International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Academic and Commercial Circles in Block Chain Secure Privacy and Scalability at Block Chain Technologies

Sony Kumari*[1], **Dr. Manoj Eknath Patil**[2]

Submitted: 28/11/2023 **Revised**: 08/01/2024 **Accepted**: 18/01/2024

Abstract: In today's world, technological advancements and high-speed internet are indispensable in our daily lives, but these advancements come with their own set of challenges, especially in security. Blockchain technology, one of the most significant innovations in recent years, is gaining attention for its security applications across various sectors, including supply chain management and shipping. The education sector, particularly higher education institutions, is now exploring the use of blockchain to enhance teaching, learning, and collaboration among key stakeholders like students, teachers, and parents. Applications such as e-transcripts, digital degrees, certifications, cloud storage, and identity management stand to benefit from blockchain integration. This ongoing research delves into the potential application of blockchain in education, a topic that has recently garnered much interest across various industries. The study aims to provide a comprehensive overview of the current state of blockchain in education, which could inform future initiatives in this area. A thorough review of scholarly articles was undertaken, focusing exclusively on works that discuss blockchain in the context of education. Eleven different databases were meticulously searched to identify relevant publications, and 28 significant papers were selected for examination. To ensure objectivity and minimize biases in selection and analysis, three researchers were involved in the review process. Their analysis of the selected papers yielded crucial insights, addressing questions about the current application of blockchain in education, its beneficial features for the sector, and the challenges that need to be addressed for its wider adoption. This led to the development of several proofs of concept for blockchain in education. Blockchain can be widely implemented in the educational sector, several key challenges need to be addressed, including technical, legislative, and academic hurdles. Overcoming these challenges is essential for the successful integration and utilization of blockchain technology in educational settings.

Keywords: *Blockchain Technology, Supply Chain Management, Stakeholders, Educational Sector, E-Transcripts.*

1. Introduction

It was Satoshi Nakamoto, the mysterious man behind Bit coin’s creation, who first used the distributed ledger technology known as Block chain in his work. Incorporating multiple technologies, block chain has a distinct commercial value. It is this shared ledger, which operates as the only source of truth in commercial transactions that is enabled by Block chain. There is no longer a requirement for a centralized authority to verify the transactions on the Block chain platform. In both Permission and Non-Permission models, Block chain may be employed. Education, government, banking, health care, logistics, cyber security, the media and the law are just a few of the many industries that might benefit from using these models. Across the world and in the United States, there are a number of initiatives underway to adopt Block chain-based applications. There have been successful pilot deployments and proof-of-concepts (Pocks). There is a need for a national strategy on Block chain technology in order to realize the advantages of this technology. For data transmission to be safe, networking means connecting one peer to another over a connected (Wired) or disconnected (Wireless) channel. We'll go through a few of the network's characteristics, parameters, and goals in short. In the late 1970s, when the ARPANET, the forerunner of the contemporary Internet, was developed, networking was primarily seen as a computational middleware discipline. One of the most significant discoveries of the 20th century, Internet use has undergone a dramatic increase since the early 2000s. Networking infrastructure has become an integral part of the research process in all fields of study. To meet the ever-increasing demands of the World Wide Web, new technologies with traditional networking models have been developed to enable massive data utilisation and storage, including smart and advanced storage area networks, computational intelligence, backend processing, and data optimization on communication lines. The age of networking has made data transmission through a channel easier and more reliable in terms of connection and dependability. Wireless ecosystems have emerged as a consequence of the expansion of networking technology and research, which has enabled the construction of contemporary infrastructures and the connection of remote communication nodes over a single line of channel.

[1,2]Department of Computer Science and Engineering
[1] Research Scholar, Dr. A. P. J. Abdul Kalam University, Indore
[2] Research Supervisor, Dr. A. P. J. Abdul Kalam University, Indore, (M.P.), India.
E-mail Id: [1] sony.nayan@gmail.com, [2] mepatil@gmail.com
** Corresponding Author: Sony Kumari*
Email: sony.nayan@gmail.com

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the dominant protocols in the infrastructure (UDP). 2 Disruptive protocols in networking models have evolved from the examination of such protocols, which has led to a skewed culture of processing and liabilities on resources. Networking is entering a new age because of the evolution of TCP and the Open System Interconnection (OSI) protocols. An interdisciplinary approach is needed in light of the rising need for network and developing infrastructure, which calls for study in this area. In today's networking landscape, separate technologies such as storage, entertainment, communication, and social interaction have all come together in a single domain. Infrastructure validation and processing must adapt to the changing demands of the network as it grows. As a result, the field of networking research has progressed beyond the traditional wireless sensor and non-wire technologies. P2P file transmission and sharing has been the centre of attention because of the inherent intricacies and infrastructure problems that must be overcome. One of the most popular ways to communicate is via Peer to Peer (P2P). For data security and portability in an unsupervised method of communication, P2P architecture is ideal.

It all starts with a weak node of new devices linking peers in a large loop of interaction. Node formation and node dilution in relation to a configuration are two of the most sought-after solutions in modern networking ecologies. Using a P2P 3 connection model, this thesis' study examines file sharing across several infrastructural domains. File types, sizes, and formats, for example, generally fall into a predefined "freeze zone" while examining a file in a networking environment. Data transmission channels and communication lines may be used to change these properties. The absence of intelligence in recognizing the route and address of each of the most often sought or requested file data locations is a big setback with the evolution of technology. That's why I've included it in my thesis. Designing and developing an intelligent P2P file-sharing infrastructure in a Block chain framework is the major goal of this thesis and study. As of today, the network covers almost every area of connection or communication, having developed quickly since the early 2000s. The government of India's telecommunications ministry conducted a study in FY 2016-17 and found that the peak of data dependency has climbed 97.4 percent compared to the consumption in FY 2015-16. In addition, this has opened the door to a wide range of high-tech frameworks.

1.1 Block Chain Technology : Data nodes and streams of information are transferred from one informatics centre to another depending on the value of Bit coins in order to create a specialized, public and secure network for interpreting the information chain reaction that results from this technology's implementation. Most Block chains are made up of interconnected patterns of information to carry out a safe transaction. It was at this point that block chain technology began to gain traction in the fields of information technology and financial transactions.

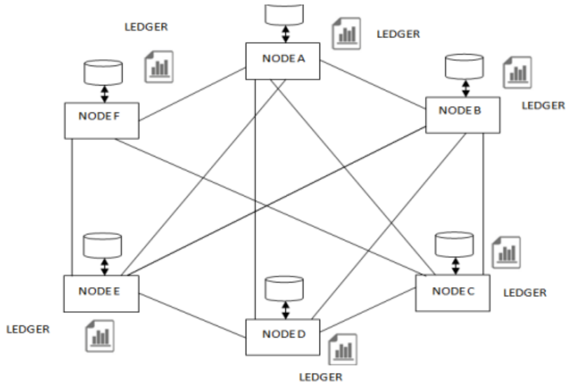


Fig 1: Distributed Ledgers

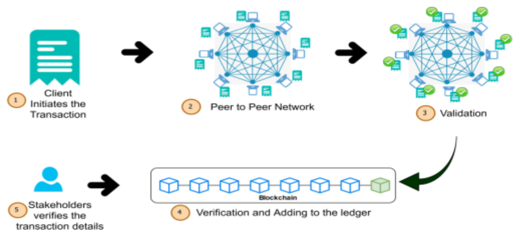

1 Client Initiates the Transaction
2 Peer to Peer Network
3 Validation
Blockchain
4 Verification and Adding to the ledger
5 Stakeholders verifies the transaction details

Fig 2. Block chain Network and the Process of Adding New Transaction to Ledger.

