance to ensure the authenticity and the ability to trace the source of the content. To curb misuse of copyrighted content, mechanism to identify the tampering and track the source of such piracy.
- **Privacy compliance (GDPR):** The meta-analysis of recording assets through copyright, trademark content or any other such signature cannot be effective presently because of non-compliance of privacy laws and thus it needs to work within this framework.
- **Trusted and Transparent Media Distribution System**: Alongside with enabling a secure media consumption path, it is essential to create a transparent and secure media distribution environment for publishers and creative artists.
- **Rights management:** A single platform to secure the digital rights of the artists at a universal level accepted and governed by local laws.
- **Contract management:** Standard operational smart contract models that could auto generate with customised versioning to allow seamless transition between the buyer and seller.
- Wang ,[69] Xin in their 2003 study state that digital piracy has impacted even the global market leaders like Sony. In the quarter ending on June 30, 2002 Sony suffered a loss of 10.3 billion yen ($160 million) and this was attributed to digital piracy. To curb the infringement of commercial digital intellectual content and govern against piracy, it is paramount to set up systems that restrict unauthorised access.

Business Rules

Dair, [80]Marcus O, Neilson, David & Pacifico, Paul in 2016 estimated the global music industry at $45 billion and of that the recorded music industry accounts for about $15 billion as per Rethink music 2015. The IFPI 2016 data shows that the year 2015 recorded a growth of 3.2%, but that is after two decades of inexorable decline. The tides are now turning in the digital piracy domain with the digital consumption focus working on access rather than ownership, but this comes with its challenges.

Sachdev, Deepika (2020) [91] explains for **Multiplicity of Music Metadata.** There are atleast two copyrights in Recorded music pieces. One for the sound recording itself, owned by the performer and the record label. The other for the underlying lyrics and music attributed to the

songwriter and composer. This is defined in the blockchain with the help of a cryptographic hash. This does not take away the need for a single database enlisting copyright and ownership. There are various databases that exist in the current time without any synchronisation or Centralized authority for dispute settlement.

The value chain for music lacks transparency. Royalty is at times paid to the wrong party and are often not remitted to the due artist. Layers of non-disclosure agreements make the specific details of record deals inaccessible, in turn making it impossible for the artist to access or verify the authenticity of their payment processing.

Hosoi [34]et al in 2015 researched that labels still claim 50% of the share in spite of a shift in the dynamics in the labels role in the supply chain. This could be due to structure of the existing contracts. Imogen Heap [96] in 2017 have also attributed the lack of a universal database as the underlying cause for the $150 million class action legal action against Spotify.

According to Shelkovnikov, Alexander [19] in 2016 the news media have now resorted to put their digital content under paywalls where they charge nominal subscription fees for access to digital content, articles, stories, each with this own level of success. Even though the blockchain model is not implemented here, it works towards finding a commercial model that could benefit the content creator, the consumer and the corporation at the same time

Copyright information of music data is distributed across multiple databases of companies. This is owned by Publishers, distributors and Content aggregators,

Savelyev et al. in [15] mentioned that there are no incentives to share. The issue is accelerated when the artists of different countries started releasing their albums with multiple labels. In 2017, a study on ASCAP Music Reports showed the increasing number of Writers, composers and Publishers per content in the last few years. This complicates Metadata tracking. Data required to correlate the underlying Musical Composition with the Copyright information from the recording does not exist. The legacy databases such as MRI and HFA are not standardized and reliable. For Metadata attributes different label fields are chosen by database and this creates issues. For example the credits will be lost if in a case where “Recording team” is identified as “ProTools Recorders” but the Metadata label introduces a space between Pro and Tools and identifies the field as “Pro Tools Engineers”.

Inter-Operability

As described by Lee, [63]Junseok, Hwang, Seong Oun, Jeong, Sang Won, Yoon, Ki Song, Park, Chang Soon & Ryou, Jae Cheol (2003), the central point for the legacy industry for multimedia contents distribution and publishing was through physical media such as tapes and CD’s. Complex and difficult technologies are required to produce movies and music albums. The delivery to consumers is through complex supply chains of distribution networks. The media is packaged in multiple type of containers, such as videotapes, reel tapes and CD-ROMs. Modern contents production has become very efficient with digitized multimedia contents production and digital distribution. High-speed Internet and 5G are transforming

consumer contents consumption.Systematizing the structure and process of production, distribution and consumption of digital contents online, is the key area of focus and effort now.

Contents distribution systems are of two types-

1. Content Distribution systems which support content of only their own media type e.g. Microsoft and Adobe. Contents distribution systems from these organizations works on there legacy platform. For e.g. MS's Window Media Player runs on Microsodft and Acrobat Reader for Adobe.
2. Those that use their own renderers regardless of what the content type is e.g. InterTrust, ContentGuard, and IBM

Support is provided by both systems for distribution of content between the media distributors and the various purchasers. The real issue here is that they complete value chain does not get supported. The content creators, the various rights holders, the providers of contents, media distributors and distribution channels and finally the purchasers, the systems have to evolve to support the role of all of these in the supply chain.

There are two reasons for the charge-based content distribution models not gaining popularity:

1. A sense of insecurity among the creators of contents related to the protection of their work.
2. Under this evolved environment, creation of high quality content becomes a much more extensive process.

Therefore, the need to design a DRM framework which guarantees the rights for all the contributors in the value chain.

Decentralization

The hidden 'artist penalty' is a key limitation of the internet, as pointed out by Mcconaghy, Trent & Holtzman, [72]David (2015). Digital content creators are not adequately compensated for their work. Websites, streamlining systems and portals are designed by people who are not the artists, singers, photographers or writers. They are not original content creators but are expressing themselves by the changing the context or framework into which the original creators work is copied. This may providing a different expression or meaning to the original work. In this scenario the deserving candidates, the original creators of the content rarely receive the right payment for their work. The fear of revenue loss has pushed the publishers to create complex, less-practicle and end-consumer unfriendly Digital Rights Management (DRM) systems. Inefficiencies of this technology has led to the music industry stopping the use of DRM. A workable system is still required.

In practise, consumer grabs the content as per the displayed image. The fact is that 85% of images are pirated [8]. Generally, the individuals who are the actual rights holder often doesn't know about the infringement and even they become aware, they are sceptical for the legal process. Legal action does get taken by large Corporations and organizations that create content commercially (e.g., professional photographers, various media sites). Whenever they find a

license violation, they publish the images (e.g., as part of a news story) and issue a legal notice to the infringer(s).

The concept of locking down a file with a key in DRM has not proven to be effective. There might be attached unintended consequences or they're easily decoded. For example- while developing a DRM for DVDs large sum of money was spent. Within days of the release of DVDs, it got hacked by a young hacker named DVD Jon A [9]. AS highlighted in Torrent[12] this provides proof of the fact that all DRMs are susceptible to piracy. Moreover it involves only a fraction of the resources invested in the system to break the systesm.

2.1.3 Theme: Cost Challenges of Information Sharing for Provenance Tracking

Education

Tapascott & Kaplan in (2019), have pointed out that universities charge transaction fees in order to provide transcripts, and transcript issuance is growing. In the last five years sixty-two percent of the universities have seen an increase in the number of official transcripts issued. The average cost to a student of a transcript is between $5.00 and $9.99.15. A quick, tustable and lower cost system for issuing transcripts can be enabled by a blockchain credential solution. Such a system which would provides easy portability of information with lesser dependence on the issuing institution could have significant benefits. Wider adoption could help typical usecases, for example refugees wanting to continue their education or seeking a job in the country of asylum. Or may a world where a university pro-actively offers admission to a deserving student in an underserved community based upon a public available highly trusted portfolio of credentials.

Health Care

As explained by Azaram et. al (2015) Kevin [65] Leonard's interoperable HIS failure reasons include cases of Lack of a thorough cost benefit analysis due to the complexity of measuring tangible benefits such as "ability of someone doing the job in better fashion"; lack of industry-wide consistent data; absence of a universally unique patient id identifier primarily due to security and privacy reasons; the big gap between application developers as well as healthcare professionals; wrong belief that technology is the solution to solve all the problems; and development of various disintegrated databases in different healthcare sectors as opposed to a centralized repository. On the contrary, success factors as explained by Abernethy include: detailed review by a "project owner"; involvement of key stakeholders in design and development process; and considering future external as well as internal organizational needs such as affordability, provision of long term support, reporting, and long term co-operation of actors and sites involved.

Media

Ingraham[48] et. al (2020) exaplin the importance of assessing the total cost of ownership (TCO) which is reflected in the budget. TCO should be clearly understood for all projects, especially understanding when those costs are realized.

Blockchain
As explained by Mc Kinsey & Co that in the short term Blockchain's will contribute value predominantly through cost reduction. Transformative business models will be a longer term benefit.

2.1.4 Theme: Blockchain Models for Information Sharing

Business Rules
As Stated by Cristina Turcu [88], Cornel Turcu, Iuliana Chiuchișan. In Education a system that allows fast verification of the authenticity of documents issued inclusive to the secondary education area or other levels of education is paramount. Alomng with high security, blockchain provides the ability to combine data from disparate databases into a unified business workflow.

Decentralization
Atzori (2017), mentioned "The blockchain is a trust-free, auditable, tamper-proof, and self-regulating system, with no manual arbitration required to carry out logic valiation" The Blockchain is an encrypted repository is a incorruptible repository of data and that has the functionality of irreversibility. It "enables, for the first time, untrusted people to reach consensus on the occurrence of a particular event or extraction without the requirements for a regulating authority" (Wright & De Filippi, 2015).

Cuore, [26]Sacro & Coelho, Rebanda (2018)- the primary statement for blockchain systems is that authentication and remuneration will give a boost to the creators, and would be allowing them to license their films and to terminate the obstructions associated with Author's Rights and Related Rights, subtracting intermediaries that take money through fees associated with the sale, distribution, and author's rights protection of original content.

Grech Alexander & F. Camilleri Anthony[41] (2017) stated that with Blockchain technology users can verify the validity of certificates directly avoiding the need to contact the original issuer. Data management structures that give increased ownership and control over the data to the data owners can be enabled using Blockchain. The benefit to educational institutions is significant reduction in data management costs and reduction in exposure to liability which normally result from issues related to data management.

Kuo, Tsung Ting, Kim, Hyeon Eui & Ohno-Machado, Lucila[59] (2017) point to decentralization as the main benefit of Blockchain. Databases are logically centrally managed (i.e., even if the underlying infrastructure is physically distributed the users logically feel that

they are operating a centralized database), while blockchain provides decentralized database management through in a peer to-peer networked system. Each node in the blockchain runs independently while still following the standard procedures that have been defined atv the overarching levels. This makes blockchain ideally positioned as the system of choice for applications which require independently managed stakeholders to communicate amopung themselves without giving controls to any central intermediary. As an example health care or biomedical stakeholders (e.g., patients, hospitals, providers, and payers) having a peer to peer connect rather than seeing a centrally managed intermediary controlling the data and its access.

Sandhu, Ramandeep Kaur & Weistroffer, Heinz Roland [93](2018) point out that Blockchain is a decentralized peer-to-peer network structure. This ensure that any kind of transactions and assets does not need to be managed by the centralized middle-parties. More efficient ways of encoding, verification, transaction and ultimately maintenenace will be possible through this approach compared to the current scenario for the management of personal health records, financial transactions information, and confidential documents storage and distribution.

Immutable

(Gräther et al., 2018) [56]Blockchain is a system that has very high compatiblility to systems for storing fingerprint-based biometrics of certificates or other educational items. This is because on the block chain each transaction is permanent, recorded and immutable.

Kuo, Tsung Ting, Kim, Hyeon Eui & Ohno-Machado, Lucila (2017) [59]state that Blockchain provides an advantage over the inflexible audit trails of traditional systems. DBMs support create, read, update, and delete functions, whereas in blockchain only create and read functions exist i.e., it is very difficult to change the records or data). This makes blockchain suitable as a consistent ledger used to record critical information (eg, insurance claim records). Blockchain also offers data provenance. On DDBMS, the system can modify the ownership of digital assets this is not possible on Blockchain.

Onik, Md. Mehedi Hassan, Aich, Satyabrata, Yang, Jinhong, Kim, Chul-Soo & Kim, Hee-Cheol[85] (2019)
Highlight the immutability of blockcain data. Blockcahin technology provides for tamper-proof storage of contracts, decisions, transactions, and information. The Pentagon and Washington Times both have mentioned that the US military is looking at this technology as a safeguard against cybersecurity threats.. Blockchains store data in a decentralised fashion, this redistributed way of information storage can prevent data manipulation. Nugent et al. [68] have defined the use case for distribution and sharing of clinical data by blockchain technology. Matanovi~c [69] reported that the use of hash algorithms, the consensus algorithms, and data immutability make blockchain as a safe technology.

Access Control

With blockchain there is a chance to satify the requirements of the European General Data Protection Regulation and infact it will provide the chance to go way beyond what is mandated there (Smolenski, 2017) [114].

Sun, Han, Wang, Xiaoyue & Wang, Xinge (2018)[99] point to the decentralized, distributed, di-trusted capabilities for data-storage structures that are enabled by the blockchain technologies. Coupled with cryptographic techniques, this technology can guarantee that transaction data cannot be manipulated and the same can be backtracked and is completely verifiable. Collective maintenance across the network and the distributed nature of storage keeps Blockchain's distributed and decentralized nature secure. Compared to standard centralized databases, the risk and probability of entire netwoek suffering data loss when a single node is compromised by any form of malicious activity is heavily mitigated on the Blockchai. With the digital signature algorithms, the public key and the private key are used to secure a transaction, seldom disclosing the identities of the participating nodes. The use becomes invisible in whole procedure.

Role Based Access Control

Sachdev, Deepika, Studies, [91](2020) mentions that in the Current Systems, fine grained Access Control Policies trigger execution of Coarse grained Policies e.g., User role determined Content Access rights. Much need User attributes or Multiuser approvals are incompatible through fine grained policies based on User Identity. Some examples are highlighted below:
Time Based: Do not allow Metadata editing if in the last "Y" hours the user has edited higher than a threshold quantum of Meta Data.
Provenance Based: Deny Edit access if the User fails to satisfy or furnish the requisite provenance inputs. For e.g., inactivity of the User or user not in association with the Content for a threshold period say "Y" Months would lead to access being denied.
Aggregate policies: MetaData edit is not allowed unless approved if the sales price is less than "R" dollars or unless the edit has been approved by a minimum numer of Owners.
Based on Category of the Content: An amalgamation on access rules based on user provenance conditions and Content Category being accessed.

Framework

Al-Saqaf, Walid & Seidler, Nicolas (2017) [4] a permission less blockchain is free for anyone to participate and individuals can act as per their conviction to transact or exchange information. The consequence of this is that it is impossibile to enforce rules, policies or regulations on individual members in a manner that they don't affect the whole infrastructure of the blockchain. The blockchain puts the user at the centre and the periphery of the network, and is possibly perhaps the first ever innovation which allows this.

As mentioned by Arndt, Timothy (2019) [8] presently three types of blockchain systems are generally acknowledged, according to their differing governance and architecture approaches (Zheng, 2017) [68]:
Public Blockchain – Everyone participates in the consensus process and the records are open for the public to access. Profund Immutability and low efficiency level characterize this type of

Blockchain.

Private Blockchain –Owned by and limited to a particular organization or entituy, and only nodes coming from that entity would be allowed to join the consensus process. Lower level of immutability compared to Public blockchains but that is traded off with a higher level of efficiency;

Consortium Blockchain – also referred to as the permissioned block chain, merges the two previous systems. A pre-chosen group of users is allowed to participate in the consensus process. All users don't have to belong to the same organization or entity. More Immutability than a Private Block chain and more efficiency compared to a Public Blockchain make the consortium blockchain an intermediate approach. Higher centralization comnpared to public and higher decentralization compared to Private Blockchains are achieved in this approach.

Arndt, Timothy (2019)[8] mention that API availability also drives Blockchain choice. Researchers will naturally prefer a solutions that allow them to program in their language of choise. In secondary education projects Ethereum is popular because of its features like the smart contracts and its generalist format. At the same time other platforms have also been used quite widely.

Chakravorty, Antorweep & Rong, Chunming (2017)[21] mention that in Blockchains the primary differentiation for the category of blockchain is dependent on the authorization requirements for different elements in a network and functioning as validators, along with connecting to the blockchain data.

Liang, Xueping, Zhao, Juan, Shetty, Sachin, Liu, Jihong & Li, Danyi (2018)[65] mentioned that they chose to build their system on Hyperledger Fabric [7] because of the advantages it offered due to as a permissioned blockchain. Hyper ledger requires the network nodes to validate thus allowing them to realize a privacy preserving personal healthcare system with a broader spectrum. With Hyperledger they can cover all of the healthcare ecosystems to the cloud, from the various devices, and at the same time it allows the emphasis on health data ownership by the users.

PRIVACY AND DATA SIZE DRIVEN OFF-CHAIN DATA STORAGE

Off chain data storage facilities are becoming popular given the restrictions imposed due to personal data privacy norms. Due to the decentralized model Blockchain is unable to store large amounts of data. Biological and Healthcare data are organically massive in numbers. Off-chain solutions are a good option for such use cases.

Radjenovic, Zarko (2020) [87]accepts, supports and promotes off-chain approach in using blockchain for e-Health purposes. An off-chain method also known as "data lakes" is a kind of approach whereby encrypted health information can be stored in a data warehouses that lives off the blockchain. Germany, France, Spain and Switzerland are among the main contributors for successfully executing the blockchain technology in the healthcare sector.

Cost of Investment

Dair, Marcus O, Neilson, David & Pacifico, Paul (2016)[27] stated that Blockchain technology has the potential to alter this situation related to high cost of transactions and inability to handle micro payments which persist in many tradition systems ways of transacting business. Cryptocurrencies with theirb low transaction costs, their huge range of denomination, typically to eight decimal places enabled by their digital nature, makes it possible to handle micropayments in an effective manner.

Interoperability

Kamel Boulos, Maged N., Wilson, James T. & Clauson, Kevin A. (2018) point out that a critical issue is interoperability. The need is to have the different blockchains in use with various providers and in various services to talk seamlessly with each other in order to have complete and effective systems.

Radjenovic, Zarko (2020) [87]mention that for enabling blockchain technology to achieve a certain interoperability level, it is also necessary to choose the right blockchain platform, which could be possible through making decisions in a multi-criteria scenario. Some authors suggest that these parameters such as transaction speed, innovation capability, keep the overall maintenance costs of the platform, and the availability of the platform.

Taylor, Karen, Sanghera, Amen, Steedman, Mark & Thaxter, Matthew (2018)[103] mentioned that for Medtech the massive challenge is interoperability along with compliance to the multiplicity of the protocols and standards for utilization and exchange of data that exist at national and international levels. The creation of integrated frameworks for governance and obtaining permissions and access rights for health care data also pose serious technological and procedural problems. Open Platforms which are based on transparent open systems and create better availability of data to the ecosystem through the collaborative efforts of providers and technology vendors are the best way forward for effective and efficient interoperability.

Business Rules

Grech Alexander & F. Camilleri Anthony (2017) [41]suggests that within some instutions the acceptance of cryptocurrencies based on the blockchain technology for executing payments is likely to gain ground. In many countries where there is a requirement of grants or a system of voucher-based funding of education, the ability to create and customize cryptocurrencies for different usecases will possibly lead to significant blockchain adoption. For such use cases in order to enable the development of open blockchain implementations significant governmental support will be required. For EU and its Member States we suggest that they should acknowledge the idea of label for ‘open’ educational records and actively promote the creation and promotion of this concept. This concept should house the principles of decentralised verification, ownership by recipient and vendor independence – and the governments should provide support to and utilize technologies with show conformance to the standards set in such a label.

Health Care

Kamel Boulos, Maged N., Wilson, James T. & Clauson, Kevin A. (2018)[51] mentioned that a clear indication of the growing interest in Blockchain for Helatchare and medical sacience is the gowth in the research interest in this area. In 2018 a query with the keyword 'blockchain' fetched 40 indexed papers. Health care organisations globally are looking to Blockchain's primary principle of decentralisation of authority, cryptography based security and immutability for redefinig their systems and processes. The main areas of interest around Blockchain in Healthcare are: (1) security of identity for patient and providers; (2) managing wupply chains for the pharmaceutical and medical devices; (3) monetization of clinical research and data; (4) Detecting medical fraud; (5) public health surveillance; (6) enablement of geo-tagged data which is truly public and open; (7) In smart cities, to improve organisation and provide transparency and visibility through Internet of Things-connected autonomous devices, drones, vehicles and wearables, utilizing the distributed peer-to-peer applications they operate; and (8) utilizing Blockchain for enabling augmented reality.

Khezr, Seyed Nima, Moniruzzaman, Md, Yassine, Abdulsalam & Benlamri, Rachid (2019) [53] Stated that the essential requirement for the development of smarter healthcare systems that enhance the quality of healthcare providers is the sharing of the healthcare and medical data. This sharing could happen between individuals say between a patient sharing with a new doctor he or she is consulting [66]. IIt can also happen between a stakeholder and an individual. As an example individual patients sharing their medical history with a research center or an insurance provider. There could also be cross-border medical record sharing use cases [67]. The key problem that hinders these scenarios are the observed setbacks in the operational mechanism of the prevalent health-related systems. These systems do not allow any access to health reports to the patient. Hence, patients do not have any capability of sharing their own health data with other parties [68]. Blockchain technology can help to improve the interaction and collaboration among the healthcare industry participants. It can do so by enabling a userfriendly, secure and trusted data sharing mechanism for digital health data. This will be one of the most significant aspects of contribution by blockchain based healthcare systems[69].

Maddux [70] while describing the blockchain opportunity in the healthcare big data sector stated in his study that Blocklcahin technology makes data mobility and distribution more secure. Use of Blockchain helps to grow the interparty communication between data owners & researchers for example. In the Blockchain each and every detail of data distribution is stored . Data such as identity justification, information validation and time proof etc are stored and can be accessed and verified. This is benifical to collaborative work.

Healthcare Data leakage is estimated to cost $380 USD per second, according to IBM and Ponemon, compared to industry sector data breaching which is valued at 141 USD per second. In order to curb these expensive losses due cybercriminal activities, blockchain based technologies can buttress and extend system security [71]. Again the challenge is the interconnectivity and interoperability of current medical records, which has not proven to be sufficient. Blockchain technology can extend data security, provide open environements, enable trust and with

blockchain technologies interconnectivity can be a multifold increase. The consensus driven approach which include all the players, provides for maintanence of data quality, data reliance, and upholding of stakeholder's opinion within the same platform [35–39]. Smart contracts can help to implement the healthcare policies between the patients, providers and the insurers.

Pilkington, Marc (2017)[86] quote a Deloitte report, which states that 35% of surveyed healthcare and life sciences organisations are planning to launch blockchain technology in the coming year: this adoption by healtcare and sciences organisatyions could potentially alsio speed up the he protocol development and accelerate adoption of blockchain technology in other industry verticals.

Radjenovic, Zarko (2020)[87] mention that using blockchain technology would reduce the danger of misusing health information, asymmetry of information and the increasing transaction costs in a very short time. Blockchain is an agile mathematical algorithm that can offer maximum transaction security with the help of cryptographic methods. This type of technology is based on a shared database that comprises encrypted data that is immutable or undisturbed.

Radjenovic, Zarko (2020) mention that documents and recordings are in the data created by clinical diagnostic equipment with the help of the health information system. These important data should be processed in an adequate manner for serving important medical decisions and to be used in a heterogeneous clinical administration system. Through this, the process of providing electronic healthcare services, as well as the optimization of the patients' treatment in the health institution, is improving.

Acceleration of research via standardization of databases and the enabling of non-identifiable patient data is another key contribution possible from Blockchain technologies as per Sandhu, Ramandeep Kaur & Weistroffer, Heinz Roland (2018)

Education

Lam, Tsz Yiu & Dongol, Brijesh (2020)[62] mention that as seen from patterns in Higher education, interdisciplinary research has grown, there is higher cross-collaboration in teaching and there is an increase in student degree offerings – both within an institution and across two or multiple institutes. This is seen from examples of the Universitas 21 network and also the model offered by Semester Online consortium (Jacob, 2015, p. 4). Alammary, Alhazmi, Almasri, and Gillani proposed that the collaboration and partnership between educational institutions could be a possible primary ground for blockchain adoption. Multiple educational institutions have declared Blockchain as a ledger which is secure and reliable for them to record their students data.

University of Nicosia(UNIC) as highlighted by Saleh, Omar S, Ghazali, Osman & Rana, Muhammad Ehsan (2020) is using the Bitcoin blockchain for many activities. These include the recognition of bitcoin for tuition fees for their degree programs. They are also issuing academic certificates on blockchain [26]. UNIC has started Educational certificates in the blockchain

which are aimed towards educating international students in the elimination and reduction of fraud in payments

Sun, Han, Wang, Xiaoyue & Wang, Xinge (2018) have written that chronological records of the students' learning data can be stored on the blockchain with proper timestamping. The data could include learning times, the learning objectives and course files and also the test transcripts. Cryptography based recording methods protect the data accuracy, aremoving the risks of deletion and tampering. The key characteristics of distributed databases, decentralization and combined operations of the blockchain the education platform will be capable in logging and auditing the learning portfolioes of students across geographic locations and time zones. This will increase the efficiency of the platform and deduct the hardware costs.

The data's security and credibility is maintained by the blockchain by using uneven encryption algorithms in cryptography. Using this architecture pattern, it is quite convenient to architect a secure learning result certification systems. The first step will be the recording of the learners learning data on the blockchain. This would be done by the the online education platform or the accredition or certificate issuing organization. Data included would contain the learner basic information, scores for the courses taken, information about the courses themselves, result dates etc. This is used to secure the data by using hashed key of the platform.

These secure digital certificates are distributed to the end consumers including universities, organization and students. The organization's public key is used to verify the digital certificates.

Sun, Han, Wang, Xiaoyue & Wang, Xinge (2018) highlight that Smart contracts are a prerequisite for the building of secure information sharing platforms for online learning. On the basis of smart contracts, the education platforms will be able to do the settlement with the value chain contributors, enable the purchase of courses and accredited programs and verify the validity of program acceptance. Due to the distributed storage mechanism used by Blockchain in addition to decentralization architecture ensure that students can log into a central platform and access complete education information securely.

Also as a strong guarantee of data security the data will not be corrupted when individual nodes get destroyed during hardware failure or piracy attacks.

With Blockchain enabled networks, Global knowledge databases can be developed through the collaboration of research and academic institutions, participation of academic journals, content from open sources such as Wikipedia, and other education data from various providers. The hubs in any blockchain organization can be offered admittance to these secure information assets. This significantly upgrades the productivity of the learning organization and enhancement of the learning strategies.

Media

Sachdev, Deepika, (2020) states that Fine Grained Access Control for Content Metadata needs to be created by aggregation of data related to Timeing, Identity Provenance, Categorization of

Content and Hierarchy structures for users. Blockchain enables this by considering Role Categories as Type and Roles as an Asset. Seggregating and detaching information utilizing Private Information Executions for low-volume profoundly security sensitive information is done on Blockchaion deployments like Hyperledger, enabling, or infact guaranteeing Fine Grained Admittance Control.

Interoperable Metadata Repository

The point of a Decentralized MetaData vault is to ensure that interoperability exists across stages. This can be cultivated by means of holding fast to an interoperable MetaData standard that will guarantee Information Sharing utilizing Connected Records through URI's. Additionally, Relay Chains are proposed for IBC for structures that have low idleness and are viable with Multi Signature.

During its 78th JPEG meeting (February 2018), the JPEG board of trustees led a select meeting on blockchain and its effect on JPEG norms. Thus, the board of trustees chose to investigate use cases and normalization needs identified with blockchain innovation in an interactive media climate. JPEG is pioneering in accepting contributions from experts for portraying these client cases. It explores necessities and advantages to help a normalization method that essentially centers around the applying blockchain in media.

Sachdev, Deepika, Blockchain Interoperability (2020) mentions the siloed functioning of present Blockchain Platforms. Unique, proprietary data storage formats used by application make inter application compatibility difficult. They suffer from a lack of Interoperability in media.

For e.g., if a content producer is required to move, access or copy his metadata from one Blockchain application to the next, it creates inconsistencies in the final output. This is due to the fact that every application has their own exclusive configurations. Application Based ACL's: are completed based on marks which are referable by the Blockchain applications. Existing structures rarely have a process to create signatures which can be confirmed by other Blockchain applications. In this way, if an Uber Clients need to execute Smart Contracts on Disney Media, it will not be applicable in the current scenario.

Regulatory

Need for Shared Write Access:

In view of the Business prerequisites, a few or all Clients will have composite Access. In the consortium, it is conceivable that public Admittance is conceded to all individuals, yet full Access is allowed distinctly to restricted Super Clients

Business Rules complexity: As referenced in [4] it is hard to implement laws in a Permissionless blockchain on people without affecting the entire blockchain Framework. As depicted by Thurimella et. Al in [107], since in a Permissioned Blockchain, the members have given consent forthright. Hence it is a lot simpler to construct secure applications. In Permissionless Blockchains, since the Hubs are controlled by various proprietors, to roll out any

improvement in the Business Rules carried out by complex Agreements, it should be acknowledged by greater part of Hub Proprietors before the Business Change can be executed in the Blockchain.

Time for Contract Closure: In Open Blockchains, settlement conclusiveness is just probabilistic since an other long chain a single transaction can switch the current exchanges.

Owner: Can be possessed by one or by a Consortium dependent on the Administrative and Protection prerequisites of the Application.

Transaction Volumes in TPS: points to the hypothetical most extreme measure of TPS can be supported by Blockchain Algorithms[86]. As depicted by Thurimella et. Al in [107] a key factor going down for Public Blockchains is the capacity to help higher Volumes of Exchanges in comparison to current Visa networks

Anonynmous requirements: As referenced in Worldwide Benchmarking Study[43], Exchanges information need to have a specific degree of protection. Unexpectedly, in open blockchains, by design all exchanges ought to be apparent to each member. In light of Business Necessities, information in the Blockchain can either be accessible for CRUD operations to all Clients or to a select collection of clients dependent on Access Rights.

Limitations

Since the time of transaction execution can be long resulting in delays in processing.Hence latency is an important limitation of blockchain,. In addition the increased storage capacity due to fast growing data as well as redundancy needs poses a significant challenge while adopting blockchain.

Kamel Boulos, James T. and Clauson, Maged N., Wilson, Kevin A. (2018) [50] notice that similar to any nascent innovation in medical services, the blockchain execution benefits are clung to its own arrangement of limitations. Challenges spring out because of:

- the upkeep of truly validated patient information
- varieties in agreement are making blockchains interoperability a challenge
- the known measure of variations in delivered clinical information

Many blockchain applications for storing patient data actually take an approach that is hybrid. It stores references and validation rules that are related to data stored in a system that is protected, centrally owned or utilized by a private blockchain [13, 14]. This defeats the main objective as it is only a step away from centralised ownership.
This compromises the rights of the data owner. Hence, managing the encoded data adds complexity to the management level. The major disadvantage in such an operation is that anybody linked with that particular local data can access the data sans requiring mutual consensus from other nodes. In addition, the GDPR versus blockchain is still a mystery. There

are still further open items on the off-chain data storing mechanism. They are:
• Plausibility of encryption of off-chain information?

• Is information access dependably controllable or not?

• What occurs in the far-fetched situation when off-chain information is duplicated unlawfully?

Umeh, Jude (2016) [108] According to the Technology Director of the Open Data Institute, 'the transparency and irreversibility of blockchains prove them to be unsuitable for storing personal data.' In compliance to GDPR, it gets extremely difficult for the owners to use the 'right to be forgotten' as that requires modifying or deleting the blockchain-based transactions.

Blockchain Limitations – The Scalability Trilemma
As explained by Abdelatif Hafid et. al (2020) One of the key limitations of blockchain is scalability; indeed, the number of transactions that can be processed per second is small and insufficient (e.g., up to 7 TPS for Bitcoin and 15 TPS for Ethereum). This is unacceptable for most traditional centralized payment systems that require 1000s of transactions per second (tx/s); as a comparison, Visa handles an average of 1700 tx/s [33]. The scalability trilemma is well-known in blockchain; it was first described by Vitalik Buterin, the cofounder of Ethereum. Vitalik states that trade-offs are inevitable between three important properties: decentralization, scalability, and security.

- Decentralization is the core and the nature of blockchain,
- Security is an essential propriety,
- Scalability is the main challenge.

In other words, the scalability trilemma states that we can only have two properties out of either decentralization, scalability or security. This implies that we can pick just two sides of the triangle and hence trade-offs will always happen.

2.2 Summary of Literature Gaps:

2.2.1 Theme: Organization Information Sharing Behaviours

Document Name	Findings	Inference	Gap

"Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework – 2014" "Supply chain information and relational alignments: mediators of EDI on firm performance Keah Choon Tan , Vijay R. Kannan ,Chin-Chun Hsu , G. Keong Leong - 2010"[4] "Examining the Impact of Interorganizational Systems on Process Efficiency and Sourcing Leverage in Buyer"–Supplier Dyads, Khawaja A. Saeed, Manoj K. Malhotra, Varun Grover - 2005[17] "Inter Orgainizational communication as a relational competency" Antony Paulraja, , , Augustine A. Ladob, 1, , Injazz J. Chenc, - 2007[33] "Knowledge sharing—A key role in the downstream supply chain" Stephen C. Shiha, , , Sonya H.Y. Hsub, 1, , Zhiwei Zhuc, 2, , Siva K. Balasubramaniand - 2012[63] "The Role of	Examination inspects the impacts of inter-organization data trade on Bury Associations and social arrangement. Drawing on accomplice connections, it makes a multidimensional structure for considering electronic information exchange (EDI) selection in provider the board and its impact on data and social arrangement. There is additionally examination to investigate what hypothetical focal points have been utilized to dissect and comprehend data partaking in supply chains. Assembling firms are looking for financial and other advantages, by forming a firm coupling in their provider relationship. Of the different components, cross organizational frameworks that work with limited crossing exercises of a firm empower them to viably oversee various sorts of purchaser provider connections. Exploration incorporates writing from the tasks and data frameworks fields to make a joint point of view in understanding	The discoveries present a multidimensional system for considering Data Trade appropriation in Bury Association connections and its impact on data and social arrangement. It gives a protected and effective system for bury association data trade. It likewise illuminates the distinctions in how firms use Data SHARING while working under changing degrees of serious force and item normalization. Exact information is given on data trade gathered from assembling firms. The outcomes show that solitary more elevated levels of outer mix that go past basic acquirement frameworks, just as who starts the Data SHARING, permit fabricating firms to upgrade measure productivity. The outcomes offer solid help for the idea of between authoritative correspondence as a social capability that upgrades purchasers' and providers' exhibition. Exploration likewise focusses on a SCM climate and confirms the significance of	Research is focused on the value of Trust in Information Sharing and how it increases value for the Organization. However there was no research found which shows an impact on Provenance Intensities in Information Sharing governed by Trust with a need for Immutability.

Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea" Jeffrey H. Dyer and Wujin Chu - 2003[21] "A strategic analysis of inter organizational information sharing "Jingquan Lia, Riyaz Sikorab, , , Michael J. Shawa, Gek Woo Tanc - 2005 Information sharing and supply chain performance: the role of connectivity and willingness Stanley E. Fawcett , Paul Osterhaus - 2007[1] Flow Coordination and Information Sharing in Supply Chains: Review, Implications, and Directions for Future Research - 2002 Benefits of information sharing with supply chain partnerships Zhenxin Yu Hong Yan T.C. Edwin Cheng [69] - 2001 Incentive and Trust Issues in Assured Information Sharing Ryan Layfield, Murat Kantarcioglu, and Bhavani Thuraisingham - 2009[22]	the linkages between the idea of the Data SHARING, purchaser provider connections. Outer mix, broadness, and commencement are utilized to catch Data SHARING usefulness, and their impact on measure proficiency and sourcing influence is analyzed. Between authoritative correspondence has been recorded as a basic factor in advancing vital coordinated effort among firms. The flood of examination in store network the executives is enhanced by deliberately researching the predecessors and execution results of between hierarchical correspondence. In particular, between authoritative correspondence is proposed as a social skill that may yield competitive edges for inventory network accomplices. Exploration likewise examines the connection between provider trust in the purchaser and exchange expenses and data partaking in an example of 344 provider automaker trade	Information Sharing and how it assists with expanding the efficiency of the association. The discoveries show that apparent dependability decreases exchange costs and is associated with more prominent data partaking in provider purchaser connections. Additionally, the discoveries propose that the worth made for exchanges, as far as lower exchange costs, might be generous. The outcomes additionally show that close total data sharing that consolidates more than one sort of data being shared has better execution in unpredictable economic situations Two particular measurements to data sharing – availability and eagerness – are distinguished and broke down. The two measurements are discovered to affect operational execution and to be basic to the advancement of a genuine data sharing capacity. Be that as it may, numerous organizations are found to have put the vast	

	connections in the US, Japan, and Korea. Examination utilizes data trade in a production network as a portrayal of bury hierarchical data sharing, and studies five methodologies for data sharing that range from insignificant to approach total data trade. There is additionally research centered around two particular measurements to data sharing – availability and eagerness – are recognized and investigated. There is a hidden need of ability in the association before Data stream begins Advances in data innovation, especially in the e-business field, are empowering associations to reexamine their data share systems and investigate new roads for between hierarchical collaboration. In any case, a fragmented comprehension of the worth of data sharing and actual stream coordination prevent these endeavors. This examination endeavors to help fill these holes by studying earlier exploration around there,	majority of their accentuation on availability, frequently disregarding the eagerness develop. Therefore, data sharing rarely follows through on its guarantee to empower the production of the durable inventory network group. It shows that expanding data dividing between the individuals in a decentralized inventory network will prompt Pareto improvement in the exhibition of the whole chain. In particular, the store network individuals can receive rewards as far as decreases in stock levels and cost investment funds from framing associations with each other. There are recognized issues and difficulties in Data Sharing. Exploration utilizes a punishment based way to deal with battle these issues	

	ordered as far as data sharing and stream coordination. It likewise investigates the impacts of various motivators and trust issues that can happen among associations related to the guaranteed data sharing cycle by fostering a developmental game hypothetical system.		

2.2.2 Theme: Challenges of Provenance Tracking for Information Sharing

Details	Findings	Inference	Gap
The W3C PROV family of specifications for modelling provenance metadata Paolo Missier, Khalid Belhajjame 2013 Principles of Provenance - 2012 by James Cheney1 , Anthony Finkelstein2, , Bertram Ludäscher3 , and Stijn Vansummeren4[97]w3 The credibility of volunteered geographic information. Andrew J. Flanagin and Miriam J. Metzger, GeoJournal (2008) Tracing where and who provenance in Linked Data: a calculus. Dezani-Ciancaglini, Mariangiola; Horne, Ross; Sassone, Vladimiro Main reference M. Dezani, R. Horne, V. Sassone, Provenance Threat Modeling Oluwakemi Hambolu, Lu Yu, Jon Oakley and Richard R. Brooks Ujan Mukhopadhyay and Anthony Skjellum Data Provenance: Some Basic Issues Peter Buneman,	Provenance is a class of meta-information with security needs that vary from those of "conventional information". PROV-DM built as an information model for provenance and depicts the elements, individuals and exercises engaged with delivering a piece of information or thing on the planet. Provenance on Data Archive Demonstrating has been getting expanded concentration in Exploration as of late with the expansion of Computerized Data through Web, Large Information and IOT. They are conventional models accessible for Provenance age of Data set and Interaction produced archives. This is finished utilizing comment based methodologies and non-comment based methodologies. Since provenance catches history it ought to be unchanging. The diagram that portrays the provenance is coordinated and non-cyclic. There are	Based on the existing studies in Provenance Management, it is noted that there is Open Source Models which help to map Information profile into industry agreed conventions. This is based on open source standards agreed and identified between participating organizations. The PROV organization has created PROV variants based on Data Source and Domains which can be tailored as per the Industry Needs. There is varied Research which is focused on deriving linkage between Provenance and Trust. This is focused across Database, Workflow, Information Sharing and Social Media Research. Research has been done to classify provenance into frameworks based on data source, storage and granularity. The studies confirm the relationship between Trust and Provenance, and also help to establish processes wherein the Trust for	Research is focused on the Cost of Information Sharing for sectors. However, there is no specific research that correlates various Use Case based requirements of a sector and compares them with Blockchain Cost Challenges.

Sanjeev Khanna and Wang-Chiew Tan 2000 Peter Buneman, Adriane P. Chapman, James Cheney Data Provenance: A Categorization of Existing Approaches 2015 Hao Fan and Alexandra Poulovassilis 2005 The problem of data lineage tracing in data warehousing environments by Cui et al - 2000 Characterizing Provenance in Visualization and Data Analysis: An Organizational Framework of Provenance Types and Purposes – 2015 Eric D. Ragan, Alex Endert, Jibonananda Sanyal, and Jian Chen Provenance in Databases: Why, How, and Where By James Cheney, Laura Chiticariu and Wang-Chiew Tan Why and Where: A Characterization of Data Provenance[25] Peter Buneman Sanjeev Khanna Wang-Chiew Tan University of Pennsylvania - 2001 Securing Provenance Uri Braun, Avraham Shinnar1, Margo	applications where this data should be gotten. How - is the courses which are utilized to show up at the question. How provenance discloses to us how the source tuples witness the yield question Where Provenance - reveals to us where in the information base segments the Provenance was put away. Why - the insignificant arrangement of witnesses that are expected to check a question It depicts both straightforward access systems for finding provenance data related with pages or assets, just as provenance question administrations for more mind boggling organizations. Guidelines, for example, the Open Provenance Model, come about because of a local area exertion beginning with the Principal Provenance Challenge workshop are intended to give a lowest shared factor. In any case, they don't have an inbuild model for heredity examination. PROV Model has been stretched out for	Provenance can be increased. A line of examination is centered around that of gathering the Provenance change's properties, Either by inspecting the particular (e.g., utilizing program examination methods over the code), or by running example information through the change and looking at the outcomes.An alternative to Provenance Storage Issues is to store approximate provenance data records. The size of the querry or the update influences the size of storage needed. Hence compared to the size of the full provenance table, the size of this data is quite negligible.	

Seltzer - 2006 A Security Model for Provenance Braun, Uri and Avi Shinnar - 2006 Introducing Secure Provenance: Problems and Challenges Ragib Hasan, Radu Sion - 2007	information bases and logical work processes. For provenance of information we need to monitor the wellspring of information and how it gets across sources. In the event that the source transforms, it is critical to refresh the objective connections. Fostering a provenance the board framework for open world models is a difficult issue. Source and change provenance are not totally autonomous and it is fascinating to examine under which conditions it is feasible to change over one into the other and study how much excess is presented by putting away source and change provenance. Heredity following is finished utilizing Change Properties. The strategies for improving heredity following execution, including building files and consolidating changes for genealogy following. There is likewise examination to give a UI that is adequate to the custodian; that is, it ought not be excessively not the		

	same as the thing is at present being utilized		

2.2.3 Theme: Blockchain Frameworks for Information Sharing

Document Name	Findings	Inference	Gap
The role of trust in understanding the effects of blockchain on business models Rajala, Risto - 2016 Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review Swan, M[40].: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol A maturity model for blockchain adoption Huaiqing Wang1 , Kun Chen2[112] and Dongming Xu3 BlockChain technology: beyond bitcoin. Applied Innovation Review : Nachiappan, Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain-based sharing services: What blockchain technology can contribute to smart cities BLOCKCHAINS IN NATIONAL DEFENSE: TRUSTWORTHY SYSTEMS IN A TRUSTLESS WORLD, Neil B. Barnas,[27] 2016	Blockchain innovation is a fundamental exchange development in data handling. It empowers trust-dependent exchanges between parties that were beforehand unfit to confide in one another through a permanent exchange log and confirmation of request and legitimacy of exchanges, in addition to other things. Blockchain innovation is another approach to incorporate old advances, like computerized marks, cryptography, and hash capacities, yet as a development it is exactly toward the beginning of its advancement. This work concentrates how blockchain innovation could change plans of action, and particularly what is the job of trust in this change. Blockchain innovation is relied upon to reform the manner in which exchanges are performed, consequently influencing an immense assortment of likely	Examination explains the essential comprehension of blockchain innovation by introducing a structure for use case assessment and by opening the chance offered by blockchain to build trust or to refute the requirement for it in an exchange. Further, the job of trust in an industry appears to affect what sorts of changes blockchain can cause in plans of action. Blockchain innovation would thus be able to be viewed as both a mechanical and a plan of action development, and making a qualification between the two is significant. As a plan of action development, blockchain could disturb plans of action in a wide scope of ventures and geological areas. Research also provides relevant insights into the influence of Blockchain on the	There is research in the areas of Industry Framework for Blockchain based on specific Use Cases. However, there is no existing research in the area of Blockchain Frameworks based on Provenance Needs of an Organization defined by the Trust Requirements of Information Sharing

Provenance Threat Modeling Oluwakemi Hambolu, Lu Yu, Jon Oakley and Richard R. Brooks Ujan Mukhopadhyay and Anthony Skjellum Where Is Current Research on Blockchain Technology?—A Systematic Review Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4, Sooyong Park2, Kari Smolander [114] The bitcoin lightning network, Prron & Dryja[66] Bitcoin A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 2008	spaces of utilization. While assumptions are high, certifiable effect and advantage are as yet hazy. To have the option to evaluate its effect, the principal organized writing audit of companion explored articles is led. As blockchain innovation is based on a distributed organization, empowering coordinated effort between various gatherings, the assistance framework is picked as unit investigation to analyze its likely commitment. Examination has recognized a bunch of qualities that empower trust and decentralization, working with the development and coordination of a help framework. Exploration Structures are broke down for Blockchains. The relative investigation strategy is utilized to examine various components of the development model, which is basically founded on the ordinarily utilized ability development model	Industry and how the impact of Trust will significantly influence Blockchain applications in the industry. Blockchain decentralization and immutability is a key factor that will influence its usage into the Industry There is ongoing research on various Maturity Models and how the industry should analyze Blockchain based needs to identify what is the relevant maturity model. Blockchain provides multiple benefits to varied users. Based on the industry needs, the user should focus on the available Blockchain frameworks available and apply them to their specific needs There is empirical evidence how Blockchain will help enable Smarter Cities through the features of decentralization, Distributed Ledgers and a Trusted Protocols There is a Framework which can be used by the defense to use	

	Examination additionally focusses on business utilizations of Blockchain and how significant ventures ought to distinguish the Blockchain needs This is a valuable knowledge gave to the US Govt how Blockchain Trust cam be utilized to give extra security in Data Sharing and Guard conversations of the US Govt Blockchains's security is managed by keeping a cryptographically marked chain of secure hash esteems. This chain is placed at various destinations and is additionally refreshed persistently, it's practically unthinkable that fraudsters can control this chain. This capability of the blockchain can guarantee the authenticity as well as the secure nature of provenance information." There is progressing issues raised on TPS and Square size restrictions on Square Chain. Examination	Blockchain effectively. Information Sharing usingTrusted Protocols is used to enhance the security Blockchain Security does provide relevance to Provenance Storage. Research in blockchain is focused on frameworks, applications, blockchain security and Smarter Contracts. Lightning Network has been applied to micro transactions where the required TPS is much more than the existing 7 TPS of bitcoin	

	gives a knowledge on how Blockchain will conquer TPS issues by executing a Lighting Organization convention		

2.3 Gap Summary

The key gaps identified based on the themes are:

- Research is focused on the value of Trust in Information Sharing and how it increases value for the Organization. However, there was no research found which shows an impact on Provenance Intensities in Information Sharing governed by Trust with a need for Immutability.
- Research is extensively focused on the Cost of Information Sharing for sectors. However, there is limited research that correlates various Use Case based requirements of a sector and compares them with Blockchain Cost Challenges.

- There is research in the areas of Industry Framework for Blockchain based on specific Use Cases. However, there is no existing research in the area of Blockchain Frameworks based on Provenance Needs of an Organization defined by the Trust Requirements of Information Sharing

3. Theoretical Premise

3.1 Theory of Firm

Theory of firm* is a set of Economic theories which was created around the first world war. Its purpose is to explain the theoretical framework of the nature and existence of the firm is what it explains. The theory explains that a firm will exists when the enviroenment is such that it becomes efficient to produce in a Non-Market Environment. Key Questions addressed by Theory of Firm are:

1. Existence. Why causes firms to emerge? What ios the reason that not all the transactions within the existing economic environement get mediated over the market?
2. Boundaries. Eith relation to size and output variety, where exactly is the boundary between firms and the market located? Which are the transaction that are defined by the marked and which are are performed in the organization?
3. Organization. What is the reason for the specific structures of the firm, for example as to the specific forms of hierarchy or centralization or decentralization? How do the formal & informal relationships interplay?
4. Heterogenous actions a of firms performances. What are the drivers behind the different types of performances and actions of firms?
5. Evidence. For the respective theories of the firm, what are the reliable tests?

3.2 Transaction Term

- Was coined by John R Commons in 1931
- Explains that actions are formed by Transactions and not by individual people or exchange of commodities

3.3 Transaction Cost Theory of Firm

Ronald Coase is the creator of the transaction cost approach to the theory of the firm. The cost of providing for goods or services from the market instead of having them provided from within the firm is referred to as the Transaction cost.

It was in 1937 that Ronald Coase set out this transaction cost theory of the firm. It became one of the first (neo-classical) attempts to theoretically define the firm in relation to the market. As per Ronald Coase given the imperfect market information, when the transaction cost of coordinating production through the market exchange is greater than what exists within the firm, then people start to organize production of goods within the firm.

3.4 Transaction Cost Breakup

Clemons & Row in 1992 split the cost of Transaction into Coordination cost & Risk Cost. The difference in the two categories is explained in the below table:

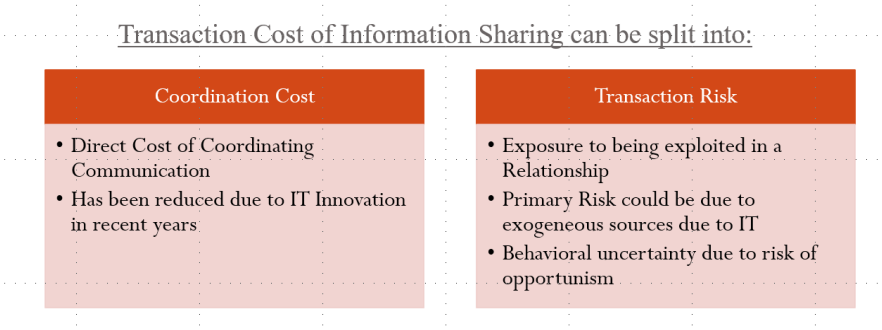


Figure 8: Transaction Cost Breakup

3.5 Information Sharing Based on Transaction Cost Theory of Firm

- Yigitbasioglu, Ogan 2010 gave the theory of Information Sharing based on Transaction Cost Theory.
- The theory analyzes why certain buyers and sellers exchange more Information than others
- The characteristics of the Transaction i.e. the Risk in the Transaction influences the amount of information shared between Partners
- Given the high risks of Information Sharing they cannot be fitted into a one size fit all approach

3.6 Consolidated Literature Review of Theoretical Premise

Document Name	Findings	Inference	Gap
"Information sharing with key suppliers: a transaction cost theory perspective Ogan M. Yigitbasioglu (Department of Accounting, Hanken School of Economics, Helsinki, Finland)" - 2010 Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework Joakim Kembro , Kostas Selviaridis , Dag Näslund - 2014 "Information sharing in supply chains, myth or reality? A critical analysis of empirical literature" - Joakim Kembro, Dag Näslund - 2016 Securing electronic health records without impeding the flow of information Rakesh Agrawal1, Christopher Johnson - 2007 "Knowledge sharing behavior in virtual communities: The relationshipbetween trust, self-efficacy, and outcome expectations Meng-Hsiang Hsua,, Teresa L. Jub , Chia-Hui Yenc , Chun-	As per the study interdependencies of the environment and of the demand characterisitcs and uncertainty can explain to an extent the level of information which is shared between buyers their keu partners in the supply chain. A Model that fits all cannot not be applied due to the significantly high risk of information sharing. Hence the study recommends customized frameworks. Increased Trust will reduce Cost of Information Sharing The research clearly indetifies a linkage between Information Sharing and Perceived Trust and how the two have a strong correlation. An elaboration on the theories that are predominant is provided in the paper and their integration for researching different aspects of information sharing is also discussed.	The study of transaction cost theory in comparison to the to the neo classical theory of Information Sharing provides a valuable lens to interpret and view interorganizational sharing of information. Also based on Risk Analysis it is strongly recommended to have a customized Framework for Information sharing and not use a single model fit all approach. Environment uncertainty has a direct correlation to the intensity of information shared with Key Partners. It also states that the risk of oppurtunism grows higher when there is more at stake. The paper also concludes the significance of Trust in Information Sharing based on emperical evidence. From the results of the empirical study it is suggested that relational benefits have a critical role in ensuring the information sharing as they reinforce the connectedness between members of the supply	The existing literature focusses on the importance of Information Sharing. It highlights the risks associated with Information Sharing. The Trust increase costs and in turn negatively influence the Information Sharing. However, the literature does not extend to find a correlation between Trust and Information Provenance and how the Provenance Tracking would in turn influence the Cost of Information Sharing between Organizations.

Ming Changa" - 2007 Inter-organizational relationships and information sharing in supply chains Jao Hong Cheng 2011 "Inter-organizational relationships and information sharing in supply chains Jao-Hong Cheng∗" 2010 "Interagency Information Sharing: Expected Ben efit s , Manageable Risks Sharon S. Dawes" 1996[7] Acquisti A., Gross R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Danezis G., Golle P. (eds) Privacy Enhancing Technologies. PET 2006. Lectures in Computer Science, vol 4258. Springer, Berlin, Heidelberg - 2006 Supply chain information and relational alignments: mediators of EDI on firm performance , Keah Choon Tan, Vijay R. Kannan , Chin-Chun Hsu , G. Keong Leong 2010k The Impact of Product, Market, and Relationship Characteristics on Interorganizational System	A literature review on the use and adoption of EDI (electronic data interchange) systems (a type of IOS) demonstrates that the adoption has been examined from multiple theoretical view points. The shaping of EDI use in the context of the risks that exist in relation to organisation, resource & technology have been studied by researchers. The impact on IOS pf the conditions under which transactions have been conducted has seen limited attention. Our argument is that an important antecedents to IOS integration are the tranasactional characteristics. It is proposed that key characteristics are captured in the complexity, fragmentation, demand and maket uncertainty and volatility. Is is hypothesized that the combination of these factors with information-sharing environments which are open in nature influence the adoption and integration of IOS Research is also focused for the Health Industry.	chain and this also helps to mitigate the dysfunctional conflicts. Information Sharing incurs cost which is not planned. The central premise that firms have to consider EDI adoption in supplier management in order enhance information and relational alignment between the supply chain partners is supported by thew results. Superior performance is achieved by firms through this alignment. In today's online media, the security risks have been classified based on various factors such as Age and Demographics. Age and Student Status are the key factors that infleunce the Security risk in Peer to Peer Sharing. The research provides confirmation that at the intra Organisation level, policies that govern disclosure of health records stored in digital form can enforced and audited in an efficient and reliable to the database level. The research also shows that advanced data analytics, mining and	

Integration in Manufacturer-Supplier Dyads , Grover and Saeed 2014	In this industry a lot of secure data related to patients health is shared via a set of integrated technologies, known as the Hippocratic Database. Using these technologies security and privacy laws can be complied to, without any hinderance to the analysis, sharing and management of information related to personal health in a legitimate manner. Privacy is of utmost importance in healthe Care Information sharing.	anonymization techniques are feasible for health records aggregation and analysis while maintaining privacy security of the data and identity information of individual patients. It also demonstrates that sensitive information can be shared selectively among autonomous entities by using web services and commutative encryption and this can be done without compromising security or privacy.	

3.7 Summary - Theoretical Gap

The Transaction Cost Theory of Firm analyzes different patterns of Information Sharing across Organizations. The Transaction Propensity is influenced directly by the Risk involved in the Transaction for either parties and this directly influences the amount of information shared between Partners. More importantly the Risks of Information Sharing cannot fit a one size fit all approach.

This research bridges the theoretical gap by creating a framework to understand the influence of Information Sharing Transactions Costs based on Provenance Intensities governed by varying levels of Trust Requirements between Organizations.

4. Research Design & Methodology

This is a Qualitative Research for identification of Challenges in Industry Verticals and verifying application of Blockchain Models. The Research uses Grounded Theory and Framework Analysis Technique for Verifying the Research objectives. Data Pattern Identification is done by Grounded Theory based analysis of underlying transcripts. Semi Structured Questions which are verified using Framework Analysis are applied on a Research Population based on experts.

4.1 Research Problem

As explained in Theoretical Gap, there is reduced information sharing across Organizations due to varying Provenance Intensity requirements. Blockchain is a Trust enabler for Information sharing providing Provenance Immutability, however has known limitations such as scalability and Operational Efficiency. Hence the researcher shall create a framework vector to define the Trust requirements for Industry Verticals based on Provenance Intensities governed by varying levels of Trust Requirements between Organizations. The impelementation of the same shall be done as follows:

- Analyze the Trust Requirements for identified Key Use Cases in the verticals
- Blockchain Framework creation based on Industry standard Blockchains specifying the Trust requirements for each
- Creating of a Framework Vector identifying Transaction Costs for Information Sharing in relation to the identified Trust needs provided by Blockchain

4.2 Research Gaps

Following Research Gaps are identified based on Literature Review:

- Provenance Tracking Models for Information Sharing based on specific Trust Needs
- Blockchain Frameworks based on Information Provenance Propensity

4.3 Research Questions

The following research questions are formulated based on the research gap:

1. What is the influence on Provenance Tracking Intensity Models of an Organization based on Specific Trust Needs of Information Sharing with Partner?

2. What are the applicable Blockchain Patterns when used for Information Provenance Tracking based on Specific Trust Needs

4.4 Research Objectives

The following g research objectives are formulated based on the research gap:

3. To identify the influence of Provenance Tracking Intensities based on the Organization Trust Needs for:

- Immutability
- Business Verification Rules
- Volume of Information Share (TPS)

4. To create an Industry framework of Blockchain Patterns based on Provenance Tracking Needs for:
   - Immutability
   - TPS Scalability
   - Business Logic Implementation using Smart Contracts

4.5 Research Methodology

.

The Research will use Grounded Theory and Framework Analysis Technique for Verifying the objectives. Framework Analysis is a Qualitative Technique which is used to get feedback from the Users who implement the Policies.

4.5.1 Justification of Framework Analysis Methodology

Key Reasons for choosing Framework Analysis as the Research Methodology are:

Table 2: Justification for Framework Analysis

Criteria	Applicability to Research
Research has specific questions	A pre-defined set of questions has been prepared which will be used to ask the Users targeted questions for their needs for Information Sharing Based on Trust. For a detailed set of questions please refer to Appendix
Predefined Sample of Interviewers	Since the audience is limited to Organizations who have Information Sharing Needs and possible candidates for Block Chain based Implementation, the set is pre-defined. For a detailed set of Interviewers please refer to Appendix
Has a predefined set of Issues	The issues faced by the Organization are predefined as Information Sharing issues due to lack of Trust between Partners.

Note: Both the Research Objectives will be verified as part of a Single Methodology. Before focusing on relationships between parts of the data, this approach first identifies commonalities and differences in the qualitative data. This gives the methodology a descriptive conclusion which is focussed around identified themes which are verified through a rigorius process of Literature Study as well as Interviews by industry experts. Hence both the research objectives shall use Framework Analysis technique for methology.

4.5.2 Research Method

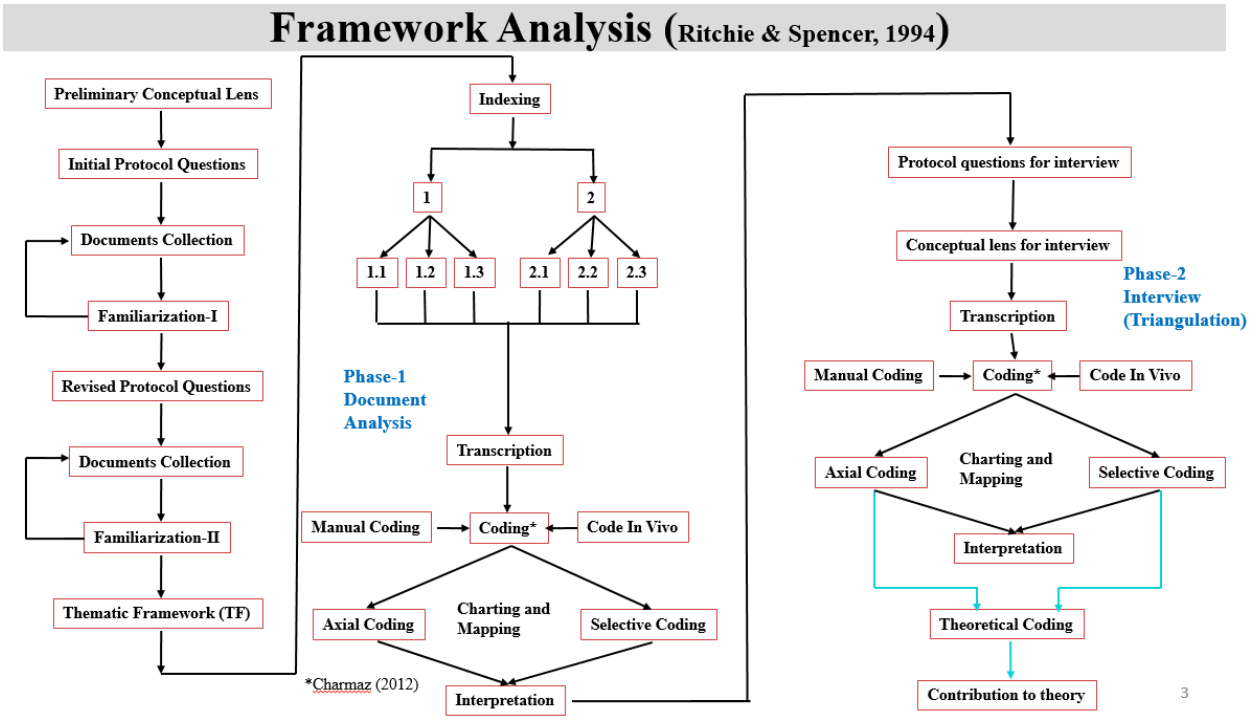


Figure 9: Framework Analysis. Source: Ritchie & Spencer

Framework Analysis provides a "Systematic Approach" to qualitative data analysis. Framework Analysis helps to reduce or summarize interview transcripts to rows and columns of Framework matrix. It saves times and efforts of the researcher by providing only the relevant portions of the text for further analysis. The charted data from various respondents can be compared and contrasted for getting an in-depth understanding of the phenomenon/problem under study. Framework analysis provides a systematic review of different perspectives from the respondents. The Researcher can analyze the patterns of underlying relationships from the row and columns of the matrix. Framework analysis leaves an "audit trail" from the initial framework to final interpretations.

Steps Involved in Framework Analysis:

1. Transcription: The Researcher prepares the interview transcripts for analysis. If the researcher is going for manual analysis, there should be sufficient space or margin on both sides of the transcript to code or to make important remarks/observations.
2. Interview Transcript Familiarization: The researcher goes through the interview transcripts, again and again, to get thoroughly familiarized with it. The Researcher notes the Important observations/insights on both margins of the transcripts.
3. Coding: If the researcher is employing a deductive approach of analysis, the predefined codes from the existing theories and studies are applied. If the researcher is employing an inductive approach, the codes emerge from the transcripts. The process of coding explained earlier for Grounded Theory is followed for Framework analysis as well.
4. Creating a Preliminary Analytical Framework / Conceptual Lens: The coding of the initial transcripts helps the researcher to draft a Preliminary Framework / Conceptual Lens. In purely deductive studies, the Researcher creates the Preliminary Framework from the existing theories and studies by combining the Factor Stream and Process Stream of Research.
5. Application of the Preliminary Analytical Framework / Conceptual Lens: The Researcher applies Preliminary Analytical Framework or Conceptual Lens to subsequent transcripts, and repeats the process of coding. The initial framework gets tested or validated in different stages of analysis. In Ritchie and Spencer's Version of Framework Analysis – the Preliminary Framework / Conceptual Lens gets modified or validated at four stages of data analysis – Two stages of Documents analysis followed by two stages of Grounded Theory. New codes or Relationships may emerge, and existing codes or relationship gets modified or deleted.
6. Charting the data into Rows and Columns of the Framework Matrix: At each stage of Framework Analysis – the relevant portions of the transcripts are taken into the Rows and Columns of Framework Matrix for easy analysis - Comparing and contrasting the concepts within and between the transcripts.
7. Interpreting the data: The Final Framework from the Fourth and Final Stage of data analysis can be used to answer the Research Problem. The Researcher draws Inferences or Insights about the problem/phenomenon under study from the Framework or the charted data. The study of diverse perspectives from the respondents helps the researcher to tackle the research problem from different angles.

The Research Methods involved in the Framework Analysis are Document Analysis and Grounded Theory. Two stages of Documents analysis followed by two stages of Interview analysis using Grounded Theory.

4.5.3 Document Analysis

Document Analysis is a qualitative method for systematically reviewing the documents to answer the research questions. The coding techniques used for document analysis is the same as that of Grounded Theory. Document analysis is used to analyze three types of documents, namely (1) Public Records (2) Physical Evidence (3) Personal Documents. Before starting the document analysis, the researcher should have a "Proper Document Management Plan." Document Analysis gives multiple perspectives from different documents for the same question. It is up to the researcher to accept or reject these dimensions for final analysis. The Researcher indexes these perspectives and takes the best answer or appropriate answers to the transcript for further analysis. The steps involved in Document Analysis are as follows:

1. Collect the relevant documents
2. Develop a "Proper Document Management Plan"
3. Photo Copy the Documents for coding/ or import documents to software for coding and analysis
4. Ensure the Document authenticity, purpose, target audience and biases
5. Interview/Explore the documents for appropriate answers
6. Select the best/appropriate answers to the final transcript for analysis.
7. Draw Inferenences

4.5.4 Grounded Theory

Grounded Theory helps to generate a theory from the qualitative data collected and which has been analyzed systematically. As the name signifies, the theory is grounded in the reseachers data collected. Grounded Theory can help to identify the patterns of relationships hidden in the data and transcripts. Codes here are labels to high light the relevant parts of the transcript.

The process of coding starts first with "Open coding." The researcher reviews the transcript or data line by line multiple times and evolves with the initial codes. These codes are further reviewed for patterns of relationships and aggregated to form "Code Categories" The process is rightly termed as Axial coding. These categories of codes are further connected to a "Core category" by the process called Selective coding.

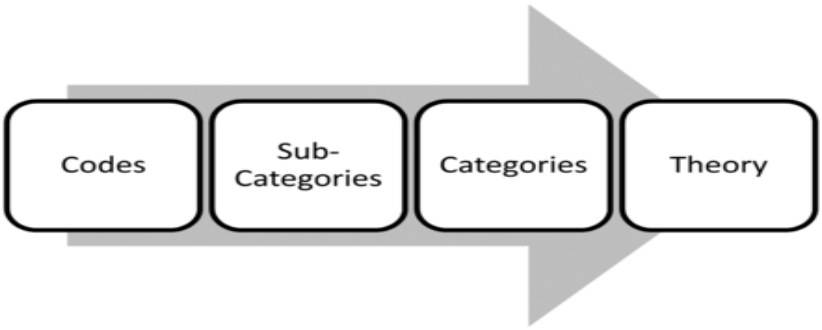


Figure 10: Grounded Theory Data Analysis (adapted from Strauss and Corbin, 2016)

Glaser's Version of Grounded Theory proposes to keep an open approach for data analysis. Glaser' Version does not use Existing theories or Pre-Defined Theories. The codes should emerge from the data collected – proposes an Inductive approach for analysis. Strauss and Corbin propose a Deductive approach – where the existing studies and theories can be used to generate pre-defined codes or conceptual lens for data analysis. In this study, the researcher follows Strauss, and Corbin's version of Grounded Theory as Glaser's version is very time-consuming. Initial findings can be further validated with the help of Grounded Theory. As the data analysis progresses, the researcher will get an idea as to where the relevant information is to searched to support or refute the findings. This process is called Theoretical Sampling. The interview protocol can be modified as the analysis progresses. The researcher should be able to generate useful insights from the data collected. The process of generating useful insights is called Theoretical Sensitivity. Theoretical Sensitivity depends on Experience and Expertise of the researcher.

4.5.5 Tools Used for Research Method

To aid Qualitative Data Analysis Nvivo 12 was used. The key reason for using Nvivo is the ability of NVIVO to make the analysis transparently available for review. Based on Literature survey, NVivo was used initially to do open Coding to create Theme Nodes. The Theme Nodes were analysed further to identify Patterns and similarities and do Axial Coding.

4.5.6 Research Population

Research Population: The target population of the Research is based on Judgmental sampling since it is a qualitative research. The population is divided into two categories

a). Experts in Vertical Domain including Health Care, Education and Media who contribute to the Industry Challenges and

b). Blockchain Experts to provide inputs on the Blockchain Framework Capability and verify the outcomes of the Model Capability Mapping

The respondents with deep expertise in there respective Verticals (More than 20 Years of Experience) were selected.

Patton (2002) has suggested that for qualitative studies, best sample size depends on study objectives, the time allocated, availability of resource and ease of access. Creswell (2003) recommends 5 to 25 and Morse (1998) at least 6. As suggested by Glaser and Strauss (1967) "Principle of saturation" is used for determining the sample size. When the addition of one more respondent does not contribute any further information or dimension for the study saturation occurs.

4.5.7 Interview Protocol

Semi-structured interviews were conducted to collect data from Industry experts. This saves time as well as provides the researcher the flexibility to ask relevant questions as and when deemed necessary and appropriate. The Validity and Relibaility of Semi-Structured interview protocol was tested twice in two stages of Framework analysis by

- Respoondent Validation
- Constant Testing & Comparision of data

5. Conceptual Lens Formation

Research Methodology is defined as the systematic study of the principles that guide an investigation, along with the ways in which theory finds its application. As explained above the Researcher Methodology includes a combination of Document Analysis and Strauss and Corbin's (1998) version of Grounded theory to create a conceptual lens for data analysis.

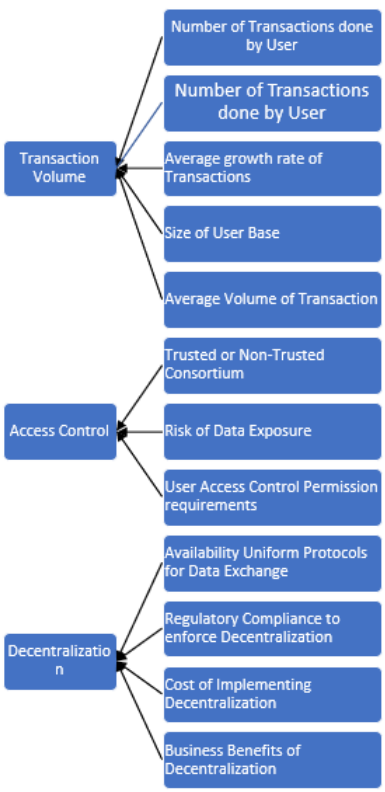
The initial conceptual lens (CONCEPTUAL LENS -1) is framed based on Literature Survey and is used to draft the interview protocol (INTERVIEW PROTOCOL – 1). To aid Qualitative Data Analysis Nvivo 12 was used. The key reason for using Nvivo is the ability of NVIVO to make the analysis transparently available for review. All the research papers which were analysed for the literature review in the study were imported into Nvivo & using the tool identification of themes and classification of the literature data was done. Managing the vast amount of research papers over the five year period of research was significantly enabled by NVIVO.

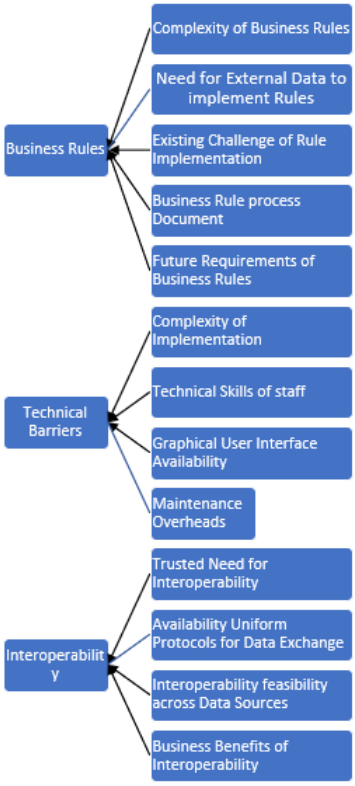
The Categorization of Data has been done based on following basis:

- Use Cases
- Themes

5.1 Research Variables

Twenty Five Independent and six Dependent Variables were used as part the Research to forumalate the Research Questions.





5.2 Initial Conceptual Lens - Based On Literature Survey

5.2.1 Education

Table 3: Conceptual Lens 1: Education

S.No	Variable	Use Case	Themes (Trust Requirements)
1	Suspectibility of Centralized data-storage and management systems to hacking	Identity Mgmt	
2	Student privacy and cybersecurity protection paramount		
3	Lack of Permissioned Access Control for university data.	Intellectual Property	Access Control

4	Solely dependy on the centralized online education platform for Data Security		
5	Accountability and transparency are important		
6	Permissioned Access to student Data	Record Keeping	
7	Current security features on the certificates were not sufficient		
8	University systems have been hacked		
9	Provides users learning incentives by using Gamified interactive education platform such as scholarships & exchange programs	Intellectual Property	Business Rules
10	In majority of cases the presenter or lecturers is responsible for any third party content		
11	Practice of using partially-automated lecture recording systems in institutes		
13	The value and legitimacy of online education is acceptable by less than thirty percent of university faculties accep		
14	Third-party permissioned access tto student data to verify the authenticity	Identity Mgmt	
15	Process Challenges for individuals when they transfer from one institute to another	Record Keeping	
16	Paper certificates and diplomas need to be manually issued and verified		
17	Selling fake certificates and diplomas		
18	The internet has reversed the trend of geographical limitation of degree mills		
21	How do institutions bring all of their legacy data onto newer systems	Intellectual Property	Transaction Volmes
22	Academic records of a person, such as diplomas,, degrees and mark sheets are identity driven belonging to the country or instiure	Identity Mgmt	
23	Need for distributed and trustable data storage method		
24	Students or graduates do not have direct access to their own records from this aggregated database	Identity Mgmt	Decentralization
25	Physically localized and not connected to each other	Intellectual Property	
26	No mature cross-platform course sharing mechanism		
27	P2P distributed architecture over a centralized one		
28	disconnection among institutes	Record Keeping	
29	Universities and governments could be collective caretakers		

30	Elimination of scenarios where some entities control the information of a large number of people;		
31	Education companies and universities must transfer ownership of individual data into the hands of students	Identity Mgmt	
32	Discrepancies were frequently related to educational qualifications	Record Keeping	
33	Limit the tamperability of data		
34	Students cannot alter their grades, degrees, and certification		
35	Information can remain immutable unchanged, and decentralized over time	Managing Intellectual Property	Immutability
36	Education Industry taxonomy, and metadata	Record Keeping	
37	Variation of , barriers of language, protocols and different terminologies.	Intellectual Property	
38	Process challenges including creating a decentralized governance framework		
39	Data is stored in diverse incompatible formats		Interoperability
40	Current process does not regulate the copyright relations between lecturer and the university in educational process.	Intellectual Property	
41	MOOCs present complex copyright issues		IP Protection
42	Access rights predicated on the role the Student has vis a vis the content and Policies that are Coarse grained	Identity Mgmt	RBAC
43	Attitudes towards Technology	Intellectual Property	
44	Acceptance and actual use of computers		
45	Reluctant towards adopting new technologies.due to the lack of necessary knowledge	Record Keeping	
46	Lack of training on using a new skill		Technology Usage
47	Trusted and Comprehensive system for ,storing recording and retrieving educational information	Record Keeping	
48	Higher education institutions that operate without any accreditation		Trust

49	Trust can influence the employees' behaviour to share information	Intellectual Property	

5.2.2 Health Care

Table 4: Conceptual Lens 1: Health

S. No	Variable	Use Case	Themes (Trust Requirements)
1	Data security and privacy are continuously violated in EHR	Clinical Data for Research	Access Control
2	Vital services across NHS were infected by malicious software with a virus		
3	Enormous loss of reputation and capital for Health Care due to counterfiet Drugs	Counterfeit Drugs	
4	Health data needs to be secure and privacy-sensitive	Patient Data Privacy	
5	Large volumes of data is stored in public cloud resluting in increased Privacy issues		
6	Risks of data exposure for Patient Privacy increasing due online access		
7	The risk of misusing health information and increasing transaction costs are increasing		
8	HIPAA privacy regulations require the confidentiality and protection of individually identifiable health information		
9	Only the minimum health information necessary to conduct business should be used or shared		
10	Obtaining consent for access to health care data will become mandatory		
11	Consumer's medical records of approximately 25% patients were breached in the United States	PayForPerformance	
12	Design of EHR systems withprivacy preservation and user-centric access control		
13	Ten percent of drugs sold are counterfeit globally., In developing countries the number can be to 30 percent	Counterfeit Drugs	Business Rules
14	Patients hardly have access to their health records.	Patient Data Privacy	
15	Self-reported data is frequent in health care however it needs to be consistent		
16	Patient frequently share medical history with an insurance organization for claim settlements		
17	Sharing health records can happen between individuals and/or stakeholder		

18	Coordination, elimination of duplication, and outcome tracking among other things is key to tracking	PayForPerformance	
19	Relying on new payment systems for automated payouts		
20	Strong quality side incentives to be put in place for Pay for Performance Data Tracking accuracy		
21	Sharing of healthcare data is essential step to improve the quality	Clinical Data for Research	
22	Data driven smart health care is on rise		
23	The process challenges in getting consent for accessing health care data		
24	Sharing of medical and healthcare data is a critical step to improve the quality of healthcare globally		
25	35% of surveyed life sciences and healthcare institutes plan to deploy blockchain technology		
26	Volume of sensor and EMR data from wearable IoT devicesand patients is increasing	Patient Data Privacy	Data Storage
27	Patients are reluctnat about storing their personal data due to the data leakage		
28	Biological and Healthcare data are organically massive in numbers	Clinical Data for Research	
29	The trade-off in the available computing devices versus the amount of medical records could limit the scalability of such healthcare systems.		
30	DDBMSs are logically centralized-managed leading to access issues		
31	With a 48% rate of increase annually, it shall to enter the yottabyte (one yottabyte ¼ 10008 bytes) range by 2020	PayForPerformance	
32	Users have limited control over personal health data	Patient Data Privacy	Decentralization
33	Current EHR systems use centralized architecture	Clinical Data for Research	
34	Sharing of medical data is one critical step to make the healthcare system smarter		
35	Patient is less likely to repeat diagnostic tests with decentralization		
36	Sharing health records could happen between individuals or across all	PayForPerformance	

37	Notion of self-sovereignty is rarely implemeented	PayForPerformance	Identity Managament
38	Intra-organizational, EHR platforms are also fragmented	Clinical Data for Research	Interoperability
39	Lack of data standardization is a challenge in EHR data transfer		
40	Limited interoperability is one of the biggest challenges for big data centralization		
41	Integration of health data to ensure interoperability across healthcare systems remain a challenging task	PayForPerformance	
42	The primary challenge is modification in current electronic health records (EHR/EMR) is maintaining the interoperability among various involved stakeholders	Patient Data Privacy	
43	Complying with various regulatory protocols and standards is critical	Clinical Data for Research	
44	Current interoperability and nterconnectivity of medical records is not sufficient		
45	Globalization of data is pending due to lack of interoperability		
46	Different users of health data have different roles	Patient Data Privacy	RBAC
47	At about 50% rate of increase in health care data annually the analytics industries is growing at an exponential rate of 28%	Patient Data Privacy	Transaction Volumes
48	Centralized trust is critical for P4P	PayForPerformance	Trust

5.2.3 Media

Table 5: Conceptual Lens1: Media

S. No	Context	Use Case	Themes (Trust Requirements)
1	Privacy compliance (GDPR) is not comprehensive	Digital Content Aggregation Platform	
2	Digital Piracy recognised by Sony as the key cause for loss of profits in its music business		
3	With JPEG the great potential of using blockchain and other distributed ledger technologies (DLT) has been verified.		
4	Digital rights management not reliable	Digital Rights Mgmt Platform	
5	Rights management needs to be optimized		
6	Fake news, privacy, copyright violation, media forensics, and security are key challenges in digital media.	Direct Distribution Model by Artist	Access Control
7	Multimedia distribution currently does not preserve self accesible information of transaction data	Digital Content Aggregation Platform	Audit Trail
8	Record labels claim the largest piece of the revenue share. This is despite the reduced value to the supply chain	Digital Content Aggregation Platform	
9	Systems do not provide support for the end to end value chain. The evolving media value chain now includes the creators and providers of the contents, those who hold rights on the content, the multiple distributors of media, and the purchasers.		
10	Payments by consumers of very small sums of money to read individual articles or even portions of article	Digital Rights Mgmt Platform	
11	Originators rarely receive compensation and don't frequently get attribution		
12	Large pools of royalty revenue do not reach the artist	Direct Distribution Model by Artist	
13	Under the evolving Media Supply chain models the creation of high quality content is a very challenging process.		
14	One challenge the Internet is the hidden 'artist penalty'. The actual artist or the one who has created the content is not identified due to the		Business Rules

	basic nature of the internet, fair compensation to them for their work becomes a challenge.		
15	Volume of data generateddue to the increase of IoT is growing significantly	Digital Content Aggregation Platform	Transaction Volumes
16	Costs associated with storing and securing data remain high	Direct Distribution Model by Artist	
17	Information varies across one database and another. There is no central authority to resolve conflicts	Digital Content Aggregation Platform	Decentralization
18	For recorded music there is a lack of transparency in the value chain	Digital Rights Mgmt Platform	
19	Original media is frequently edited for content generation	Direct Distribution Model by Artist	Immutability
20	Multiple Formats Complicates data acquisition and cleansing	Digital Content Aggregation Platform	Interoperability
21	Problem in the industry currently is that there is no certified registry of music creatives		
22	The key issues as Multiplicity of Music Metadata	Digital Rights Mgmt Platform	
23	Data is rarely standardized		
24	There does not exist a verifiable source (deemed as a “single source of truth”) for validation of Copyright information with the underlying composition	Direct Distribution Model by Artist	
25	Due to geographical variations of language Artists release the same album with multiple labels		
26	Copyright protection needs to be secured	Direct Distribution Model by Artist	IP Protection
27	There is no way for content creators to verify their copyright protection rights	Digital Rights Mgmt Platform	
28	Two big issues that trouble the music industry are piracy and inaccurate ownership information	Digital Content Aggregation Platform	Ownership
29	Improvements in authorship and attribution will enhance Provenance Tracking		