In the Block chain, the entire information about the network is fully safe and disseminated by all the peers engaged in the transaction (Figure 1) in a specific network. "Ledgers" are often used to keep track of this data. Records of system, node value, and configuration datasets are kept in ledger records (sometimes called a "record log"). The ledger is tasked with retaining the whole network information at a certain moment in time. Thus, each node is allocated a number that represents the total censure factor for processing the node. Using the node's value as Bit coins or digital money, the remitter's network address may be used to draught a payment to the recipient. Because INR (Indian National Rupee) is converted automatically when Bit coins are sent to India, the physical market now has six times the amount of cash available in the digital market. A framework is needed to forecast, identify, and map the system with the networking devices in order to increase the ratio of performance and security for these currencies (Bit coin s). In most cases, file sharing is the most affected by network traffic. ' As the value of each address connected with the network structure is increased, so is the network's confluence under Bit coin s. Trade in Bit coin s in India is now subject to legal proceedings, but the attackers are still using the Virtual Private Network (VPN) to access resources in an undetected way. As a result, the whole lawful trade market has collapsed as a result of the Bit coins' manipulation of the value of node addresses. These currencies are simple to move around and don't raise any red flags when it comes to trading or operations. Since the operating principle of the nodes in the block chain ecosystem must be determined via iteration, a stated system is required.

1.2 Peer to Peer Computing with Block Chain : When resources are spread among a large number of interconnected processes, scalability issues arise. Peer-to-peer (P2P) networking attempts to solve these issues . It is up to each individual client computer to decide whether or not to join or quit the network. No ace slave tactic exists over the companions, implying that this is the case. There's no need for any kind of targeted coordination or data at this point. The P2P system cannot be read in its entirety by any peer computer. System interconnects the cluster processors that participate in the event. It's an 8-incorporated computing asset that functions seamlessly together. In this sense, a cluster is local, since the bulk of their components subsystems are confined to a single body region, and in some circumstances, even occupy a single square foot of space. Local space systems connect each choice in a bunch to the other options. In a block chain, transactions in bit coin or advanced cash are stored and tracked in a decentralized, public ledger. A block is the 'most recent or current' portion of a block chain, which records all of the current transactions taking place in the network. Once completed, a block is added to the block chain as a piece of immutable data. Once the current block is completed, a new block is constructed.

In a block chain, each choice in a direct, written record request is linked with an unnumbered number of such blocks. A hash of the previous block, the contents of the current block, and the block's own hash data are all included in each block. Using a block chain, which is a limited enhanced record, makes it incredibly difficult to alter the data in the block, which is why this kind of technology is used in applications like financial services and real estate. Substituting Block chain, a block chain-based innovation, enables customers to execute net apps on their local and basic devices. As a server-less platform, block chain enables users to store and manage their data and apps wherever they have access to their devices. Peer-to-peer networks are used to maintain a Block chain. Rather than needing a centralized authority or server to manage it, this distributed ledger may be maintained by using database replication and computational trust to keep its data of high quality. One of the nine distributed ledger technologies is the block chain. A chain of blocks isn't required by all distributed ledgers to achieve a distributed consensus that is both safe and legitimate. The Block chain has a unique structure that sets it apart from other distributed ledger systems. Encryption and grouping of data on a block chain is done in this manner.

2. Literature Review

Cornelius C. Agbo (2019) explored the expansion of blockchain technology from its initial application in Bitcoin to various non-financial sectors, particularly healthcare. This study conducts a comprehensive review of blockchain in healthcare, employing the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) criteria and a systematic mapping study approach. Despite several studies proposing various healthcare applications for blockchain, a lack of concrete prototype implementations and evaluative studies was noted. The paper also discusses the current state of blockchain applications in healthcare, their limitations, and future research directions, emphasizing the need for more thorough research to evaluate blockchain's value in healthcare settings.

Tareq Ahram et al. (2017) examine the transformation of the digital world through the integration of mobile, IoT, social media, analytics, and cloud technologies. The emerging blockchain technology is reshaping digital systems, offering enhanced security, resilience, and efficiency. Beyond its initial use in digital currency, blockchain enables secure exchange of a variety of products, services, and transactions. The paper discusses blockchain's application in industrial sectors hampered by regulation, cybercrime, and fraud, and how it could facilitate flexible value chains, faster product development, and integration with IoT and cloud technologies. IBM's Blockchain initiative, Healthchain, is used as a case study to demonstrate blockchain's potential in healthcare and other industries.

Yasin Akın (2019) addresses the growing use of electric cars and the importance of securing data and financial flows within the supply chain. This research takes a holistic approach to designing an energy ecosystem on the Ethereum Blockchain network, encompassing energy producers, consumers, suppliers, dealers, electric charge stations, and electric car owners. Smart contracts enable user-to-user transactions, recorded on the Blockchain network, ensuring confidentiality, integrity, and accessibility. The paper also discusses the use of PROMETHEE, a multi-criteria decision method, for user requests with multiple suitable offers.

Goknur Arzu Akyuz (2020) investigates the transformative potential of blockchain in supply chain management (SCM). The study categorizes SCM and blockchain into four areas: basic characteristics, transparency/visibility and traceability; automated controls with smart contracts; and trust-building and collaboration. The findings, based on a comprehensive literature review, suggest that blockchain can significantly improve transaction authenticity, visibility, and traceability in SCM, facilitating the development of collaborative, interconnected, and transparent ecosystems.

Malak Alamri (2019) discusses the rise of IoT-based smart applications and the accompanying need for robust security solutions. The study combines IoT applications with blockchain, initially focusing on the basics of blockchain technology for IoT applications. It addresses challenges in power consumption, privacy and security concerns, throughput and latency, block size and bandwidth, usability, and multi-chain management. The paper concludes with insights into how blockchain can provide substantial security and privacy solutions for IoT-based applications.

Francis Nwebonyi Nwebonyi (2019) highlights the popularity of distributed networks, like edge computing, essential for IoT and 5G technologies. However, their vulnerability to attacks is a concern. The study looks at the Trust and Reputation System (TRS) as a solution for securing distributed networked agents. It addresses issues with existing computing systems and proposes a new approach, targeting mobile edge clouds and supporting traditional protocols like BitTorrent. The solution, tested in various scenarios, uses Ethereum's blockchain for publishing trust ratings and introduces a new consensus process to avoid the limitations of current methods.

Imran Ali (2019) examines the rise of internet-based gaming and the corresponding need for secure gaming networks. The study presents a distributed system model based on blockchain to address security issues in gaming networks. It utilizes a decentralised and low-range wide area network (LoRa WAN) mechanism with a gateway mechanism for network protection. The approach addresses security and privacy concerns in gaming networks, proposing a shift from traditional centralized systems to distributed, decentralized ones.

Muhammad Salek Ali (2018) discusses the impact of Bitcoin's blockchain technology on the digital currency market and its potential applications beyond finance, particularly in the IoT. The paper provides a comprehensive overview of blockchain's functionality, its role in decentralization, security, and transparency, and examines the current centralised IoT models, recent advancements, and the application of blockchain as a secure medium for IoT.

Walid Al-Saqaf (2017) explores the potential of blockchain technology in various social impact areas, including human rights. The paper examines if blockchain's core operational principles, like transparency and accountability, can limit online surveillance, censorship, and human rights abuses, thus encouraging scholarly interest in blockchain's societal impact.

Supriya Thakur Aras (2017) describes blockchain as the fifth disruptive innovation in computing. The survey collates key developments in blockchain practice, exploring its applications beyond the financial and banking domain. The paper presents a detailed survey of blockchain technology literature and applications, covering consensus algorithms, variations, and future applications.

Arshdeep Bahga (2016) discusses the application of IoT in various industrial and manufacturing sectors, focusing on Cloud-Based Manufacturing (CBM) and the introduction of BPIIoT, a decentralized platform based on blockchain technology for the Industrial Internet of Things. The platform's use of blockchain enables the establishment of decentralized, trustless, peer-to-peer networks without a trusted intermediary.

Nelson Bore (2017) emphasizes the need for analyzing data in educational systems to aid decision-making. The paper highlights the lack of systematic validation mechanisms for data acquired in educational systems, particularly in developing countries, and presents a blockchain-enabled School Information Hub (SIH) as a case study using Kenya's school system.

Nikola Bozic (2016) investigates potential applications of blockchain technology beyond cryptocurrency. The article introduces blockchain and analyzes its applications in network systems, particularly focusing on Bitcoin's use of blockchain for an independent payment system that stores and traces all transactions securely and publicly.