30	The Recording Industry Association of America (RIAA) has attempted educational campaigns, litigation, and technology processes to reduce file sharing.	Digital Rights Mgmt Platform	
31	85% of images are actually 'stolen' without Copyright protection		
32	Contract management needs to be instituted	Direct Distribution Model by Artist	
33	Need for UGC applications targetted by Older Users	Direct Distribution Model by Artist	
34	Non Professional Users become Content Creators	Digital Content Aggregation Platfor	Technology Use
35	There is no current trusted mechanism that can easily get the transaction logs	Digital Content Aggregatio	
36	Privacy Trust,and Security in Media Consumption lifecycle	Digital Rights Mgmt Platform	
37	Trusted and Transparent Media Distribution System		Trust

5.2.4 Blockchain

Variable	Classification	Theme
Public & Private key are used to transmit data	Implementation Methodology	
authorization requirements for nodes in a network		
a robust mathematical algorithm using cryptographic methods to secure transactions		
based on an encrypted distributed database which cannot be altered or disturbed.		
security and credibility of data using asymmetric encryption algorithm in cryptography		
A technology as a cybersecurity shield (as seen by the US Military)	Oppurtunity	Access Control
Meeting and exceeding the European General Data Protection Regulation		
Improve & accelerate healthcare& medical sciences by database standardization and ensuring availability of anonimyzed patient information for demographic profile such as age, gender and health index values		
audit trail which is immutable	Oppurtunity	Audit Trail
The very feature of immutabvility makes blockchain unsuitable for various situations of personal data management	Challenge	Business Rules
Unique feature of enabling unrelated people to reach consensus without central mediation or control	Implementation Methodology	
authentication and remuneration will empower creators,		
cutting out intermediaries that take money		
blockchain only supports create and read functions		
blockchain enabels unrelated people to reach consensus without central mediation or control	Opportunity	
instant verification of the authenticity of these documents		
blockchain is self- regulating i.e. does not require human intervention for execution of computations while being a “trust-free”, tamper-proof and auditable system		
Users should be able to directly check the authenticity of health information directly with the database		

Ensures that there is data redundancy due to multiple nodes replicating the same information		
Cryptocurrencies ensures a range of denomionations, even upto eight decimal places and their low transaction costs means that this medium is highly suited for micropayments.		
creating an integrated governance framework		
Product roadmap should have open standard based platforms		
custom cryptocurrencies		
is innovating on Blockcahin use cases and even using Bitcoin for tuition fees		
University of Nicosia (UNIC) has initiated Educational certificates on the blockchain which will eliminate fraud & will alsio ensure easier diemmination. They are also ensuring fraud awareness & working on eliminating fraud in Student cohorts on MooCs using Blockchain.		
significantly reduce educational organisations' data management costs		
exposure to liability resulting from data management issue	Opportunity	Cost
Vvery limited on-chain data storage (limitation of Blockchain Architecture)		
High cost for data storage due to the decentralized and hashed architecture		
Costly data access, management, and operations for bigger sizes		
Blockchain is not ideal to store huge Volumes of data		
increasing storage capacity to meet requirements of data redundancy (a copy of data exists at each node of the Blockchain) could also become an issue in blockchain deployment and adoption.	Challenge	
encrypted database		
serves as an irreversible and incorruptible repository of information		
Data in Blockchain is stored in encoded fashion to ensure verifiability		
record critical information		
data provenance is stored in Blockchain		
decentralized, de-trusted, distributed data storage structure	Implementation Methodology	
Ability to generate data management structures which allow increased ownership for users	Oppurtunity	Data Storage

decentralized management.	Implementation Methodology	Decentralization
peerto-peer, decentralized database management system		
centralized intermediary not required to manage transactions and assets		
key benefit of blockchain is decentralized management.	Oppurtunity	
capability to integrate data from disparate data sources.		
eliminate the constraints associated with Author's Rights and Related Rights		
control over their own data		
Off-chain blockchain limitation and disadvantages is that users with access to local data transact on it without consensus from other nodes.	Challenge	Framework
Owner of the off-chained data is not defined?		
Encryption the off-chain data is not controlled through the Blockchain		
Offchain data access manageability with proper processes and technology is unclear. Blockchain based control against illegal copyiong of offchain data is not possible.		
permissionless blockchain, i.e. open public participation	Implementation Methodology	
Public Blockchain – public visibility of all records		
Private Blockchain – belong to a specific organization		
Consortium Blockchain – a combination of Private & Public with preselected group of users neing allowed to participate in the consensus process		
Data hashing backed off-chain data storage is emerging as a good option		
"data lakes" for off-chain access allows encrypted to be stored in a data warehouses which resides off the blockchain.		
cryptography-based recording methods provide data protection	Implementation Methodology	Immutability
each transaction is permanent recorded and immutable	Oppurtunity	
suitable as an unchangeable ledger		

Data stored by blockchain technology are immutable		
tamper-proof technology		
decentralized way of informations storage can reduced data manipulation		
guarantees that transaction data is not tampered and the same is backtracked and verifiable		
interoperability is arguably the biggest challenge for medtech	Challenge	Interoperability
Current deployments work in siloes which limit Interoperability		
Across provider interoperability will ke a key requirement which needs to be worked upon	Oppurtunity	
Compliance to national & international standards for data exchange		
Fine grained Access Control Policies	Challenge	RBAC
allows them to program in their chosen language	Challenge	Technology Usage
each node runs independently while following the protocols.	Implementation Methodology	
decentralized P2P network structure,		
hash algorithm makles blockchain a secure technology		
different blockchains have various differing consensus algorithm,		
Use cryptographic technique		
without the need to contact the original organisation issuer	Oppurtunity	
Latency is a limitation of blockchain, transaction at volume are slow	Challenge	Transaction Volumes

5.2.5 Interview Protocol – Based on Literature Survey

5.2.5.1 Education

Table 6: Interview Protocol1: Education

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Do you feel that more Information Exchange across Organizations will bring Operational Efficiencies?

Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
How is different set of data is maintained in your University?
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion what is the tasks for cost optimization? And how would it have an impact total revenue generated by Organization?
Data Security / Access Control /RBAC/Trust/Identity Management/Audit Trail/Ownership
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the importance of Trust in Information Sharing with Partners
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection - Education

What are the challenges faced at the time of admission for verification of the information like certificates, rank and merit of students?
How is the verification process done for students that are coming in for different university / colleges? Any problem faced during the same
How much time is taken to complete the process?
How are the other Universities are doing the same process and if they are using any digital verification process to verify
If yes then have your university considered in apply the same process in your verification system?
If not, then what are challenges faced to implement same within your University?
Is the University / Govt open to sharing data with other University at National level or Globally?
What are the restrictions that University is facing in sharing data nationwide or Globally? Example any govt policy that does not allow to do the same, legal framework that does not allow to share
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see Operational reductions by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Will tranparency and trust with Partners increase with information sharing on Blockchain?
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Monetization of Information, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain

5.2.5.2 Health Care

Table 7: Interview Protocol1: Health

Information Categories
What are the categories of Information you share across Organizations ?
What process do you follow for Information Sharing ?
Technical Usage Barriers
Do you feel that more Information Exchange across Organizations will bring Operational Efficiencies?
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?

What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High ?
Information Data Storage & Volumetrics
What is the Volume of Information Shared in your hospital ?
How is different set of data is maintained in your hospital ?
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing ?
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. ?E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties ?
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties ?
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match ?
Has there been a case where you could not receive information from other Organization due to regulatory challenge ?
Cost of Information Sharing
How many people are involved in information sharing across your department ?
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization ?
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Data Security / Access Control /RBAC/Trust/Identity Management/Audit Trail/Ownership
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the importance of Trust in Information Sharing with Partners ?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing ?
Business Rules /Interoperability/IP Protection – Health Care
Does the patient have to repeat the examination when he moves from one hospital to the other ?
Is there a way to review the Data entered by Drug Companies into the database ?

Is there sufficient transparency in Health Care Information available across Organizations ?
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing) ?
Do you have an identified used case which the organisation can gain benifit from??
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market) ?
Will tranparency and trust with Partners increase with information sharing on Blockchain?
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain for security ?

5.2.5.3 Media

Table 8: Interview Protocol 1: Media

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Do you feel that more Information Exchange across Organizations will bring Operational Efficiencies?
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
How is different set of data is maintained in your University?
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization

What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Data Security / Access Control /RBAC/Trust/Identity Management/Audit Trail/Ownership
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the importance of Trust in Information Sharing with Partners
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Media Specific Queries
Are there any preferred channels for information sharing
What is the revenue share arrangement for information sharing across various providers
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Will tranparency and trust with Partners increase with information sharing on Blockchain?
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)

Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain ?

5.2.5.4 Blockchain

Table 9: Interview Protocol1: Blockchain

Decentralization
What is the current status of Decentralization in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Decentralization ?
What are the growth patterns in Decentralization in Blockchain ?
Does Blockchain support Decentralization ?
Interoperability
What is the current maturity index of InterOperability in Blockchain ?
Across the Four Blockchain categories which of them provides optimized Maximum and Minimum Interoperability ?
What is the growth trends in InterOperability in Blockchain ?
Does Blockchain support InterOperability ?
Access Control
What is the current status of Access Control in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Access Control ?
What is the growth trends in Access Control in Blockchain ?
Does Blockchain support Access Control ?
Transaction Volumes
What is the current status of Transaction Volumes in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Transaction Volumes ?
What is the growth trends in Transaction Volumes in Blockchain ?
What is your opninon on Blockchain support for Transaction Volumes ?
Data Storage
What is the present status of Data Storage requirements in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Data Storage ?
What is the growth trends in Data Storage in Blockchain ?
What is your opninon on Blockchain support for Data Storage ?
Operational Ease
What is the current status of Operational Ease in Blockchain ?

Across the Four Blockchain Types which provides Maximum and Minimum Operational Ease ?
What is the growth trends in Operational Ease in Blockchain ?
What is your opninon on Blockchain support for Operational Ease ?
Business Rules
What is the current status of Business Rules in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Business Rules ?
What is the growth trends in Business Rules in Blockchain ?
What is your opninon on Blockchain support for Operational Ease ?
Generic
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Is the system data required to be stored On Chain or Off Chain

5.3 Stage 1 – Familiarization Based on Use Cases

5.3.1 Media Industry Use Cases – Familiarization Stages

5.3.1.1 Industry Use Case – Ujo

While the Banking Industry clears settlements in days, Artists in the Music Industry wait for years to receive their royalties. Ujo a Music Service which is Ethereum recording of works by artistys as smart contractsw. This enables instant settlement of payments upon content purchase and download.
Phil Barry the founding partner says that the Business Objective is automation of royalty payment by creating open platform which is based on comprehensive Meta Data

- This makes Music fungible. It enables purchase of atomic components by splitting of the music into micro components individually e.g. the vocal tracks lyrics, and instrument's creating new opportunities for revenue generation.
- Ujo founders plan to use ERC721 for tokenizing the rights, this is designed on a COALA IP based Metadata format
- As of 2019 October, The number of registered users for buying music was 2,062 on the site. 2,144 songs had been registered b. 662 musicians. Purchasing total to only 275 transactions for a vlaue of $509.

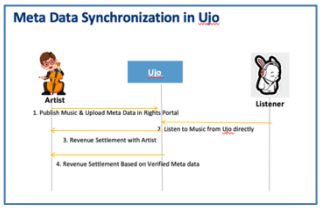


Figure 11: Content Distribution Process

5.3.1.2 Industry Use Case – PeerTracks

Peertracks is a peer to peer discovery based Music Streaming and retail platform. Cedric Cobban, Peertracks CEO has set the Business Objective to enable artists find new wayd of Monetization for their content. Built on SounDAC engine which is in internally based on Ethereum. James explained in [89] that Royalty Payments are reconciled once day. The revenue is computed based on Peertracks currency. These are based on the number of listening tracks per minute. PeerTracks supports up to100,000 Transactions Per Second by running on the SoundAC engine. As explained by Opal [38] this runs on Delegated Proof Of Stake.

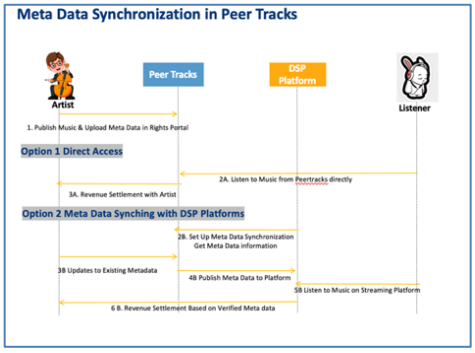


Figure 12: Meta Data Synchronization in Peer Tracks

5.3.1.3 Industry Use Case – Verifi Media (previously DotBlockChain)

Established by the PledgeMusic Company in New York, Verifi Media has created .bc or dotBC a proprietary music format. On this platform, on publishing their works instead of a regular format audio file , the artist or rights holder create a .bc file. Composition data, including songwriters information, performers, and music title is bundled into a .bc file. On completion of the setup, the music schema is published to the blockchain and exposed to end users.

The .bc rules will be used by specialized players to interpret the metadata and perform validation on the play request. As of 2012, December Verifi Media received permission for 60+ million plus songs. The .bc files are used by Veri Media to protect and verify copyright information. Only the proprietary players ensure that the decoding is possible. Richard Skidmore (Head of Business Development), explained that Role Based Read Access is supported by Verify Media to ensure access to only the legitimate users for reading the Meta Data Properties

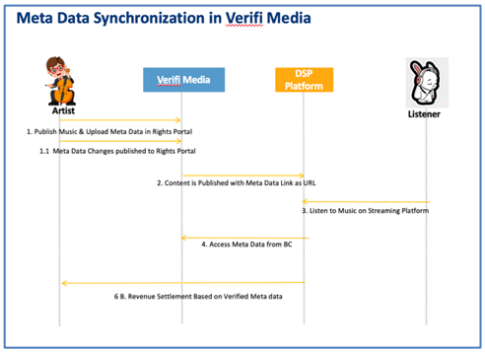


Figure 13: Meta Data Synchronization in Verifi Media

5.3.2 Education Industry Use Cases – Familiarization Stages

5.3.2.1 Industry Use Case – Education Blockcerts

Blockcert is working to create an open standard for Digital Certificates. A digital JSON file forms the Blockcert. It is readable by humans and machines. Any student record for e.g. transcript, academic record or diploma can be denoted through the JSON file.

These can also be enriched with metadata to bring in greater clarity. For Blockcerts the blockchain becomes a global notary to verify the authenticity of a record, and also to verify that it has not been changed from what was issued originally. The Blockcerts can be instantly verified by a decentralized without the need for any intermediaries. A record on Blockcert can be verified by an third party using a decentralized global connection. Bitcoin, Ethereum, Hyperledger, and other decentralized networks can verify Blockcerts. Blockcerts complies to Open Badges based on Linked Data. Connected Data publishes data which is understandable in many contexts.

- The Massachusetts Institute of Technology uses Blockcerts to issue digital certificates for all of their graduates
- In the Maltese Government project as explained by Alessie [6] on top of the Public Bitcoin network an access control layer which is governed by the Consortium Partners is built. This forms a federated governance which is truly decentralized.

5.3.2.2 Industry Use Case - OpenCerts

As explained by Asiri in [9] Government Technology Agency, Ngee Ann Polytechnic and Skills Future Singapore Ministry of Education, came together to setup the OpenCerts platfrom based on the Etherium Blockchain. From 2019, OpenCerts has started to issue academic records for students' from seventeen universities in Singapore. Their project in the Blockchain relies on signing unique document hashes. Personal information from the students is not required. On creation of a unique OpenCerts certificate, automatically a unique Digital tag gets associated with it. The Blockcahin securely stores, the unique digital code with the automated hashed information

from the certificate. On opening the .opencert file, automatically its contents get compared to the original hash value which is stored on the Blockchain, thus verifying the contents.

5.3.2.3 Industry Use Case - Sony Fujitsu

As explained by Sun et. al in [99] in collaboration with Hyperledger, Sony Fujitsu is creating a Blockchain enabled Platform to enable the following:

- Easy contribution of data to the Blockchain by education and training institutes
- Collation & storage of individual data in verifiable formats
- To control access and verification of the data for training and other requirements it provides permissions to authorized organizations.

Don Tapascott et al explain in [101] that Sony Global Education become the first consumer of this technology by permitting sharing of official academic records safely with each other. Global Education plans to verify the platform by storing transactional data generated by 250,000 participants of Global Math Barrier, Sony Global Education's world-wide maths competition.

Binded: Managing Intellectual Property

As explained by Grech in [41] Binded (started as BlockAI) is a service for registering digitial copyrights. The service is being offered for storing digital images on the blockchain. The uploaded images are stored with their hash, timestamp and the author identity, ensuring a proof of publication that is immutable and utilizable for enforcing copyright claims.

5.3.2.4 Industry Use Case - Identity Management - Sovrn

A decentralized identifier (DID) it the concept on an online identity created, controlled and owned by the owner. The absence of a decentralized entity results in Red tape bureaucratic processes which cost C$ Ten Billion each year to British Columbia based companies in Canadian [47]. Hyperledger Indy based solution supports SSI controlled identity owner and Sovrn uses this approach to provide an optimal solution to the decentralized identity problem. Identity details are housed in a wallet, this data is stored in Postgres SQL. Use of Postgress allows support for up to 2600 verifications per minute, with a permissioned blockchain deployment, with secure propagation of trust information amongst participating entities. In their White Paper [98] Sovrn promoters state – the "Internet of Identify" deployment which is built on Hyperledger Indy creates a separate DID for every relation ship, this is achieved by implementing a pairwise-pseudonymous identifiers. This ensures identity information has complete privacy.

5.3.3 Health Industry Use Cases – Familiarization Stages

5.3.3.1 Industry Use Case - Guard Time:

Guard Time is a UAE based healthcare provider. Guard Time is pioneering blockchain application in Health Care with its work on online and offline mode on the KSI blockchain. The KSI blockchain operates on Proof of Authority algorithm. Being a hybrid Blockchain, it energy

efficient but has limited decentralization, as the control is with a limited number of actors. Each of the validating node publishes blocks which in tuen are then validated by other nodes, these nodes have the the power to reject. Matthias Mettler have mentioned that Guard Time is being used by Govt. of Iceland, Estonia[74] and in Hungary for the purpose of maintaining Vaccination information for:
Proof of Vaccination: Yellow Card like functionality to maintain vaccination information
Eligibility Priority Management: to help the Government to make the process for Priority Management fair and accountable
Monitor Uptake amongst population: Geo monitoring of Vaccination progress in order to ensure reduction in transmissions.

5.3.3.2 Industry Use Case - Mediledger

Mediledger: In partnership with Genentech and Abbvie, Pfizer has piloted a Blockchain project coined as Mediledger. It uses a Closed/Private Blockchain to keep patient and drug traceability as recorded by Liang et. al[30]. Counterfeit Drug production is stopped at the source by giving access rights only to manufacturers for serial number and product id association. Zero-knowledge proofs are key to ensure Data Privacy across Organizations. It ensures strong privacy and security arrangements by adopting key principles of data minimisation, similar to the Education Sector as explained by Deepika et. al in [24]. In addition patients are given control of their information including viewing rights to see who has accessed their information.
As mentioned by Sohail Jabbar (2020)s if a supply chain partner is using an unreliable system to record information, then the addition of Blockchain technology can become more detrimental rather than facilitating the user. The immutability of the Blockchain does not guarantee the quality of the data.

5.3.3.3 Indusrty Use Case - MedRec

A blockchain pilot project led by the Beth Israel Deaconess Medical Centre and MIT Media Lab is addressing interoperability in Medical Data[106]. MedRec operates in Offline storage mode wherein only the hash of the prescription is stored on Blockchain. The patient has full access of the information and visibility into people accessing the information. MedRec is based on Ethereum. However, like typical Blockchain based systems, there exist no process automation to verify the data published on the blockchain as explained by Espisote et. al [31].

5.3.4 Summary of Industry Applications Study Across Use Case Verticals

Table 10: Industry Applications study Summary

Application	Domain	Business Use Case	Block chain Platform	Block chain Type	Key Features	Key Challenges

Bittunes	**Media**	Focusses on Non Major music industry music which as per them forms 99% of the Music	Bitcoin	Public Permissionless	No Single Owner Low Transaction Volumes	Since it has a limitation on TPS the scalability is a concern
BlockCerts	**Education**	Used for record authentication: a global notary whose role is to ensure authentic records unmodified from the time of record creation.	Blockcerts can issue records on a wide variety of blockchains including Bitcoin, Ethereum, and Hyperledger	Public /Public Permssioned	Implementing recipient controlled, user claims utilizing tools that offer ease of use e.g. certificate wallets as mobile apps Permissioned Read Depends on underlying Platform	Enhanced integration with Decentralized Identifiers Improving decentralization and longevity by removing dependencies on issuer-hosted data
Dot Blockchain/Verifi Media	**Media**		Bitcoin/ Hyper Ledger Saw Tooth		• Dot Blockchain Music plans to add wrappers that store configuration information relating to who should be paid and contact details Hyper Ledger enables higher Volumes but in Private Blockchain Mode Only	

Guard Time	Health Care	Used to keep Vaccinatiion Information, Priority Management Eligibility and Monitor uptake amognst population	KSI Blockchain	Hybrid Public Permissioned	UAE Based company currently used by Govt of Iceland and Estonia and Hungary Read level access High due to Hybrid Blockchain	Since it is hybrid blockchain, Data Privacy can be compromised
Jaak	**Media**	Music Rights Platform Afordable Content	Ethereum		Swarm Low Transaction Volumes	
Media Chain	**Media**	Ensure that artist gets his share of the revenue and not the labels Meta Data for content is not completely sufficient so revenue share across partners cannot be accurate	IPFS	Permissioned	Spotify bought MediaChain Mediachain offers flexible permission modes for writing to domains, including: custom governance and permissionless consortium through smart contracts. BlockStack, KeyBase, is used for identification Mediachain provides long-term storage which is scalable, for application data with a standard API. This permits data to be reused by others, creating	JSON-LD format is used to store the meta data from multiple systems. On top of this a resolver is used to identify meta data across multiple sources. The Meta Data is then stored off chain on IPFS

					additional value for users.	
Mediledger	Health Care	Drug Traceability		Private	Zero Knowledge proofs are used to provide Data Privacy Patient has access control for Read & View Permissions	There is no way to validate the data at source
MedRec	Health Care	Interoperability in Health Care promoted by a Decentralized Blockchain Platform	Ethereum	Public	Project is led by MIT and Beth Israel Patient has access control for Read & View Permissions Only the hash is stored in blockchain while Data is stored Off Chain	Due to Off Chain Data storage, there is probability of Data Privacy Compromise

Mycelia	**Media**	To makle sure that revenue transfer to the artist is immediate rthe Meta Data of the content is augmented end enriched.			• Imogen Heap of Mycelia envisages to include key, lyrics, tempo, instruments, the location in which a piece of music was written, even the type tea she was sipping as she wrote it. Identity Management through Creative Passports are used for identification	
OpenCerts	**Education**	Validating and Issuing academic certificates that are permanent and tamper-resistant	Etherrum	Public /Public Permssioned	educational institutions will see substantially reduction in the time spent on vouching for their authenticity and re-issuing certificates. Per mssioned Reads Stores records of 18+ Universtities in SG	degree mills—organisations that claim to be institutes of higher learning but dole out substandard or illegitimate academic certificates for profit—could also utilize OpenCerts for publishing certificates on the public blockchain. Mobile

						App for access
PeerTracks	**Media**	Super Distribution Modelwith transperency focussed on Indie Bands. Purchaser gets currency which can be exchanged with fan club activities. Real Time Streamring for Free	MUSE/SounDAC		SounDAC enabled for payment They want to become a DSP	Crowd curated Meta Data is supported. It makes sure all the metadata is compliant to the standards in the industry. From composer, artist , genre selection, to label splits, to UPC codes and ISR

Resonate	**Media**	Allow listeners to pay as they stream until they own the song. The first play of a track is cheap. Each each play costs progressively higher until user has paid the price of a digital download and outright own the track. Resonate charges 30% commission on all revenue. However figures suggest artists would receive approximately $1,526 for every 100,000 plays on Resonate	IPDB	Permissioned	Life ID which is a blockchain based system is used for this Supports medium Transaction Volumes due to IPDB Capability	Track Title, Artist Name, Track Number, Album Title, Year, Genra, Comments, Composer, Album Artist is tracked
Sony Fujitsu	**Education**	Digital Record Keping	Hyperledger Fabric	Private	it allows for additional business logic and flexible data models as compared to other blockchain solutions Permissioned Read & Write 250,000 Student Data is stored	Interoprability with other Blockchains

Sovrin	**Education**	Internet for education Identity. It is used to create a decentralized database of student profiles that contain both as well as learning records as well as profile data	Hyperledger Indy	Hybrid Public Permissioned	ZKP Permissioned Read High due to separate Validator and Observer Nodes	
Ujo	**Media**	Shared Infrastructure for the Music industry to ensure returns more value to the artist. 100% of collections go to the Musicians	Ethereum	Permissioned	The artist content has its own Meta Data. Connects to a decentalized Payment Platform Artist can sell directly from there platform. uPort (Consensys) is used for identification Off Chain hosting of Content hence Volumes can be higher	Off Chain storage of Meta data Blobs utilizing Swarm or IPFS. Meta Data is stored in machine readable format.

5.3.5 Cost Challenges of Information Sharing

Focussing on the benefits of decentarlization Walker et. al (2015) mentioned that based on review of the key elements of interoperability for which a dollar value can be assigned, it is forecasted that net savings from national implementation of standardized and fully interoperability between providers and other health organizations could yield upto $78 billion annually. This will be approximately 5 percent of the total projected spent on U.S. health care in 2003 to 2014. In addition, the model did not include many other potentially important benefits and costs. On an aggregated view it is computed that their total value is hugely positive. The value of standardized full interoperability is most probably to be higher than the projected results. This creates a very compelling business case exists for fully standardized HIEI at national level.

Importantly as mentioned by Esposito et al (2018), there are limitations associated with a blockchain-based implementation that need to be carefully studied as with any security solutions,. To highlight, blockchain technology can be disruptive and requires significant investment as well as radical rethinking in the entire ecosystem (e.g. redesigning of business processes and replacement of existing systems). In simple terms, before starting on Blockchain, healthcare organizations especially publicly funded providers should conduct a cost benefit review to verify the return on investment and any potential implications (including. financial and legal). In some cases, the same record can reside in different nodes of the network, located in different locations with different data protection and privacy requirements (e.g. US and EU).

5.3.6 Blockchain Frameworks – Familiariation Stage

Following an efficient survey methodology, researchers previously inspected blockchain writing from white papers and gathering procedures that cover substantial use cases and frameworks across different areas including Health Care, Media and Education. Notwithstanding the area, there is a typical rundown of difficulties that blockchain applications face, like normalization and interoperability, framework execution and adaptability,resource information security and protection, security, just as lawful and administrative issues. In view of the investigation following is a segment based examination system to work with a typical comprehension for blockchain

5.3.6.1 Ownership Based Blockchain Frameworks

The below diagram demonstrated the Blockchain Quadrant based on Ownership. The key characteristics for each are:

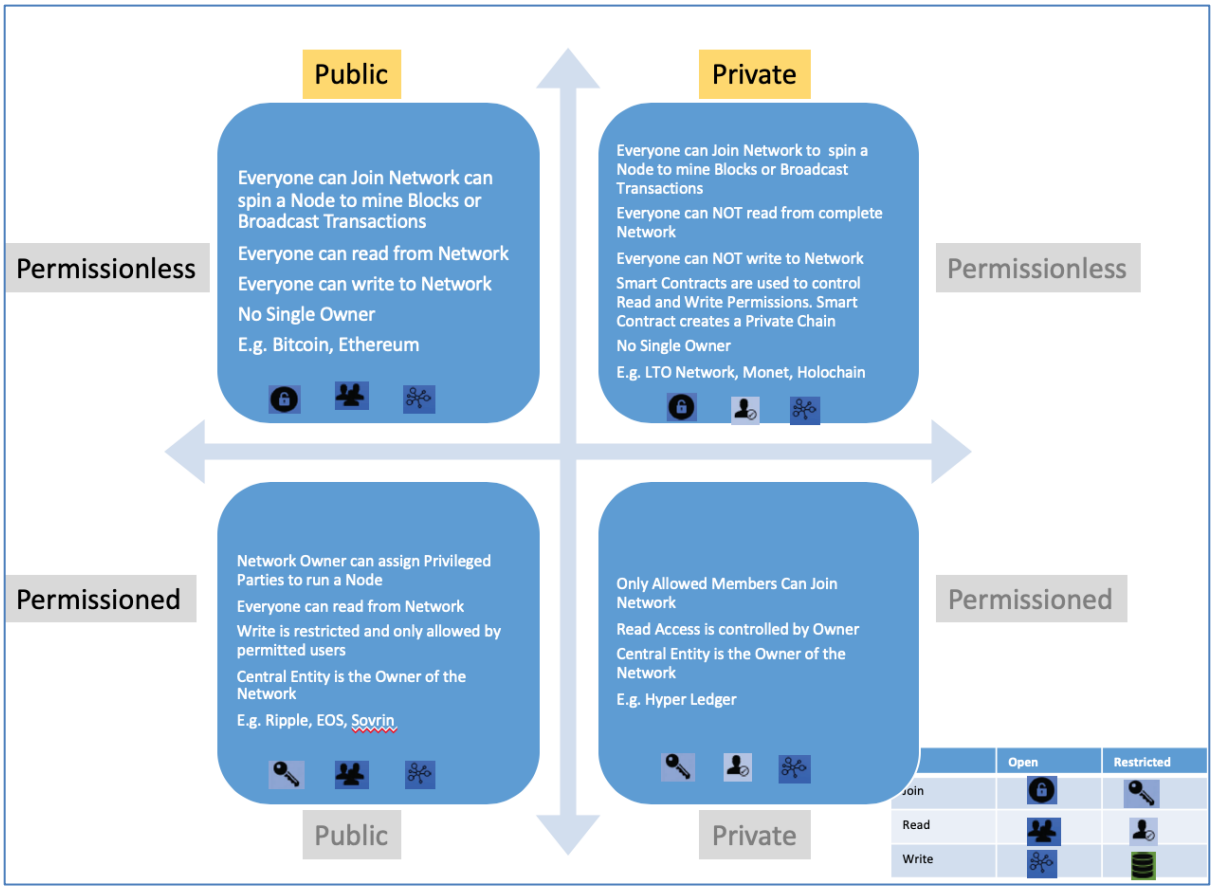


Figure 14: Ownership Based Blockchain Quadrant

Permissionless blockchains
Permissionless Blockchains have are open and transparent and have Public Ownership. As mentioned in [70] it is called Permissionless if anyone can join the Blockchain. However, they are relatively slower in comaparison to Permissioned Blockchains. Such networks are vastly censorship resistant.

Private Permissionless Blockchain
In such blockchains there is no restriction on external participants who can take part in the Consensus Mechanism. However there is known restriction on which user can write and read the content in the Blockchain.

Public Permissionless Blockchain
Any participant can take part in the validation of the blocks, record transactions, or read data in the Blockchain. These are publicly accessible to everybody. Consensus is reached through protocols like Proof of Stake or Proof of Work. These have high limitations on maximum number of Transactions supported per second [73]. All Users have access for Read and Write in the public Permissionless Blockchain.Any of the participants can start recording transactions and

start a node. Ethereum and Bitcoin are the most common examples of Public Permissionless Blockchains.

Permissioned blockchains

The network of nodes is permissioned and Governance is closed. New nodes can only join with permission from the validator nodes as mentioned in [73]. Permissioned Blockchains typically are trusted, have Private Membership, and do not have the Performance problem of Permissionless Blockchains.

Private Permissioned Blockchain

These Blockchains are controlled by Unique group of multiple or one owners. Participants are decided using the Consensus Mechanism. A pre-defined group of whitelisted users can write or read to the Blockchains links as is mentioned in [60]. As mentioned in [7], the most popular Permissioned Blockchain Hyperledger can scale up to 3500+ TPS. These are mostly a group of partners that benefit by sharing data in an immutable database and are connected through Business Operations. As mentioned in [73], in case public verifiability of the records is not mandatory then Private Permissioned Blockchain should be considered.

Public Permissioned Blockchain

Public Permissioned Blockchains have configurations that determine which user can start nodes and take part in the validation process. Whitelisted nodes can coordinate in the Consensus Mechanism. This is normally preferred by Public institutions like Corporates, Government Agencies or Educational Institutes. The owner defines Validator Nodes that configure the Governance rules for the Blockchain including parties that can write to the Blockchain or that can create new nodes. Unlike other Blockchains, read access is open to all making the Blockchain publicly accessible as mentioned in [73].

Operational Usage

In case a passenger has to build their own vehicle before they could drive on the road is a similar scenario. This is similar to the state of Blockchain tool development maturity currently for developers. To help save expensive resources, including finances time, and resources, it is critical to have ready to market and semi-automated, exchangable protocols for blockchain applications that make development convenient and flexible like all development languages currently. By having pre-build configurable custom modules for blockchain will help reduce development time and operational costs.

As per Forbes (2019) the most critical requirement for Blockchain Mass Adoption is to moving of infrastructure and removing the low level building. The average developer spends additional effort on, rather than building features for the application to work on top of the blockchain. The blockchain community needs to focus on ease of development for developers for long-term solutions and not just temporary bandaids.

5.3.7 Data Analysis 1 – Based on Use Case Study

5.3.7.1 Education

The following was Data Analysis relevant to the research based on following criteria:

a. Data Storage Requirements in Education are not extremely large since Degree Certificates do not have large Volume. Hence the focus on this variable has been reduced
b. Immutability and IP Protection have been merged into single theme since based on study since the two are inter-relatable for Education Industry
c. Trust is a derived variable based on direct influencer variables inclusing decentralization and Immutability. The research will influence Trust based on influencer variables, hence Trust as an attribute has been distributed into the influencer variables
d. RBAC has been merged with Access Control as theme since both use the same underlying technology

Summary: Reduced Conceptual lens from 47 to 37 Variables

Table 11: Interview Protcol 2: Education

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
How is different set of data is maintained in your University?

Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection
Health Care Specific Queries
Does the patient have to repeat the examination when he moves from one hospital to the other
Is there sufficient transparency in Health Care Information available across Organizations
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your organisation? What are the known challenges(For e.g.: Lack of trust in Technological systems of Business Sharing, Lack of Business Vision for Information Sharing)
Do you have an identified used case which the organisation can gain benifit from?

Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain
Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.3.7.2 Health Care

The following was Data Analysis relevant to the research based on following criteria:

a. RBAC & Identity Management is important for Health Care for patient data since privacy issues are preventing patients from sharing data. Based on study of existing system RBAC & Identity Management is a sub-component of Access Control and hence has been merged into a single theme
b. Data Storage and Transaction Volumes will be critical for Health Care and have been merged into single theme since Transaction Volumes directly inpacts Data Storage. Data Volumetrics in Health Care industry are large since EMR Volume in huge.
c. Based on study if Use Cases it was verified that basic Decentralization is supported across all Helath Care Applications. Hence variables related to Decentralization for Blockchain have been removed. However, variables related to challenges in health care industry for decentralization have been retained.
d. It has been observed that there is limitation of external factors influencing Supply Chain inputs for Counterfeit Drug Supply. Hence those Use Caes might not be relevant for Blockchain application. Those variables have been retained for further analysis

Summary: Reduced from 48 to 34 Variables.