Francesco Buccafurri (2017) discusses blockchain's potential in IoT applications, considering IoT devices' limited processing and storage capacities. The paper proposes a solution using Twitter to create a secure chain of tweets, leveraging Twitter's absence as a trustworthy third party or ledger provider.

Cha, Hyun-Jong (2018) highlights the need for systems to organize and utilize large data volumes, emphasizing the development of encryption technology to protect individuals' privacy. The paper presents an attribute-based encryption approach for effective management in medical information monitoring systems, using Fog Computing's network.

Guang Chen (2018) focuses on the educational applications of blockchain technology, exploring how it can address specific educational challenges. The paper begins with an overview of blockchain's features and benefits before discussing its current educational uses, highlighting blockchain's potential in transforming the educational sector.

Olivia Choudhury, (2018) addresses updates to the Common Rule governing Institutional Review Boards (IRB), proposing a new blockchain-based system to ensure compliance with IRB data collection standards. The paper shows how smart contracts can meet IRB protocol criteria and secure research activities using blockchain's immutable transaction log.

Kyungyong Chung (2019) discusses cognitive manufacturing, combining blockchain distributed ledger technology with intelligent information technology. The paper suggests a topic mining method for blockchain-based cognitive manufacturing, using Fourier transform algorithm for context analysis and securing smart devices through a side-chain-based distributed consensus blockchain network.

3. Architecture of a Blockchain

3.1 A Decentralized Digital Network for trading Assets : Blockchain technology, a form of network-oriented software, operates by decentralizing both code execution and data storage, moving away from centralized workstations. It facilitates the recording of digital asset exchanges in a distributed ledger. The most basic asset utilized by many blockchain protocols is tokens, a type of cryptocurrency. However, blockchain can also be used to trade other types of assets, such as land titles or identification certificates. Each blockchain network operates under a specific set of rules that determine what assets can be traded and under what conditions. These rules are embedded within the blockchain's software.

In a blockchain network, a node refers to a computer or device that runs the blockchain software and connects to other nodes in the network. Public blockchain networks are open to anyone; any individual can set up a node and engage in direct transactions with other nodes. Conversely, a private blockchain network, akin to an intranet, restricts access to a select group of users, allowing transactions only among these authorized individuals.

The blockchain software is designed so that only identical versions can interact with each other. Altering a version of the software essentially creates a new, separate blockchain, a process known as "forking." Since Bitcoin's introduction in 2009, numerous forks of blockchain software have occurred. For instance, in August 2017, the Bitcoin blockchain underwent a fork, resulting in the creation of a new blockchain called Bitcoin Cash.

In blockchain networks, all devices transact under a uniform set of rules, eliminating the need for a central authority to ensure compliance with these rules. This decentralized structure is a defining characteristic of blockchain technology, promoting a more autonomous and direct form of digital asset exchange.

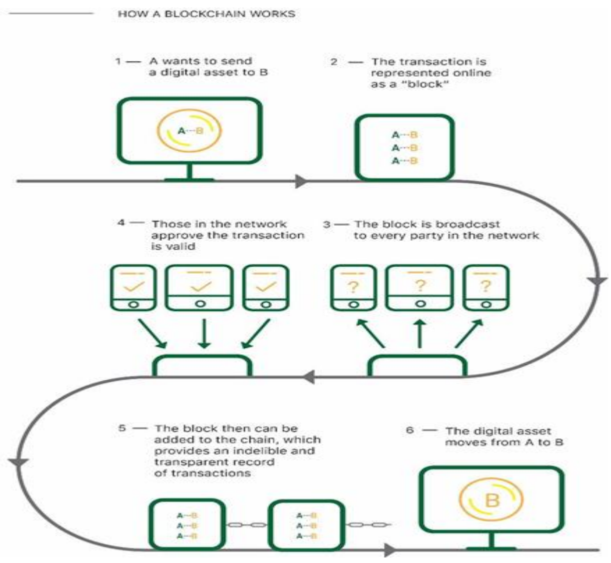

HOW A BLOCKCHAIN WORKS
1 — A wants to send a digital asset to B
2 — The transaction is represented online as a "block"
A---B
A---B
A---B
A---B
4 — Those in the network approve the transaction is valid
3 — The block is broadcast to every party in the network
?
?
?
5 — The block then can be added to the chain, which provides an indelible and transparent record of transactions
6 — The digital asset moves from A to B
A---B
A---B
A---B
A---B
A---B
A---B
B

Fig 3. How a Bitcoin Blockchain Work.

3.2 A Decentralized, Distributed Ledger

A decentralized, open, and transparent ledger lies at the heart of a blockchain. Each blockchain software instance is unique:

- Maintains a thorough record of all transactions;
- As soon as the rest of the network agrees, it updates its ledger;
- The network broadcasts user transactions for consensus verification and recording;
- Maintaining a consistent copy of the ledger across all nodes is a top priority.

3.3 A System for anonymously verifying Identity and Ownership : The following is the format in which transactions are recorded on a blockchain:

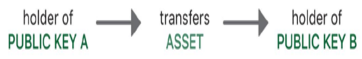


Fig 4. Transactions on a blockchain

Bitcoin addresses tied to a person's unique public key and their cryptographically related private key can be generated via blockchain software.

It is necessary for a user to input a bitcoin address's secret private key, which was issued to them when the address was formed, before they can add a new transaction to the blockchain, which is to say they can move an asset linked with that bitcoin address.

Bitcoin addresses and public keys may only be used to verify ownership of assets that have been transferred to them.

It is thus possible to determine who owns what in a transaction, even without knowing the identities of the persons involved (Nakamoto, 2013).

When the transaction is complete, each of the participants can use their assets by simply inputting their private key into the bitcoin program, without revealing or proving their identity to any third party or intermediary.

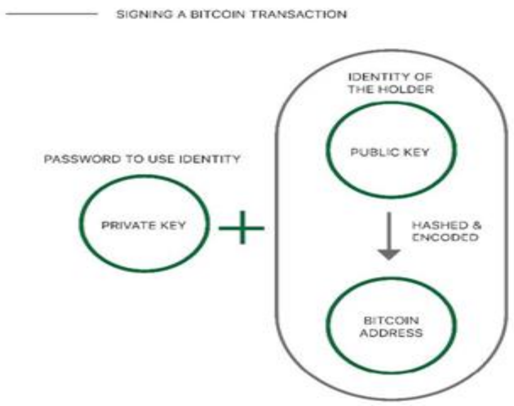


Fig 5 Signing a Transaction on a blockchain.

3.4 A System for ensuring Permanent Indestructible Records

Transactions on the Bitcoin blockchain ledger can only be added, not modified or removed, because the ledger is "append-only."

There is a chain of blocks that are linked together by the addition of a new transaction each time a transaction is made.

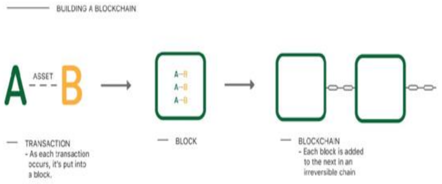

BUILDING A BLOCKCHAIN
A
ASSET
B
A--B
A--B
A--B
TRANSACTION
- As each transaction occurs, it's put into a block.
BLOCK
BLOCKCHAIN
- Each block is added to the next in an irreversible chain

Fig 6. Building a Blockchain

Figure 6 illustrates the mechanism ensuring the integrity of a blockchain through a dual hashing process:

1. **Merkle Root Hashing**: Each block in the blockchain encapsulates all its transactions using a specific hash function known as the Merkle root. This hash is included in the block's header.
2. **Hash of the Previous Block**: Additionally, the header of each block contains the hash of the previous block's header.

This structure ensures that any alteration in a transaction within the blockchain would disrupt the hash value of all subsequent blocks. Maintaining the chain's integrity would then necessitate altering the header information of every transaction and doing so on more than half of the computers in the network, which is highly impractical.