5.3.7.3 Media

The following was Data Analysis relevant to the research based on following criteria:

a. RBAC is important for Producer & Consumer and is a sub-component of Access Control and hence has been merged into a single theme
b. Immutability and Audit Trail have are extremely important in Media Meta Data. However this is a basic trait of Blockchain and hence has been merged into Business Process Theme
c. Trust is a derived attrribut for Media and basic attribute for Blockchain and hence has been removed

Summary: Reduced from 37 to 32 Variables

5.3.7.4 Blockchain:

Basic support for all six variables has been found in Blockchain. Hence Variables related to Basic support have been removed from Conceptual Lens and Questionaire

5.3.8 Revised Conceptual Lens – Based on Use Case Study

5.3.8.1 Education

Table 12: Revised Conceptual Lens2: Education

S.No	Variable	Use Case	Theme
1	Centralized management and data storage systems are open to hacking	Identity Mgmt	Access Control
3	Lack of Permissioned Access Control for university data.	Intellectual Property	
4	The online platform brings limited Data Security		
5	Access rights predicated on the role the Student has vis a vis the content and Policies that are Coarse grained		
7	Current security features on the certificates were not sufficient	Record Keeping	
8	University systems have been hacked		
9	Provides users learning incentives by using Gamified interactive education platform such as scholarships & exchange programs	Intellectual Property	Business Rules
11	Practice of using partially-automated lecture recording systems in institutes		

13	The value and legitimacy of online education is acceptable by less than thirty percent of university faculties accep		
14	Third-party permissioned access to student data to verify the authenticity	Identity Mgmt	
15	Process Challenges for individuals when they transfer from one institute to another	Record Keeping	
16	Paper certificates and diplomas need to be manually issued and verified		
21	How do institutions bring all of their legacy data onto newer systems	Intellectual Property	
22	Academic records of a person, such as diplomas,, degrees and mark sheets are identity driven belonging to the country or institure but Volume is low	Identity Mgmt	Transaction Volmes
24	Students or graduates do not have direct access to their own records from this aggregated database	Identity Mgmt	
25	Physically localized and not connected to each other	Intellectual Property	
26	No mature cross-platform course sharing mechanism		
30	Elimination of scenarios where some entities control the information of a large number of people;	Record Keeping	
31	Education companies and universities must transfer ownership of individual data into the hands of students	Identity Mgmt	Decentralization
32	Current process does not regulate the copyright relations between lecturer and the university in educational process.	Record Keeping	
34	Students cannot alter their grades, degrees, and certification		
35	Information can remain immutable unchanged, and decentralized over time	Intellectual Property	Immutability
36	Education Industry taxonomy, and metadata	Record Keeping	
37	Variation of , barriers of language, protocols and different terminologies.	Intellectual Property	
39	Data is stored in diverse incompatible formats		Interoperability

43	Attitudes towards Technology	Intellectual Property	Technology Usage
45	Reluctant towards adopting new technologies.due to the lack of necessary knowledge	Record Keeping	
46	Lack of training on using a new skill		

5.3.8.2 Health Care

Table 13: Revised Conceptual lens: Health Care

S. No	Variable	Use Case	Theme
1	Data security and privacy are continuously violated in EHR	Clinical Data for Research	Access Control
2	Vital services across NHS were infected by malicious software with a virus		
3	Enormous loss of reputation and capital for Health Care due to counterfiet Drugs	Counterfeit Drugs	
4	Different users of health data have different roles	Patient Data Privacy	
5	Large volumes of data is stored in public cloud resluting in increased Privacy issues		
6	Risks of data exposure for Patient Privacy increasing due online access		
7	Notion of self-sovereignty is rarely implemeented		
8	HIPAA privacy regulations require the confidentiality and protection of individually identifiable health information		
9	Only the minimum health information necessary to conduct business should be used or shared		
10	Obtaining consent for access to health care data will become mandatory		
12	Design of EHR systems withprivacy preservation and user-centric access control	PayForPerformance	
14	Patients hardly have access to their health records.	Patient Data Privacy	
15	Self-reported data is frequent in health care however it needs to be consistent		
16	Patient frequently share medical history with an insurance organization for claim settlements		

13	Ten percent of drugs sold are counterfeit globally., In developing countries the number can be to 30 percent	Counterfeit Drugs	
17	If Supply chain partner is using an unreliable system to record information then it impacts the Data Quality		
18	Coordination, elimination of duplication, and outcome tracking among other things is key to tracking	PayForPerformance	
19	Relying on new payment systems for automated payouts		
20	Strong quality side incentives to be put in place for Pay for Performance Data Tracking accuracy		
21	Sharing of healthcare data is essential step to improve the quality		
24	Sharing of medical and healthcare data is a critical step to improve the quality of healthcare globally	Clinical Data for Researc h	
26	Volume of sensor and EMR data from wearable IoT devicesand patients is increasing	Patient Data Privacy	Transaction Volumes
27	Patients are reluctnat about storing their personal data due to the data leakage		
28	At about 50% rate of increase in health care data annually the analytics industries is growing at an exponential rate of 28% o enter the yottabyte (one yottabyte ¼ 10008 bytes) range by 2020	Clinical Data for Research	
29	The trade-off in the available computing devices versus the amount of medical records could limit the scalability of such healthcare systems.		
32	Current EHR systems use centralized architecture	Clinical Data for Research	Decentralization
33	Users have limited control over personal health data		
35	Patient is less likely to repeat diagnostic tests with decentralization	Patien t Data Privac y	
38	Intra-organizational, EHR platforms are also fragmented	Clinical Data for Research	Interoperability
39	Lack of data standardization is a challenge in EHR data transfer		
42	Globalization of data is pending due to lack of interoperability		

43	Complying with various regulatory protocols and standards is critical		
45	The primary challenge is modification in current electronic health records (EHR/EMR) is maintaining the interoperability among various involved stakeholders	Patient Data Privacy	

5.3.8.3 Media

Table 14: Revised Conceptual Lens: Media

S. No	Context	Use Case	Theme
1	Privacy compliance (GDPR) is not comprehensive	Digital Content Aggregation Platform	Access Control
2	Digital Piracy recognised by Sony as the key cause for loss of profits in its music business	Digital Content Aggregation Platform	
3	JPEG has verified that distributed ledger technologies (DLT) and blockchain have great potential	Digital Content Aggregation Platform	
4	Digital rights management not reliable	Digital Rights Mgmt Platform	
19	Original media is frequently edited for content generation	Digital Rights Mgmt Platform	
6	Fake news, privacy, copyright violation, media forensics, and security are key challenges in digital media.	Direct Distribution Model by Artist	
8	Record labels claim the largest piece of the revenue share. This is despite the reduced value to the supply chain	Digital Content Aggregation Platform	Business Rules
7	Multimedia distribution currently does not preserve self accesible information of transaction data	Digital Content Aggregation Platform	
10	Payments by consumers of very small sums of money to read individual articles or even portions of article	Digital Rights Mgmt Platform	
11	Originators rarely receive compensation and don't frequently get attribution	Digital Rights Mgmt Platform	
12	Large pools of royalty revenue do not reach the artist	Direct Distribution Model by Artist	
13	Under the evolving Media Supply chain models the creation of high quality content is a very challenging process.	Direct Distribution Model by Artist	
14	One challenge the Internet is the hidden 'artist penalty'. The actual artist or the one who has created the content is not identified due to the basic nature of the internet, fair compensation to them for their work becomes a challenge.	Direct Distribution Model by Artist	
15	Volume of data generated due to the increase of IoT is growing significantly	Digital Content Aggregation Platform	Transaction Volumes

16	Costs associated with storing and securing data remain high	Direct Distribution Model by Artist	
17	Information varies across one database and another. There is no central authority to resolve conflicts	Digital Content Aggregation Platform	
18	For recorded music there is a lack of transparency in the value chain	Digital Rights Mgmt Platform	Decentralization
20	Complicates data acquisition and cleansing	Digital Content Aggregation Platform	
21	Problem in the industry currently is that there is no certified registry of music creatives	Digital Content Aggregation Platform	
22	The key issues as Multiplicity of Music Metadata	Digital Rights Mgmt Platform	
23	There does not exist a verifiable source (deemed as a “single source of truth”) for validation of Copyright information with the underlying composition	Direct Distribution Model by Artist	
24	Data is rarely standardized	Digital Rights Mgmt Platform	
25	Due to geographical variations of language etc, Artists release the same album with multiple labels	Direct Distribution Model by Artist	Interoperability
26	Copyright protection needs to be secured	Direct Distribution Model by Artist	
27	There is no way for content creators to verify their copyright protection rights	Digital Rights Mgmt Platform	IP Protection
28	Two big issues that trouble the music industry are piracy and inaccurate ownership information	Digital Content Aggregation Platform	
29	Improvements in authorship and attribution will enhance Provenance Tracking	Digital Content Aggregation Platform	
30	The Recording Industry Association of America (RIAA) has attempted educational campaigns, litigation, and technology processes to reduce file sharing.	Digital Rights Mgmt Platform	
31	85% of images are actually ‘stolen’ without Copyright protection	Digital Rights Mgmt Platform	
32	Contract management needs to be instituted	Direct Distribution Model by Artist	Ownership
33	Need for UGC applications targetted by Older Users	Direct Distribution Model by Artist	Technology Use

34	Non Professional Users become Content Creators	Digital Content Aggregation Platform	

5.3.8.4 Blockchain

Table 15: Revised Conceptual Lens: Blockchain

Variable	Classification	Theme
Fine grained Access Control Policies		
Accelerating and Improving research for healthcare by making available to researchers databases that carry standardized healthcare information anonymizing the patient information as symptomns, gender, age.		Access Control
The transparency and irreversibility of blockchains make them not usable for personal data.	Challenge	
blockchain is suitable where independently managed stakeholders plan to collaborate with each another without giving control to a central management intermediary		
instant verification of the authenticity of these documents		
Blockchain is a tamper-proof, auditable, trust-free and auto regulating system, which requires minimal human intervention required to execute computation		
Users ability to directly verify of health information with the database		
Ensures that there is data redundancy due to multiple nodes replicating the same information		
The low transaction effort of cryptocurrencies, which have a large variety of denomination, typically to multiple decimal places, helps to enable micropayments		
creating an integrated governance framework		
Initiated by the University of Nicosia - Educational certificates in the blockchain is planned to also overcome fraud in payments from international students	Oppurtunity	Business Rules
significantly reduce educational organisations' data management costs		
exposure to liability resulting from data management issue	Oppurtunity	Cost
limited on-chain data storage is supported by blockchain architecture		
There is high cost of data charing due to Blockchain's hashed and decentralized architecture		
blockchain management, data access, and operations can also be expensive if the data volume is bigger.		
Blockchain is not ideal to store huge Volumes of data		
Due to data redundancy requirements (each node has a copy of the Blockchain)increasing storage capacity could also be an issue of blockchain usage.	Challenge	Transaction Volumes

Since the transaction can take too long Latency is another known limitation of blockchain,	Oppurtunity	
key benefit of blockchain is decentralized management.	Oppurtunity	Decentralization
capability to integrate data from disparate data sources.		
eliminate the constraints associated with Author's Rights and Related Rights		
control over their own data		
Any user linked with that particular local data can access the data without the consensus from other nodes is a serious disadvantage of Off-chain blockchain data	Challenge	Framework
Who is the primary owner of the off-chain stored data?		
Is encrypt the off-chain data possible		
Is data access manageable or not by processes and technology? What happens in the scenario when off-chain data is copied illegally?		
each transaction is permanent recorded and immutable	Oppurtunity	Immutability
suitable as an unchangeable ledger		
Data stored by blockchain technology are immutable		
tamper-proof technology		
decentralized way of informations storage can reduced data manipulation		
Guaranteed tamper proofing of transaction data which is verifiable and can be backtracked		
interoperability is arguably the biggest challenge for medtech	Challenge	Interoperability
Current Blockchain Platforms have Interoperability limitations and work in siloes		
to have blockchains from different services and providers seamlessly talk to each other as required	Oppurtunity	
Compliant to data exchange protocols and standards both at national and international level		
allows them to program in their chosen language	Challenge	Technology Usage

5.3.9 Revised Interview Protocol – Based on Familiarization Stage 1

5.3.9.1 Education Sector

Table 16: Revised Interview Protocol: Education

Information Categories

What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
How is different set of data is maintained in your University?
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. Trusted Parties
What is process for data update when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?

How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection
Education Specific Queries
What are the challenges faced at the time of admission for verification of the information like certificates, rank and merit of students?
How is the verification process done for students that are coming in for different university / colleges? Any problem faced during the same
How are the other Universities are doing the same process and if they are using any digital verification process to verify
Is the University / Govt open to sharing data with other University at National level or Globally?
What are the restrictions that University is facing in sharing data nationwide or Globally? Example any govt policy that does not allow to do the same, legal framework that does not allow to share
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain
Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.3.9.2 Health Care Sector

Table 17: Revised Interview Protocol: Health Care

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing

Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
How is different set of data is maintained in your University?
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing

Business Rules /Interoperability/IP Protection
Health Care Specific Queries
Does the patient have to repeat the examination when he moves from one hospital to the other
Is there sufficient transparency in Health Care Information available across Organizations
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain
Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.3.9.3 Media Sector

Table 18: Revised Interview Protocol: Media

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
How is different set of data is maintained in your University?

Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection
Media Specific Queries
Are there any preferred channels for information sharing
What is the revenue share arrangement for information sharing across various providers
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?

Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Will Blockchain based information sharing enhance Stakeholder Satisfaction?
Is the system data required to be stored On Chain or Off Chain
Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.3.9.4 Blockchain:

Table 19: Revised Interview Protocol: Blockchain

Decentralization
What is the current status of Decentralization in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Decentralization ?
What is the growth trends in Decentralization in Blockchain ?
Interoperability
What is the current maturity index of InterOperability in Blockchain ?
Across the Four Blockchain categories which of them provides optimized Maximum and Minimum Interoperability ?
What is the growth trends in InterOperability in Blockchain ?
Access Control
What is the current status of Access Control in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Access Control ?
What is the growth trends in Access Control in Blockchain ?
Transaction Volumes
What is the current status of Transaction Volumes in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Transaction Volumes ?
What is the growth trends in Transaction Volumes in Blockchain ?
Data Storage
What is the present status of Data Storage requirements in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Data Storage ?
What is the growth trends in Data Storage in Blockchain ?
Operational Ease
What is the current status of Operational Ease in Blockchain ?

Across the Four Blockchain Types which provides Maximum and Minimum Operational Ease ?
What is the growth trends in Operational Ease in Blockchain ?
Business Rules
What is the current status of Business Rules in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Business Rules ?
What is the growth trends in Business Rules in Blockchain ?
Generic
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
Is the system data required to be stored On Chain or Off Chain

5.4 Stage 2 – Familiarization - Use Case Based Literature review

5.4.1 Education Sector

Insights on Types of Blockchains for the Education Sector

As mentioned by Garcia in [36] and E.Garc et. al [35] to overcome the lack of Trust in intermediary barrier of Federated Identity Blockchain is very important for Education sector. The key relevance of Blockchain for the Education Sector is:

- **Decentralization:** There data has global read and write view on the blockchain, as the ownership is not at any single point. This makes sure that there is no centralized control on access and information. Through Decentralized Access management both the students and the instutions are enabled to manage their information.
- **Transparency & Immutability:** Traceability of changes to information, Off Chain or On Chain, and visible to all participants ensure immutability. Through this Blockchain ensures that across Organizations the shared data or information is transparently visible to all.

Based on an industry key use case analysis identified in the Industry are as explained by Tapscott and Kaplan (2019)

Empowering the learners (self-sovereignty)

Blockchain shifts the ownership of the data (*e.g.*, credentials, skills learned, etc.) associated with students' identity to the student. With blockchain the data is not owed by a central administrator such as a university anymore. Students would be able to store their complete learning data (the University, college, classroom data and credentials gained from outside) on the Blockchain, they will fully own and control it, and decide who has access to it (*e.g.*, employers or prospective employers). The student gets both the ability to prove the accuracy & authenticity of the

credentials in the resumes and the ability to control what can be accessed by their employers or by the others where they may need toi provide such data.

Enhanced Security and efficiency for learners,educational institutions and businesses.

While students look for security, convenience and control in being able to have their data in one place in a secure and trusted manner, the education institutions and busineses look for the ease of receiving, authenticed information which they can also manage in a secure manner. Blockchain offers the capability to ensure this for the identity & credentials data of students providing layers of privacy, and security on top. As highlighted earlier in this paper, blockchain manages security and validity, this is domne through the capability to ensure immutability through the hash chain. As an example students cannot alter any of their credentials stored on the blockchain, on paper records such protection is not available. As block chain stores the hash of the data & not the data itself, additionally privacy is ensured. Optionally, it is also possible to encrypt the data before storing it on the blockchain.

Integration of trust and transparency

Data on the Blockchain cannot be altered, students will not be able to alter their credentials be it the grades, degrees or any certification. This offers to the employers a guarantee the job applicants is presenting authentic credentials. This makes blockchain a "trust anchor of one truth for credentials" (Tapscott and Kaplan, 2019).

Existing Blockchain applications for key Use Cases in the Education Sector are analyzed below. Literature survey was done to create a Concepotual Lens which led to the identification of these cases:

Record Keeping

Blockcerts

Blockcert is working to create an open standard for Digital Certificates. A digital JSON file forms the Blockcert. It is readable by humans and machines. Any student record for e.g. transcript, academic record or diploma can be denoted through the JSON file.

These can also be enriched with metadata to bring in greater clarity. For Blockcerts the blockchain becomes a global notary to verify the authenticity of a record, and also to verify that it has not been changed from what was issued originally. The Blockcerts can be instantly verified by a decentralized without the need for any intermediaries. A record on Blockcert can be verified by an third party using a decentralized global connection. Bitcoin, Ethereum, Hyperledger, and other decentralized networks can verify Blockcerts. Blockcerts complies to Open Badges based on Linked Data. Connected Data publishes data which is understandable in many contexts.

- The Massachusetts Institute of Technology uses Blockcerts to issue digital certificates for all of their graduates

OpenCerts

As explained by Asiri in [9] Government Technology Agency, Ngee Ann Polytechnic and Skills Future Singapore Ministry of Education, came together to setup the OpenCerts platfrom based on the Etherium Blockchain. From 2019, OpenCerts has started to issue academic records for students' from seventeen universities in Singapore. Their project in the Blockchain relies on signing unique document hashes. Personal information from the students is not required. On creation of a unique OpenCerts certificate, automatically a unique Digital tag gets associated with it. The Blockcahin securely stores, the unique digital code with the automated hashed information from the certificate. On opening the .opencert file, automatically its contents get compared to the original hash value which is stored on the Blockchain, thus verifying the contents.

Sony Fujitsu

As explained by Sun et. al in [99] in collaboration with Hyperledger, Sony Fujitsu is creating a Blockchain enabled Platform to enable the following:

- Easy contribution of data to the Blockchain by education and training institutes
- Collation & storage of individual data in verifiable formats
- To control access and verification of the data for training and other requirements it provides permissions to authorized organizations.

Don Tapascott et al explain in [101] that Sony Global Education become the first consumer of this technology by permitting sharing of official academic records safely with each other. Global Education plans to verify the platform by storing transactional data generated by 250,000 participants of Global Math Barrier, Sony Global Education's world-wide maths competition.

Binded: Managing Intellectual Property

As explained by Grech in [41] Binded (started as BlockAI) is a service for registering digitial copyrights. The service is being offered for storing digital images on the blockchain. The uploaded images are stored with their hash, timestamp and the author identity, ensuring a proof of publication that is immutable and utilizable for enforcing copyright claims.

Identity Management - Sovrn

A decentralized identifier (DID) it the concept on an online identity created, controlled and owned by the owner. The absence of a decentralized entity results in Red tape bureaucratic processes which cost C$ Ten Billion each year to British Columbia based companies in Canadian [47]. Hyperledger Indy based solution supports SSI controlled identity owner and Sovrn uses this approach to provide an optimal solution to the decentralized identity problem. Identity details are housed in a wallet, this data is stored in Postgres SQL. Use of Postgress allows support for up to 2600 verifications per minute, with a permissioned blockchain deployment, with secure propagation of trust information amongst participating entities. In their White Paper [98] Sovrn promoters state – the "Internet of Identify" deployment which is built on Hyperledger Indy creates a separate DID for every relation ship, this is achieved by implementing a pairwise-pseudonymous identifiers. This ensures identity information has complete privacy.

Table 20: Application and Barriers of Industry Blockchain Types

Blockchain Type	Blockchain Provider	Use Case	Applications	Access Control	Volumetric	Barriers
	OpenCerts on Ethereum	Issue and validation of academic certificates which are tamper-proof and permanent	Substantial reduction in time spent by Educational institutions on re-issue and validation of certificates	Permissioned Reads	Stores records of 18+ Universities in SG	Degree mills could also [92] make use of OpenCerts to publish certifications onto the public blockchain Interoperability
Public Permissioned	BlockCerts on a wide variety of blockchains including Bitcoin, Ethereum, and Hyperledger	Working as a Global Notary. Verify that a record is unaltered since original generation / issue and also to authenticate the record.	Implementing recipient controlled, user claims utilizing tools that offer ease of use e.g. certificate wallets as mobile apps	Permissioned Read	Depends on underlying Platform	Enhanced integration with Decentralized Identifiers
	Sovrin on Hyperledger Indy	Internet for Identity – A decentralized repository for storing student profiles and educational credentials	ZKP	Permissioned Read	High due to separate Validator and Observer Nodes	Interoperable in Permissioned Group
Private	Sony Fujitsu on Hyperledger Fabric	Digital Record Keeping	Higer flexibility in data modelling and business logic in comparison	Permissioned Read & Write	250,000 Student Data is stored	Interoperability with other Blockchains

			to other blockchain solutions				
Public	Binded on Bitcoin	Copyright platform" for blockchain, creating "a unique Immutable fingerprint (cryptographic hash) for each copyright record"	Democratize Copyright due to a Truly decentralized Platform	Public Access	Imposed by Bitcoin	Initial authentication in the uploads. That is, how to prove ownership when a user uploads an image?	

Based on the analysis above a summary by Blockchain Type of the attributes of the key themes based on Literature Survey is presented below:

Table 21: Attribute Analysis: Key Themes per Blockchain Type

Blockchain Framework	**Decentralization**	**Immutability**	**Business Rules**	**Permissioned Write/Read**	**Interoperability**	**Technology Barriers/Data Entry**
Public	High	High	Medium	All	High	Low
Private	Low	Medium	High	User Roles based control on Write Access	Low	High
Public Permissioned	Medium	Medium	High	User Roles based Control on Write Access	Medium	Medium

Summary of Conceptual Lens Based on Literature Review

In this research Analysis of a total of 90 Key Node Items has been done. Based on the analysis, from the the 90 nodes, six key themes have been aggregated for the three Use Cases. Further research is based on these six themes:

Table 22: Matrix Coding for Conceptual Lens - Axial Code Generation

Theme	Intellectual Property Management	Record Keeping	Identity Management
Access Control	6	8	8
Business Rules	6	2	4
Decentralization	5	2	2
Immutability	9	9	7
Interoperability	2	3	2
Technology Use Barrier	5	5	5

5.4.2 Online Media Sector

Lets look at how the management of Metadata work in the Online Media Sector and what challenges exist. Provided in the Metadata is the data context, such as genre, lyrics, date. This can be extended for providing additional information such as the production equipment used, the recording location, the inspiration and more. Dair et al. in [27] have explained for any content the embedded Metadata can also have the terms of use of the content and details of the holders of copyrights relayed to the content such as the contact detaiisl, thus making it easy to locate and contact content owners and to license its use.
A key challenge is that there is no reliable Global source for Content Meta Data. To further complicate the problems, WAV and MP3 the commonly used file extensions are very easy to edit. There are Metadata repositories managed by Public Societies such as ASACP and BMI but they suffer from inconsistencies amongst themselves. Cares et.al point out in [20] that when Spotify was sued for unpaid royalties worth $200 Million they responded by stating that the information about the rightful recipient to whom they should make payment was not available to them due to missing Meta Data.

Challenges for Metadata in existing Digital Content Distribution
Hidden ‘artist penalty’[71] has been a persistent problem on the internet. Fair recognition of for the creators of digital content and the correct compensation for their work becomes difficult on the internet. Mc Conaghy et al. in [71] has pointed out the problem of online attribution ows its origin to the unidirectional links in the 1989 design of the World Wide Web. This results in no built-in attribution or ownership. Digital piracy as mentioned in [110] is identified by Sony, one of the big three in music labels, as a cause for profit erosion in its music business. Sony reported an approximate loss of $160 million in the quarter ending in June 30, 2002

Content Distribution platforms have evolved through three generations as explained by Rinaldi [89]. These are on Centralization, Reliability, Scalability and Content Structure. All three generation have face the below mentioned challenges:

Multiplicity of Music Metadata

Two copyrights exist for every track of music which is recorded for distribution:

Copyright Category	Description	Meta Data Quality
Musical Composition	Includes the music and lyrics created by Songwriters	Was historically a B2B business, most settlements were based on Sampling or Blanket licensing hence not very detailed information is available
Recording Composition	Created by the recording artists and owned by the labels	Well documented since owned by recording Labels and required for Revenue Settlements

Figure 15: Multiplicity of Music Meta Data

Owners copyright information gets scattered avross the various databases of the record companies, the aggregator societies, and the publishers. These entities do not have any incentives to share or consolidate the copyright information as described by Savelyev et al. in [95]. The fact that artists end up releasing their albums with multiple labels across different countries proliferates the problem. The complexity of Metadata tracking is highlighted as per a 2017 study from Music Reports based on ASCAP as explained by N. Baym, L. Swartz, A. Alarcon, in Convening technologies: Blockchain and the music industry [12] below. It shows that for each song, the numbers of Song Writers and Publishers has been continuously increasing over the last few decades:

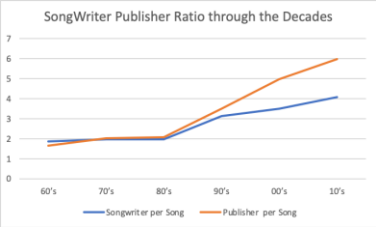


Figure 16: Ratio per Song of Publishers and Song Writer through the decades

Lack of Standardization for Metadata

Based on Copyright Category, following is the status of standardization:

Copyright Category	Standards	Utilization
Musical Composition	ISWCs - International Standard (Musical) Work Codes	Not so widely used since historically involved B2B settlements which were done in Wholesale and not based on Itemized Transaction Tracking
Recording Composition	ISRC - International Standard Recording Code	Widely Used since this is important for Revenue Settlements

Figure 17: Music Standardization

No single source of truth exists, which can be used to correlate Copyright information of the Recordings with the underlying Composition. Some proprietary databases exist, for example the HFA and MRI, but these are neither standardized nor are they very comprehensive as explained by N. Baym, L. Swartz, A. Alarcon, in Convening technologies: Blockchain and the music industry [12]. These databases have used different Label Fields for the Metadata attributes. As an example, say the label for identifying the Engineering team is “ProTools Engineers” but when defining the Label Metadata a sapcing is introduced between Pro and Tools ane the lable becomes “Pro Tools Engineers” the credits will end up getting lost.

Tampering of Metsdata

Almost All commercial-based digital content have DRM and CAS applied have for protection. These Content Super Distribution systems [54] as explained by J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu in The Blockchain-Based Digital Content Distribution. are constantly targeted by pirates. They pirates hack them with the intent to steal the content or alter the Metadata without the due legal procedure.

CSS (Content Scramble System) which along with regional coding is still used to protect DVDs was hacked by a teenager in 1999. Lee [63] has explained the critical problem that the DRM systems in vogue today only focus on the Media Distributor and Consumer relationship. The complex chain of actors involved in creation of content and its processing gets completely ignored.

As explained by Bhowmik et. al in [14] MPEG formats were developed as a result of significant effort directed toward creating an efficient multimedia distribution systems. This end result is that the networking for Multimedia Delivery has become very content centric. However, the indexes can be easily removed [80] due to which content integrity and security can still be compromised as explained by T. Höppner, P. Westerhoff, J. Weber in Taking a Bite at the Apple: Ensuring a Level-Playing-Field for Competition on App Stores[46].

Human Error

Normally when a song is completed, the composer, artist or producer compiles the Metadata and publishes to the Distributors, Labels, and Digital Streaming Providers [116]. The Metadata entry is complex. Mostly initial submission are rushed and this leads to incorrect or missing entries. These lead to human error in submissions.

International Regulations

Music is heard in all countries and languages. Music distribution has multiple challenges including different copyright laws per country, multiple languages and an overall hesitation to share Information. This results in siloed Meta Data which is fragemented for the same piece of Music Content [4]. The US mandates that Creative Work is copyrighted as soon as it is created. In addition there is also a mandate in case of lawsuites to be registered with the UC Copyrights office. This is not sufficient to prevent piracy.

Transparency in Revenue Settlement

A primary trait and the key advantage of online channels being utilized for Digital Media Distribution is the direct nature of the medium. Critical for successful marketing and Revenue distribution [12] is the transparency, correctness and validity of Content Meta Data. This includes the identity of the artists, the content aggregator and the composer. This transparency with the Content owners is completely compromised due to the siloed pipelines which results in fragementation of Metadata.

5.4.3 Health Care Sector

The Health Information National Trends Survey data highlights a tectonic shift in the trends for how patients are consumeing their health and medical information. More and more patients are now looking for information online before they talk to their physicians as reported by Hesse et al in [44]. Blockchain Research gaining momentum as evidenced by approximately 40 papers in PubMed Journals focussed on Blockchain. These papers have focused on the introduction of Trust and Decentralization of Information Sharing in the Health Care sector as per research by Kovacs [51]

The optimized balance of Care, health and Cost[13] was aptly coined as the Triple Aim of successful healthcare by Donald M. Berwick[13] et. Al. A combination of 5G, IoT, Blockchain and AI will be required to achieve this. Deloitte in their report [103] highlight that IoMT "Health Care Monitoring and Diagnosis via IoT Devices" is expected to grow more than three times in five years (to $52.2 billion by 2022 from $14.9 billion in 2017). Connected Devices will be critical components for helping to improve care quality and efficiency, optimize costs and enable the transition to value-based care (VBC). Growth of Analytics in healthcare industry is will be another significant contributor, as per Onik et. Analytics is growing at an exponential rate of 27.3% annually and is projected to reach 29.84 Billion USD by 2022 [85].

Aggregated Clinical/administrative data Availability for Research: While there is progress in digitization of paper records, enablement of the sharing of patient data across providers has still not happened. Patients medical records get created with multiple healthcare providers as patients visit different specialists, change healthcare plans or move to a new city [85]. The records typically reside in separate discrete data silos, which have their own storage structures, security mechanisms and descriptive semantics. This complicates secure data sharing between patients, providers and the payers.

A key factor for electronic medical record (EMR) global adoption is by ensuring interoperability in medical standards[17].

Interoperability in standards is a primary prerequistite for ensuring that EMR gives us the requisite economic, social and trust benefits. EMR adoption will further augment the challenges in information that are wide spread in the current manual based medical files as explained by [53] if we do not cross the barriers of interoperability. This will increase the control of patient information by some limited institutes and lack of global data availability. As explained by Tanesh (2019), The primary challenge is modification in current electronic healthrecords (EHR/EMR) is the maintainence of interoperability among various stakeholders who are involved in patient healthcare.

More than 500,000 different types of medical devices, including wearables, implanted and stationary medical devices are manufactured by Medical technology (Medtech) companies [105]. Big Data Analytics in Healthcare can take advantage of connected devices only with the

improved availability of data structure standardization, access security, as well as storage and exchange as explained by [57] et. al.

With a 48% rate of annual increase as explained by Mehndi Hassan (2019), Halthcare data is expected to enter the yottabyte (one yottabyte ¼ 10008 bytes) range by 2020. Healthcare analytics industries are growing exponentially with a compounded annual growth rate (CAGR) of 27.3%. By 2022, this is anticipated to reach 29.84 Billion USD from 8.92 Billion USD in 2017.

Patient Data Security: HIPPA, Health Insurance Portability, and Accountability Act regul;ates and governs the privacy of a patient's data [51]. A key requirement of HIPPA is that PHI (Patient health information) has to be secure from breaches and modification. At the same time patient data cannot be restricted and the security regulations need to be manged to allow this. Healthcare is a complex system involving multiple entities and there is a requirement for patients to share their medical records and data across the ecosystem.

Malware attacks on Health Care records are quite common, as explained by [86] in May 2017 the treatement to thousands of British patients was delayed as GPs and other vital services across NHS were iimpacted by malicious software. US cyber-warfare agents had manually created a virus for hacking of data which caused this effect. Across the UK approximately 30 health service organizations had malware attacks, many more had to be temporarily shut down as a precautionary measure.

The data leakage and potential shortcoming in security mechanism has made the patients hesitant to share and store their personal medical information as mentioned by Tanesh Kumar (2018) [51].

The is also a trade-off between the availability of computing capabilities versus the quantum of medical transactions and this can potentially limit the scalability of healthcare systems.

The growth of data and Connected Devices is creating more difficulties in securing patient information at the hospitals and clinics. The factors critical for success will be:

- An interoperable network for validating Health Care Information Access Control [31]
- Automated Business processes that enables micro-payments for Revenue sharing and enables the access to Healthcare Literature, as explained by Bram et. al in [18]

Thhe data accuracy needs are different for regulated and non-regulated health data as mentioned by [37]. Unlike Marketeers, Health care providers require very accurate patient data. Hence Security and Provenance related requirements vary across Business Needs.

PayForPerformance: As explained by Roxanne J. Kovacs (2020) Pay for performance (P4P) schemes have been implemented in medical centers in low cost countries such as India and Africa. Based on pre agreed KPI's the healthe care workers are given financial bonus upon achieving the agreed targets.

Studies show there is a lot of variation in the effect of P4P schemes on outcomes based on Performance Plans and Information availability. Incentive design is being adequately reported is a key observation. Many studies fail to report key design features. Mehmet [11] explains that a key enabler for P4P based models will be the availability of Digital Health Information exchanges (HIE) which are able to accurately provide information tracking points. The validity of such HIE is subject to trust of the provider and the Health Care provider can manipulate data to tamper the results [13].

Insights of Blockchain Type for Healthcare Sector

As per an IBM study, about 16% of healthcare engineers are planning execution strategies to operate blockchain based solutions in respective their fields of work. Blockchain's key characteristics for the Healthcare Sector are:

Transparency & Immutability: Blockchain Data is immutable, On Chain or Off Chain changes to information are traceable and will be visible to all. TRhis will ensure transparency and visibility of Information shared across Organizations as researched by Liang [66].

Decentralization: Yang et. al analyze that [113] Decentralized Access Control provides the meand to ensures that Health Care information is not controlled by any Central Authority. Informationa becomes Globally accessible as there will not be any single owner or administrator of the Blockchain.

Scalability: Kumar establishes that [58] Scalability is a potential challenges for blockchain adoption in healthcare. The balance between quantum of medical records to be managed and the available computing capabilities could possibly limit the potential of Blockchain for Healthcare[61].

Interoperability: The siloed operationa approach of Current Blockchain Platforms has limitations of interoperability as verified by Siyal et. al [97].

Table 23: Application and Barriers of Industry Blockchain Types

Blockchain Type	Blockchain Provider	Use Case	Applications	Access Control	Volumetric	Barriers
Public Permissioned	MediLedger		ZK Proofs used for drug ownership validation	Permissioned Reads	Stores records of Patients	Interoperability with other Blockchains

Private	Guard Time	Issuing and validating health certificates that are tamper-resistant and permanent	It allows for more flexible API Based integration compare to other blockchain solutions	Permissioned Read & Write	KSI ensures volume limitations are removed	Source Data Verification
Public	MedRec	Patient Health Care information with Access Control	Democratize Copyright due to a Truly decentralized Platform	Public Access	Imposed by Ethereum	Transaction Volume supported by system

5.4.4 Cost Challenges of Information Sharing

Based on a study by Ernst & Young below are the key factors that influence the cost of implementing a Blockchain are:

Table 24: Cost Influencers for Blockchain

Attribute	Description
Number of Users	Someone who signs up on behalf of a member is a user. In a college, an Admin resource who logs into the system to make Student entries would be a User
Number of Members	A participant organization in a project is referred to as a member. First an organization creates a project and then it may invite other organizations to participate. For example, a consortium of 5 Colleges coming together for a specific collabarative project
Project Type	Can be both Private or Public
Transaction Size	The storage required for one discrete unit of value which is transacted on the network.
Transaction volume	A measure of the speed of a database system is its transaction "throughput," referring to the transaction volume per second supported by the database.

The below diagram shows the sensitivity matrix at which point the Cost of Ownership of a Zero Knowledge Proof Public Network becomes more expensive than a Private Blockchain. However,

it is important to note that Blockchain being almost in its infancy stage, it is not possible to conclusively calculate the Governance Cost of Blockchain Frameworks.

Transactions per day	25	160	1,000	**1,912**	10,000	300,000
Transactions per year	9,125	58,400	365,000	**697,880**	3,650,000	109,500,000
Private blockchains	$34.296	$5.359	$0.858	**$0.449**	$0.086	$0.003
ZKP – future state	$2.856	$0.798	$0.478	**$0.449**	$0.423	$0.417

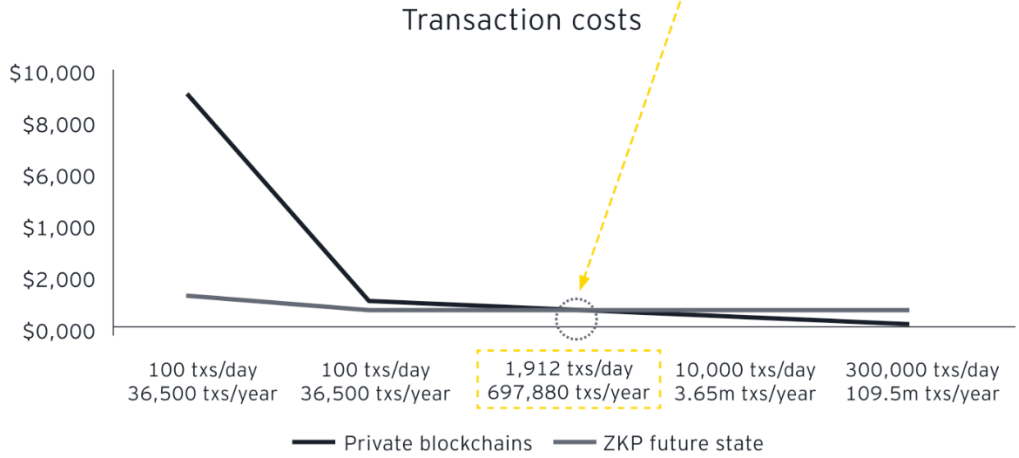


Figure 18: EY (2019) Total Cost of Ownership of Blockchains

5.4.5 Blockchain

Blockchain as a Data Store

The Blockchain immutably store transaction records. It is a Distributed Ledger with public or private access. The below table compares characteristics of a Blockchain with a standard RDBMS:

Table 25: Blockchain Attributes

Attribute	Traditional Database	Blockchain
Concurrency Control	Two-phase commit is typically implemented in order to avoid concurrency control	The Blockchain is built to handle Byzantine attacks in hostile environment. .Blockchain implements various protocals, like Proof of Activity Proof Of Work,or Proof of Stake and Proof of Burn. The protocols implemented on Blockchain have higher computational overheads in comparison to two-phase commits and this results in **lower TPS**

Event Chaining Structure	Transaction's in a regular database, organically, are not connected by the database by default. Developer by using Foreign Keys are able to create Chains across entities.	Merkle Tree or Hash Chain mechanisms are available on the Blockchain as mechanisms to emnsure that Transactions in a given time frame are chained.
Immutable Data Stores	Immutability is not a feature of Traditional Databases. The admin revokes, update or delete privilege's User groups, however this is not tamper proof and is under Centralized Control. Changes happen due to Fraud or due to Use Case requirement	The Blockchain is an immutable data store. Event Chaining combibes with Consensus Algorithms to provide this capability. Since blockchain implements event chains it is not possible to update one event in the chain without impacting all upward chains. The Consensus mechanism ensures that the Majority of the Users receive the transmission of Chaining information and approve it.

Blockchain Framework Based on Ownership:

Driven from the analysis above matrix below captures a framework to highlight the Blockchain characteristics based on the Application or the Business requirements:

Table 26: Blockchain Framework Characteristics

Blockchain Framework	Owner	Transaction Volumes	Access Control for Consensus	Participants have existing Relationship	Shared Write Access	Anonymity Requirement	Business Rule Complexity	Security	Time for Contract Closure
Permissionless Public	No Single Owner	Low	All	Not Required	All	Visible to All	Low	Very High	High
Permissionless Private	Consortium	Low to Medium	All	Good to Have	Can Control Write Access based on User Roles	Permissioned Access to Read Data	Medium	Depends on the Validating Entities	Low to Medium

Permissioned Private	Consortium	Medium to High	Restricted	Required	Can Control Write Access based on User Roles	Permissioned Access to Read Data	High	Depends on the Validating Entities	Low
Permissioned Public	Consortium	Low to Medium	Restricted	required	Can Control Write Access based on User Roles	Visible to All	Medium	Very High	Medium

5.4.6 Data Analysis 2 – Based on Use Case Review of Existing Literature

5.4.6.1 Education

- Permissioned Public Blockchain for verified for Education Use Cases. Most of the scenarios need either true Global access or Consortium Based access. Hence the pattern does not seem relevant
- Based on Literature survey it is established that Security systems in current Paper based certificates hence those variable have been reduced
- Interoperability of Data & Access Control is observed as a significant challenge in all studies and since this is an area which the nature of the application can control focus on this area will continue

Summary: Reduced from 37 to 28 Variables

5.4.6.2 Health Care

1. The information available in Health care for EHR can be digitized easily. For manual inputs going in, Iot will be a major influencer. Given the nature of Blockchain as an

application, there will be no significant improvement in Data Input based on Manual User inputs. The significant improvement will come from IoT based automated inputs. Hence going ahead Counterfeit Drugs as Use Case will not be purused by the researcher
2. All the use cases observe that different formats are used across the Health Industry. Interoperability of Data is observed as a significant challenge in all studies and since this is an area which the nature of the application can control focus on this area will continue
3. Volume of EHR record is very significant. Data Storage limitaions across various Blockchain Types has a significant impact on the Blockchain Framework selection based on the nature of Use Case. Hence going ahead the researcher will focus more on this area
4. Since Blockchain is decentralized and has multiple copies, it is Virus Proof, hence the variable is removed

Summary: 34 Variables reduced to 26 Variables

5.4.6.3 Media

1. Media industry is primarily focused on Public Blockchain since there will also be new particpants joining the group
2. Ownership and IP Protection are achieved by Access Control. Hence they have been merged into single theme
3. Because of the nature of Meta Data interoperability is a serious challenge. Interoperability of Data is observed as a significant challenge in all studies and since this is an area which the nature of the application can control focus on this area will continue
4. Volume of Meta Data stored is not huge compared to actual content. Data Storage limitaions across various Blockchain Types has a significant impact on the Blockchain Framework selection based on the nature of Use Case. Hence going ahead the researcher will focus more on this area

Summary: 32 Variables reduced to 23 Variables

5.4.6.4 Blockchain

There is a correlation between Transaction Volumes and Data Storage. Hence the themese have been merged into a single theme.