The feasibility of changing transactions on a large blockchain is virtually impossible due to:

a) The enormous amount of computing power required to alter the blockchain. Such a level of computational effort is impractical to achieve.

b) The continuously growing number of blocks on the chain, which means that the computing power needed for alterations is also constantly increasing.

It's important to note that even with advancements in computational power, the security of the blockchain remains robust. This inherent security feature of blockchain makes it a highly secure and tamper-resistant technology.

4. Implementations of Blockchain Technology in Education

Blockchain technology holds significant potential for various stakeholders in the education sector, including individuals, institutions, groups, countries, and the global community. Its applications are relevant across all educational settings, from K-12 to university levels. Instead of relying on traditional hierarchical structures, there's a growing trust in technology, particularly in blockchain, known for its disintermediation capabilities.

One challenge in the current educational landscape involves the issuance and verification of digital documents. Often, these documents are provided in proprietary formats, requiring specific software for access and validation. This can make the verification process not only time-consuming but also uncertain. Moreover, even in regions where digital signatures are legally required, there's a wide variety of formats and security levels, with not all being recognized as legal proof.

Additionally, email, the most common method of data exchange, poses security risks, especially for sensitive information like medical records. This necessitates the development of specialized transmission infrastructures to enhance security, akin to the security improvements over traditional postal letters. However, this advancement also brings about new challenges in interoperability.

Paper documents, digital documents are susceptible to forgery, often in ways that are hard to detect. Blockchain technology, with its inherent security and verification mechanisms, can provide solutions to these challenges. Its ability to securely and transparently manage records and transactions makes it an attractive option for handling educational data, credentials, and other sensitive information. By leveraging blockchain, the education sector can overcome issues related to document verification, security, and interoperability, paving the way for a more efficient and trustworthy educational environment.

4.1 Issuing Certificates : The use of blockchain technology in issuing certifications presents an opportunity to enhance and add value to the existing digital certification ecosystem, going beyond mere credential validation. Prominent academic institutions are currently utilizing platforms like BADGR and Mozilla Open Badge to issue digital credentials. The integration of blockchain aims to transform these private digital certificates into immutable proof systems on a public blockchain, accessible by third parties.

Under current practices, accessing a public platform often requires students to provide sensitive metadata, including private information. However, utilizing blockchain as a 'proof of knowledge' system eliminates the need to disclose such private information during public consultation of certification metadata. This approach offers the prospect of students engaging with academic institutions and employers while maintaining a discreet level of confidentiality. Only the information that students choose to mark as public during the proof generation process would be accessible to third parties.

Agility (2017b) points out opportunities for software companies to facilitate easier access to the blockchain for students and badge issuers, including institutes, companies, and schools. Applications built on open-source frameworks are particularly advantageous, as they ensure data continuity of lifetime and life-wide learning achievements without being tied to a single solution.

The blockchain's accountability and consistency will be beneficial to a broad spectrum of organizations, not just educational ones. For instance, students could use public metadata to find similar profiles, fostering new models of social inclusion and entrepreneurship. This can be done without relying on an authoritative body to verify the information's legitimacy, thus democratizing access to educational credentials and promoting wider societal benefits.

4.2 Blockcerts: An open Standard for Blockchain educational certificates

The foundational principle of the Blockcerts open standard is that individuals should have the ability to own and prove ownership of their essential digital records. Rooted in the principles of self-sovereign identity, these documents are immutable and verifiable, allowing individuals to demonstrate various aspects of their identity as outlined by sources such as Allen (2016), Jagers (2017b), and Lewis (2017). The blockchain technology underpinning Blockcerts empowers individuals with control over their official records, enabling them to share these documents for swift verification without the risk of tampering or alteration.

Developed by the MIT Media Lab and Learning Machine, a software company in the industry, Blockcerts is an open-source standard based on Bitcoin's blockchain. Although currently no other open standards exist for creating and verifying blockchain records, Blockcerts aspires to become a globally recognized standard in this domain, particularly in terms of social adoption.

Blockcerts' base code is designed for use by any user, including educational institutions and governments, to create their own applications for issuing and verifying digital records. The Blockcerts Community forum illustrates how a wide range of organizations, startups, and individuals globally are leveraging this free and open-source platform to develop various applications. Furthermore, Blockcerts offers a free wallet and mobile application, compatible with both iOS and Android platforms, with open access to the code for community-driven improvements.

To avoid standard wars and vendor lock-in, the creators of Blockcerts chose to make it open source. This decision promotes easy interoperability and broad adoption of official records, addressing what they saw as significant barriers. Currently, the Blockcerts community views data silos as a major challenge that needs addressing, with blockchain technology providing a viable solution.

Blockcerts sets a precedent for a mobile wallet that aligns with the key overarching principles of digital self-sovereignty: recipient ownership and vendor independence. This approach reflects a growing trend towards empowering individuals with control over their digital identities and records.

- **Recipient ownership** means that individuals are in charge of their own private keys, which they can use to prove that they own money or digital data.
- **Vendor independence** means that there is no reliance on a single vendor for access, display, or verification. Records can be moved, exchanged, and validated independently of vendors when they are based on open-source standards.

To ensure that individuals have full control over their personal data, the two conditions must be met.

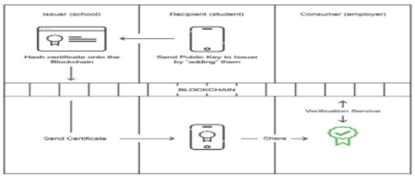
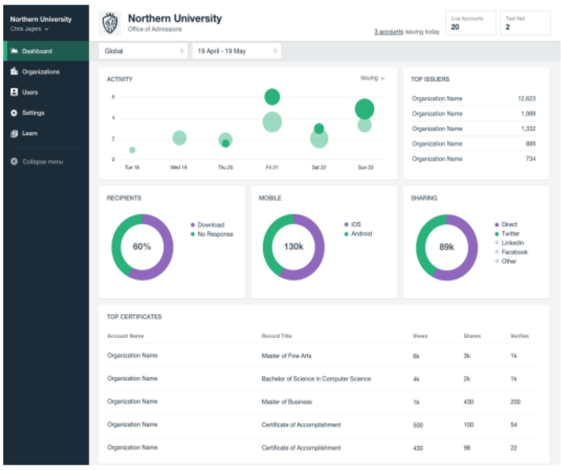


Fig 7. A straightforward flowchart on the Blockchain that illustrates the process of issuing and confirming a certificate.

Blockers allow for the issuance and authentication of credentials on any blockchain and in any market area, independent of the technology that is being used. According to the primary developers, the Bitcoin blockchain was a fair option for the underlying blockchain to which to bind lifetime digital records when the project started in 2015. This was the case when the project was first initiated in 2015. Because of the hard split that occurred in 2016, Ethereum became untrustworthy for credentials that need to be valid for a lifetime. As a result, there was a significant amount of debate over the possibility of boosting resources to Ethereum in 2016. A number of decisions were made in order to make the documentation for Bitcoin as helpful as possible while maintaining its openness to the possibility of additional Blockchains being covered in the future. As a result of the substantial growth that occurred in the Ethereum development community in 2017, many individuals are requesting that Blockcerts include Ethereal into its documentation and reference implementations. Due to the fact that this extension is an open-source project, a lot of programmers are now working on it extensively.

The IMS Open Badges, W3C Verifiable Claims28, W3C Linked Data Signatures, and W3C / Rebooting Web of Trust Decentralised Identifiers are all projects that are connected to the Blockcerts community and contribute to it.

For the purpose of developing their own solutions, researchers from the University of Birmingham31, the Massachusetts Institute of Technology (MIT), and the University of Nicosia are all using the Blockcerts open standard.



TOP ISSUERS

Organization Name	12,623
Organization Name	1,989
Organization Name	1,332
Organization Name	889
Organization Name	734

TOP CERTIFICATES

Account Name	Record Title	Views	Shares	Verifies
Organization Name	Master of Fine Arts	6k	3k	1k
Organization Name	Bachelor of Science in Computer Science	4k	2k	1k
Organization Name	Master of Business	1k	430	200
Organization Name	Certificate of Accomplishment	500	100	54
Organization Name	Certificate of Accomplishment	430	98	22

Fig 8. Example of a Learning Machine Analytics Dashboard.