5.4.7 Conceptual Lens 3

5.4.7.1 Revised Conceptual Lens – Education

Table 27: Revised Conceptual Lens: Education

S.No	Variable	Use Casse	Themes (Trust Requirements)
3	Lack of Permissioned Access Control for university data.	Intellectual Property	Access Control
4	The online platform brings limited Data Security		
7	Current security features on the certificates were not sufficient	Record Keeping	
9	Provides users learning incentives by using Gamified interactive education platform such as scholarships & exchange programs	Intellectual Property	Business Rules
10	In majority of cases the presenter or lecturers is responsible for any third party content		
11	Practice of using partially-automated lecture recording systems in institutes		
14	Third-party permissioned access tto student data to verify the authenticity	Identity Mgmt	
16	Paper certificates and diplomas need to be manually issued and verified	Record Keeping	
17	Selling fake certificates and diplomas		
18	The internet has reversed the trend of geographical limitation of degree mills		
21	How do institutions bring all of their legacy data onto newer systems	Intellectual Property	Transaction Volmes
22	Academic records of a person, such as diplomas,, degrees and mark sheets are identity driven belonging to the country or institure	Identity Mgmt	
24	Students or graduates do not have direct access to their own records from this aggregated database	Identity Mgmt	Decentralizatio n
25	Physically localized and not connected to each other	Intellectual Property	
26	No mature cross-platform course sharing mechanism		
27	P2P distributed architecture over a centralized one		
28	disconnection among institutes	Record Keeping	

29	Universities and governments could be collective caretakers		
30	Elimination of scenarios where some entities control the information of a large number of people;		
31	Education companies and universities must transfer ownership of individual data into the hands of students	Identity Mgmt	
32	Current process does not regulate the copyright relations between lecturer and the university in educational process.	Record Keeping	Immutability
33	Limit the tamperability of data		
34	Students cannot alter their grades, degrees, and certification		
35	Information can remain immutable unchanged, and decentralized over time	Intellectual Property	
36	Education Industry taxonomy, and metadata	Record Keeping	Interoperability
37	Variation of , barriers of language, protocols and different terminologies.	Intellectual Property	
38	Process challenges including creating a decentralized governance framework		
39	Data is stored in diverse incompatible formats		
43	Attitudes towards Technology	Intellectual Property	Technology Usage
44	Acceptance and actual use of computers		
45	Reluctant towards adopting new technologies.due to the lack of necessary knowledge	Record Keeping	
46	Lack of training on using a new skill		

5.4.7.2 Revised Conceptual Lens – Media

S. No	Context	Use Case	Themes (Trust Requirements)
2	Sony has seend serious decline to its profits and the key reason for the same is digital piracy	Digital Content Aggregation Platform	
3	JPEG has verified that distributed ledger technologies (DLT) and blockchain have great potential		
28	Two big issues that trouble the music industry are piracy and inaccurate ownership information		Access Control

29	Improvements in authorship and attribution will enhance Provenance Tracking	Digital Content Aggregation Platform	
19	Original media is frequently edited for content generation	Digital Rights Mgmt Platform	
27	There is no way for content creators to verify there copyright protection rights		
31	85% of images are actually 'stolen' without Copyright protection		
8	Record labels claim the largest piece of the revenue share. This is despite the reduced value to the supply chain	Digital Content Aggregation Platform	Business Rules
7	Multimedia distribution currently does not preserve self accesible information of transaction data		
10	Payments by consumers of very small sums of money to read individual articles or even portions of article	Digital Rights Mgmt Platform	
11	Originators rarely receive compensation and don't frequently get attribution		
15	Volume of data generateddue to the increase of IoT is growing significantly	Digital Content Aggregation Platfor	Transaction Volumes
16	Costs associated with storing and securing data remain high	Direct Distribution Model by Artist	
17	Information varies across one database and another. There is no central authority to resolve conflicts	Digital Content Aggregation Platform	Decentralization
18	For recorded music there is a lack of transparency in the value chain	Digital Rights Mgmt Platform	
20	Complicates data acquisition and cleansing	Digital Content Aggregation Platform	Interoperability
21	Problem in the industry currently is that there is no certified registry of music creatives		
22	The key issues as Multiplicity of Music Metadata	Digital Rights Mgmt Platform	
23	Data is rarely standardized		
24	There does not exist a verifiable source (deemed as a "single source of truth") for validation of Copyright information with the underlying composition	Direct Distribution Model by Artist	

25	Due to geographical variations of language Artists release the same album with multiple labels		
33	Need for UGC applications targetted by Older Users	Direct Distribution Model by Artist	Technology Use
34	Non Professional Users become Content Creators	Digital Content Aggregation Platform	

5.4.7.3 Revised Conceptual Lens -Health Care

Table 28: Revised Conceptual Lens: Health Care

S. No	Variable	Use Case	Themes (Trust Requirements)
1	Data security and privacy are continuously violated in HER	Clinical Data for Research	Access Control
4	Different users of health data have different roles	Patient Data Privacy	
5	Large volumes of data is stored in public cloud resluting in increased Privacy issues		
6	Risks of data exposure for Patient Privacy increasing due online access		
9	Only the minimum health information necessary to conduct business should be used or shared		
10	Obtaining consent for access to health care data will become mandatory		
12	Design of EHR systems withprivacy preservation and user-centric access control	PayFor Performance	
13	Patients hardly have access to their health records.	Patient Data Privacy	Business Rules
18	Coordination, elimination of duplication, and outcome tracking among other things is key to tracking	PayForPerformance	
19	Relying on new payment systems for automated payouts will help imprved the Customer Experience		
20	Strong quality side incentives to be put in place for Pay for Performance Data Tracking accuracy		

21	Sharing of healthcare data is essential step to improve the quality		
24	Sharing of medical and healthcare data is a critical step to improve the quality of healthcare globally	Clinical Data for Research	
26	Volume of sensor and EMR data from wearable IoT devicesand patients is increasing	Patient Data Privacy	Transaction Volumes
27	Patients are reluctnat about storing their personal data due to the data leakage		
28	At about 50% rate of increase in health care data annually the analytics industries is growing at an exponential rate of 28% o enter the yottabyte (one yottabyte ¼ 10008 bytes) range by 2020	Clinical Data for Research	
29	The trade-off in the available computing devices versus the amount of medical records could limit the scalability of such healthcare systems.		
32	Current EHR systems use centralized architecture	Clinical Data for Research	Decentralization
33	Users have limited control over personal health data		
35	Patient is less likely to repeat diagnostic tests with decentralization	Patient Data Privacy	
38	Intra-organizational, EHR platforms are also fragmented	Clinical Data for Research	Interoperability
39	Lack of data standardization is a challenge in EHR data transfer		
42	Globalization of data is pending due to lack of interoperability		
43	Complying with various regulatory protocols and standards is critical		
45	The primary challenge is modification in current electronic health records (EHR/EMR) is maintaining the interoperability among various involved stakeholders	Patient Data Privacy	

5.4.7.4 Revised Conceptual Lens -Blockchain

Table 29: Revised Conceptual Lens: Blockchain

Variable	Classification	Themes

		(Trust Requirements)
Fine grained Access Control Policies		
Accelerating and Improving research for healthcare by making available to researchers databases that carry standardized healthcare information anonymizing the patient information as symptomns, gender, age.		Access Control
The transparency and irreversibility of blockchains make them not usable for personal data.	Challenge	
instant verification of the authenticity of these documents		
Blockchain is a tamper-proof, auditable, trust-free and auto regulating system, which requires minimal human intervention required to execute computation		
Users ability to directly verify of health information with the database		
Ensures that there is data redundancy due to multiple nodes replicating the same information		
The low transaction effort of cryptocurrencies, which have a large variety of denomination, typically to multiple decimal places, helps to enable micropayments		
blockchain is suitable where independently managed stakeholders plan to collaborate with each another without giving control to a central management intermediary		Business Rules
significantly reduce organisations' data management costs		
reduces exposure to liability resulting from data management issue	Oppurtunity	Cost
limited on-chain data storage is supported by blockchain architecture		
There is high cost of data charing due to Blockchain's hashed and decentralized architecture		
blockchain management, data access, and operations can also be expensive if the data volume is bigger.		
Due to data redundancy requirements (each node has a copy of the Blockchain)increasing storage capacity could also be an issue of blockchain usage.	Challenge	
Since the transaction can take too long Latency is another known limitation of blockchain,	Oppurtunity	Transaction Volumes
eliminate the constraints associated with Author's Rights and Related Rights		
capability to integrate data from disparate data sources.	Oppurtunity	Decentralizatio n
Any user linked with that particular local data can access the data without the consensus from other nodes is a serious disadvantage of Off-chain blockchain data		
Who is the primary owner of the off-chain stored data?	Challenge	Framework

Is encrypt the off-chain data possible		
Is data access manageable or not by processes and technology? What happens in the scenario when off-chain data is copied illegally?		
suitable as an unchangeable ledger		
Data stored by blockchain technology are immutable, each transaction is permanent recorded and immutable		
decentralized way of informations storage can reduced data manipulation		
Guaranteed tamper proofing of transaction data which is verifiable and can be backtracked	Oppurtunity	Immutability
interoperability is arguably the biggest challenge for medtech		
Current Blockchain Platforms have Interoperability limitations and work in siloes	Challenge	
to have blockchains from different services and providers seamlessly talk to each other as required		
Compliant to data exchange protocols and standards both at national and international level	Oppurtunity	Interoperability

5.4.8 Revised Interview Protocol

5.4.8.1 Education

Table 30: Revised Interview Protocol: Education

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.

Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection
Education Specific Queries
What are the challenges faced at the time of admission for verification of the information like certificates, rank and merit of students?
How is the verification process done for students that are coming in for different university / colleges? Any problem faced during the same
How are the other Universities are doing the same process and if they are using any digital verification process to verify
Is the University / Govt open to sharing data with other University at National level or Globally?
What are the restrictions that University is facing in sharing data nationwide or Globally? Example any govt policy that does not allow to do the same, legal framework that does not allow to share
Perceived Benefits of Information Sharing on Blockchain

Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
What is the volume of data that needs to be stored in the Blockchain.
Is the system data required to be stored On Chain or Off Chain
Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.4.8.2 Health Care

Table 31: Revised Interview Protocol: Health Care

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties

Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection
Health Care Specific Queries
Does the patient have to repeat the examination when he moves from one hospital to the other
Is there sufficient transparency in Health Care Information available across Organizations
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
What is the volume of data that needs to be stored in the Blockchain.
Is the system data required to be stored On Chain or Off Chain

Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.4.8.3 Media

Table 32: Revised Interview Protocol: Media

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Do you get inputs or updates if your information is modified by Third Parties
Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties
How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?
What is the impact of Interoperability & Regulatory in Data Sharing
Was there a scenario where you could not exchange information with other organization since the Data Formats did not match
Has there been a case where you could not receive information from other Organization due to regulatory challenge
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
What is the total Volume of Data shared in the Organization

In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules /Interoperability/IP Protection
Media Specific Queries
Are there any preferred channels for information sharing
What is the revenue share arrangement for information sharing across various providers
Perceived Benefits of Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
What is the volume of data that needs to be stored in the Blockchain.
Is the system data required to be stored On Chain or Off Chain
Do you need to be shared with a trusted consortium or with any untrusted party globally ?

5.4.8.4 Blockchain:

Table 33: Revised Interview Protocol: Blockchain

Decentralization
What is the current status of Decentralization in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Decentralization ?
What is the growth trends in Decentralization in Blockchain ?
Interoperability
What is the current maturity index of InterOperability in Blockchain ?

Across the Four Blockchain categories which of them provides optimized Maximum and Minimum Interoperability ?
What is the growth trends in InterOperability in Blockchain ?
Access Control
What is the current status of Access Control in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Access Control ?
What is the growth trends in Access Control in Blockchain ?
Transaction Volumes
What is the current status of Transaction Volumes & Data Storagein Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Transaction Volumes ?
What is your recommendation on data storage in On Chain as well as Off Chain Storage Mode ?
Operational Ease
What is the current status of Operational Ease in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Operational Ease ?
What is the growth trends in Operational Ease in Blockchain ?
Business Rules
What is the current status of Business Rules in Blockchain ?
Across the Four Blockchain Types which provides Maximum and Minimum Business Rules ?
What is the growth trends in Business Rules in Blockchain ?
Generic
Are Cost Savings/Optimizations achieveable with Blockchain based Information sharing?(For e.g.: Automation of Processes and significantly Reduced Paperwork & Human Effort) ?
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.) ?

5.5 Stage 3 – (Preliminary Interview)

5.5.1 Education Interview Response

The interview was *conducted* for 5 experts including University Registrar (Gujarat, India), Director Accredition (India), University Registrar (Malaysia), Cyber Security Expert (Florida) and Professor (IIT Delhi).

Table 34: Interview responses: Education

Interview Theme	Questions	Observation

INFORMATION CATEGORIES -	What are the categories of Information you share across Organizations What process do you follow for Information Sharing	Students Academic Records and Degree Certificates is the most commonly shared Information Course Material Sharing is currently not institutioanalized in the university Email and Certified Hard Copy is the most frequently use means of Information Sharing
TECHNOLOGY BARRIER: Barriers for cross Organization Information Sharing	Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ? What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High	. Verification of Records due to lack of Trust was identified as a major problem. 76% of the respondents faced this problem which they said caused Operational overheads and time delays. 48% of the respondents pointed to Cost of Digitization as a key barrier. The challenges with Digitzation come up due to issues of Availability of Resources and the lack of adequatre Infrastructure.
IMMUTABLE: Intra Orgamnisation & Inter Organisation Information Sharing in a n Immutable manner.	What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified Do you get inputs or updates if your information is modified by Third Parties Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties How is data updated done reliably when any correction is required? What	83% of the people strongly agreed with the need for data immutability. They felt that this will lead to enhancew trust in Information Sharing Organisations, unfortunately do not have any standardized process to track Information Change. For this rreason data and information pn this front is lacking

	is the average Time taken in the completion of whole process?	
INTEROPERABLE: Average Frequency of repeated Information sharing in Intra and Inter Organization scenarios	What is the impact of Interoperability & Regulatory in Data Sharing Was there a scenario where you could not exchange information with other organization since the Data Formats did not match Has there been a case where you could not receive information from other Organization due to regulatory challenge	About 60% of the respondents mentioned that they share Information betweent one to thousane times in a month 24+% above five thousand times in a month, 4+% share information up to ten thousane times in a months and for 8.33 share 10,000+ times per Month
Information Data Storage & Volumetrics	What is the Volume of Information Shared Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.	60+% of the people responded that data could be shared with trusted Organizations . The balance are not sharing date digitally with third party organisations due to Trust issues. Audit logs to the granularity of Read Access was seen as a strong need by 48% of the respondents. This is key for Role Based Access Control
ACCESS PERMISSION: How to ensure data security in education institues?	How is data reliably secured in your Organization? ? What are the challenges faced in maintaining a secure system? How many times leak of information being reported? What significant action were taken to prevent it proactively? What is the process of giving Unique Identitifiers to atomic entities in the Organization ? Do you see a significant need for Role Based Access Control in Information Sharing	66% of Organizations utilize only password protection for data exchange. Access breach is quite easy when there is single factor authentication based on password. This highlights the need for more advance data protection protocols like Firewalls and encryption.

DECENTRALIZED: Blockchain Applicability for Decentralized Information Sharing in the Education Sector	Has Blockhain for Information sharing been considered by your organisation/institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing) Do you have an identified used case which the organisation can gain benifit from? Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)	52% Respondents see a role for Block chain in cost optimization for the Organisatioon ans the students 30% people feel that operational savings are possible by using blockchain.
BUSINESS RULES: What are the Key Use Cases for application of Blockchain based technologies?	Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.) What is the volume of data that needs to be stored in the Blockchain. Is the system data required to be stored On Chain or Off Chain Do you need to be shared with a trusted consortium or with any untrusted party globally ? What are the challenges faced at the time of admission for verification of the information like certificates, rank and merit of students? How is the verification process done for students that are coming in for different university / colleges? Any problem faced during the same How are the other Universities are	**Key Business Oppurtunities Identified:** Degree Certificates Sharing (Storage of student credentials) is the most prominent Use Case . Identity verification butilizing th blockchain. Currently there isn't any identity System for the students which is single and centralized. Automated Payments for 1) Student academic records exchange and 2) Exchange of academic information course material

	doing the same process and if they are using any digital verification process to verify Is the University / Govt open to sharing data with other University at National level or Globally? What are the restrictions that University is facing in sharing data nationwide or Globally? Example any govt policy that does not allow to do the same, legal framework that does not allow to share	
COST OF INFORMATION SHARING	How many people are involved in information sharing across your department Total Average monthly salary for people involved in information sharing? What is the total Volume of Data shared in the Organization In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?	Most of the Organizations believe that there is no dedicated staff for Informatiion Sharing. The same resource does multiple activities a part of which is Information Sharing. Approximately 15% of time of employees is spend in Information Sharing

5.5.2 Health Care Interview Response

The interview was done for 6 Health Care experts from India & UK.

Interview Theme	Questions	Observation
INFORMATION CATEGORIES -	What are the categories of Information you share across Organizations What process do you follow for Information Sharing	Electronic Medical records are shared across Organizations
TECHNOLOGY BARRIER: Barriers for cross Organization Information Sharing	Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?	A major problem is Verification of Records as Digital Information is not made available by Doctors. This was faced by 67.9% of respondents. They identified this

	What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High	as a cause for Operational Overheads and time delays.
IMMUTABLE: Need for Immutable Information Share in Inter Organization and External Organization Information Sharing	What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified Do you get inputs or updates if your information is modified by Third Parties Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?	• 80% of respondents did not prefer sharing data with any external organization or any public source from where the data could be stolen. • According to the responses gathered 7.4% of respondents felt that their health information is being illegally used.
INTEROPERABLE: Average Frequency of repeated Information sharing in Intra and Inter Organization scenarios	What is the impact of Interoperability & Regulatory in Data Sharing Was there a scenario where you could not exchange information with other organization since the Data Formats did not match Has there been a case where you could not receive information from other Organization due to regulatory challenge	• 36.1% of respondents need to transfer the data from one health centre to another. • 91.3% of the 36.1% of respondents did this transfer of data in written format i.e. the written prescription • 5.8% of the 36.1% of the respondents transferred the data digitally • 46.3% of respondents had to repeat their medical examinations when they had to switch

		from one hospital to another.
Information Data Storage & Volumetrics	What is the Volume of Information Shared Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.	Medical Health Records have large volumes There is no impact based on size of Organization
ACCESS PERMISSION: How does the university secure its data?	How is data reliably secured in your Organization? ? What are the challenges faced in maintaining a secure system? How many times leak of information being reported? What significant action were taken to prevent it proactively? What is the process of giving Unique Identitifiers to atomic entities in the Organization ? Do you see a significant need for Role Based Access Control in Information Sharing	7.4% of the respondents who were getting their prescriptions digitally, their data was accessed by the doctors of the same organization, and no external organization doctors were allowed to access their data. EHR data other than the regular health check-up was kept confidential and was only accessed by limited people.
DECENTRALIZED: Applicability of Decentralized Blockchain to Information Sharing in Education Sector	Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing) Do you have an identified used case which the organisation can gain benifit from? Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to	Less awareness of blockchain technology More than 80% of the respondents found blockchain safer and secured for storing and sharing their data.

	Market)	
BUSINESS RULES: What are the Key Use Cases for application of Blockchain based technologies?	Does the patient have to repeat the examination when he moves from one hospital to the other Is there sufficient transparency in Health Care Information available across Organizations	Yes patients have t repeat tests across Organizations based on the category of test
COST OF INFORMATION SHARING	How many people are involved in information sharing across your department Total Average monthly salary for people involved in information sharing? What is the total Volume of Data shared in the Organization In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?	In the Administration Dept. App. 20% time of employee time is spend in Information Sharing. EMR Records are shared with other Organizations. They are automatically shared with Trusted Organizations.
Blockchain Frameworks	What is the volume of data that needs to be stored in the Blockchain. Is the system data required to be stored On Chain or Off Chain Do you need to be shared with a trusted consortium or with any untrusted party globally ?	EMR Record needs to be stored in the Blockchain. Volume of EMR record is significantly large.

5.5.3 Media Interview Response

The interview was done for 5 Content Generators who supply content to Online Channels with 50,000+ Following:

Interview Theme	Questions	Observation
INFORMATION CATEGORIES -	What are the categories of Information you share across Organizations What process do you follow for Information Sharing	Content Meta Dta is shared across Organizations

TECHNOLOGY BARRIER: Barriers for cross Organization Information Sharing	Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ? What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High	1. No central platform for publishing the content at the same time on different platforms 2. As such there is strong mechanism used by any of the organizations for data security, verification and protection 3. And mostly people are open to share their personal details on the online platforms for getting their results or requirements. And no proper security on these sites has increased the cases of data mutability, data loss and loss of privacy. 4. No fixed revenue sharing mechanism among peer has left the artists, content creators and other attached people to lose their identity. 5. Legal and technical barriers; 62.5% point to the distribution channel as the major technological barrier in sharing information; while 25% highlight security and safety while the remaining 12.5% point to the cost involved. It's a time intensive platform for sharing the content.

IMMUTABLE: Need for Immutable Information Share in Inter Organization and External Organization Information Sharing	What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified Do you get inputs or updates if your information is modified by Third Parties Are there some Organizations whom you would allow to modify the Information while others cannot i.e. some Trusted Parties How is data updated done reliably when any correction is required? What is the average Time taken in the completion of whole process?	Easy mutability has also raised the issues as 37.5% people say that the platform on which they work are not secured and the content and information which was shared on these platforms is copied or pirated with ease.
INTEROPERABLE: Average Frequency of repeated Information sharing in Intra and Inter Organization scenarios	What is the impact of Interoperability & Regulatory in Data Sharing Was there a scenario where you could not exchange information with other organization since the Data Formats did not match Has there been a case where you could not receive information from other Organization due to regulatory challenge	87.5% say point to government or private organisational legal barriers as key barrier in sharing information.
Information Data Storage & Volumetrics	What is the Volume of Information Shared Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.	62.5% people use 3 month old historical data and the balance 37.5% rely on I month old data.

ACCESS PERMISSION: How does the University secure its data?	How is data reliably secured in your Organization? ? What are the challenges faced in maintaining a secure system? How many times leak of information being reported? What significant action were taken to prevent it proactively? What is the process of giving Unique Identitifiers to atomic entities in the Organization ? Do you see a significant need for Role Based Access Control in Information Sharing	50 % respondents have faced challenges related to data security and illegal breach.
DECENTRALIZED: What is the Applicability of Decentralized Blockchain for Information Sharing in the Educational Sector	Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing) Do you have an identified used case which the organisation can gain benifit from? Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)	If the requirement of a distributor or aggregator becomes a must for information sharing then 62.5% of respondents want that the distributor should not charge at all, 25% are willing to pay charges on every content that is uploaded while the remaining 12.5% prefer onetime fees on a yearly basis. There is no fixed mechanism or rule for sharing the revenue among the peers. This gives a loophole in revenue sharing mechanism among the group.
BUSINESS RULES: What are the Key Use Cases for application of Blockchain based technologies?		62.5% respondents say that receipt of revenue is delayed from the platform where they have shared information or content. 87.5% respondents will find new business opportunities via peer to peer sharing mechanism of blockchain

		Lastly the trust and the owner's right would be easily maintained on such a platform as there is 100% agreement to it.
COST OF INFORMATION SHARING	How many people are involved in information sharing across your department Total Average monthly salary for people involved in information sharing? What is the total Volume of Data shared in the Organization In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?	It takes a week to upload content for 37.5%, another 37.5% experience a time frame of take hours and for 25% it takes between one to two days. The range of average volume of sharing the information per month caries from 0 – 20.
Blockchain Frameworks	Is the system data required to be stored On Chain or Off Chain Do you need to be shared with a trusted consortium or with any untrusted party globally ?	Content Meta Data should be stored On Chain. Since the Data Volume for Media Content is high it can be stored Off Chain Content Upload to be done by Trusted Parties. The Content Access should be done by untrusted parties.

5.5.4 Data Analysis 3 – Based on Interview Responses

As part of qualitative analysis the researcher has read the interview transcripts and observational notes for initial analysis. Categories and themes were formulated from the interview memos, explore the relationships between them. Summary of the key findings based on the interviews is presented below:

5.5.4.1 Education

- Immutability is identified as basic requirement for Education which is catered by all Blockchains. Hence it is removed.

- Most of the Education institues shared Data with other University in a semi-automated fashion. There is no feedback loop or monitoring process in place for Data Modification. Hence variables related to same have been removed
- Most Organizations have information of employee time spend on Information Sharing. Cost is also influenced by indirect factors such as credibility of University since a single fraud case can bring bad name to the University

Summary: Reduced from 32 to 22 Variables

5.5.4.2 Health Care

- All the hospitals take Patient consent before sharing Data. Hence the relevant variables have been removed
- Interoperable Records will lead to Globalization. Hence variables are removed.
- All the hospitals request the patient to share the tests from there trusted providers. There is no feedback loop or monitoring process in place for Data Modification. Hence variable related to same have been removed
- All Hospitals have the need to share research information with Trusted Organizations. Hence Public Permissioned Blockchain has been identified as potential candidate for removing from Framework
- All Hospitals have information of employee average time spend on Information Sharing. However, it is not possible to assign Cost to loss of opportunity or Trust

Summary: 26 Variables reduced to 21 Variables

5.5.4.3 Media

- Interoperability is a key requirement across all Use Cases. The variables have been merged for reinforcement
- Media institutes still work in Trusted mode with a consortium of known partners. Hence Public Permissioned Blockchain has been removed from Questionaire
- There is no feedback loop or monitoring process in place for Data Modification. Hence questions related to same have been removed from questionnaire

Summary: Reduced from 23 to 17 Variables

5.5.4.4 Blockchain*:*

- There is varied opnions on On Chain and Off Chain storage. Hence variables have been added for that theme
- Cost is a factor based on multiple external factors and Governance for the same is in formative stage
- Zero Knowledge Proofs introduced in BlockChain which is imporiving Privacy in Public Blockchains

5.5.5 Framework Summary

Identified Use Cases:

The Researcher has done Framework Based analysis of three IndustryVerticals, namely Health Care, Education and Media for applicable Use Cases for Blockchain. The key identified Use Cases are:

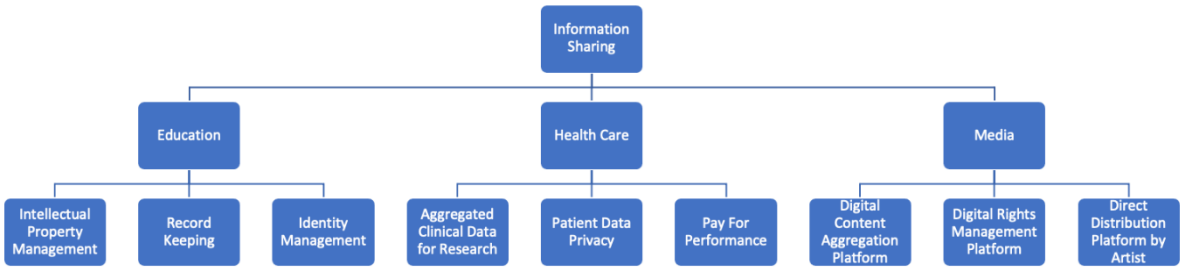


Figure 19: Use Case Summary

Trust Requirements:

The key variables to identify Trust Requirements across the Key Use Cases based on Framework Analysis are:

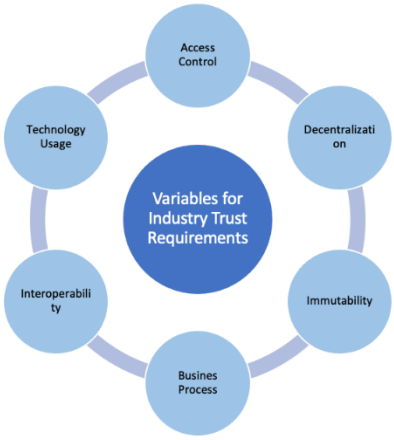


Figure 20: Trust requirements for Verticals

Industry Standard Blockchain Frameworks:
The Industry standard Framework for Blockchain applications is as below:

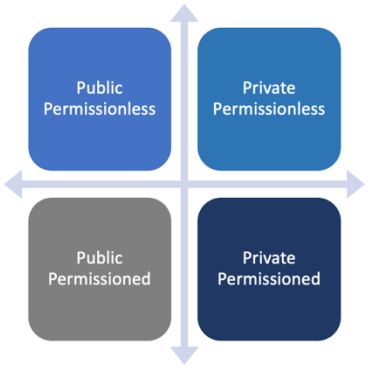


Figure 21: Industry Standard Blockchain Framework

5.5.6 Validated Framework – Education

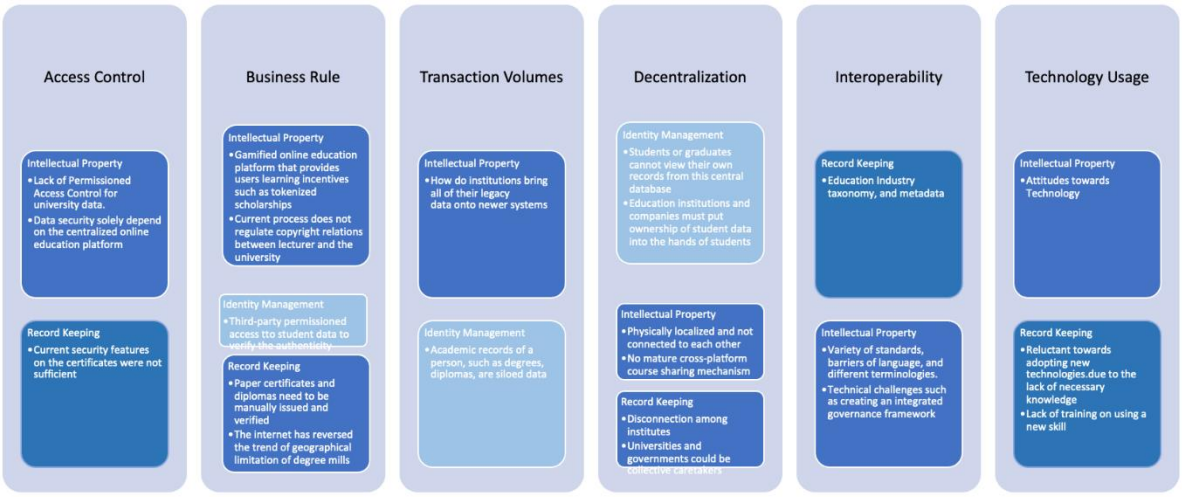


Figure 22: Validated Framework: Education

<u>Key findings from the above framework are:</u>

Interoperability & Transaction Volumes

- Singapore has implemented all Student Records on Blockchain to ensure access by students. However, this information is currently interoperable at Singapore Level Only and is not Globally acceptable

- Data Volumes of Degree Certificates is small. Hence this is a good candidate for On Chain Storage. However Volume of MOOC records is huge and rate of generation is high and hence not permissible for Off Chain Storage

Business Process & Operational Usage

- There is concern on Migration of Historical Data for Degree Records from Indian University. In Singapore this has been completed and Malaysia is in progress.
- In partnership with NPTEL, IIT's have started creating MOOC courseware. The content is openly available on YouTube. However, since there is no Central student identity there is no mechanism to integrate this with the student courseware. Currently exams are charged and physical.
- In a Small University, which currently has a Manual process for Degree record Verification, the process takes two-three Days. The cost per Degree Certificate Verification ranges from eight tofifteen US Dollars. In India Transcript cost is 1000 Rs and there is a 30 day SLA for delivery. For students these are time and cost concerns.
- Payment Automation can be done on Blockchain which involves simple level of complexity.
- Digitization is a serious challenge for Indian Universities and the complexity of Blockchain based systems in terms of Operational and Usage overheads is a serious concern.

Current Status of Decentralization and Access Control

- There is Country specific Regulatory process in place for Information Sharing**,** For e.g. Digicom in India. However there is no international level regulatory available.
- Currently the systems for digital certification, digital signatures and certificates are based on systems from trusted third parties. The process is susceptible to malicious attacks, human error and fraud – for example the 2018 case of Trustico CEO of CA mailing out the private keys of 23,000 certificates. UGC is seriously concerned about this and Niti Aayog in 2020 setup a task commission to enable Degree Certificates based on the Blockchain.

5.5.7 Validate Framework – Health Care

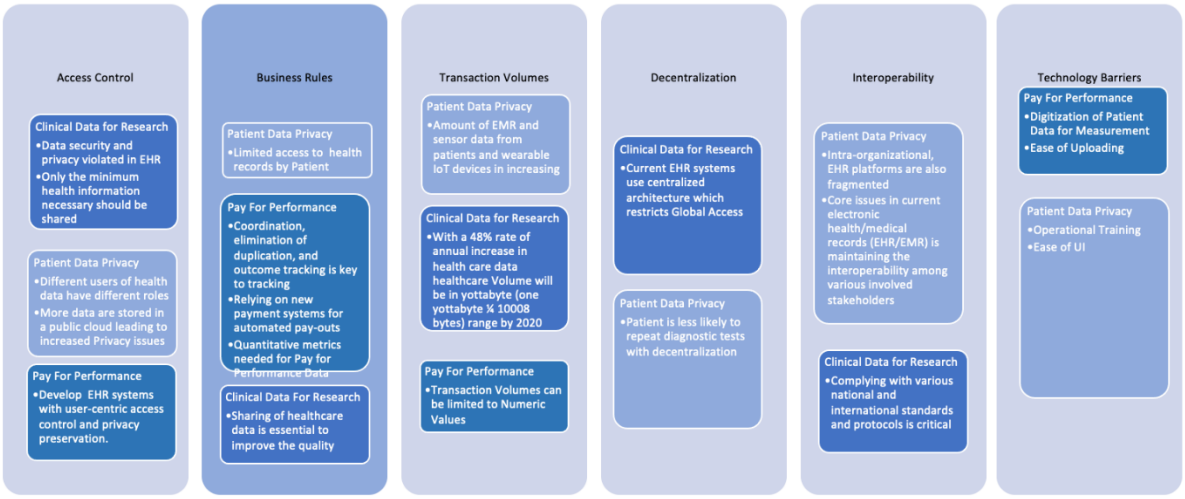


Figure 23: Validated Framework: Health Care

Key findings from the above framework are:

Transaction Volumes

In UK, P4P for Health Care is identified as a strong use case for blockchain since it enables trust. P4P clearly requires measuring of performance based on patient health registers. Disease and health registers are the medical equivalent of ledgers. They record limited data sets such as blood pressure, pulse, heart rate on weekly/monthly visits and hence do not need high data storage or off-chain storage requirements. In addition, there are extensively documented rules sets for Incentivization which can be coded using Smart Contracts. In addition, payments can be automated based on Smart Contract trigger rules.

Globally, Health Care data will significantly increase with the advent of IoT, 5G and Connected Devices. This will have significant improvements in Health Care Research and is currently restrained due to privacy concerns. Personal transactional data storage on Blockchain will have significantly high volume.

Access Control

Role Based Access Control for Patient Data as well as Aggregated Clinical Data is extremely important. This necessitates the need for Permissioned systems.

Business Rules

Business Rules for all 3 Use Cases of Health Care are not complex. The UK has well documented rules for Pay4Performance which can be automated using Smart Contracts.

Decentralization & Interoperability

Patient Data including Covid Health Cares need to have global access. However, Aggregated Clinical Data and Pay4Performance have a pre-defined set of actors and hence limited decentralization is acceptable.

Technology Barrier

Patient Data passport has started to be ported to Blockchain since it is operated by Trained staff. For porting Patient & Aggregated Data to Blockchains Patient Data , there is concerns on System Operation Usage as well Usability.

5.5.8 Validated Framework – Media

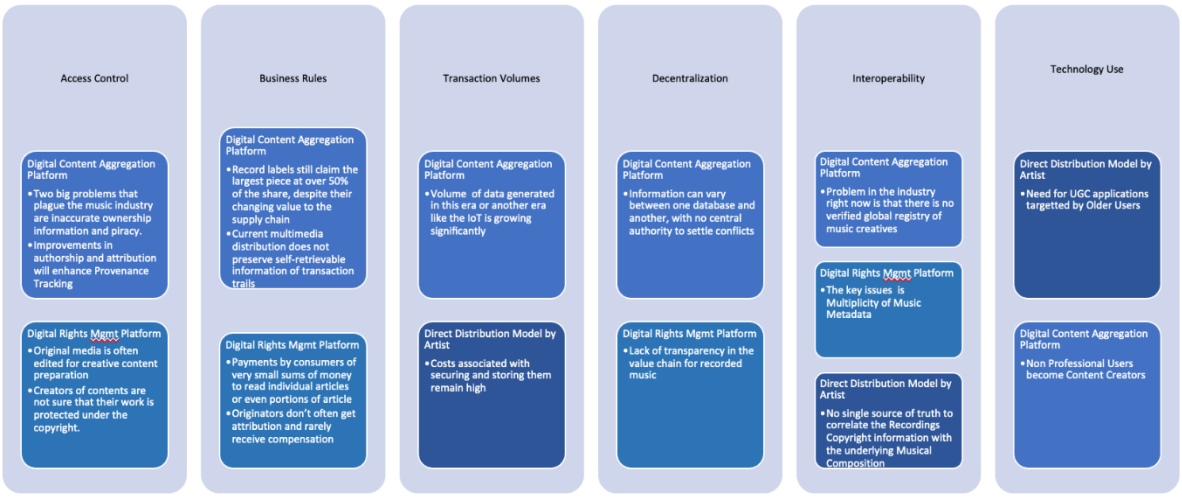


Figure 24: Validated Framework: Media

Key findings from the above framework are:

Interoperability
Current Media Platforms have Interoperability challenges on proprietary Formats since they work in siloes. Data storage formats are not Interoperable and are unique to every application, and. In case a song composer intends to transfer, replicate or duplicate his metadata across application, it has limitations. This is due to the fact that current applications do not support this since each application has their own legacy formats

Transaction Volumes

The Content Metadata size is limited to Kilo Bytes and hence is applicable to storing on Block Chain. However actual Content Meta Data has size varying from Mega to Giga Bytes and hence is a candidate for storing Off Chain

Business Rules
Business Rule complexity is limited to Payment of Revenue. Complexity increases when multiple partners are involved in the Value chain for Revenue Distribution. Each track of recorded music has two copyrights – Musical Composition and Recording Composition.

Decentralization
Control is currently limited in the hand of Major Players for Media Distribution. Information regarding copyright owners are distributed in varied sources of collecting societies, publishers, record companies, and other entities,. These do not have incentives to share the information. The industry will see significant increase in operational as well as financial benefits by using a decentralized Meta Data database.

Operational Usage:
Artists currently upload content on Paid sites such as You Tube which provide statistics of Usage. They do not have a process to verify the Audit Trail of Usage and hence trust the service provider. An automated payment mechanism for direct pay-outs will improve cash flow.
Access Control
Current systems have Access rights based on Media Partner varying based on Coarse grained Policies as well as content categories. The system has a limitation that access policies based on fine grained control defined based on User attributes such as Composer Identity, or Multiuser approvals are not feasible.

5.5.9 Validated Framework – Blockchain

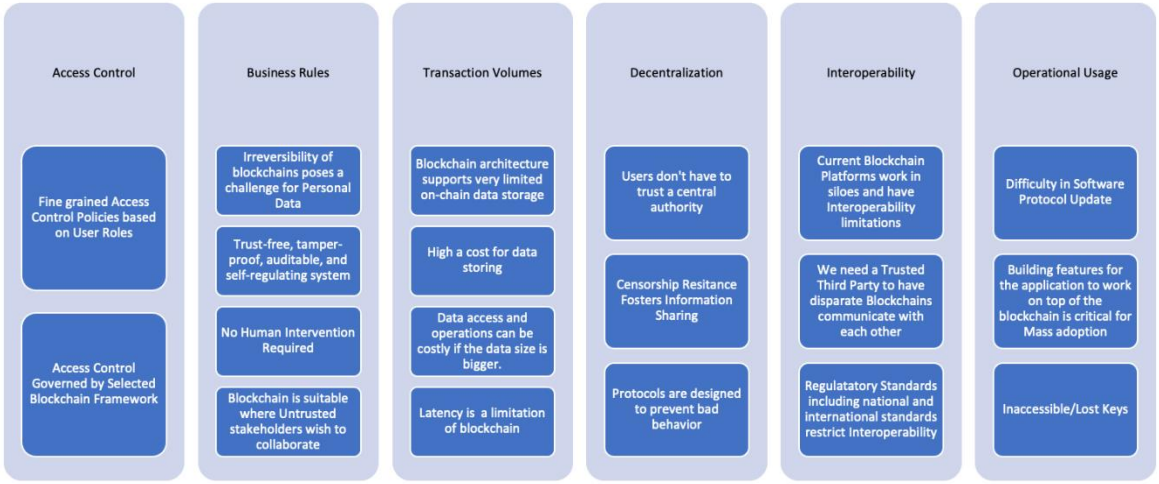


Figure 25: Validated Framework: Blockchain

Key findings from the above framework are:

Interoperability

Public blockchains have a deep understanding about how blockchain networks should operate. Hence they are intrinsically more interoperable. On the contrary, private blockchains are dependent on different entities within an ecosystem defining their own shared standards based on mutual agreements. Public Permissioned Blockchains do not inherit the same disadvantage as Private Blockchains since they are not owned by a Consortium.

Transaction Volumes:

- In Public blockchains the speed at which transactions are inserted and read by the blockchain, is slower comparsed to private versions. This is attributed to polling to achieve consensus and limits on transactions or block sizes.
- Storing large volumes of data on the a public chain is not recommended.

Access Control:

- In a public blockchain access is open to everybody while in Private Blockchain only invited and approved parties can participate. Hence Private Blockchains (both Permissioned and Permissionless) can grant User level access control, including Read and Write Permissions at an atomic level. Data stored in Public Blockchain is visible to all and hence has Privacy issues.
- Permissioned Blockchains have a significant advantage over Permissionless Blockchains since they have controlled access.

Decentralization:

Public blockchains (both Permissioned and Permissionless) are governed by no Central Authority and hence support decentralization intrinsically. Private Blockchains (Permissioned and Permissionless) are owned by a Central Authority and hence there is no True Decentralization.

Business Rules:
Business Rules are implemented in Blockchain through Smart Contracts. In Public Blockchains, the Smart Contracts have limitations since the rules need to be replicated on all Nodes which is Time Consuming. Private Blockchains give more flexibility on Smart Contract implementation compared to Public Blockchains.

Operational Usage:

- Operational Usage incurs Operating system upgrades and Ease of Data Entry. This is important is Use Cases where the Data Entry is to be done by unskilled Users and not trained IT staff. Public Blockchains due to limitation of every Node replication offer significantly more Operational overheads compared to Private Blockchains.
- Governance around Blockchains is in early stages and is expected to evolve rapidly over the next few years for mass adoption.

5.5.10 Final Interview Protocol – Based on Familiarization Stage 2

5.5.10.1 Education

Table 35: Final Interview Protocol: Education

Information Categories
What are the categories of Information you share across Institute
Operational Usage
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
How frequently do you share information with other Institues
Is the information shared in Digital Format or Hard Copy. What is the typical size of information shared
Decentralization
What is the impact of Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
Is there any Regulatory challenge in Data Sharing
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
Access Control

How is data reliably secured in your Organization? ?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
Interoperability
Is there a specified template in which Information needs to be shared with other Organizations
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Business Rules - Education Specific Queries
What are the challenges faced at the time of admission for verification of the information like certificates, rank and merit of students?
How is the verification process done for students that are coming in for different university / colleges? Any problem faced during the same
Do you share Course ware material with other Universities. How if the IP protected
Is the University / Govt open to sharing data with other University at National level or Globally?
Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Is there a perceived Use Case or New Business Oppurtunity (For e.g.: Information Monetization, New University Partnerships etc.) where it is recognized that Blockchain will bring major benefits to the educational institute
What is the typical Volume of Data that would need to be stored on Blockchain
How secure does the shared data need to be
Do you visualize the need to be shared with a trusted consortium or with any untrusted party globally ?