4.3 Snapshot of Vendors in the Certificate and Identity Workspace

Solutions that are associated with blockchain technology are being made available by an increasing number of suppliers in the certificate industry. According to Mesropyan (2017), more and more companies are now developing blockchain-based solutions for their corresponding customers. A significant number of their traits are same.

These goods have been differentiated from one another based on the use of four fundamental distinction criteria. As a starting point, they are used in order to compare the products and services provided by a limited number of companies:

Existence solutions that provide proof It is possible to utilise a notary who has time-stamped a document in order to verify that the document has not been altered since a certain date and time. The blockchain may be used for verification without any continuous dependent on the vendor, provided that the suppliers in question follow open-source procedures that are consistent with industry standards. It is not the case that vendors operating in this sector encode recipient public keys into documents or deliver them to recipients; rather, they offer data verification services. This indicates that the receivers of the document will not be able to demonstrate that they were given an original copy of the document. The claims of identification made by individuals should not be confused with those made by these corporations.

A vendor that acts as a notary may provide solutions for data and identification papers, such as university credentials, in addition to providing certification of the presence of data. Individuals are able to examine and verify their own data, but only in a manner that is dependent on a third-party provider for access, hosting, and verification. The use of blockchain technology for the purpose of record verification and maintenance also lends support to a vendor-centric approach.

The solutions for "Know Your Customer" Apps that enable users to establish ownership of their verified data are often offered by the service providers at the time of implementation. There is a possibility that vendor-controlled networks will profit from this; nevertheless, this data is only applicable to receivers who are located inside the perimeter of the vendor-controlled network; hence, it is not valuable to consumers who are located outside of this network. The dependency of the seller on the receiver is clearly established as a consequence of this. KYC solutions have great potential for a wide variety of use cases; nevertheless, it is important to note that these solutions should not be confused with solutions that provide verifiable assertions that can be used in any circumstance.

Solutions that promote digital self-sovereignty For the purpose of accessing, exchanging, or verifying information, individual records that are solely theirs and do not need the assistance of any third party may be sent. There are three things that contribute to the acquisition of this degree of freedom:

- The distribution of records in a format that adheres to open standards
- The issuance of documents that include the public key identification of recipients
- The use of an open-source container (such a mobile application) for the purpose of storing data, which gives receivers the right to control their own private keys and which continues to function and survive independent of the vendor.

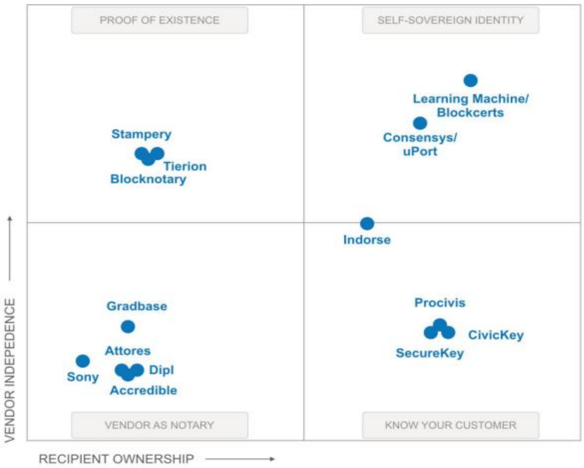


Fig 9. Current Positioning of Vendor Independence vs Recipient Ownership

4.4 Certification Solution Vendors : An increasing range of vendors with certification products and services that could be used in education is represented by the organizations listed below.

Learning Machine Certificates deployed over Blockcerts : These certificates can be utilized by commercial providers to customize their products for unique market needs. Blockchain-based records can now be issued, tracked, and verified using Learning Machine's Registrar CRM and APIs over the open-source Blockcerts platform, a commercial environment. The issuing institution is Learning Machine's paying customer; the service is free for recipients, including mobile apps and wallets, and verifiers have quick and free access to record verification through web browsers and mobile apps. This is how the business model works.

Ownership can be proven and third parties can verify instantaneously without the need for a central authority thanks to the use of tamper-proof formats Governments, corporations, educational institutions, accreditation authorities, and other organizations are among the customers for issuing digital records. No matter what type of information you're dealing with, the technology is being sold as a solution that doesn't require any in-house blockchain technology expertise and capabilities. Education institutions are clearly a main target market for Blockchain-based notarizations of official documents, which is why the technology is ideal for this type of use case.

Digital files that have been cryptographically verified and registered on the Blockchain, says Learning Machine's Blockcerts standards-based solution, make it impossible to alter the data. It is possible to prove ownership of a record without the use of a certificate authority since each record has a unique recipient's public key. With Blockcerts, there is a new way of doing business:

- In addition, the display layer can be customized to resemble the appearance of traditional records;
- data and images are stored on the content layer;
- An encrypted hash of the transaction's content is stored in the receipt layer.

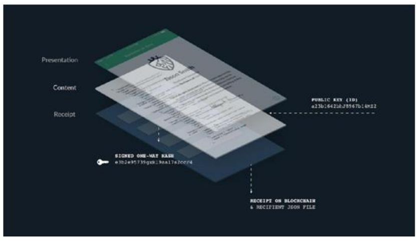


Fig 10. Multiple layers in production of a certificate notarized on the Blockchain

4.5 Sony Global Education : Since 2016, Sony's development of a blockchain-based certificate-issuing system has been a focal point of discussion (Sony 2016, Russell 2017). Sony Corporation and Sony Global Education (SGE) announced a blockchain solution for the education sector on August 10, 2017. As per their press release, this system centralizes the management of data from multiple educational institutions, enabling the recording and referencing of educational data and digital transcripts securely and openly. This system is built on Hyperledger Fabric 1.0, a blockchain framework hosted by the Linux Foundation and part of the Hyperledger projects. It integrates a function for authenticating and managing educational data, along with an API tailored for educational institutions. Sony plans to roll out its services starting in 2018 with its Global Math Challenge, initially targeting 150,000 participants worldwide.

Attores Solutions has launched Open Certificates to provide educational certificates on the Ethereum blockchain. This product is currently in the testing phase, with reports of collaborations with Singaporean educational institutions.

Other companies, such as Gradbase and Stampery, are also entering the blockchain certificate issuance domain, aiming to set new global standards for rapid certification verification.

In the realm of identity solutions, several companies are offering products that could be relevant to the education sector:

- **Civic** claims to be an identity platform on the blockchain. Having raised $33 million, the company is focusing on product development and launch. Civic's solution stores the hash of a user's personal data on the blockchain, allowing users to control which information they share with entities like university admissions. It also offers an attestation feature where organizations can certify the verification of user data.

- **U port** is a self-sovereign identity solution developed by ConsenSys and built on Ethereum. It includes smart contracts, developer libraries, and a mobile or web-based wallet. The app securely holds the user's keys, while Ethereum smart contracts enable users to recover their identity if their mobile device is lost. U port identities, which can be individuals, devices, or institutions, are self-sovereign and can sign and validate claims or transactions. They can link to off-chain data repositories and store the hash of attributed data, which users can manage or allow others to access. U port identities can interact with blockchains, handling digital assets like cryptocurrency.

These developments illustrate the growing use of blockchain in education and identity management, offering innovative solutions for certification, data security, and personal data sovereignty.

5. Blockchain System Security Domains

5.1 Blockchain is decentralized, but its system is not : There's no need for refuelling or central control with blockchain technology. As a result of these limitations, it is not possible to increase user participation in the technology without a public (decentralised) and business model-based incentive structure. Table 1 below outlines the components of the cryptocurrency system, which is now the most popular type of Blockchain. There are centralised and decentralised components in the Blockchain system, according to the table. The complexity of a system's architecture increases as its components are intertwined in an elaborate manner. Because of this, it is more difficult to secure a complex system and requires additional security measures. Because of this, relying on a single database to safeguard the perimeter of the entire system seems unlikely. Finally, just like centralised systems, a Blockchain system should safeguard its components from cyberattacks.

Table 1 Different types of forks in terms of compatibility.

Type of Fork	Compatibility
Soft	A soft fork in the Blockchain network represents a software update that maintains backward compatibility with previous versions. In this scenario, nodes, or users, can continue to engage in the network activities like transaction validation and verification, even without upgrading their software. However, one of the consequences of a soft fork is that it can render blocks, which were previously considered valid, as invalid. This could potentially introduce security vulnerabilities for nodes that do not undergo the upgrade.
Hard	A hard fork in a Blockchain network refers to an incompatible software upgrade that is not backward compatible with previous versions. In the case of a hard fork, it's necessary for nodes (users) to upgrade their software to continue participating in the Blockchain network. This type of upgrade leads to a permanent split in the network, effectively creating two separate Blockchain networks that operate concurrently. During a hard fork, the network's rules are altered in such a way that blocks previously deemed invalid are now considered valid. Consequently, nodes that do not upgrade their software become incompatible with the new version of the Blockchain.

5.2 Difficulty securing a decentralized system in autonomous operation

To illustrate how the components of a Blockchain system interact with one another, the simplified data flow diagram that can be seen below in Figure 11 is shown. Distributed apps (dApps), web-based wallets with MultiSig verification, or third-party organisations or exchanges (as in the case of cryptocurrency) are the three techniques that are often used by a node (user) in order to communicate with the Blockchain. After a node (or user) has been authenticated, the data from that node (or user) will be transferred to the Blockchain without any further data protection or security measures being implemented. This is the only need.

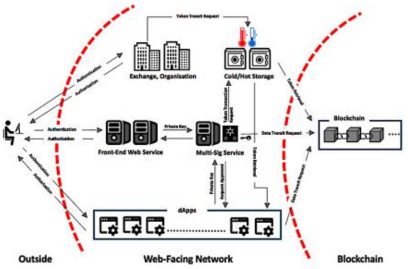


Fig 11. Simplified data flow in Blockchain system.

In light of this, the only method by which the Blockchain system can guarantee its users' safety is via authentication. A portion of this may be attributed to the characteristics of the technology itself, which need unrestricted access to a network node (the user) in order to function completely independently. Because of this structure, it is not possible to construct a robust authentication system that is based on cryptography. In addition, the only way to ensure the safety of system data inside the Blockchain border is via the use of Blockchain technology, which is guarded from external attacks. It is not possible for effective authentication methods to offer enough safety for the whole system on their own, regardless of how secure your data is inside Blockchain.

The following image provides an illustration of a comparison between the two systems in terms of their design and the flow of data. The many components of the centralised system, which can be seen on the right, are arranged in hierarchies according to the various duties and tasks that they are responsible for. When information can only go via certain pathways, both within and outside of the system, the attack surface is reduced, resulting in a smaller attack surface. This indicates that its security control components may be positioned in a manner that enables them to be protected against cyber assaults to the greatest extent possible. On the other hand, the levels of the system are not clearly defined in decentralised systems that are based on blockchain technology. When the borders of the system are not adequately secured, there is an increase in the number of attempts to exploit and hack the system. As a result of an increase in the number of attempts to hack and exploit the system, we are able to draw the conclusion that the system is susceptible to cyber assaults. When it comes to the distributed design of the Blockchain system, the absence of centralised control and administration may have a disastrous effect on the system's capacity to react to disasters or emergencies.

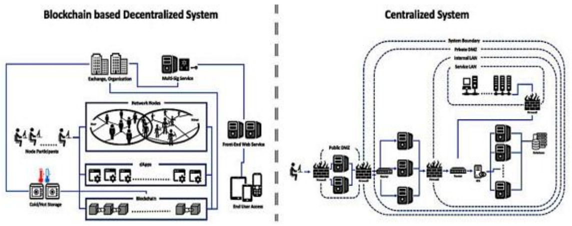


Fig 12. Distributed (Blockchain) vs. Centralized System

An attacker has to be able to breach or circumvent a firewall, an intrusion detection system, and network monitoring in order to exploit a centralised system. This allows the attacker to access genuine hacking targets, such as a database or an application server, among other things. A Blockchain system, on the other hand, has a far smaller number of security-related components that are responsible for protecting and monitoring cyber threats than conventional centralised systems do. To the best of our knowledge, the Blockchain system border does not include any additional security system control components beyond user authentication.

5.3 Threat modeling

In order to deal with cyber threats in a more systematic manner and to predict potential security challenges, threat modelling is a methodology that is widely used by the majority of businesses. For the purpose of gaining a deeper comprehension of the hacking and security incidents that have occurred to Blockchain systems, threat modelling exercises were carried out. The objective of these exercises is to first define the components of the Blockchain system with regard to system security, and then to establish particular security domains for Blockchain systems.

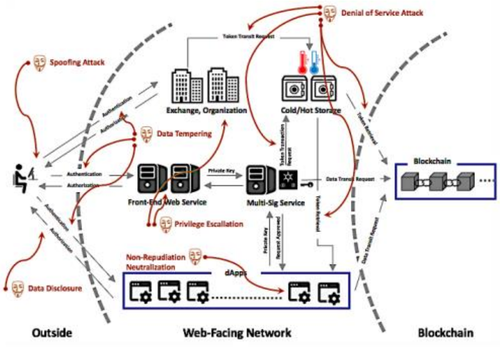


Fig 13. Results of threat modeling on Blockchain system.

A total of six possible weaknesses in the security of the Blockchain system were discovered during this threat modelling exercise, as shown in Figure 4.3, which can be seen above. This information is based on the data flow shown in Figure 11. First and foremost, it was found that data spoofing, which is the act of a person or machine pretending to be someone else in order to gain an unfair advantage, is a cyber threat. In order to take advantage of this vulnerability, there are a number of different methods that may be used. Some of these methods include listening in on communication channels with the intention of obtaining personal information, breaking into a secure channel, or interrupting user access. Additionally, the cyber danger of data tampering, which is an act in which data that was supplied by users is transformed into malicious data, was discovered via the process of threat modelling. Examples of data tampering that might disrupt the Blockchain protocol include component tampering, data corruption, data manipulation, and ledger malleability. All of these types of data tampering are equally problematic. In the context of the network, the term "denial of service" refers to the intentional disruption of the access of an authorised user to the network. The components of the system that are available via the public internet are susceptible to cyber assaults, which may result in the breakdown of the system, the corruption of data, or the cessation of operations. Regarding privilege escalation, there is also the chance of a cyber assault being launched. As a result of privilege escalation, system components such as Multi-Sig authentication or bit coin exchange are susceptible to attacks that include the circumvention of access control, the bypassing of monitoring, or the breaking in of third-party security solutions. Similar vulnerabilities exist for system components that are designed to handle or store sensitive data, such as cold/hot wallets and online/offline storage. These components are susceptible to data leaks. Any publication of data, in general, poses a number of security hazards, including the possibility of data theft or loss. Distributed applications (dApps), such as smart contracts, suffer a cyber hazard of non-repudiation breakdown. As a general rule, this threat comprises security hazards such as circumventing security logic, re-entry or race conditions inside source code, or manipulation of consensus protocols.

5.4 Four security domains of Blockchain system

Figure 14 illustrates the four security domains that were modeled Blockchain system components. Throughout this book, a naming convention (D-N) will be used to designate the domains that will be discussed.

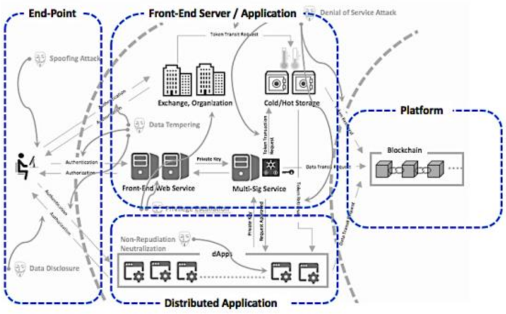


Fig 14. Throughout the course of threat modelling activities, four different Blockchain system security domains are categorised.