5.5.10.2 Health Care

Table 36: Final Interview Protocol: Health Care

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared

Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
What is the impact of Regulatory in Data Sharing
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules - Health Care Specific Queries
Does the patient have to repeat the examination when he moves from one hospital to the other
Is there sufficient transparency in Health Care Information available across Organizations
Information Sharing on Blockchain
Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
What is the volume of data that needs to be stored in the Blockchain.
Is the system data required to be stored On Chain or Off Chain
Do you visualize the need to be shared with a trusted consortium or with any untrusted party globally ?

5.5.10.3 Media

Table 37: Final Interview Protocol: Media

Information Categories
What are the categories of Information you share across Organizations
What process do you follow for Information Sharing
Technical Usage Barriers
Have you ever faced a scenario where Information from your Organization has been plagiarized by others without getting consent from your Organization ?
What are the challenges that may come in place during Digitalization of Information Sharing System in the organization? Example Unskilled Employee/ Lack of Infrastructure/Very High Maintenance Cost/ Cost of Digitalization is High
Information Data Storage & Volumetrics
What is the Volume of Information Shared
Does the size of organization (large /small) contribute to how efficiently information is being shared ? example Large organisation require more time in information sharing from one department to other / In small organisation lack of sufficient people and infrastructure causes delay in information sharing.
Immutability & Decentralization
What is the impact if Information shared by you is modified by Third Party Organizations. E.g. if student tampers with degree certificate or if Course Content is modified
What is the impact of Regulatory in Data Sharing
Cost of Information Sharing
How many people are involved in information sharing across your department
Total Average monthly salary for people involved in information sharing?
In your opinion how can this cost be reduced? And how would it have a postive or negative impact on the total revenue generated by Organization?
Access Control
How is data reliably secured in your Organization? ?
What are the challenges faced in maintaining a secure system?
How many times leak of information being reported? What significant action were taken to prevent it proactively?
What is the process of giving Unique Identitifiers to atomic entities in the Organization ?
Do you see a significant need for Role Based Access Control in Information Sharing
Business Rules - Media Specific Queries
Are there any preferred channels for information sharing
What is the revenue share arrangement for information sharing across various providers
Sharing on Blockchain

Has Information sharing on Blockchain been considered by your institute? What are the perceived challenges(For e.g.: Lack of Business Vision for Information Sharing Lack of trust in Technological systems of Business Sharing)
Do you have an identified used case which the organisation can gain benifit from?
Do you see significant operational improvementss by introducing Blockchain for Information Sharing? (For e.g. Reduced Human Effort, Reduced Paperwork, Faster Time to Market)
Do you see new Business Opportunities emerging in the industry by introducing Blockchain for Information Sharing? (For e.g. Information Monetization, University new Partnerships etc.)
What is the volume of data that needs to be stored in the Blockchain.
Is the system data required to be stored On Chain or Off Chain
Do you visualize the need to be shared with a trusted consortium or with any untrusted party globally ?

5.5.10.4 Blockchain

5.6 Final Interview Response

5.6.1 Health Care

To verify the Blockchain applications in Health Care the researcher has conducted interviews with Industry experts including Senior Professor, GB Pant Hospital (New Delhi), Head of Innovation, Celcom, Malaysia), Consultant Radiologist, Wockhardt Hospital (Mumbai), Senior VP, Siemens Health Care (Bangalore) and Director Philips Innovation Campus (Bangalore). Key observation is that:

Business Rules

- **Access Control:** Healthcare Stakeholders do not have trust on other institutes that content not will be altered without the owners permission. Technology is a barrier to IT adoption since some members are not familiar with IT tools making Data access automation challenging.
- **Transaction Volumes:** Blockchain has the benefit of an Immutable database. However, it has a limitation on the size of data stored due to block limitations and performance. Typical healthcare data comprising of electronic imaging records require large storage requirements and cannot be stored in its entirety on the blockchain. This necessitates the use of hybrid blockchains which enable storage of large data Volumes. However, this introduces complexity which is hard to justify.

- **Decentralization:** In addition to an immutable database, a key feature is Decentralization. Key use cases for Blockchain are focused on areas where the involved parties do not trust human agency and need to remove the intermediary.
- **Business Rules:** P4P for Health Care is identified as a strong use case for blockchain since it enables trust. P4P necessitates measuring of performance based on disease registers. Disease registers are the healthcare equivalent of ledgers. They record limited data sets such as blood pressure, heart rate on monthly visits and hence do not need high data storage or off-chain storage requirements. In addition, there are extensively documented rules sets for Incentivization which can be coded using Smart Contracts. In addition, payments can be automated based on Smart Contract trigger rules.
- **Operational Usage:** All that said, the trustworthiness of blockchain technology does not preclude the necessity of audits in the real world. Registers maintained on blockchain have to be verified by physical visits to the GP and meeting with some of the patients to verify the numbers recorded in the registers.
- **Interoperability:** Interoperability of data does not work seamlessly across various Institute. There is no mechanism to verify the authenticity of data uploaded by the Institutes in the blockchain

5.6.2 Education

To verify the Blockchain applications in Education the researcher has conducted interviews with Industry experts including Dr M. Menon (Head of Innovation, Celcom, Malaysia), Nizar Jamal (Transformation and Cyber Security Expert, Florida), Mr Rajesh Dudhu (Tech Mahindra, Blockchain Head), Ms Zainon Mustaffa (Registrar, Asia School of Business, Malaysia), Mr Subramonia Sarma (Senior Director of Action Learning, ASB, Malaysia) and Zheng Wei QUAH (Accredify CoFounder & CEO).

Business Process

- There is no automated process for Student Degree Verification for Universities of small size
- The process of verification takes upto 3 Days . The cost per Degree Certificate Verification can range from 8Dollars

Interoperability

- Technology is a challenge in implementation since many staff members a not familiar with IT
- Access control Implementation is a challenge
- Content is very frequently illegally modified. Hence there is lack of Trust with Information Partners.

Decentralization

- There is geography specific Regulatory process for Information Sharing in institutes

Operational Challenges

- Verification of student health records is not automated
- Lack of an Interoperable Blockchain makes it hard to ensure Data Trust amongst institutes
- Organizations trust the certificates shared by Employee . There is no automated mechansism to verify the Academic Records of new joinees

Access Control

- There is no Revenue Share regulation in place when IP information is shared across partners. Hence Content Plagiarism is a serious challenge
- There is no Traceability of changes or Audit Log, for changes done by Partner institutes

Transaction Volumes:

- Blockchain is transforming from hosted environment to BAAS (Blockchain as a Service). This is enabled by Cloud Providers like Azure, AWS, and Alibaba. This is based on operational usage by the end client. This significantly brings down the cost of Operational Blockchain

Key Barriers of Blockchain Implementation

- No mechanism to check the Data uploaded by the Institutes
- Multiple educational institutions remain hesitant towards adopting newer technologies. A key reason for this is lack of trust. This is due to lack of knowledge and skills for managing students' data on a blockchain platform.
- Blockchain is a nascent technology. Hence availability of Blockchain trained employees is a constraint and cost consideration for new projects.
- India has recently come up with a Nation wide direction for implementation of Blockchain in Education. This is a nascent technology which will evolve over time.
- Interoperability of Data Across Blockchains in Institutes creates hurdles
-

5.6.3 Media

To verify the Blockchain applications in Media the researcher has conducted interviews with Industry experts including Head of Business Development, Verifi Media (UK), You Tuber with 50,000+ Followers (India), CEO of Content Aggregator Company (India) and CTO of Real Time Campaign Company (India).

Access Control

Current systems implement Access rights based on Media partner based on Coarse grained Policies and content categories. Access Control based on atomic rules such as User attributes User Identity, or Multiuser approvals are not applicable.

Interoperability
Current Media Platforms have Interoperability challenges on proprietary Formats since they work in siloes. Data storage formats are not Interoperable and are unique to every application, and. In case a song composer intends to transfer, replicate or duplicate his metadata across application, it has limitations. This is due to the fact that current applications do not support this since each application has their own legacy formats the other.

Operational Usage:
Blockchain has limitation on the operational usage since it is currently constrained by User Interface flexibility as well as lack of trained users. Blockchain frameworks do not provide automation which enables cross platform signatures verification. Hence if YouTube Users wish to execute Smart Contracts on Verizon Media, the same is not supported currently.

Transaction Volumes
The Content Metadata size is limited to Kilo Bytes and hence is applicabe to storing on Block Chain. However actual Content Meta Data has size varying from Mega to Giga Bytes and hence is a candidate for storing Off Chain

Business Rules
Business Rule complexity is limited to Payment of Revenue. Complexity comes to multiple partners in the Value chain for Revenue Distribution.

Decentralization
Control is currently limited in the hand of Major Players for Media Distribution

5.6.4 Blockchain:

To verify the Blockchain Framework the researcher has conducted interviews with Industry experts including Dr Manohar Menon (Head of Innovation, Celcom, Malaysia), and Zheng Wei QUAH (Accredify CoFounder & CEO) Mr Rajesh Dudhu (India, Tech Mahindra, Blockchain Head), Nizar Jamal (Transformation and Cyber Security Expert, Florida),. Key observation is that:

Interoperability and standards:

Public blockchains have a deep understanding about how blockchain networks should operate. Hence they are intrinsically more interoperable. On the contrary, private blockchains are dependent on different entities within an ecosystem defining their own shared standards based on

mutual agreements. Public Permissioned Blockchains do not inherit the same disadvantage as Private Blockchains since they are not owned by a Consortium.

Transaction Volumes:

- In Public blockchains the speed at which transactions are inserted and read by the blockchain, is slower comparsed to private versions. This is attributed to polling to achieve consensus and limits on transactions or block sizes.
- This is attributed to polling to achieve consensus and limits on transactions or block sizes. Storing large amounts of data on the a public chain is not reccomended. Permissioned Blockchains have a significant advantage over Permissionless Blockchains since they have controlled access.

Access Control:

In a public blockchain access is open to everybody while in Private Blockchain only invited and approved parties can participate. Hence Private Blockchains (both Permissioned and Permissionless) can grant User level access contro, including Read and Write Permissions at an atomic level. Data stored in Public Blockchain is visible to all and hence has Privacy issues.

Decentralization:

Public blockchains (Permissioned and Permissionless) are governed by no Central Authority and hence support decentralization intrinsically. Private Blockchains (Permissioned and Permissionless) are owned by a Central Authority and hence there is no True Decentralization. This can make decision making faster, however can also introduce challenges of authority.

Business Rules:

Business Rules are implemented in Blockchain through Smart Contracts. In Public Blockchains, the Smart Contracts have limitations since the rules need to be replicated on all Nodes which is Time Consuming. Hence Private Blockchains provide more flexibility on Smart Contract implementation compared to that from Public Blockchains.

Operaional Usage:

Operational Usage incurs Operating system upgrades and Ease of Data Entry. This is important is Use Cases where the Data Entry is to be done by unskilled Users and not trained IT staff. Public Blockchains due to limitation of every Node replication offer significantly more Operational overheads compared to Private Blockchains. However, Governance around Blockchains is in early stages and is expected to evolve rapidly overg next few years for mass adoption.

5.7 Reliability and Validity in Qualitative Research

To appreciate reliability and validity, it is important to present the various aspects of reliability and validity provided by many qualitative researchers from different angles.

Reliability : The idea of reliability is most often used in all kinds of research. It is a concept used for evaluating quantitative research and verification. Considering that testing as a way of information extraction then the quality is the most important aspect of qualitative study. The importance of Qualitative study is to make a confusing situation easy to interpret. The concept of reliability in qualitative study has the purpose of making understanding simpler. Contratily, reliability is a concept in quantitative study to evaluate quality with the objective of explaining. It is very important to understand the different of quality of studies in quantitative and quantitative research. This explains why the concept of reliability is not important in qualitative research.

Validity : Creswell & Miller (2000) propose that the validity is influenced by the researcher's view of validity in the study. It is also influenced by researchers choice of sample assumptions. Owing to this many researchers have created their definitions of validity. The researchers definition encompasses what they consider to be more valid definitions, such as, rigor quality, and trust. Since there were serious concerns about quality is research stemming from the researchers perceptions in qualitative research, hence the words reliability and validity were coined.
Issues in Validity and Reliability :
NVivo has been used for generating and documenting high quality qualitative research. This was to ensure that the validity or trustworthiness can be tested or maximized. This will produce more credible and defensible outputs. The quality of a research is related to adapting of the result to varied scenarios. This generalization is used to test and improve the trustworthiness or validity of the research.

In a qualitative study the data gathering is primarily done by the researcher. Hence the influence of researcher competency and bias needs to verified carefully. If not verified this may impact the data trustworthiness of seriously. This can be very hazardous for research since the very object of research may impact the final results. The way in which the researcher poses, posts and records the responses with the participants can impact the final outcome of the research. This has explained by Argyris 1952

Hence as per Framework Analysis Methodology inorder to ensure Reliability and Validity in Research, there are multiple iterations done for Literature Analysis as well as Interview Protocols by the Researcher to ensure trust in Data and Findings. The respondents who have deep expertise in there respective Verticals (More than 20 Years of Experience) were selected to ensure no samplaing error.

6. Study Findings

6.1 Research Question #1: What is the influence on Provenance Tracking Intensity Models of an Organization based on Specific Trust Needs of Information Sharing with Partner?

6.1.1 Trust Model

The researcher has created a Trust Model of Information sharing that will be used further across all Industry Verticals to identify the Provenance requirements of the use case.

Table 38: Trust Model for Information Sharing

Access Control	Refers to the level of defense a system a system needs from external attacks. It also indicates the Access Control flexibility needed in terms of Role Based Access Control.
Decentralization	Refers to the degree of diversification in ownership, influence and value required by the system.
Interoperability	For interaction with any external system, Interoperability is key. This is governed by Regulatory Framework, system data adaptability as well as Meta Data formats
Transaction Volumes	Indicates the number of Transactions Per Second the system can scale up to. Bitcoin can support up to 7 TPS and Visa handles up to 2000 Transactions Per Second.
Business Process	This is governed by complex of Business Rule automation that is required for a
Technical Barriers	Based on the level of Trained Users operating the system, the Technical Barriers are defined. Also it encompasses Operational overheads including periodic updates

6.1.2 Health Care

Summary of Industry Requirements based on the Identified Variables are as follows:

Table 39: Use Case Study Summary: Health Care

Use Case	Decentralization	Business Rules	Access Control	Transaction Volumes	Inter-Operability	Technology Barrier
Aggregated Clinical/administrative data Availability for Research	**Very Significant** since need for access by Untrusted Parties	**Medium Complexity** Reduced Entities in Value Chain	**Medium Significant** since Access Control defined in rules for Trusted Parties	**High Volume** Accessible by all and Large Data Volumes	**High Requirement** Need for Accessible by Multiple Platforms	**High Barrier** since used by Hospital Staff
Patient Data Privacy	**Very Significant** since need for access by Untrusted Parties	**Medium** Multi Party Value Chain	**Very significant** since Need for RBAC to control permission	**High Volume** Accessible by all and Large Data Volumes	**High Requirement** Accessible by Multiple Platforms	**High Barrier** since used by Hospital Staff
Pay4Performance	**Less Significant** since need for access by Untrusted Parties	**Medium:** Rules restricted to Pre-Defined set	**Medium Significant** since Access Control defined in rules for Trusted Parties	**Low Volume** Data Volumes are low since Data Sets are small	**High Requirements** Accessible by Multiple Platforms	**Medium Barrier** since Used by skilled Staff

- **Access Control:** For Patient Data Privacy, Access Control is highly significant to ensure that Patient has ful control of HIS data stored in Public Databases. However, for Clinical Data Aggregation and Pay4Performance this has Medium Significance since the User Consortium is limited to Tusted Users and the known Risk of exposure is limited.
- **Transaction Volumes:**. Standard healthcare data constitutes of electronic imaging records require large storage requirements and cannot be stored in its entirety on the blockchain. This imposes the requirement for a Blockchain Platform that can support High Transaction Volumes. However, for Pay4Performance Use Case limited data sets since the complete EIR record is not stored. Hence it has medium significance for Transaction Volumes Variable.
- **Decentralization:** In addition to an immutable database, a key feature is Decentralization. For Patient Data privacy and Aggregated Clinical Data the involved parties need to trust the human agency and need to remove the intermediary.Hence decentralization requirement is high. Information stored in Pay4Performance is shared across Trusted Parties and hence the significance is Medium.
- **Business Rules:** P4P for Health Care is identified as a strong use case for blockchain since it enables trust. P4P necessitates measuring of performance based on disease registers which record limited data sets and hence do not need high data storage requirements. In addition, there are extensively documented rules sets for Incentivization which can be coded using Smart Contracts. Patient Data Privacy and Aggregated Clinical Data also have less complex rules for Data Sharing and hence Business Rule requirement is of Medium Complexity.

- **Operational Usage:** For Aggregated Clinical Data and Patient Data Privacy Registers maintained on blockchain have to be verified by physical visits to the GP and meeting with some of the patients to verify the numbers recorded in the registers. Hence it is important to have reduced Operational complexity. However, for Patient Data Privacy the requirements is limited since it is used by trained users only.
- **Interoperability:** Data across all thress Use Cases needs to be exchanged across Health care Instititues hence the requirement is high. However, due to limitations of Digital Information and Varies protocols the prevalence is low in current Health Care ecosystem.

6.1.3 Education

Summary of Industry Requirements based on the Dependent Variables are as follows:

Table 40: Use Case Study Summary: Education

Use Case	Decentralization	Business Rules	Access Control	Transaction Volumes	Inter-Operability	Technology Barrier
Record Keeping	**Very significant** to provide access for Non Trusted Parties	Pre Defined set of Rules exist with **Medium Complexity**	**Very Significant** to give control to Student	**Low Volume since** Limited to Student Records	**High Requirement** since Need for sharing across Multiple Organizations	**High Barrier** since Operations to be run by Multiple Levels
Managing Intellectual Property	Sharing can be restricted to Pre-Defined University hence **less significant**	Pre Defined set of Rules exist with **Medium Complexity**	**Less Significant** since Read Access Only	**High Volume since many** Course Material with large size	**Medium Requirement** Limited to Course Ware Format like pdf	**Medium Barrier** since Only used by Skill Staff
Identity Management	**Very significant** to provide access for Global Non Trusted Parties	Simplified Rules for Identity hence **Low Complexity**	**Less Significant** since Read Access Only	**Low Volume since** Limited to Student Records	**High Requirement** since Need for sharing across Multiple Organizations	**Low Barrier** since Implemented by Back End IT

Business Rules

In record Keping, the process of verification takes upto 3 Days and cost per Degree Certificate Verification can range from 8Dollars. In addition, there is no automated process for Student Degree Verification for smaller Universities. For Intellectual Property Management the rules are well defined and hence the Business Rule complexity is medium.

Interoperability

Technology is a challenge in implementation since many staff members a not familiar with IT. Hence Access control Implementation is a challenge. Moreover Content is very frequently

illegally modified. Hence there is lack of Trust with Information Partners. This increases the Interoperability requirements for record Keeping and identity management.

Decentralization

There is geography specific Regulatory process for Information Sharing in institutes for record keeping and identity management. This increases the complexity. However for Intellectual property management, this can be owned by a Consortium and hence the complexity requirement is lowered.

Operational Challenges

Verification of student health records is not automated at the time of admission leading to increased time delays. For record keeping, Organizations trust the certificates shared by Employee further leading to time delays. There is no automated mechansism to verify the Academic Records of new joinees in Universities. Hence record keeping has high degree of influence from Operation issues. However, Identity Managemt is typically run by IT staff and hence the complexity is lower.

Access Control

There is no Revenue Share regulation in place when IP information is shared across partners. Hence Content Plagiarism is a serious challenge . There is no Traceability of changes or Audit Log, for changes done by Partner institutes.

Transaction Volumes:

The average record size and number of Transactions for Student record Keeping and identity management is limited. However, in Intellectual property large volumes of Data are stored due to which the requirements for Transaction Volumes is significantly high.

6.1.4 Media

Summary of Industry Requirements based on the Dependent Variables are as follows:

Table 41: Use Case Study Summary: Media

Use Case	Decentralization	Business Rules	Access Control	Transaction Volumes	Inter-Operability	Technology Barrier
Direct Distribution Model by Artist	**Very Significant** since Need for access by Untrusted Parties	**Medium Complexity** since Reduced Entities in Value Chain	**Very Significant** Need for RBAC to control permission	**Medium Volume** since Limited to Artist Distribution	**High Requirement** since Accessible by Multiple Platforms	**Low Barrier** since Operability by Artist primarily
Digital Content Aggregation Platform	**Very Significant** since Need for access by Untrusted Parties	**High Complexity since** Multi Party Value Chain	**Very Significant** Need for RBAC to control permission	**High Volume** since Accessible by all	**High Requirement since** Accessible by Multiple Platforms	**High Barrier** since Used by Unskilled Artists also
Digital Rights Management Platform	**Very Significant** since Need for access by Untrusted Parties	**Medium Complexity since** Rules restricted to Rights Platform	**Medium Significant** Access Control defined in Rights	**High Volume** since Accessible by all	**Medium Requirement** since logic embedded in Rights Platform	**Medium Barrier** since Used by Content Aggregator

Access Control

Current systems implement Access rights based on Media partner based on Coarse grained Policies and content categories. Access Control based on atomic rules such as User attributes User Identity, or Multiuser approvals are not applicable. However for DRM Platforms the rules are defined in the Rights Platform and hence Medium Complexity is required.

Interoperability

Current Media Platforms have Interoperability challenges on proprietary Formats since they work in siloes. Data storage formats are not Interoperable and are unique to every application, and. In case a song composer intends to transfer, replicate or duplicate his metadata across application, it has limitations. This is due to the fact that current applications do not support this since each application has their own legacy formats the other.

Technology Barrier:

Digital Content Aggregation has high requirements since it is used by unskilled Users. However, in a Direct Distribution Model the content is uploaded by the Artist who has familiarity with his content. On the contrary, blockchain has limitation on the operational usage since it is currently constrained by User Interface flexibility as well as lack of trained users. Blockchain frameworks do not provide automation which enables cross platform signatures verification

Transaction Volumes

The Content Metadata size is limited to Kilo Bytes and hence is applicabe to storing on Block Chain. However actual Content Meta Data has size varying from Mega to Giga Bytes and hence has high Transaction Volume requirements.

Business Rules
Complexity comes to multiple partners in the Value chain for Revenue Distribution for Digital Content Aggregation and hence has high complexity. For Direct Distribution and DRM Platforms, the Business Rule complexity is limited to Payment of Revenue and hence has Medium significance.

Decentralization
Control is currently limited in the hand of Major Players for Media Distribution. It is imperative for all Use Cases that the content is accessible to Public who have no Trusted relationship and hence decentralization is very significant.

6.2 Research Question#2: What are the applicable Blockchain Patterns when used for Information Provenance Tracking based on Specific Trust Needs?

6.2.1 Blockchain

Public blockchains, such as Bitcoin and Etheruem, enhance permission-less access, and collaboration. In aaddition they have limitations on Business Rule complexity and storage volumes. Private blockchains such as HyperLedger are executed within controlled environments in an environment of permissioned access, reducing Decentralization but allowing for more Privacy and Transaction VolumesSummary of Industry Requirements based on the Dependent Variables are as follows:

Transaction Volumes:

Storing large amounts of data on the a public chain is not reccomended. Permissioned Blockchains have a significant advantage over Permissionless Blockchains since they have controlled access. In Public blockchains the speed at which transactions are inserted and read by the blockchain, is slower comparsed to private versions. This is attributed to polling to achieve consensus and limits on transactions or block sizes. This is attributed to polling to achieve consensus and limits on transactions or block sizes.

Access Control:

Data stored in Public Blockchain is visible to all and hence has Privacy issues.
In a public blockchain access is open to everybody while in Private Blockchain only invited and approved parties can participate. Hence Private Blockchains (both Permissioned and Permissionless) can grant User level access contro, including Read and Write Permissions at an atomic level.

Interoperability and standards:

Public blockchains have a deep understanding about how blockchain networks should operate. Hence they are intrinsically more interoperable. On the contrary, private blockchains are dependent on different entities within an ecosystem defining their own shared standards based on mutual agreements. Public Permissioned Blockchains do not inherit the same disadvantage as Private Blockchains since they are not owned by a Consortium.

Decentralization:

Public blockchains (Permissioned and Permissionless) are governed by no Central Authority and hence support decentralization intrinsically. Private Blockchains (Permissioned and Permissionless) are owned by a Central Authority and hence there is no True Decentralization. This can make decision making faster, however can also introduce challenges of authority.

Business Rules:

In Public Blockchains, the Smart Contracts have limitations since the rules need to be replicated on all Nodes which is Time Consuming. Hence Private Blockchains provide more flexibility on Smart Contract implementation compared to that from Public Blockchains.

Operaional Usage:

Operational Usage incurs Operating system upgrades and Ease of Data Entry. This is important is Use Cases where the Data Entry is to be done by unskilled Users and not trained IT staff. Public Blockchains due to limitation of every Node replication offer significantly more Operational overheads compared to Private Blockchains. However, Governance around Blockchains is in early stages and is expected to evolve rapidly overg next few years for mass adoption.

The below framework provides summary characteristics of each Blockchain Framework category based on Industry Standard definitions:

Table 42: Blockchain Capability Matrix

Blockchain Framework	Decentralization	Business Rules	Access Control	Transaction Volumes	Interoperability	Technology Barriers
Public Permissionless	Very Significant since no central authority	Medium Complexity since Change has to be transmitted to Public Nodes	Limited since Public Access	Supports Low Volumes Only	Limited since Public Access	High since Public Keys and OS Upgrade
Private Permissionless	Medium Significant since Consortium Owned but Permissionless	High Complexity since owned by Consortium	Can Control Write Access based on User Roles	Supports High Volumes	Medium since Private Controlled	Medium since Private Controlled
Public Permissioned	Medium Significant since Public but Permissioned	Medium Complexity since Change has to be transmitted to Public Nodes	Control Write Access based on User Roles	Supports Medium Volumes	Limited since Public Access	High since Public Keys and OS Upgrade
Private Permissioned	Low since Consortium Owned and Permissioned	High Complexity since owned by Consortium	Control Write Access based on User Roles	Supports High Volumes	Medium since Private Controlled	Medium since Private Controlled

6.3 Comaprison with Past Studies

Some of the key findings of the Research with recent papers on similar topics are as follows:

Research Findings	Previous Study Reference	Comapritive Analysis
In Health Care Sector there is varied needs of Trust based on Information Sharing Use cases. Blockchain Frameworks can be used to resolve the Trust needs across Organizations. However, it is critical to do an analysis of the requirements with the Blockchain Framework Capability to ensure that the optimized Blockchain Framework Model is used	The Fourth Industrial Revolution of Healthcare Information Technology: Key Business Components to Unlock the Value of a Blockchain-Enabled Solution Ann Ingraham,1 Jim St. Clair[48]	Both the Research are consistent with there findings on applicability of Blcockahin for Health Care. Patient Data Sharing is a commonly reviewed theme. Pay4Performance is a new use case identified by the current research which significantly is a growing space for Health Care
Blockchain is a new technology that can be applied to multiple verticals. However, it is important to have a use Case based analysis framework to	A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities[56] by Klein, Sandra	Both Research have identified frameworks for use Case Analysis. The variables for identification have significant similarity including Business Process and Data.

evaluate the relevant Blockchain technology to be used	Augustin et. al	Transaction Volume is a new variable that has been identified as a part of the current research which will contribute significantly to Framework Optimization
Interoperability of Blockchain Platforms is currently limited due to lack of Regulatory standards in the domain as well as inter Blockchain communication	An Overview of Blockchain for Higher Education Timothy Arndt[8]	Both Research have identified that Blockchain will play an increasing role in Education. However due to limitation of Interoperability it is currently limited in its application.

6.4 Framework Scalability

The Trust and Blockchain Framework created as part of this research has been applied to the following verticals:

- Education
- Health Care (IoT Enabled)
- Media

The Framework is specific for Digital Information sharing applications. The scope does not include applications involving Supply Chain or Payment Transactions. Hence the same Framework is scalable to other Verticals and use Cases where digital information sharing is involved.

A key vertical where the same can be applied is Government sector. To verify the same scalability, the researcher has published a paper titled – "Review of Ownership Based Blockchain Frameworks in Government Applications". Some of the known challenges in Government sector are related to lack of Trusted data. 78% of the land is unregistered in Ghana. A large earthquake in 2010 in Haiti, spolied all the government buildings that stored information. In India, a large population of villagers do not have legal ownership of the land they work on. The research focussed on following verticals:

- Land Registries
- E-Residency
- Voting
- Smart Government

It has been verified through the research that the same Trust Model developed for Education, Health Care and Media has been extended to Government Sector also for Information Sharing. Hence it proves that it is a scalable model.

7. Contribution to Theory

Key contribution to Theory of this Research is identified in this chapter as:

- The research is proposing a Trust Framework comprising of six variables to analyze the Provenance Tracking Requirements of a Firm for Information sharing comprising of Access Control, Business Rules, Decentralization, Interoperability, Operational Usage and Transaction Volumes
- Trust Requirements Model which was absent in the Transaction Cost Theory of Firm, subsequently, this will help the Organization to create an assessment matrix to optimize the Transaction Cost of Information Sharing.

7.1 Papers Published by Researcher:

The following papers were published as part of the Pilot study by the Researcher. The concetual lens is modified as per this pilot study. The Thesis is based on the results obtained from the Original Interviews conducted after this Pilot study.

- Psychology & Education Journal – Dec-20:Education 4.0: A Systematic Industrial Case Based Review of Barriers and Applications of Decentralized Trust Using Blockchain[24]. Authors: Deepika Sachdev, Dr Shailendra Kumar Pokhriyal et. al
- IAEME Jan 20: ANALYZING BLOCKCHAIN BASED MODELS FOR DIGITAL CONTENT METADATA TRACEABILITY. Authors: Deepika Sachdev, Dr Shailendra Kumar Pokhriyal et. al
- IITM JBS: Oct 19 : Review of Ownership Based Blockchain Frameworks in Government Applications. Authors: Deepika Sachdev, Dr Deepankar Chakrabarti et. al
- IAEME Jan 19: ENABLING DATA DEMOCRACY IN SUPPLY CHAIN USING BLOCKCHAIN AND IOT. Author: Deepika Sachdev

8. Contribution to Industry

Multiple challenges inhibit Information Sharing in the Industry. The Information sharing needs vary based on the Trust Requirements of the Industry. Blockchain provides a secure Trusted Solution for Information sharing. This research paper contributes to Literature as follows:

- A new “Trust Requirements Framework” created in Health Care, Education and Media verticals to enhance Information Sharing across Organizations
- A Blockchain Industry Framework mapping application capability with “Trust Requirements”
- The framework will act as a source of reference for Industry to baseline their Trust Requirements
- It will be also beneficial for Industry Blockchain Adoption by creating a Cross Metric analysis of Trust requirement with Blockchain Solution capability

With the emergence of Technology, there are multiple Blockchain Frameworks providing varying degrees of Trust. The research provides six key pillars for defining Trust requirement based on the Industry Use Cases. It goes further to analyze the Trust capabilities delivered by

each Blockchain Framework . This will ensure that the Information sharing Industry is enabled by providing a structured methodology to analyze its Information Sharing requirements and also to analyze the Blockchain Framework that provides the optimum capability. Some key highlights of Trust requirements based on Blockchain Frameworks are:

Interoperability

Public blockchains are intrinsically more interoperable since have a deep understanding about how blockchain networks should operate. On the contrary, private blockchains are dependent on different entities within an ecosystem defining their own shared standards based on mutual agreements. Public Permissioned Blockchains do not inherit the same disadvantage as Private Blockchains since they are not owned by a Consortium.

Transaction Volumes:

- In Public blockchains as against private blockchains, the speed at which transactions are inserted and read by the blockchain. This is attributed to polling to achieve consensus and limits on transactions or block sizes.
- Large volume of data storage on the a public chain is not recommended.

Access Control:

- In a public blockchain access is open to everybody while in Private Blockchain only invited and approved parties can participate. Hence Private Blockchains (both Permissioned and Permissionless) can grant User level access control, including Read and Write Permissions at an atomic level. Data stored in Public Blockchain is visible to all and hence has Privacy issues.
- Permissioned Blockchains have a significant advantage over Permissionless Blockchains since they have controlled access.

Decentralization:

Public blockchains (both Permissioned as well as Permissionless) are not regulatd or governed by a Central Authority and hence support decentralization intrinsically. Private Blockchains (Permissioned and Permissionless) are owned by a Central Authority and hence there is no True Decentralization.

Business Rules:

Business Rules are implemented in Blockchain through Smart Contracts. In Public Blockchains, the Smart Contracts have limitations since the rules need to be replicated on all Nodes which is Time Consuming. Private Blockchains give more flexibility on Smart Contract implementation compared to Public Blockchains.

Operational Usage:

- Operational Usage incurs Operating system upgrades and Ease of Data Entry. This is important is Use Cases where the Data Entry is to be done by unskilled Users and not trained IT staff. Public Blockchains due to limitation of every Node replication offer significantly more Operational overheads compared to Private Blockchains.
- Governance around Blockchains is in early stages and is expected to evolve rapidly over the next few years for mass adoption.

The conclusion is that depending on the Trust Requirement, there are valid use cases for permissionless as well as permissioned blockchains.

9. Conclusions and Recommendations

This paper has identified a Trust Framework for Education, Health Care and Media Sector. It has also created a Conecptual Lens of the Four Blockchain Industry Standard Models against the of six identified Barriers in for Information sharing. All four Blockchain Models provide varying levels of Trust Capability which aligns with varying Trust needs of the Use Case.

Research Question #1: What is the influence on Provenance Tracking Intensity Models of an Organization based on Specific Trust Needs of Information Sharing with Partner?

Conclusion: This Research has analysed Three Use Cases across Three Industry Verticals (Health Care, Education and Media). Across all the verticals a Trust Framework has been created to identify the Provenance Tracking Needs of the Organization encompassing Access Control, Decentralization, Immutability, Business Process, Interoperability and Transaction Volumes. For each of the Use Cases the influence varies based on the above six dependent Variables. The identified Trust Model can be used a Framework for any additional Use cases that need to be analyzed for Information sharing based Trust Needs

Future Study Recommendation: The Trust Model has been verified across three verticals and three use Cases. For future study, it is recommended to apply Trust Model across varied verticals including Government and Supply Chain.

Research Question #2: What are the applicable Blockchain Patterns when used for Information Provenance Tracking based on Specific Trust Needs?

Conclusion: The Research has analysed four Industry Standard Blockchain Patterns names Public Permissioned, Public Permissionless, Private Permissioned and Private Permissioned for the capabilities based on the identified Six Trust constituents namely Access Control, Decentralization, Immutability, Business Process, Interoperability and Transaction Volumes. Finally the Researcher has done a correlation between the Trust Needs of the Industry Use Case and the Blockchain Framework to demonstrate the applicability of the matrix for identification of optimized Industry solutions.

Future Study Recommendation: Blockchain is a fast evolving technology with new capabilities being enhanced to the Frameworks continuously. For e.g. Public Blockchains are working on Zero Knowledge Proofs to enable Privacy. It is recommended for future studies to encompass upcoming technologies as part of the Blockchain Framework.

10. Limitations of Study & Scope for further Study:

Based on constraints of technology and scope following aree the limitations of this Research. These shall form scope for further research items:

- Fintech is a an area of Research that is Goverend by Regulatory and involves physical Transactions. Hence it has not been covered as part of this scope but shall form basis of a separate research
- The research is focused on the Information sharing aspects of Blockchain and has not been focused on detailed technical features of Blockchain such as encryption & mining. It is assumed that these capabilities exist and do not form the preview of this research paper. These shall be covered in future research.
- Blockchain is in an early stage of adoption where Governance costs for Operationalization are not known. In addition, the Cost of Transactions for Verticals include intangible variables such as Reputation and Opputunity. Hence at this point it is not possible to create a direct cost correlation matrix of existing Cost of Implementation in Vertical versus the actual cost of Operationalization in Blockchain. This shall be covered in future research.

11. Bibliography

[1] W.M. A., F.S. E., Data Science, Predictive Analytics, and Big Data: A Revolution That Will Transform Supply Chain Design and Management, J. Bus. Logist. 34 (2013) 77–84.

[2] J. Abadi, M. Brunnermeier, Blockchain Economics, Princet. U. Work. Pap. (2018) 1–53.

[3] A. Aggarwal, Review of Ownership Based Blockchain Frameworks in Government Applications Pages 22-32, Annu. J. Inst. Innov. Technol. Manag. Vol. 3 (2016).

[4] W. Al-Saqaf, N. Seidler, Blockchain technology for social impact: opportunities and challenges ahead, J. Cyber Policy. 0 (2017) 1–17.

[5] A. Alketbi, Q. Nasir, M.A. Talib, Blockchain for government services-Use cases, security benefits and challenges, 2018 15th Learn. Technol. Conf. L T 2018. (2018) 112–119.

[6] D. Allessie, M. Sobolewski, L. Vaccari, F. Pignatelli, Blockchain for digital government, 2019.

[7] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S.W. Cocco, J. Yellick, Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains, (2018).

[8] T. Arndt, An overview of blockchain for higher education, IC3K 2019 - Proc. 11th Int. Jt. Conf. Knowl. Discov. Knowl. Eng. Knowl. Manag. 3 (2019) 231–235.

[9] L. Asiri, Blockchain For Educational Certificate Distribution by, (2020).

[10] M. Attaran, J. Stark, D. Stotler, Opportunities and challenges for big data analytics in US higher education: A conceptual model for implementation, Ind. High. Educ. 32 (2018) 169–182.

[11] M. Ayvaci, H. Cavusoglu, Y. Kim, S. Raghunathan, Payment Mechanisms, Incentives for

Adoption And Value of Health-Information Exchanges (HIEs), SSRN Electron. J. (2017) 1–48.
[12] N. Baym, L. Swartz, A. Alarcon, Convening technologies: Blockchain and the music industry, Int. J. Commun. 13 (2019) 402–421.
[13] D.M. Berwick, T.W. Nolan, J. Whittington, The triple aim: Care, health, and cost, Health Aff. 27 (2008) 759–769.
[14] D. Bhowmik, T. Feng, The multimedia blockchain: A distributed and tamper-proof media transaction framework, Int. Conf. Digit. Signal Process. DSP. 2017-Augus (2017).
[15] J. Biggs, S.R. Hinish, M.A. Natale, M. Patronick, Blockchain: Revolutionizing the Global Supply Chain by Building Trust and Transparency, (2017).
[16] G.-W. Bock, R.W. Zmud, Y. Kim, J. Lee, Behavuirak intention formation Knowledge Sharing : Examining the roles of extrinsic motivators , socuak-psychological forces, and organizational, Spec. Issue Inf. Technol. Knowl. Manag. 29 (2005) 87–111.
[17] D.J. Brailer, Interoperability: the key to the future health care system., Health Aff. (Millwood). Suppl Web (2005) 19–21.
[18] J.T. Bram, B. Warwick-Clark, E. Obeysekare, K. Mehta, Utilization and Monetization of Healthcare Data in Developing Countries, Big Data. 3 (2015) 59–66.
[19] Cadwalladr Carole, Cambridge Analytica whistleblower: “We spent $1m harvesting millions of Facebook profiles,” Guard. (2018).
[20] S. Caress, Piracy, Policy, and Pandora: Outdated Copyright in a Digital World, Student Res. Day Abstr. Posters. (2017).
[21] A. Chakravorty, C. Rong, Ushare: User controlled social media based on blockchain, Proc. 11th Int. Conf. Ubiquitous Inf. Manag. Commun. IMCOM 2017. (2017).
[22] F. Chen, Z. Drezner, J.K. Ryan, D. Simchi-Levi, Quantifying the Bullwhip Effect in a Simple Supply Chain: The Impact of Forecasting, Lead Times, and Information, Manage. Sci. 46 (2000) 436–443.
[23] U.W. Chohan, The Concept and Criticisms of Steemit The Concept and Criticisms of Steemit, (2018).
[24] T. Choudhury, Education 4 . 0 : A Systematic Industrial Case Based Review of Barriers and Applications of Decentralized Trust Using Blockchain, 57 (2020) 882–893.
[25] D.P. Cis, P. Buneman, W. Tan, ScholarlyCommons Why and Where : A Characterization of Data Provenance Why and Where : A Characterization of Data Provenance, 1973 (2001) 316–330.
[26] S. Cuore, R. Coelho, Blockchain: a new way of distribution, promotion and improvement of the artistic, economic and cultural situation of a film in the, (2018) 408–418.
[27] M.O. Dair, D. Neilson, P. Pacifico, Music On The Blockchain Lead Researcher, (2016) 1–29.
[28] E.Y. Daraghmi, Y.A. Daraghmi, S.M. Yuan, UniChain: A design of blockchain-based system for electronic academic records access and permissions management, Appl. Sci. 9 (2019).
[29] P. Dunphy, F.A.P. Petitcolas, A first look at identity management schemes on the blockchain, IEEE Secur. Priv. 16 (2018) 20–29.
[30] G. Epiphaniou, H. Daly, H. Al-Khateeb, Blockchain and healthcare, Adv. Sci. Technol. Secur. Appl. (2019) 1–29.
[31] C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K.R. Choo, Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?, IEEE Cloud Comput. 5 (2018) 31–37.