The key components of the platform domain (D-1) on the Blockchain (public ledgers) are the users and the data that is exchanged to and from the platform. Nodes, also known as users, are the most important components of a Blockchain system. This is due to the fact that a consensus of all nodes is conducted in order to validate data and decide on the inclusion of blocks. Every piece of information that is stored in the system is kept in the ledgers. problems about redundancy, synchronisation, and communication for the processing of ledger (data) are the fundamental problems regarding security in this domain (D-1). There are many instances of front-end domains (D-2) that can be found on the internet. Some examples include digital wallets, third-party security solutions, and platforms that facilitate the trading of cryptocurrency. It is possible to draw numerous parallels between this and the conventional centralised information technology architecture. Consequently, the methodologies that are used for security assessment have to be comparable to the security assurance evaluations that are already in place, such as the OWASP Top 10. In the 38 (dApps) domain (D-3), the majority of the decentralised applications (dApps) are privately built and operate on the Blockchain. Instead of being restricted to a single web server or personal PC, decentralised applications (dApps) are distributed over the whole of the Blockchain system. This presents a significant difference from conventional software. In this context (running and execution scenarios), it is important to examine both static security evaluations, which are based on the source code, and dynamic security evaluations. Consumers may connect with a Blockchain system using terminals, computers, or even mobile devices when they are in the end-points domain (D-4). Due to the fact that data is input, received, and created in this domain, it is considered to be the most susceptible in a chain of data flow distribution. Due to the fact that this domain is likely to be a prime target for an attacker, it is imperative that it be safeguarded in the end-user environment from malware attacks on personal computers, Cross-Site Scripting attacks on web browsers, and computer virus infections.

6 Results and Observations

The Merkle Tree method involves computing hashes using the SHA-256 hash function at all levels. A variation of this method suggests using SHA-256 only for the first two levels, then switching to SHA-512 for subsequent levels. This approach aims to bolster integrity while managing computational load effectively.

In contrast, the Linear Hash Computation (LHC) typically requires two hash computations for each transaction. However, a proposed variant of LHC simplifies this by computing only one hash per transaction and, unlike Merkle Hash Trees (MHT), does not necessitate fixed-size blocks.

This proposed scheme significantly reduces computation time by utilizing both SHA-256 and SHA-512, and offers enhanced traceability for identifying tampered transactions.

It's advisable to employ the proposed LHC variant with SHA-512 for all hashing operations to optimize efficiency and security. The following table provides a comparative analysis of the number of hash computations and the time required for MHT, its variant, LHC, and the proposed LHC variant. This comparison is done across two different hashing algorithms, SHA-256 and SHA-512, to highlight the efficiency and effectiveness of each method.

Table 1: Comparison of Merkle Tree and its variants

Hashing Mechanism	Hash Computations	Time in milliSecs. String length=270 chars
MHT (SHA256)	65535	983.8
MHT (SHA256) at first 2 levels & SHA512 at rest	65535	968.7
LHC (SHA 256)	65535	916.6
LHC Variant(SHA 256)	32768	733.6
MHT (SHA512)	65535	912.7
LHC (SHA 512)	65535	1081.2
LHC Variant (SHA 512)	32768	741.4

The X-axis of the line graph seen in Figure 15 represents the amount of time spent computing, while the Y-axis indicates the kind of algorithm being used. When compared to other hashing algorithms and their modifications, it demonstrates a definite improvement in the amount of time required for processing.

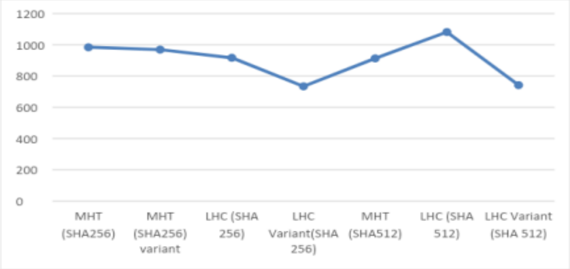


Fig 15. Computation time by various hashing algorithms

The analysis indicates that the Linear Hash Computation (LHC) variant not only provides enhanced traceability but also demonstrates greater efficiency in terms of Time Complexity when compared to the Merkle Hash Tree (MHT), its variant, and the standard LHC. This efficiency aligns well with our objective of incorporating traceability into the system while simultaneously reducing the computational time required for traceability and verification processes.

One notable aspect of the LHC variant's performance is the significant time savings per transaction. When compared to the widely used LHC 512 version, the LHC variant achieves an impressive 32% reduction in time, which translates to a substantial decrease in overall computational demands.

Given these findings, we propose a time-optimized design of the blockchain framework based on the LHC variant implementation. This design can be seamlessly integrated into existing Project Financial Lifecycle's Management Information Systems (PFL's MIS), offering an advanced, efficient solution that enhances traceability without imposing heavy computational loads. The proposed blockchain framework is thus well-suited to meet the evolving demands of modern MIS, particularly in environments where rapid processing and data integrity are paramount.

6.1 Implementing the optimized Blockchain

The evolution of real-world systems has been marked by significant milestones since the First Industrial Revolution (IR), which revolutionized industrial operations through the use of steam and water power, leading to mechanized production. This era was characterized by the introduction of machinery that significantly augmented human labor in manufacturing processes.

The Second IR further propelled this transformation by introducing electricity, which became the cornerstone for mass production. The hallmark of this era was the assembly line, powered by electricity, which brought efficiency and scale to manufacturing, allowing for the production of goods on an unprecedented level.

However, a paradigm shift occurred with the Third IR, where the focus shifted from physical to conceptual systems. This revolution was driven by the advent of information technology and computers, which allowed for the automation of processes in physical systems. This automation significantly reduced the need for human intervention, while simultaneously enhancing the speed and accuracy of these systems.

In the context of Padmavati Ferrous Limited (PFL), as discussed in section 4, this transformation is evident in their use of a Management Information System (MIS). PFL's MIS system is integral to their operations, managing key transactional data involving the purchase of raw materials, stock management of manufactured goods, and the sale of finished products. This is illustrated in Figure 16, demonstrating how the integration of MIS into their operations aligns with the broader trends of industrial evolution, leveraging technology to optimize efficiency and accuracy in business processes.

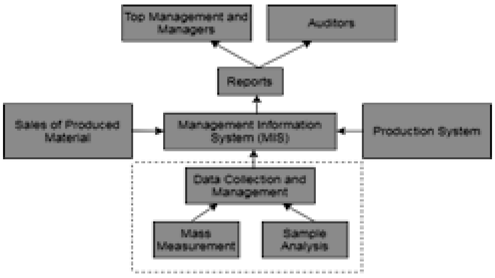

Top Management and Managers
Auditors
Reports
Sales of Produced Material
Management Information System (MIS)
Production System
Data Collection and Management
Mass Measurement
Sample Analysis

Fig 16. Management information system

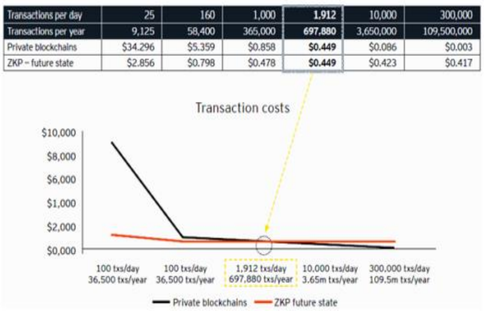
The Institute of Cost Accountants of India, in their Guidance Note on Internal Audit of the Mining and Metallurgical Industry, emphasizes the critical need for accurate measurements and correct recording of all transactions in a company's metal accounting system. This document provides auditors with guidelines to assess the controls implemented in the Management Information System (MIS) [7]. However, it acknowledges a significant risk: the potential for data manipulation within the MIS. Such manipulations are often difficult to detect and can lead to a loss of data integrity. Therefore, there's a pressing need for an effective mechanism to trace these manipulations in the MIS transaction data.

Blockchain technology presents a potential solution to this challenge, offering an effective way to trace manipulations in MIS. However, the scalability and cost-effectiveness of blockchain implementations need to be carefully evaluated to address the concerns of business managers.