[32] T.H.E. European, U. Blockchain, FOR GOVERNMENT AND PUBLIC, (n.d.).
[33] T. Faisal, N. Courtois, A. Serguieva, The Evolution of Embedding Metadata in Blockchain Transactions, Proc. Int. Jt. Conf. Neural Networks. 2018-July (2018).
[34] G. Fridgen, F. Guggenmos, J. Lockl, A. Rieger, A. Schweizer, N. Urbach, I.W. Prinz, P.H. Eds, G. Fridgen, A. Rieger, N. Urbach, Developing an Evaluation Framework for Blockchain in the Public Sector : The Example of the German Asylum Developing an Evaluation Framework for Blockchain in the Public Sector : The Example of the German Asylum Process, 4801 (2018).
[35] E. García-Barriocanal, S. Sánchez-Alonso, M.A. Sicilia, Deploying metadata on blockchain technologies, Commun. Comput. Inf. Sci. 755 (2017) 38–49.
[36] V. Garcia-Font, Blockchain: Opportunities and challenges in the educational context, 2020.
[37] R. Gellman, Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges, (2017).
[38] O. Gough, Blockchain : a new opportunity for record labels, Int. J. Music Bus. Res. 7 (2018) 26–44.
[39] U.K. Government, C. Scientific, Distributed Ledger Technology : beyond block chain, (n.d.).
[40] J.M. Graglia, C. Mellon, Blockchain and Property in 2018: At the End of the Beginning, Innov. Technol. Governance, Glob. 12 (2018) 90–116.
[41] Grech Alexander, F. Camilleri Anthony, Blockchain in Education, 2017.
[42] G. Grolleau, An Introduction to the Economics of Fake Degrees Author (s): Gilles Grolleau , Tarik Lakhal and Naoufel Mzoughi Source : Journal of Economic Issues , Vol . 42 , No . 3 (Sep ., 2008), pp . 673-693 Published by : Association for Evolutionary Economics S, 42 (2014) 673–693.
[43] P. Helo, Y. Hao, Blockchains in operations and supply chains – a review and reference implementation, Proc. Int. Conf. Comput. Ind. Eng. CIE. 2018-Decem (2018).
[44] B.W. Hesse, D.E. Nelson, G.L. Kreps, R.T. Croyle, N.K. Arora, B.K. Rimer, K. Viswanath, Trust and Sources of Health Information, Arch. Intern. Med. 165 (2005) 2618.
[45] G. Hileman, M. Rauchs, 2017-09-27-Ccaf-Globalbchain.Pdf, (2017).
[46] T. Höppner, P. Westerhoff, J. Weber, Taking a Bite at the Apple: Ensuring a Level-Playing-Field for Competition on App Stores, SSRN Electron. J. (2019).
[47] Hyperledger, Case Study : BC aims to cut government red tape with Hyperledger Indy, (2019).
[48] A. Ingraham, J. St. Clair, The Fourth Industrial Revolution of Healthcare Information Technology: Key Business Components to Unlock the Value of a Blockchain-Enabled Solution, Blockchain Healthc. Today. (2020) 1–4.
[49] D. Jonghe, BigchainDB : A Scalable Blockchain Database (DRAFT), (2016) 1–65.
[50] M. Jun, Blockchain government - a next form of infrastructure for the twenty-first century, J. Open Innov. Technol. Mark. Complex. 4 (2018) 7.
[51] M.N. Kamel Boulos, J.T. Wilson, K.A. Clauson, Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare, Int. J. Health Geogr. 17 (2018) 1–10.
[52] E. Kane, Is Blockchain a General Purpose Technology?, SSRN Electron. J. (2017) 1–27.
[53] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: A comprehensive review and directions for future research, Appl. Sci. 9 (2019) 1–28.
[54] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu, The Blockchain-Based

Digital Content Distribution System, Proc. - 2015 IEEE 5th Int. Conf. Big Data Cloud Comput. BDCloud 2015. (2015) 187–190.
[55] A. Kittu, A. PolisettyManda, Vij, Status Check on Blockchain Implementations in India, SSRN Electron. J. (2018).
[56] S. Klein, S. Augustin, W. Prinz, S. Augustin, W. Gräther, S. Augustin, A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities, (n.d.).
[57] C.S. Kruse, R. Goswamy, Y. Raval, S. Marawi, Challenges and Opportunities of Big Data in Health Care: A Systematic Review, JMIR Med. Informatics. 4 (2016) e38.
[58] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila, Blockchain utilization in healthcare: Key requirements and challenges, 2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018. (2018) 1–7.
[59] T.T. Kuo, H.E. Kim, L. Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, J. Am. Med. Informatics Assoc. 24 (2017) 1211–1220.
[60] O. Labazova, From Hype to Reality : A Taxonomy of Blockchain Applications From Hype to Reality : A Taxonomy of Blockchain Applications, (2019).
[61] O. Labazova, T. Dehling, A. Sunyaev, From Hype to Reality: A Taxonomy of Blockchain Applications, Proc. 52nd Hawaii Int. Conf. Syst. Sci. (2019).
[62] T.Y. Lam, B. Dongol, A blockchain-enabled e-learning platform, Interact. Learn. Environ. 0 (2020) 1–23.
[63] J. Lee, S.O. Hwang, S.W. Jeong, K.S. Yoon, C.S. Park, J.C. Ryou, A DRM framework for distributing digital contents through the internet, ETRI J. 25 (2003) 423–436.
[64] V.L. Lemieux, D. Ph, D. Hofman, D. Batista, Blockchain Technology & Recordkeeping Table of Contents, (2019).
[65] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability, Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGRID 2017. (2017) 468–477.
[66] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC. 2017-Octob (2018) 1–5.
[67] R. Lomotey, K. Sofranko, R. Orji, Enhancing Privacy in Wearable IoT through a Provenance Architecture, Multimodal Technol. Interact. 2 (2018) 18.
[68] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, P. Saxena, A Secure Sharding Protocol For Open Blockchains, Proc. 2016 ACM SIGSAC Conf. Comput. Commun. Secur. - CCS'16. (2016) 17–30.
[69] Z. Ma, M. Jiang, H. Gao, Z. Wang, Blockchain for digital rights management, Futur. Gener. Comput. Syst. 89 (2018) 746–764.
[70] I. Martinovic, Blockchains: Design Principles, Applications, and Case Studies, 7 (2018).
[71] T. Mcconaghy, D. Holtzman, Towards An Ownership Layer for the Internet, (2015) 1–32.
[72] T. Mcconaghy, R. Marques, A. Müller, D. De Jonghe, T. Mcconaghy, G. Mcmullen, R. Henderson, S. Bellemare, A. Granzotto, BigchainDB: A Scalable Blockchain Database (DRAFT), BigchainDB. (2016) 1–65.
[73] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: A review, IEEE Access. 6 (2018) 10179–10188.
[74] M. Mettler, Blockchain technology in healthcare: The revolution starts here, 2016 IEEE

18th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2016. (2016) 16–18.
[75] Z. Mingaleva, I. Mirskikh, The Protection of Intellectual Property in Educational Process, Procedia - Soc. Behav. Sci. 83 (2013) 1059–1062.
[76] G. Mohamedbhai, The Scourge of Fraud and Corruption in Higher Education, Int. High. Educ. (2016) 12–14.
[77] M.A. Mohammed, E.Y. Maroof, A. Thamer, I. Huda, What are the Electronic Information Sharing Factors that Influence the Participation Behavior in Higher Education Sector?, Procedia Comput. Sci. 72 (2015) 49–58.
[78] M.S. Mok, S.Y. Sohn, Y.H. Ju, Conjoint analysis for intellectual property education, World Pat. Inf. 32 (2010) 129–134.
[79] M.G. Moore, A sad reminder that diploma mills are still with us, Int. J. Phytoremediation. 21 (2009) 175–178.
[80] M. O'Dair, The networked record industry: How blockchain technology could transform the consumption and monetisation of recorded music, (2016) 42.
[81] M. O'Dair, Distributed Creativity: How Blockchain Technology will Transform the Creative Economy, 2019.
[82] M. O'Dair, R. Owen, Financing new creative enterprise through blockchain technology: Opportunities and policy implications, Strateg. Chang. 28 (2019) 9–17.
[83] I.J. Of, INTERNATIONAL JOURNAL OF Case of Kenya Certificate of Secondary Education, (2017) 52–66.
[84] S. Ølnes, J. Ubacht, M. Janssen, Blockchain in government : Bene fi ts and implications of distributed ledger technology for information sharing, 34 (2017) 355–364.
[85] M.M.H. Onik, S. Aich, J. Yang, C.-S. Kim, H.-C. Kim, Blockchain in Healthcare: Challenges and Solutions, Elsevier Inc., 2019.
[86] M. Pilkington, Can Blockchain Improve Healthcare Management? Consumer Medical Electronics and the IoMT, SSRN Electron. J. (2017).
[87] Z. Radjenovic, The Cost- Saving Role of Blockchain Technology As a Data Integrity Tool: E-health Scenario, KnE Soc. Sci. 2019 (2020) 339–352.
[88] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Futur. Gener. Comput. Syst. 88 (2018) 173–190.
[89] J. Rinaldi, Peer To Peer Digital Rights Management Using Blockchain, (2018).
[90] J. Rios-Amaya, J. Secker, C. Morrison, Lecture Recording in Higher Education: Risky Business or Evolving Open Practice, LSE Res. Online. (2016) 1–44.
[91] D. Sachdev, E. Studies, H.E. Management, E. Studies, E. Studies, ANALYZING BLOCKCHAIN BASED MODELS FOR DIGITAL CONTENT METADATA, 11 (2020) 277–292.
[92] O.S. Saleh, O. Ghazali, M.E. Rana, Review Article BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION, 7 (2020) 79–84.
[93] R.K. Sandhu, H.R. Weistroffer, A review of fundamental tasks in requirements elicitation, 2018.
[94] Satoshi Nakamato, Bitcoin: A Peer-toPeer Electronic Cash System, (2013) 1–9.
[95] A. Savelyev, Copyright in the blockchain era: Promises and challenges, Comput. Law Secur. Rev. 34 (2018) 550–561.
[96] A. Shelkovnikov, Blockchain applications in the media industry, (2016) 1–2.
[97] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives,

Cryptography. 3 (2019) 3.
[98] Sovrin Foundation, Sovrin™: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust, Sovrin. (2018) 1–41.
[99] H. Sun, X. Wang, X. Wang, Application of blockchain technology in online education, Int. J. Emerg. Technol. Learn. 13 (2018) 252–259.
[100] J. Sun, J. Yan, K.Z.K. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities, Financ. Innov. 2 (2016) 26.
[101] D. Tapscott, A. Kaplan, Blockchain Revolution in Education and LifeLong Learning: Preparing for Disruption, Leading the Transformation, (2019) 46.
[102] K. Taylor, A. Sanghera, M. Steedman, M. Thaxter, Medtech and the Internet of Medical Things: How Connected Medical Devices are Transforming Health Care, Deloitte. (2018) 1–56.
[103] K. Taylor, A. Sanghera, M. Steedman, M. Thaxter, Medtech and the internet of medical things: How connected medical devices are transforming health care, Deloitte. (2018).
[104] W. Technology, and Blockchains in the Music Industry, (n.d.).
[105] R. Thurimella, Y. Aahlad, The Hitchhiker ' s Guide to Blockchains : A Trust Based Taxonomy, (2018) 1–28.
[106] D. Trossen, C. Fine, Value Chain Dynamics in the Communication Industry, MIT Commun. Futur. Program. MIT. (2005) 1–17.
[107] B.E. Tse, I. Education, DEGREES FOR SALE : THE DIPLOMA MILLS PROBLEM CONTINUES, (2015).
[108] J. Umeh, 470631193, Itnow. 58 (2016) 58–61.
[109] R. Wahid, A. Mohd, S., B. Mat, M. Subhan, K. Saidin, Sharing Works and Copyright Issues in Massive Open Online Courseware (MOOC), Int. J. Res. Emerg. Sci. Technol. 2 (2015) 24–29.
[110] X. Wang, Digital rights management for broadband content distribution, Proc. - 2003 Symp. Appl. Internet, SAINT 2003. 21 (2003) 4.
[111] K. Wüst, A. Gervais, Do you need a Blockchain ?, (n.d.).
[112] C. Xu, K. Wang, M. Guo, Intelligent Resource Management in Blockchain-Based Cloud Datacenters, IEEE Cloud Comput. 4 (2017) 50–59.
[113] Z. Yang, L. Zhang, Information sharing in supply chain: A review, J. Digit. Inf. Manag. 11 (2013) 125–130.
[114] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where Is Current Research on Blockchain Technology?-A Systematic Review, PLoS One. 11 (2016) e0163477.
[115] Z. Yu, T.C.E. Cheng, Benefits of Information Sharing with Supply Chain Partnerships Benefits of information sharing with supply chain partnerships, (2001).
[116] M. Zhaofeng, H. Weihua, G. Hongmin, A new blockchain-based trusted DRM scheme for built-in content protection, Eurasip J. Image Video Process. 2018 (2018) 1–12.
[117] G. Zyskind, O. Nathan, A.S. Pentland, Decentralizing privacy: Using blockchain to protect personal data, Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015. (2015) 180–184.
[118] G. Zyskind, A.S. Pentland, Decentralizing Privacy : Using Blockchain to Protect Personal Data, (n.d.).

12. Annex -1– Literature Review Challenges of Provenance Tracking for Information Sharing

Details	Findings	Inference	Gap
Modelling provenance metadata Paolo Missier	Provenance on Data Archive Demonstrating has been getting expanded concentration in Exploration as of late with the increment of Advanced Data through Web, Huge Information and IOT. They are nonexclusive models accessible for Provenance age of Information base and Interaction created reports. This is finished utilizing explanation based methodologies and non-comment based methodologies. Explanation based methodologies unequivocally record data about the inference of a piece of information in the data set itself, commonly as an additional property in the table. Non-explanation based methodologies don't store provenance in the information base, yet investigate the inquiry answer, the actual question, and the information	Based on the existing studies in Provenance Management, there is Open Source Models which help to map Information profile into industry agreed conventions. This is based on open source standards agreed between participating organizations.	There is need for increased research in the areas of scientific and Process driven Research

	tables to ascertain the provenance of a piece of information. An illustration of non-comment based approach is the reason provenance		
Principles of Provenance - 2012 by James Cheney1 , Anthony Finkelstein2, , Bertram Ludäscher3 , , and Stijn Vansummeren4	PROV-DM is an information model for provenance that portrays the substances, individuals and exercises engaged with delivering a piece of information or thing on the planet. PROV-DM is area skeptic, however is outfitted with extensibility focuses permitting further space explicit and application-explicit augmentations to be characterized. PROV-N permits serializations of PROV-DM cases to be made for human utilization, which works with the planning of PROV-DM to substantial language structure, and which is utilized as the reason for a conventional semantics of PROV-DM	For the interoperability of provenance information across organizations it is very important to have mutual agreements across the organizations. The PROV organization has created PROV variants based on Data Source and Domains which can be tailored as per the Industry Needs.	There is a gap on Industry specific research models in PROV. Also, Provenance has not been seen from the perspective of Trust in the Industries

	that is right now being worked on. PROV-O depends on an OWL philosophy with the end goal of articulation of provenance in RDF. PROV-AQ indicates how one can utilize standard Web conventions, including HTTP, to get data about the provenance of Web assets. It depicts both basic access components for finding provenance data related with website pages or assets, just as provenance question administrations for more perplexing organizations.		
Andrew J. Flanagin and Miriam J. Metzger, The credibility of volunteered geographic information. GeoJournal (2008) Dezani-Ciancaglini, Mariangiola; Horne, Ross; Sassone, Vladimiro Main reference M. Dezani, R. Horne, V. Sassone, "Tracing where and who provenance in Linked Data: a calculus. Provenance Threat Modeling Oluwakemi Hambolu, Lu Yu, Jon Oakley and Richard R. Brooks Ujan Mukhopadhyay and Anthony Skjellum	Standards including OPM(Open Provenance Model), beginning with the First Provenance Challenge workshop started as community work and are designed to provide basic standards. However, they do not have an inbuild model for lineage analysis	OPM by design do not include aspects specific to provide lineage analysis for Industry Specific Models	There is continual research work pending complete or reconstruct provenance when it was not originally generated by either Databases or Process Generated documents.
	Connected Information gives some reasonable rules to distributing and burning-through information Online. Information distributed Online has no characteristic truth, yet its quality can regularly be evaluated	Companies such as Google are investing millions to find Data Provenance for Internet created data to enable linkages and reference citations of data. However,	New protocols such as IPFS for Blockchain keep emerging which need to have Provenance Models defined for them. Hence there is ongoing research gap in

	dependent on its provenance. OPM work acquaints another methodology with provenance for Connected Information. The most straightforward thought of provenance is a named chart demonstrating where the information is presently – is reached out with a more extravagant provenance design. The arrangement mirrors the conduct of cycles communicating with Connected Information, following where the information has been distributed and who distributed it.	as technology is emerging the protocols need to be updated continuously.	Provenance for emerging technologies.
Provenance Threat Modeling Oluwakemi Hambolu, Lu Yu, Jon Oakley and Richard R. Brooks Ujan Mukhopadhyay and Anthony Skjellum Where Is Current Research on Blockchain Technology?—A Systematic Review Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander	The security of the blockchain is ensured by keeping a cryptographically marked chain of secure hash esteems. Since this chain is put away at different destinations and is likewise being persistently refreshed, it will be practically unimaginable for this chain to be controlled by fraudsters. With this capacity, the blockchain can guarantee the uprightness and security of provenance information.	Blockchain Security does provide relevance to Provenance Storage. As future research, we will present using cryptocurrency primitives. a complex security model for securing metadata provenance This implies that currently there is no out of box security model in Blockchain for Provenance	Need for a Provenance Enabled Security Model for Blockchain which is based on Trust

The W3C PROV family of specifications for modelling provenance metadata Paolo Missier, Khalid Belhajjame 2013	PROV Model has been extended for databases and scientific workflows. The W3C bunch on provenance have proposed an information model (PROV-DM) that distinguishes six center parts of provenance data as it identifies with information: elements and exercises; inferences of elements from elements; specialists obligation regarding elements and exercises; a system for recording the historical backdrop of provenance data itself (provenance of provenance); properties to interface related or repetitive elements; what's more, legitimate designs to store and put together individuals [66].	It is difficult to extend the PROV for Scientific flows since the process inside is complex	There is gap for extending PROV to various industries based on Trust
Data Provenance: Some Basic Issues Peter Buneman, Sanjeev Khanna and Wang-Chiew Tan 2000	For provenance of data we need to keep track of the source of data and how it moves across sources. If the source changes then it is important to update the target links	One could envision that information is traded in bundles that are \self aware"2 and some way or another contain a total history of how they traveled through the arrangement of data sets, of how they were developed, and of how they were changed. The	There are gaps seen around self-generating provenance of System generated documents in cases when the source of the data changes

		thought is clearly engaging, yet whether it tends to be figured plainly, not to mention be carried out, is an open inquiry	
Peter Buneman University of Edinburgh Edinburgh, UK opb@inf.ed.ac.uk Adriane P. Chapman University of Michigan Ann Arbor, MI 48109 apchapma@eecs.umich.edu James Cheney University of Edinburgh Edinburgh, UK jcheney@inf.ed.ac.uk 2006	The paper talks of automatic provenance tracking in a curated scientific database. The approaches have high DB storage and are CPU Intensive. The key is that there is a Why and a How of Provenance. Why refers to the source from where it was obtained and how refers to the detailed sources where it was obtained.	A hierarchical approach is proposed to store Provenance Data.	There are gaps around the need of varied Trust Factors across Organiations for Provenance Tracking
Data Provenance: A Categorization of Existing Approaches 2015	Fostering a provenance the board framework for open world models is a difficult issue. Moreover, a considerable lot of the control offices present in the plan are excluded from the current methodologies. A conventional model planned with the understanding acquired in this article could be the premise of a provenance the board framework that handles not just different stockpiling models, yet additionally various kinds of source and change provenance.	The paper researches which of the functionalities remembered for the classification conspire prohibit or infer one another. A portion of the issues confronted when managing provenance are identified with information incorporation issues. For instance the idea of semantic personality expected to	The paper highlights the needs of varied kinds of Provenance in the Open World Integration world and how Provenance Management can be complex in an integrated environment. However it does not give a conclusive solution how this could be achieved in a decentralized fashion.

	Source and change provenance are not totally free and it is fascinating to examine under which conditions it is feasible to change over one into the other and study how much repetition is presented by putting away source and change provenance.	perceive copies or forms of information things in an open world model are concentrated by different information mix distributions. A provenance the board framework taking care of various sort of information things put away in disseminated storehouses needs to coordinate this information to acquire a brought together view on the information. Information reconciliation frameworks may profit by counting provenance the executives. For instance, provenance information could be utilized to recognize copy bits of information or could assist a client with evaluating the nature of incorporated information.	

Hao Fan and Alexandra Poulovassilis 2005	Provides a DLT for virtual intermediate data and also using general schema tramsfromation pathway. An HDM (Hypergraph based Data Model) is represented as nodes, edges and transformations. Each transformation applies to one dimension only. IQL is used to transform the attributes and relations into a transformed schema upon which DLT is then applied.	Schema Transformation is applied to constructs in the data warehouse to trace the data lineage.	There is a delta to investigate the connection between our heredity following and view support calculations, to decide whether a coordinated methodology can be received for both.
Yogesh L. Simmhan Indiana University, Bloomington, IN Beth Plale Indiana University, Bloomington, IN Dennis Gannon Indiana University, Bloomington, IN 2005	Digital Object identifiers (DOI) are used to define and track provenance for how scientific workflow relates to the research results. Provenance can be applied at Data as well as Workflow level.	This document helps to classify provenance based on data source, storage and granularity. It also describes current tools available which can be used to generated provenance for workflow and databases. Objective if document is to create high level provenance taxonomy.	Ways to explore provenance for Phantom or deleted data sources needs further studies.

		It is accepted that properties of a change are given to the heredity following framework, either by the change creator or on the grounds that the change is a prepackaged segment with known properties. A different line of examination is that of inducing a change's properties, either by inspecting the particular (e.g., utilizing program examination strategies over the code), or by running example information through the change and analyzing the outcomes.	
The problem of data lineage tracing in data warehousing environments has been formally studied by Cui et al - 2000	Lineage tracking is done using Transformation Properties. Transformations are grouped into three categories: Aggregator - Context Free and Key Pre Backbox & Dispatcher The methodology depends on an assortment of change properties that hold every now and again by and by, and that can be indicated effectively by change creators. We introduced procedures for improving heredity following execution, including building files and joining changes with the end goal of ancestry following.	It is expected that a large portion of the work for ancestry following ought to be done at following time. That is, we would prefer not to exhaust impressive additional calculation or capacity cost during the stacking interaction only for heredity following.	The paper highlights the compromise on performance however does not propose a framework based approach for Provenance Storage which will take care of all scenarios

		The other limit is the explanation approach, where extensive extra data is processed and put away at stacking time to accelerate genealogy following. The choice of which outrageous to take is reliant upon the normal following responsibility, and on any presentation necessities for stacking or ancestry following. It very well may be fascinating to investigate center ground draws near, which register and store some measure of extra data for genealogy following, yet without bringing about excessive execution corruption at stacking time.	
Characterizing Provenance in Visualization and Data Analysis: An Organizational Framework of Provenance Types and Purposes - 2015 Eric D. Ragan, Alex Endert, Jibonananda Sanyal, and Jian Chen	This paper isn't intended to be a far reaching study of provenance writing in the field of representation. All things considered, it has dissected the numerous translations of others as a methods for making	Likewise with any system, the introduced association isn't great. It will probably have to change later on, furthermore, the qualifications among classes	The paper brings a Framework based approach for Data Visualization. It is a limited study and does not cover comprehensive scenarios. Moreover, the ppaer does not

	a structure that exemplifies the center employments of provenance in the field.	won't generally be perfect at present.	focus on the need of Trust for Framework creation.
Peter Buneman University of Edinburgh Edinburgh, UK opb@inf.ed.ac.uk Adriane P. Chapman University of Michigan Ann Arbor, MI 48109 apchapma@eecs.umich.edu James Cheney University of Edinburgh Edinburgh, UK jcheney@inf.ed.ac.uk - 2016	The exploration is to give a UI that is satisfactory to the keeper; that is, it ought not be excessively unique in relation to what is right now being utilized. The current practice much of the time is to utilize internet browsers to get and refresh data. Reimer and Douglas have researched convenience and engineering contemplations in the advancement of a model Web journal called NetNotes	The methodology can be joined with such frameworks to offer help for following the provenance of both duplicated and registered information with little change to current practice. It is right now taking a gander at expansions to the fundamental language of nuclear updates to dialects that permit "mass" refreshes. For instance, it is regular in curated data sets to duplicate reference information from standard sources, and it could be arduous to do this for a great many references, every one of which may should be rebuilt as per some standard formula. The specialized test here is to interface the semantics of a mass update	Nonetheless, provenance inquiries can at this point don't be replied with assurance. All things being equal, we can just say that some information may (or can't) have come from a given source area. This might be a satisfactory cost to pay to have the option to store straightforward provenance data considerably more proficiently for mass updates.

		language dependent on duplicate glue activities with that of standard dialects, for example, the question and update dialects of SQL. In this setting conditional provenance is most regular in light of the innate parallelism in customary update and inquiry dialects. To utilize gullible provenance would invalidate practically any type of question improvement. An option is to store surmised provenance records. The capacity required for estimated provenance stays corresponding to the size of the inquiry or update, so is immaterial contrasted with the necessities for the full provenance table.	
Provenance in Databases: Why, How, and Where By James Cheney, Laura Chiticariu and Wang-Chiew Tan	Why - the minimal set of witnesses that are needed to verify a query How - is the routes which are used to arrive at the query. The Why can be derived from the how but the	The paper is a detailed overview into the semantics of Provenance and helps to explain the PROV Model and its basic constructs	The paper brings the element of minimal Provenance Information needed for ensuring Trust. However, it does not classify the

	reverse is not possible. How provenance tells us how the source tuples witness the output query Where Provenance - tells us where in the database columns the Provenance was stored		Trsu Needs for Organizations
Why and Where: A Characterization of Data Provenance[25] Peter Buneman University of Pennsylvania Sanjeev Khanna University of Pennsylvania, sanjeev@cis.upenn.edu Wang-Chiew Tan University of Pennsylvania - 2001	Provenance is a class of meta-information with security needs that vary from those of ''conventional information''. Since provenance catches history it is changeless. The diagram that depicts the provenance is coordinated and non-cyclic. There are applications where this data should be gotten.	The paper contends that the security of the provenance is unique in relation to that of the information it portrays. How might provenance be gotten? Provenance can be demonstrated as an explained causality diagram. The conversation parts a security arrangement into subsystems for the information, traits and causality chart. Every one of these need access controls.	In contrast to the information and qualities, it isn't clear how to address security consents on the causality chart. Indeed, even with a security model for the causality diagram, there are collaborations among the three security subsystems.
Securing Provenance Uri Braun, Avraham Shinnar1, Margo Seltzer - 2006	The papers focus on the current challenges of Provenance Security and how it can be modelled	Provenance Security Models for sub systems are explained based on DAG Graphs based on attributes and data	it isn't clear how the three subsystems ought to associate all in all. The test is to develop a security model for causal charts and study how that model connects with security model for the characteristics and information.

A Security Model for Provenance Braun, Uri and Avi Shinnar - 2006	The security model partitions the assignment of ensuring provenance data into ensuring the progression of data — or structure — and securing the characteristic — or level — provenance data. This division permits us to build two straightforward security models. Each model works autonomously.	In the distinguished: presence, number, uniqueness, assignment and granularity as normal prerequisites.	Characteristics default to permitting the maker full authorizations, while at first giving every other person none. Indicating an assignment strategy is even less clear. We are not satisfactory how to gather assignment data from clients.
Introducing Secure Provenance: Problems and Challenges Ragib Hasan, Radu Sion - 2007	Unapproved parties don't approach data put away in any of the provenance records • Enemies can't produce a provenance record, for example change content in the provenance record Pi or present new produced records Pforged in Compact disc without being recognized (uprightness). • Approved inspectors can confirm the respectability of the possession succession of Compact disc without knowing the individual records Pi inside the chain (accessibility). • User ui is offered the mechanisms to selectively preserve the privacy of the provenance records	To avoid adversaries from masking illicit actions, certain designated auditors exist that can read any provenance chain.	The paper does bring in a Framework for Secure provenance. However there is still a gap where Provenance can be broken by designated auditors. This is due to the Decentralization Issue nott bieng addressed in the research.

	pertaining to her own actions, e.g., privacy them available only to a predefined subset of auditors		

13. Annex -2 – Literature Review for Blockchain Frameworks for Information Sharing

Document Name	Year	Findings	Inference	Gap
The role of trust in understanding the effects of blockchain on business models Rajala, Risto	2016	Blockchain innovation is a fundamental exchange development in data handling. It empowers trust-dependent exchanges between parties that were already unfit to confide in one another through a changeless exchange log and confirmation of request and legitimacy of exchanges, in addition to other things. Blockchain innovation is another approach to coordinate old advancements, like computerized marks, cryptography, and hash capacities, yet as a development it is exactly toward the	The most important conclusions of this research is in two parts. Most importantly, the examination explains the essential comprehension of blockchain innovation by introducing a structure for use case assessment and by opening the chance offered by blockchain to expand trust or to nullify the requirement for it in an exchange. Further, the part of trust in an industry appears to affect what sorts of changes blockchain	This is an important paper which focused on the importance of trust in organizations and its impact on Blockchain. However, it does not specifically focus on the area of Provenance and how trust impacts Provenance

		beginning of its advancement. This work concentrates how blockchain innovation could change plans of action, and particularly what is the job of trust in this change. The hypothetical casing for this investigation comes from trust writing. This investigation began with a writing survey, in view of which two speculations were made that were tried with a near contextual analysis of two organizations, one from energy and one from monetary administrations industry. The essential material was gathered from 25 meetings, each going on for about 60 minutes. Notwithstanding the two case organizations, the example included specialists from the ventures and blockchain trained professionals. In light of the meetings and other material, the specialist built three speculative use cases that both show how blockchain innovation can be utilized and present a chance for examination of plans of action.	can cause in plans of action. Blockchain innovation would thus be able to be viewed as both a mechanical and a plan of action development, and making a qualification between the two is significant. As a plan of action advancement, blockchain could disturb plans of action in a wide scope of ventures and geological areas.	

Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review	2017	Blockchain technology is expected to revolutionize the way transactions are performed, thereby affecting a vast variety of potential areas of application. While expectations are high, real world impact and benefit are still unclear. To be able to assess its impact, the first structured literature review of peer-reviewed articles is conducted. As blockchain technology is centered around a peer-to-peer network, enabling collaboration between different parties, the service system is chosen as unit analysis to examine its potential contribution. The author has identified a set of characteristics that enable trust and decentralization, facilitating the formation and coordination of a service system.	The paper provides relevant insights into the influence of Blockchain on the Industry and how the impact of Trust will significantly influence Blockchain applications in the industry.	This is an important paper which researched on the importance of trust in organizations and its impact on Blockchain. However, it does not specifically focus on the area of Provenance and how trust impacts Provenance
Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol	2015	M. Swan has laid the blockchain blueprint for the industry. She provides insights and use cases where Block Chain will be used in the industry	The effectiveness of Blockchain is highlighted through this paper in the Industry. Blockchain decentralization is a key factor that will influence its usage into the Industry	The trust factor is critical to the success of Blockchain. SCM Use cases which need Blockchain have been highlighted. However, this does not focus on the linkage between Trust, Provenance and Blockchain

A maturity model for blockchain adoption Huaiqing Wang1 , Kun Chen2* and Dongming Xu3	2016	The relative investigation technique is utilized to dissect various elements of the development model, which is fundamentally founded on the ordinarily utilized ability development model	Very importantly the paper highlights various Maturity Models and how the industry should analyze Blockchain based needs to identify what is the relevant maturity model	The paper does not focus on how Trust has a direct impact on Industry Adoption of blockchain.
Nachiappan, Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: BlockChain technology: beyond bitcoin. Applied Innovation Review	2016	The paper focusses on business applications of Blockchain and how relevant industries should identify the Blockchain needs	Blockchain provides multiple benefits to varied users. Based on the industry needs, the user should focus on the available Blockchain frameworks available and apply them to their specific needs	This paper does not focus on the specific needs of blockchain from the perspective of Provenance Security and Information Managements
Blockchain-based sharing services: What blockchain technology can contribute to smart cities	2016	The thought of smart city has developed well known in the course of recent years. It accepts a few measurements relying upon the importance of "savvy" and advantages from inventive uses of new sorts of data and correspondences innovation to help public sharing.	The paper gives empirical evidence how Blockchain will help enable Smarter Cities through the features of decentralization, Distributed Ledgers and a Trusted Protocols	The factor of Trust in Smarter Cities has not been analyzed. It does not analyze how by introducing the concept of Trust varied Blockchain Frameworks can be provided to the cities.
BLOCKCHAINS IN NATIONAL DEFENSE: TRUSTWORTHY SYSTEMS IN A TRUSTLESS WORLD	2014	This is a very useful insight provided to the US Govt how Blockchain Trust cam be used to provide additional security in Information Sharing and Defense discussions of the US Govt	The paper introduces Trust Based communication which is very essential for secure communication in the Defense Govt. It provides a Framework which can be used by the defense to use Blockchain effectively.	The paper does not treat Provenance separate from Blockchain. There is an integrated view of Information security and Provenance. This is acceptable for Defense where budget is not a constraint but in cases where budget is a constraint, then

			Information Sharing Used Trusted Protocols is used to enhance the security	only the Provenance racking will have to be considered.
Provenance Threat Modeling Oluwakemi Hambolu, Lu Yu, Jon Oakley and Richard R. Brooks Ujan Mukhopadhyay and Anthony Skjellum Where Is Current Research on Blockchain Technology?—A Systematic Review Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander		The security of the blockchain is ensured by keeping a cryptographically marked chain of secure hash esteems. Since this chain is put away at various destinations and is additionally being ceaselessly refreshed, it will be practically unthinkable for this chain to be controlled by fraudsters. With this capacity, the blockchain can guarantee the honesty and security of provenance information.	Blockchain Security does provide relevance to Provenance Storage. As future research, using cryptocurrency primitives. author will sharte a detailed security model for securing provenance metadata This indicates that currently there is no out of box security model in Blockchain for Provenance	Need for a Provenance Enabled Security Model for Blockchain
Where is current research on Blockchain Jesse, Chooi	2016	This paper collates current research focus works in blockchain	Research in blockchain is focused on frameworks, applications, blockchain security and Smarter Contracts	There is research in the areas of framework for Blockchain. However, there is no existing research in the area of Provenance Based Frameworks based on Trust
The bitcoin lightning network, Prron & Dryja	2016	This paper provides an insight on how Blockchain will overcome TPS issues by implementing a Lighting Network protocol	Lightning Network has been applied to micro transactions where inthe required Transaction Speed (TPS) is much more than the existing 7 TPS of bitcoin	The paper focusses on Lightning Network applications for Blockchain. However, it does not evaluate the applicability of the same framework for Information Provenance, which

				could be a relevant area.

14. Annex -3 – Literature Review for Organization Information Sharing Behaviours

Document Name	Year	Findings	Inference	Gap
Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework	2014	The reason for this paper is to investigate what hypothetical focal points have been utilized to dissect and comprehend data partaking in supply chains. The paper expounds on the prevalent hypotheses and examines how they can be incorporated to investigate various parts of data sharing.	The discoveries recommend that four out of ten looked into articles unequivocally apply at least one hypothetical focal points. The prevalent hypotheses utilized incorporate exchange cost financial aspects, possibility hypothesis, asset based view, asset reliance hypothesis and social administration speculations like the social view and social trade hypothesis.	The literature does not give how to improve the Information Sharing with Partners. It is a good analysis, but does not give the mechanisms how Information sharing can be improved
Supply chain information and relational alignments: mediators of EDI on firm performance Keah Choon Tan (College of Business, University of Nevada Las Vegas, Las Vegas, Nevada, USA) Vijay R. Kannan (Jon M. Huntsman School	2010	The motivation behind this paper is to look at the impacts of inter-organization data trade on production network data and social arrangement. Drawing on writing on data frameworks, production network the executives, and coordinations, the paper intends to introduce a	The paper presents a varied framework for considering electronic data interchange (EDI) progress in vendor management and its effect on information and relational verification. It provides a single framework for	The paper provides a single framework for Information Exchange. In addition it focusses on the conventional approaches for Information Security, but not consider Fraud as a threat to information exchange. Also, it

of Business, Utah State University, Logan, Utah, USA) Chin-Chun Hsu (College of Business, University of Nevada Las Vegas, Las Vegas, Nevada, USA) G. Keong Leong (College of Business, University of Nevada Las Vegas, Las Vegas, Nevada, USA)		multidimensional system for considering electronic information exchange (EDI) reception in provider the board and its impact on data and social arrangement.	inter organization information exchange which is secure	does not consider the decentralization aspect of information exchange
Examining the Impact of Interorganizational Systems on Process Efficiency and Sourcing Leverage in Buyer–Supplier Dyads Khawaja A. Saeed, Manoj K. Malhotra, Varun Grover	2005	Assembling firms are progressively looking for cost and other upper hands by firmly coupling and dealing with their relationship with providers. Among different instruments, interorganizational frameworks (IOS) that work with limit traversing exercises of a firm empower them to successfully oversee various sorts of purchaser provider connections. The exploration incorporates writing from the activities and data frameworks fields to make a joint viewpoint in understanding the linkages between the idea of the IOS, purchaser provider connections, and assembling execution at the dyadic level. Outer incorporation, expansiveness, and commencement are utilized to catch IOS usefulness, and their	The investigation investigates the distinctions in how assembling firms use IOS while working under changing degrees of cutthroat force and item normalization. To test the examination models and related theory, exact information on purchaser provider dyads is gathered from assembling firms. The outcomes show that lone more elevated levels of outer mix that go past basic acquirement frameworks, just as who starts the IOS, permit producing firms to upgrade measure effectiveness.	The paper is a good analysis which highlights the needs for IT automation in the industry for exhange of information to increase productivity. However, it does not focus on how the IT Innovation can be put into frameworks in order to increase process efficiency

		impact on measure productivity and sourcing influence is analyzed.		
Inter Orgainizational communication as a relational competency Antony Paulraja, , , Augustine A. Ladob, 1, , Injazz J. Chenc,	2007	Between hierarchical correspondence has been reported as a basic factor in advancing vital cooperation among firms. This paper, looks to broaden the flood of examination in inventory network the executives by deliberately researching the forerunners and execution results of between authoritative correspondence. In particular, between hierarchical correspondence is proposed as a social ability that may yield competitive edges for inventory network accomplices.	Utilizing underlying condition displaying, it exactly tests various theorized connections dependent on an example of more than 200 US firms. The outcomes offer solid help for the idea of between hierarchical correspondence as a social skill that improves purchasers' and providers' presentation.	The paper brings deep insights into the importance and significance of inter organization communication mechanisms by using empirical values. However, it does not delve into the area of Framework based Organization communication needs ot recommendations on how to increase the communication
Knowledge sharing—A key role in the downstream supply chain Stephen C. Shiha, , , Sonya H.Y. Hsub, 1, , Zhiwei Zhuc, 2, , Siva K. Balasubramaniand	2012	The paper explores the role of knowledge sharing against a downstream two-MODE supply chain. Drawing on chaos theory and the literature on knowledge	This paper focusses on knowledge sharing in a SCM environment. It verifies the importance of Knowledge Sharing and how it helps to	The paper does not look at the aspect of security in Knowledge Sharing and on the risks of Knowledge Sharing when it reaches the corrupt resources

		management, it contrasts the information and knowledge sharing contexts. It provides a real-world case study of knowledge management methodology at a U.S. Fortune forty firm.	increase the productivity of the organization	
The Role of Trustworthiness in Reducing Transaction Costs and Improving Performance: Empirical Evidence from the United States, Japan, and Korea Jeffrey H. Dyer and Wujin Chu	2003	This paper researches the connection between provider trust in the purchaser and exchange expenses and data partaking in an example of 344 provider automaker trade connections in the US, Japan, and Korea.	The discoveries demonstrate that apparent dependability decreases exchange costs and is associated with more noteworthy data partaking in provider purchaser connections. In addition, the discoveries recommend that the worth made for exchange, as far as lower exchange costs, might be generous.	The paper highlights the benefits of Trust been suppliers. However, it does not delve into the area of Electronic Information Sharing and how Trust will reduce the cost of electronic sharing
A strategic analysis of inter organizational information sharing Jingquan Lia, Riyaz Sikorab, , , Michael J. Shawa, Gek Woo Tanc	2005	This paper considers the impact of entomb hierarchical data sharing systems on firm level execution under both steady just as unstable economic situations. It utilizes data trade in a store network as a portrayal of entomb hierarchical data sharing, and studies five systems for data sharing that range from negligible to approach total	The paper presents logical assessment of the general exhibition of these methodologies and test results from a proof-of-idea framework. The outcomes show that close total data sharing that joins more than one sort of data being shared has better execution in unstable economic situations	The paper focusses on stage of Information Sharing which is an important perspective of inter department sharing. In volatile markets, where information is not complete, it still focusses on information sharing. However, the paper does not focus on an audit trail which is needed to track this information, since

		data trade.		the information is in transit stage, the audit log aspect should have been analyzed
Information sharing and supply chain performance: the role of connectivity and willingness Stanley E. Fawcett , Paul Osterhaus	2007	The exploration zeroed in on two unmistakable measurements to data sharing – network and ability – are recognized and dissected. There is a hidden need of readiness in the association before Data stream begins	Two particular measurements to data sharing – network and readiness – are distinguished and dissected. The two measurements are discovered to affect operational execution and to be basic to the improvement of a genuine data sharing capacity. Nonetheless, numerous organizations are found to have set the majority of their accentuation on network, frequently neglecting the readiness build. Subsequently, data sharing rarely follows through on its guarantee to empower the production of the durable inventory network group.	The research focused on willingness and connectivity. However, it does not introspect in the areas of Fraud and Trust which are also key factors to a successful information sharing for data flow
Flow Coordination and Information Sharing in Supply Chains: Review, Implications, and Directions for Future Research	2002	Advances in data innovation, especially in the e-business field, are empowering firms to reconsider their inventory network methodologies and investigate new roads	The paper brings out areas where Information Sharing can be improved by using automated IT Tools in the e-business area	The gap in the Information flow is in research of domains of decentralization and the need to remove a central

		for between authoritative collaboration. Be that as it may, an inadequate comprehension of the worth of data sharing and actual stream coordination impede these endeavors. This exploration endeavors to help fill these holes by looking over earlier examination around there, sorted as far as data sharing and stream coordination.		coordinator of information
Benefits of information sharing with supply chain partnerships[115] Zhenxin Yu Hong Yan T.C. Edwin Cheng	2001	The force of data innovation can be bridled to help production network individuals build up organizations for better inventory network framework execution. Inventory network organizations can alleviate lacks related with decentralized control and lessen the "bullwhip impact". This investigation delineates the advantages of inventory network associations dependent on data sharing.	For a decentralized production network including a producer and a retailer, it determines the individuals' ideal stock arrangements under various data sharing situations. It shows that expanding data dividing between the individuals in a decentralized store network will prompt Pareto improvement in the presentation of the whole chain. In particular, the production network individuals can receive rewards as far as decreases in stock levels and cost reserve funds	The paper highlights the importance of decentralization for information sharing across Supply Chain Providers. However, it does not discuss about Audit Log and tracking of information sharing between the partners

			from framing associations with each other. A contextual analysis is accommodated representation.	
Incentive and Trust Issues in Assured Information Sharing Ryan Layfield, Murat Kantarcioglu, and Bhavani Thuraisingham	2009	This paper investigates the impacts of various motivating forces and potential trust issues among associations on the guaranteed data sharing interaction by fostering a developmental game hypothetical system. At the point when enough players pick a conduct that mirrors the way to deal with discipline, the malignant practices were effectively disposed of from thought. The fundamental idea of Living Specialist permitted it to overcome even variations of its own conduct including light mounts of deviation. Notwithstanding, a similar nature of the persevering confirmation implied that the conduct didn't prevail against the Fair conduct, which played out no check at all in spite of the conditions. Indeed, even in these	There are known issues and challenges in Information Sharing. This paper uses a penalty based approach to combat these issues	This paper talks of a punishment based approach to combat issues in Information Sharing. However, it does not look at a proactive approach where provenance security can be used to resolve the issues of Provenance

		conditions, the ideal circumstance actually emerged, permitting players to infer that genuineness is without a doubt the most ideal decision.		

15. Annex – 4- Literature Review for Theoretical Premise

Theme	Document Name	Findings	Inference	Gap
Influence of TCE on Information Sharing between Organizations	"Information sharing with key suppliers: a transaction cost theory perspective Ogan M. Yigitbasioglu (Department of Accounting, Hanken School of Economics, Helsinki, Finland)" - 2010	The aftereffects of the examination propose that (natural and request) vulnerability and interdependency can somewhat clarify the degree of data divided among a purchaser and key provider. The Dangers of Data Sharing are too high to even consider utilizing a fit all Model. Thus the investigation suggests altered structures.	This investigation of exchange cost hypothesis to the neo traditional hypothesis of Data Sharing. With this discovering, exchange cost financial matters can give an important focal point which to see and decipher interorganizational data sharing. Likewise dependent on Hazard Investigation it is emphatically prescribed to have a redone System for Data sharing and not utilize a solitary model fit all methodology.	There is a connection among's Hazard and Data Sharing dependent on TCT. It additionally discusses taking care of Dangers at singular Client levels. Anyway the hypothesis treats Hazard comprehensively and doesn't think about the effects of Provenance on the Danger attribution.

	Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework Joakim Kembro , Kostas Selviaridis , Dag Näslund - 2014	The reason for this paper is to investigate what hypothetical focal points have been utilized to dissect and comprehend data partaking in supply chains. The paper explains on the transcendent speculations and examines how they can be incorporated to explore various parts of data sharing.	The discoveries propose that four out of ten evaluated articles expressly apply at least one hypothetical focal points. The dominating speculations utilized incorporate exchange cost financial aspects, possibility hypothesis, asset based view, asset reliance hypothesis and social administration hypotheses like the social view and social trade hypothesis.	The literatute does not give how to improve the Information Sharing with Partners. It is a good analysis, but does not give the mechanisms how Information sharing can be improved
	Information sharing in supply chains, myth or reality? A critical analysis of empirical literature Joakim Kembro, Dag Näslund - 2016	The motivation behind this paper is to examine what exact proof exists with respect to advantages of data partaking in supply chains, and to recognize expected holes and openings in this exploration region.	The author could not find empirical evidence to prove the benefits of Information Sharing across Organizations. Hence the research is left open	Given the absence of proof for the asserted advantages of data sharing on an inventory network level, more examination is required in this field. The creators in this manner propose a plan for future examination expanding on four central issues.
	Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations Meng-Hsiang Hsua,, Teresa L. Jub , Chia-	This paper focusses on the benefits of Information Sharing between organizations	The paper reiterates the importance of Trust in Information Sharing	The paper does not convey how Trust Increase can happen

	Hui Yenc , Chun-Ming Changa			
	Inter-organizational relationships and information sharing in supply chains Jao-Hong Cheng∗ 2010	This paper presents an examination model to analyze factors affecting data sharing and execution in between authoritative connections. The model contains seven examination theories with six builds, including social advantages, social proclivity, connectedness, power balance, useless struggle and data sharing. The develops are estimated by very much upheld measures in the writing. The speculations are tried through an experimental investigation of supply chains. Information are gathered from 589 assembling firms	The aftereffects of the observational examination propose that the pretended by social advantages is basic in guaranteeing the data sharing as it builds up the connectedness between inventory network individuals and mitigates the useless contentions all the while. The discoveries of the investigation give valuable bits of knowledge into how inventory network individuals ought to support their communitarian practices and exercises in order to improve their social advantages and connectedness and thusly upgrade data sharing for the production network all in all.	The study provides deep insights into factors that positively influence Information Sharing. However the derived benefits of Provenance Security are not included in the ppaer.
	"Interagency Information Sharing: Expected Ben efit s , Manageable Risks Sharon S. Dawes" 1996	This study is focused on government organizations. It shows the benefits of Information Sharing. It also talks of the risks and challenges of	Information Sharing incurs cost which is not planned Five attitudes of employees were gathered that influence the Inter Organization	The study focusses on the costs of Information Sharing. However, it does not focus on the risks of Information Sharing and how

		Information Sharing	Information Sharing behaviors	that adversely adds to the cost
	Supply chain information and relational alignments: mediators of EDI on firm performance Keah Choon Tan, Vijay R. Kannan , Chin-Chun Hsu , G. Keong Leong 2010	The reason for this paper is to look at the impacts of inter-organization data trade on production network data and social arrangement. Drawing on writing on data frameworks, store network the board, and coordinations, the paper intends to introduce a multidimensional system for considering electronic information trade (EDI) appropriation in provider the executives and its impact on data and social arrangement.	Results support the focal reason that organizations should consider EDI reception in provider the executives to improve data and social arrangement between production network accomplices. It is through this arrangement that organizations accomplish prevalent execution.	This investigation utilized a solitary respondent from each firm because of cost contemplations, and consequently may have influenced the inter-rater unwavering quality of the review information.
	Acquisti A., Gross R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Danezis G., Golle P. (eds) Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, vol 4258.	Online informal communities like Friendster, MySpace, or the Facebook have encountered outstanding development in participation as of late. These organizations offer alluring methods for cooperation and correspondence,	The security risks have been classified based on various factors such as Age and Demographics. Age and Student Status are the key factors that influence the Security risk in Peer to Peer Sharing	The study plans to research further traits. However the study does not give mechanics of how to reduce the risks of the Privacy Concerns

	Springer, Berlin, Heidelberg - 2006	yet in addition raise protection and security concerns. When the guidelines of irrefutable trust are systematized, controllers can let loose information dividing among confided in parties. To forestall misuse, they ought to require extra protects and responsibility instruments.		
	The Impact of Product, Market, and Relationship Characteristics on Interorganizational System Integration in Manufacturer-Supplier Dyads Grover and Saeed 2014	A survey of writing on reception and utilization of electronic information trade (EDI) frameworks (a sort of IOS) shows that this issue has been analyzed from different hypothetical points of view. Analysts have inspected how possibilities identified with innovation, association, and climate shape EDI use. Restricted consideration has been coordinated toward seeing what conditions under which exchanges are led mean for the utilization of IOS. We contend that	Information risks are very high hence it is proposed to avoid the build once and fit all approach of Information Sharing with partners	The paper recommends an approach of custom build frameworks for communication wih partners. However there is no implementations of frameworks that recommend how to do the categorization or differentiation with partners for the customized frameworks

		value-based qualities are significant precursors to IOS combination and recommend that request vulnerability, intricacy, market fracture, and market instability catch key attributes. These components combined with an open data sharing climate are theorized to impact IOS mix. From an administrative viewpoint, IOS reconciliation is the fitting setup under states of high item intricacy and open data sharing climate, yet it blocks the firm from taking an interest in the open market and acquiring financier benefits.		
	Securing electronic health records without impeding the flow of information Rakesh Agrawal1, Christopher Johnson - 2007	The paper presents for the Wellbeing Business a coordinated arrangement of advances, known as the Hippocratic Data set, that empower medical care endeavors to conform to protection and security laws without	The exploration affirms that arrangements concerning the exposure of electronic wellbeing records can be dependably and proficiently authorized and examined at the information base level. It further exhibits that	The study does not consider scenarios where Fraud done by external parties can cause corruption in the Medical Industry. It only considers the scenario of security in Medical Information when there is no

		obstructing the genuine administration, sharing, and investigation of individual wellbeing data.	cutting-edge information mining and anonymization methods can be utilized to examine total wellbeing records without uncovering singular patient personalities. At long last, it shows that web administrations and commutative encryption can be utilized to share delicate data specifically among self-sufficient substances without bargaining security or protection.	External or Internal Fraud
	The Economics of Organization: The Transaction Cost Approach Oliver E. Williamson	The exchange cost way to deal with the investigation of financial association views the exchange as the essential unit of examination and holds that a comprehension of exchange cost conserving is integral to the investigation of associations.	The exchange cost way to deal with the investigation of monetary association views the exchange as the essential unit of examination and holds that a comprehension of exchange cost streamlining is integral to the investigation of associations.	The cost of Transaction has been studied at a Micro level including the impact of Power in the Organization. However it does not delve into the beneficial impact of Intra Organization Information sharing on TCE
	Strategic Flexibility in Information Technology Alliances: The Influence of Transaction Cost Economics and Social Exchange Theory Candace Young-Ybarra ,	Using a model drawn from both exchange cost financial aspects and social trade hypothesis, the exploration breaks down determinants of vital adaptability in an example of key	Discoveries show that, when all is said in done, determinants recommended by exchange cost financial aspects gave adaptability in adjustment and rigidity in exit. From social trade	The paper does a detailed study of Information Sharing and its impact on Trust. However, this focused on the social aspects of Information Sharing and does not explore the

	Margarethe Wiersema	collusions engaged with joint advancement arrangements or joint examination agreements.	hypothesis, trust was discovered to be emphatically identified with the two sorts of adaptability while another segment of social trade hypothesis, reliance, was discovered to be adversely identified with the essential adaptability of the partnership. Results likewise found that elements recommended by both exchange cost monetary hypothesis and social trade hypothesis were identified with the idea of trust.	impact of Information technology and how this would impact Trust in Information Sharing in a social background.
	Inter-organizational relationships and information sharing in supply chains Jao Hong Cheng 2011	The paper focusses on benefits of Inter Organization Communications and the electronic methods used for communication. Dysfunctional conflict has a positive influence on Organization Information Sharing	It provides positive recommendations how supply chain members should increase their communication skills	The study focusses on Information Sharing strategies however does not consider the techniques using which inter organization communication can be increased

16. Annex 5 - Data Analysis - NVivo

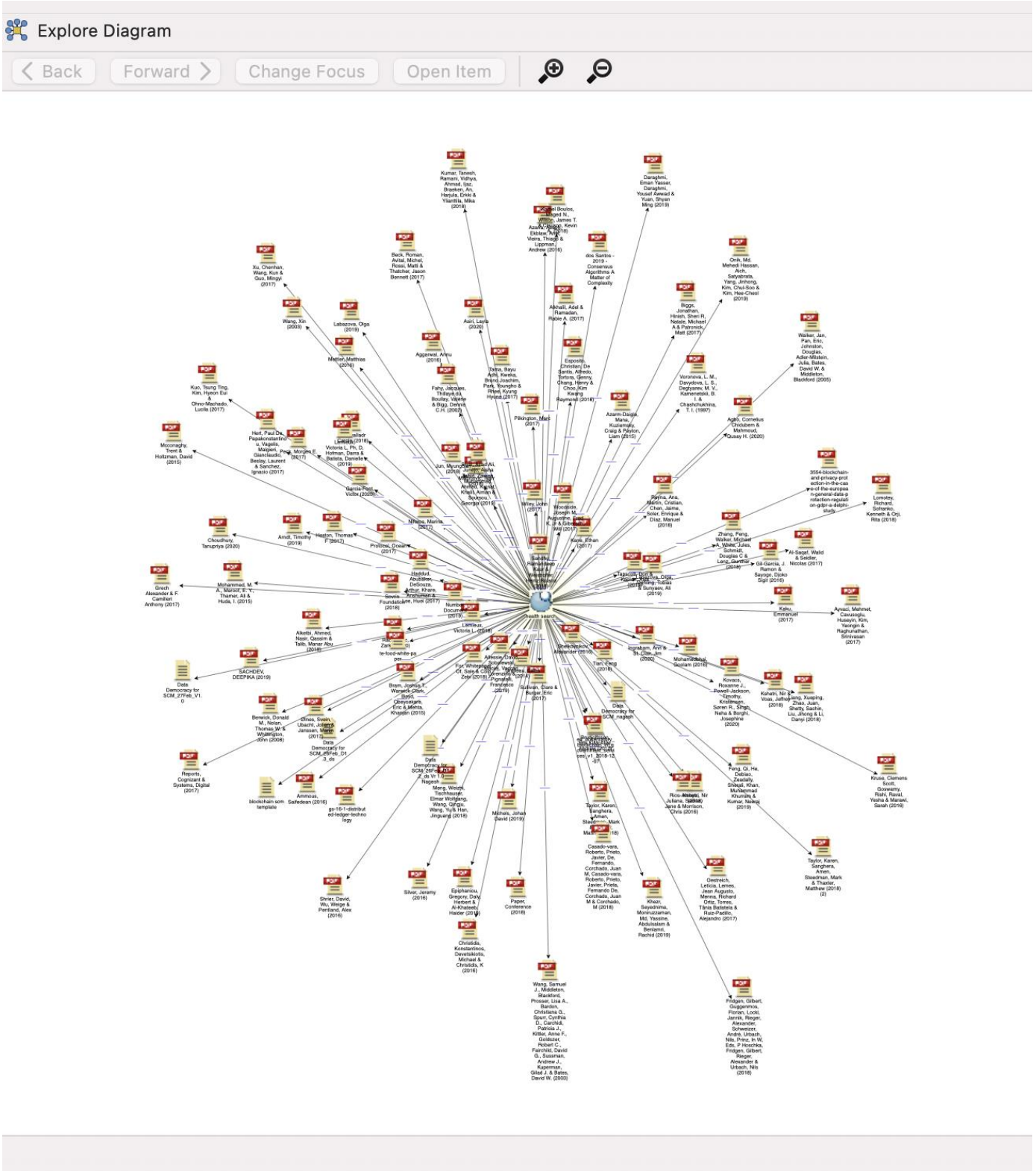


Figure 26: Healthe Care Node Analysis

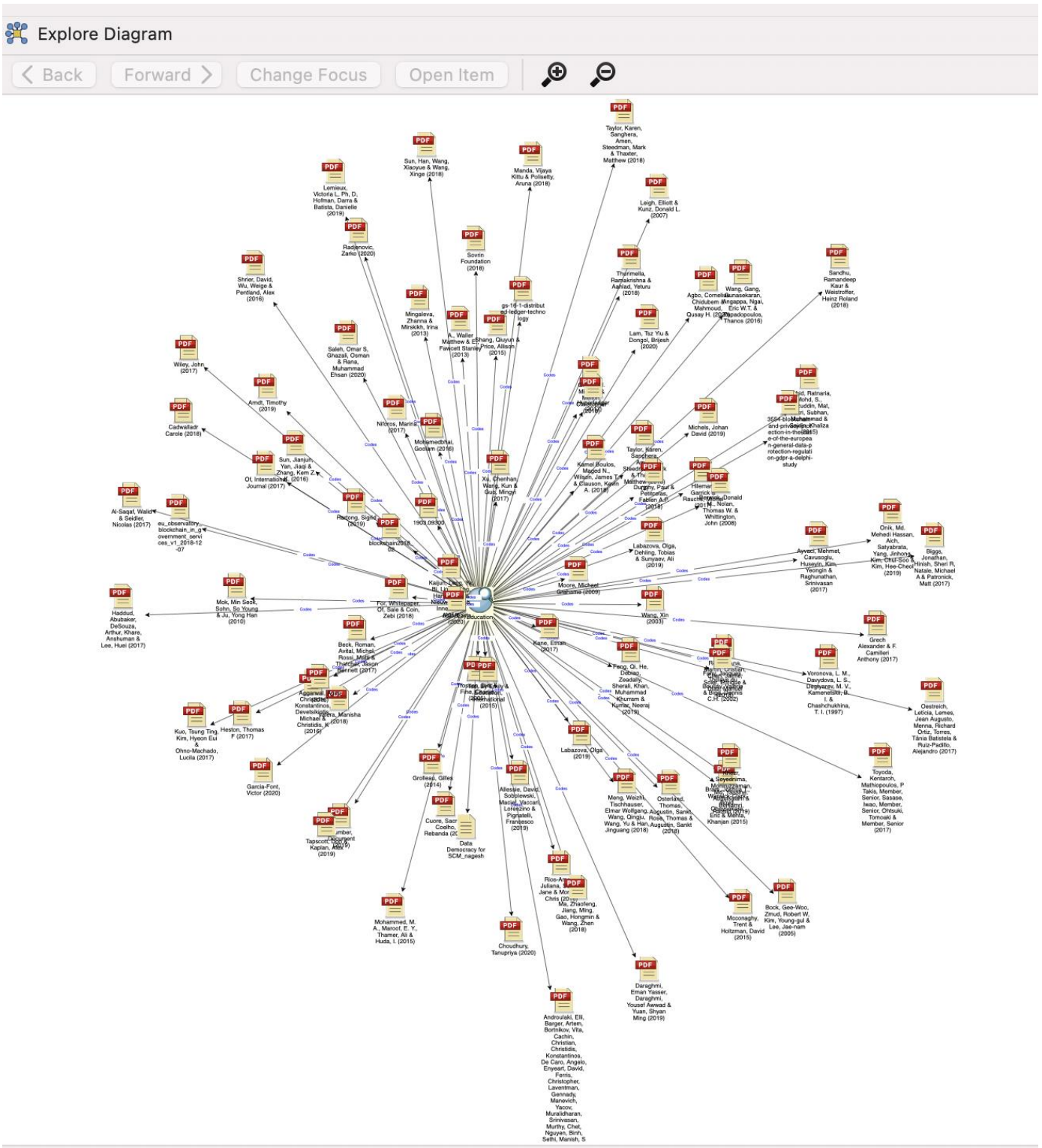


Figure 27: Education Node Wise Analysis

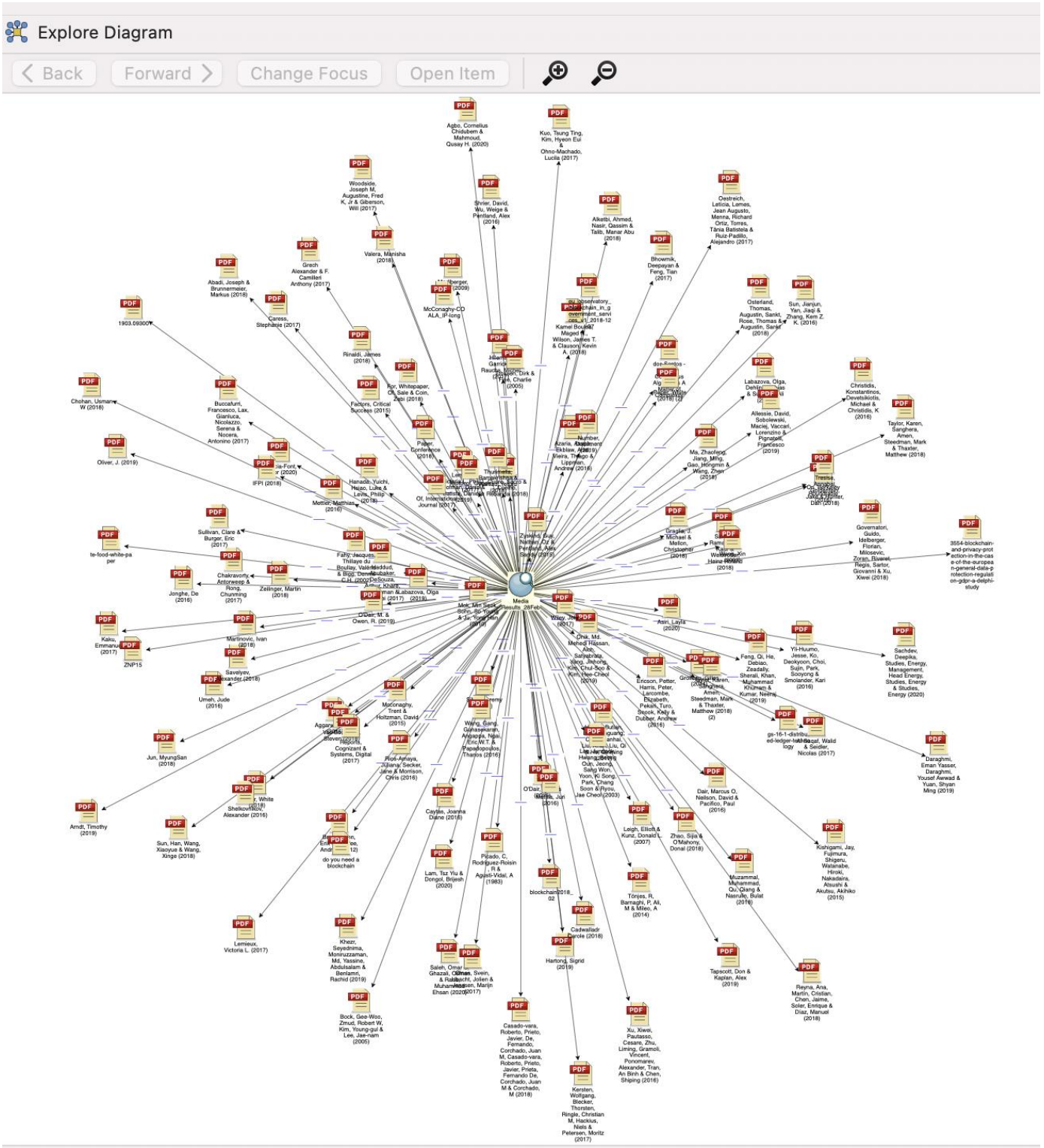


Figure 28: Media Node Analysis

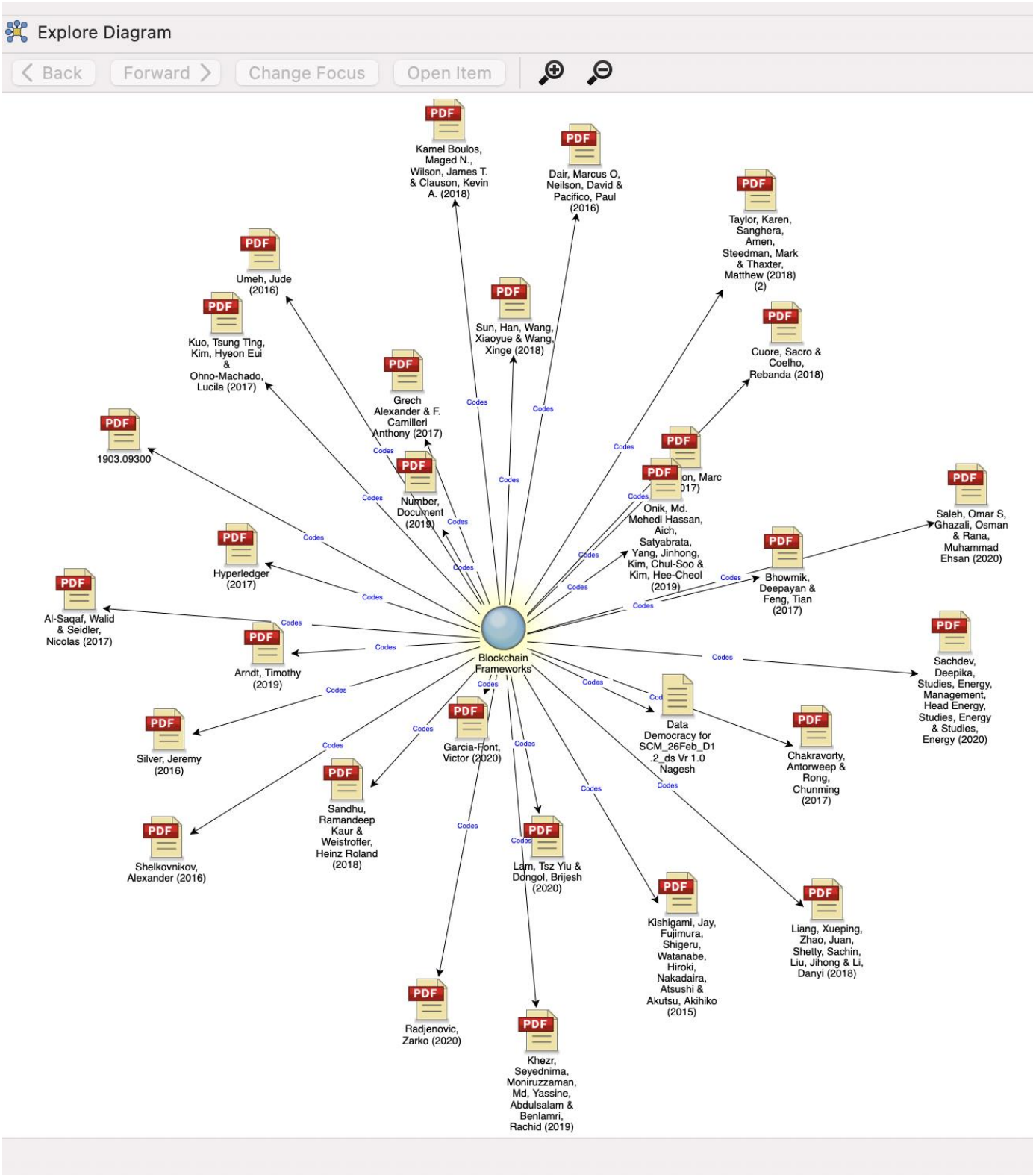
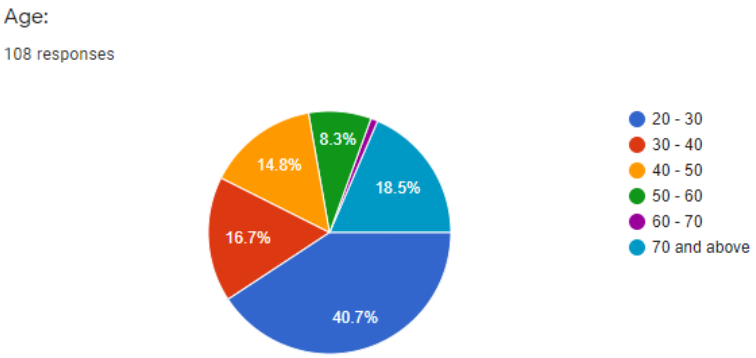


Figure 29: Blockchain Node Wise Analysis

17. Annex 6 – Responder Profile for Survey

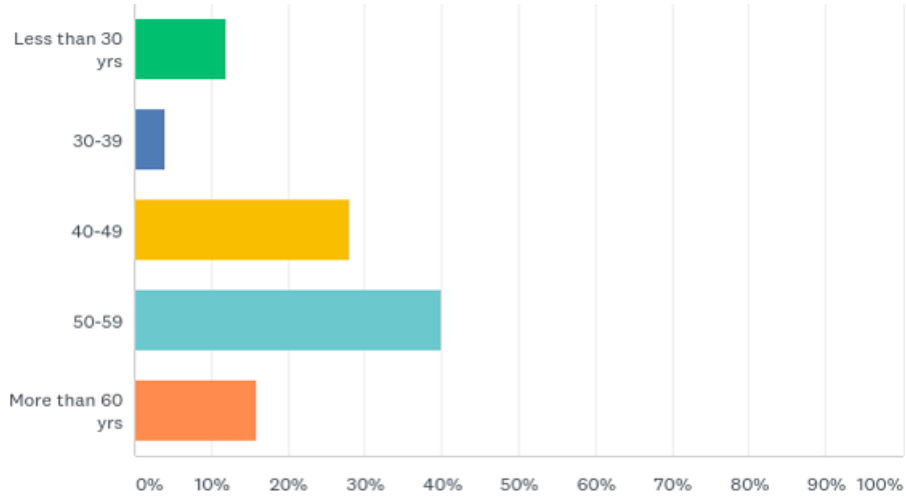
17.1 Health Care

Characterizing based on Profile Information the researcher understands the distribution of expertise, the strength (and durations) of their attachments to current jobs, and seniority in the Organization. There is a common concept that Information Sharing is dominated by Younger respondents who are open to newer ideas. Hence Research Questions were focussed on Age, Demographics, Profession, and Seniority. This will also help us determine the Cost of Information Sharing in the Organization.

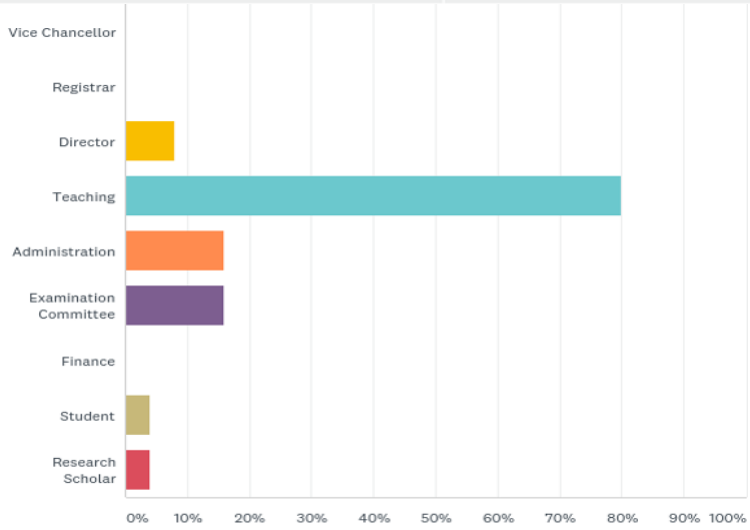


17.2 Education

As part of the survey, our respondents are employees working across all departments of Education including Administration, Teaching, Examination Committee, Admission Committee. The respondents vary from an Age Group of 30-60+ with majority of them in the 50-59 age group.



ANSWER CHOICES	RESPONSES	
Less than 30 yrs	12.00%	3
30-39	4.00%	1
40-49	28.00%	7
50-59	40.00%	10
More than 60 yrs	16.00%	4
TOTAL		25



17.3 Media:

The following is the profile of the survey responders:

Gender	Age Group	City/Country	Names of the platforms used for sharing the content	Select your Department	Experience in Media Sector	Number of people working in the group/organization
Male	Less than 30 years	Bangalore	Youtube	Content Creator/artist	0 - 1 year	7
Female	Less than 30 years	Dehradun	YouTube	Content Creator/artist	0 - 1 year	0
Male	Less than 30 years	Nagpur/India	Instagram, youtube, facebook	Content Creator/artist	3 - 5 year	6

Male	Less than 30 years	Patna	YouTube	Content Creator/artist	0 - 1 year	1
Male	Less than 30 years	Bihar	YouTube	Content Creator/artist	0 - 1 year	1
Male	Less than 30 years	Dehradun	YouTube	Content Creator/artist	0 - 1 year	1
Male	Less than 30 years	Nagpur	Youtube	Producer	3 - 5 year	5
Male	Less than 30 years	Mumbai / India	Youtube	Content Creator/artist	More than 5	50

Based on the analysis we conclude that:

1. 100% youth is involved in information sharing in media sector
2. The most common platform for sharing the information is 'YouTube', as it is an open platform and no investment is needed for sharing or uploading the content.
3. Out of 8 respondents, 7 are content creators/artists who are involved in information sharing.
4. Based on the channel or the type of content shared the number of people involved varies for each respondent, where the maximum is = 50 and the minimum is = 1.

18. Annex - 7 - Glossary

Information

- Refers to the information as well as knowledge sharing and exchange of data among independent organizations.

- **Digital Information**
  - Refers to any piece of Information which resides in Digital Format such as Documents, Databases or Processes

- **Provenance of Digital Information**
  - Refers to the origin, context, derivation, ownership or history of the Digital Information
  - *Provenance* is meta-data that denotes and characterizes the ancestry of an object.

Plagiarism Report

UPES

PLAGIARISM CERTIFICATE

1. We Dr S.K.Pokhriyal (Internal Guide), Dr Subir Purkayastha (Co Guide/ External Guide) certify that the Thesis titled

Framework of Provenance Tracking of Digital Information using Blockchain

submitted by Scholar Mr/ Ms Deepika Sachdev having SAP ID 500049525 has been run through a Plagiarism Check Software and the Plagiarism Percentage is reported to be 3 %.

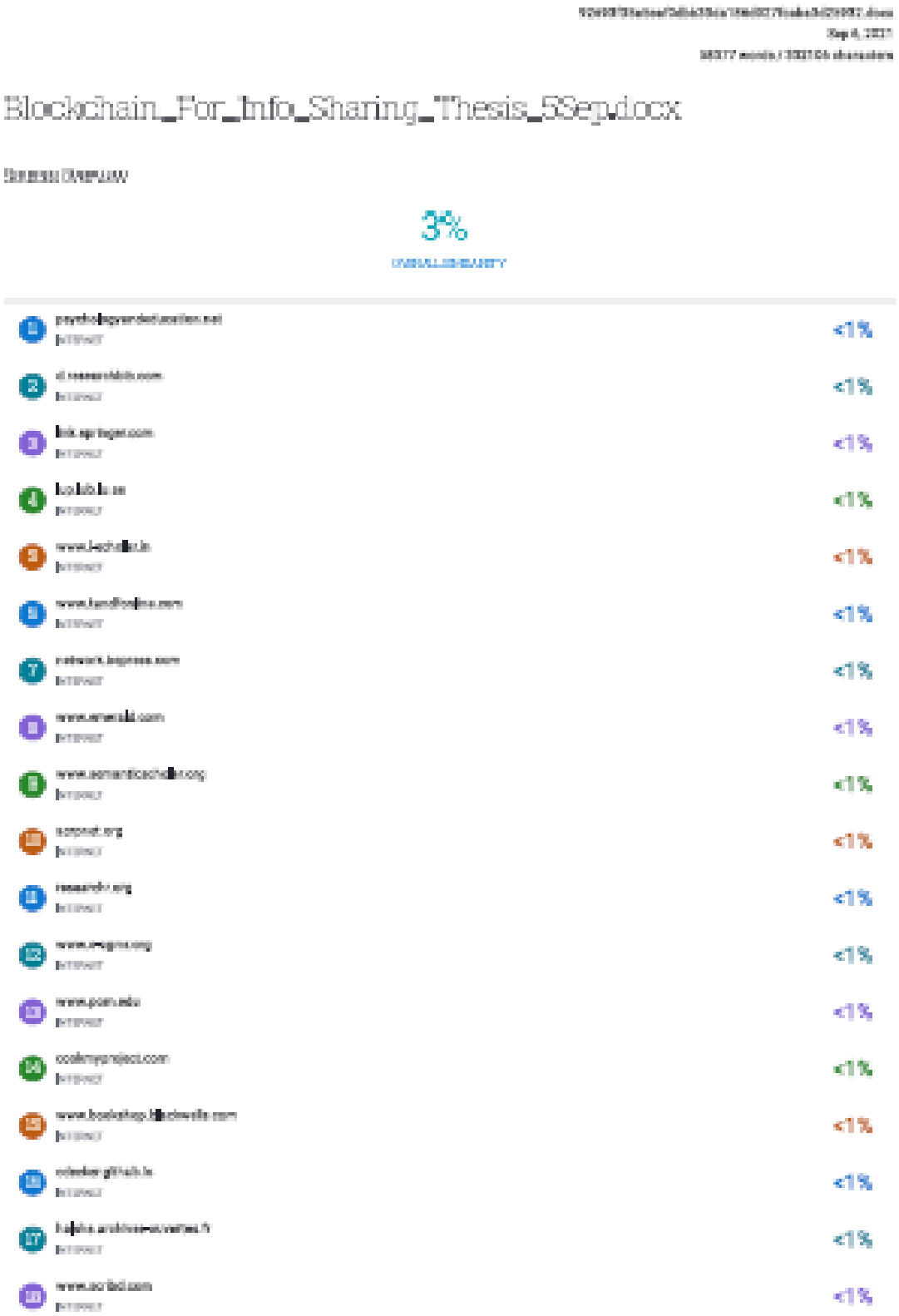
2. Plagiarism Report generated by the Plagiarism Software is attached.

Signature of the Internal Guide

Signature of External Guide/Co Guide

Signature of the Scholar

Similaarity Index Report



19	[illegible] INTERNET	<1%
20	www.[illegible].org INTERNET	<1%
21	discovery.ucl[illegible].uk INTERNET	<1%
22	dokumen.pub INTERNET	<1%
23	vbio.wfl.edu INTERNET	<1%
24	pub[illegible].fraunhofer.de INTERNET	<1%
25	repository.upenn.edu INTERNET	<1%
26	dr.ntu.edu.sg INTERNET	<1%
27	www.deepdyve.com INTERNET	<1%
28	[illegible].academic-oup.com INTERNET	<1%
29	[illegible].lsi.psu.edu INTERNET	<1%
30	www.apologeticsprofessionalism.com INTERNET	<1%
31	bonsaiscience.or.kr INTERNET	<1%
32	[illegible]@dallas.edu INTERNET	<1%
33	www.[illegible].nl INTERNET	<1%
34	[illegible].org INTERNET	<1%
35	www.[illegible].com INTERNET	<1%
36	academic.oup.com INTERNET	<1%
37	[illegible].[illegible].com INTERNET	<1%
38	[illegible].[illegible].org INTERNET	<1%
39	www.[illegible].com INTERNET	<1%
40	[illegible].org INTERNET	<1%
41	[illegible]-[illegible].[illegible].com INTERNET	<1%
42	[illegible].[illegible].com INTERNET	<1%

29	en.wikipedia.org Internet	<1 %
30	www.mendeley.com Internet	<1 %
31	www.myassignmenthelp.com Internet	<1 %
32	scribd.com Internet	<1 %
33	"Transaction cost theory", Salem Press Encyclopedia, 2018 Publication	<1 %
34	eprints[redacted].ac.uk Internet	<1 %
35	eprints.usm.edu.my Internet	<1 %
36	[redacted].be Internet	<1 %
37	www.researchgate.net Internet	<1 %

Excluded search repositories:
- None

Excluded from Similarity Report:
- Small Matches (less than 8 words)

Excluded sources:
- None