The rise in new projects and upgrade proposals in blockchain-based systems, particularly in the supply chain domain, is noteworthy [9]. For organizations, a private blockchain scheme could be more suitable as it facilitates control over participating nodes and ensures the immutability and traceability of any manipulations [10]. However, any plans to implement such systems require a thorough cost analysis to justify the business case.

Ernst & Young (EY), in their recent research, utilized data from global client proof-of-concept, pilot, and production engagements to estimate and forecast the cost of a production-scale blockchain solution [9]. They found that the total cost of ownership of blockchain-based systems includes development cost, infrastructure costs, and the cost of implementing components necessary for running the chain code. EY's results indicate that the total cost of ownership for blockchain solutions is primarily influenced by factors such as transaction volume, transaction size, node hosting method, and consensus protocol.

This analysis underscores the importance of considering various cost and operational factors when evaluating blockchain solutions, ensuring that such implementations are not only technologically sound but also financially viable for businesses.



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

Fig 17. Transaction Cost Comparison

The analysis reveals that deploying a fully developed private or public blockchain solution, especially those based on Zero-Knowledge Proof (ZKP), incurs substantial costs, whether implemented on-premises or cloud-based. As indicated in Figure 17, these systems not only have high initial development and setup costs but also significant operational expenses, including transaction costs. The data suggest that such blockchain implementations are most advantageous for organizations with high transaction volumes. Small and medium-sized enterprises (SMEs), typically characterized by lower transaction volumes, may not find these solutions as beneficial financially.

Blockchain technology can potentially enhance the overall net benefits by improving the efficiency of invoice processing [3]. Suppliers could find blockchain platforms advantageous if the platform fees are lower than the immediate profits they could secure. Conversely, buyers might benefit from extended payment due dates. Funders might see advantages in blockchain solutions due to shorter processing times, allowing more transactions within the same timeframe. Meanwhile, platform providers would gain a fee per transaction. However, this scenario underscores that reaping the benefits of blockchain technology involves significant upfront investments and ongoing operational costs, including maintenance expenses.

For SMEs using MIS with lower transaction volumes, investing in a complete blockchain-based system may not present a viable business case. Therefore, a reengineering approach to integrate blockchain capabilities into existing MIS systems could be a more practical and cost-effective solution than developing an entirely new blockchain-based system. Such integration would prevent the discarding of existing systems and the high costs associated with entirely new developments.

However, applying reengineering to redesign MIS processes using blockchain is not a straightforward task. Hybrid models that redesign inter-organizational transactions to incorporate blockchain solutions, smart contracts, and sensor-based devices are necessary [3]. This presents significant challenges, particularly concerning costs, scalability, and the integration of existing systems. A critical consideration in this process is determining the fate of current systems and estimating the time and resources required to develop a new blockchain-based system. This requires careful planning and assessment to ensure that any transition to blockchain technology is both feasible and beneficial.

6.2 Blockchain based MIS

Blockchain is a distributed ledger that maintains records of all transactions and has qualities such as robustness, trustworthiness, and security [5]. Transactions are recorded on the blockchain. As can be seen in figure 18, a typical blockchain is comprised of a number of different components and transaction procedures. When a transaction is initiated by a node, it is joined together with other transactions to create a block block. The block is then verified by the network nodes, and after the verification is successful according to the consensus mechanism, the node is added to the blockchain.

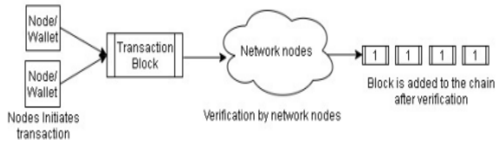

Node/ Wallet
Node/ Wallet
Nodes Initiates transaction
Transaction Block
Network nodes
Verification by network nodes
1
1
1
1
Block is added to the chain after verification

Fig 18. Transaction flow in a Blockchain

6.3 Reengineering Approach for Blockchain based MIS

Reengineering is the process of reorganising a business process in order to produce significant improvements in metrics such as cost, development time, quality, service, and speed. Managers need to explicitly establish goals, as well as rethink and innovate new business processes, in order to keep their businesses profitable and retain their level of competitive advantage. The author offers a conceptual framework that is based on blockchain technology, in which three entities the buyer, the logistics provider, and the supplier transact across a blockchain-based system that is equipped with smart contracts. It is possible to make things easier for supply chain management by redesigning an existing system using this framework in conjunction with autonomous contracts. They are able to monitor the development of cash flows and logistics, and as a result, they may devise plans according to such developments in order to reduce inefficiencies. It has been noticed in this section that a blockchain-based system that is fully functional demands a significant amount of time and expenditure. Therefore, it is recommended that if we use reengineering to restructure existing systems and add a Blockchain module based on the principles of Private blockchain alongside, we will be able to obtain the desired advantages at a low cost and with minimum modifications to the operations of the system that are now in place. An existing system that is based on a centralised client server paradigm and consists of three components (front end, web server, and database) is shown in Figure 19(a). This system is used in an organisation that is either small or medium in size. Using reengineering, the Blockchain architecture for management information systems is shown in Figure 19(b).

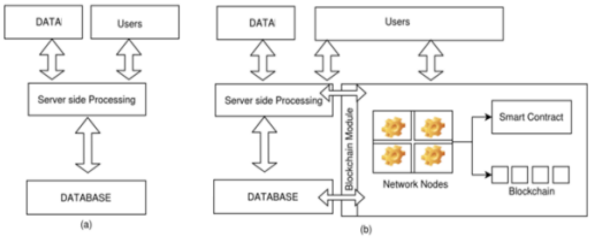


Fig 19. Blockchain framework for MIS using reengineering

The integration of a Blockchain Module into an existing Management Information System (MIS) introduces a significant enhancement in terms of security, transparency, and decentralization. This module comprises three main components, each serving a crucial role in the blockchain ecosystem:

1. **Network Nodes**: These are the fundamental units of the blockchain network. They are responsible for distributed transaction validation. Every node in the network receives data about each transaction initiated in the existing system. Transactions are validated using smart contracts, and upon successful validation, they are added to the blockchain. This process ensures real-time updates are efficiently and effectively disseminated across the network.

2. **Smart Contract**: This component embodies the business process logic and the specifications related to transactions, including clauses that address the concerns of all involved parties. Smart contracts automate the validation process; if any discrepancy or violation is detected, the transaction is automatically declined, citing the specific flaw in the input data. The specifications within smart contracts are based on terms and conditions agreed upon by all stakeholders and participants of the system.

3. **Blockchain**: This is the core component, consisting of a coded chain of transactions, each with their unique hash codes. An efficient linear hash computation scheme is utilized to ensure both traceability and optimization. The chain is replicated across all network nodes, mitigating the risk associated with centralized systems' single points of failure.

The Blockchain Module can be integrated into the existing MIS like a plugin, ensuring minimal interaction with the current systems. The size and complexity of the Blockchain Module can be assessed using the Function Point Analysis (FPA) method, which considers the number of input data items, output items, and files involved.

Development efforts for the Blockchain Module include the following activities:

- Setting up network nodes through a web application.
- Coding and deploying the smart contract code.
- Writing scripts for the consensus mechanism.
- Developing scripts for updating the chain of transactions.

Designed to be cost-effective, the Blockchain Module offers the advantages of blockchain technology without necessitating a complete overhaul of the existing MIS. This approach allows organizations to leverage the benefits of blockchain while maintaining the integrity and functionality of their current systems.

6.4 Implementation Setup

The proof of concept for the proposed framework was implemented using WampServer, a web application platform, on a laptop running Windows 10 with an Intel Core i3 7th Gen processor, 4GB RAM, and a clock speed of 2.3 GHz. The key components of this setup included:

- **Apache Web Server (Apache 2.4.41)**: This software provided the necessary environment for hosting the web application. Apache is a widely-used web server software known for its stability and flexibility.
- **MySQL Database (MySQL 5.7.28)**: For managing the data, MySQL, a popular database management system, was used. It stores and retrieves all the data related to the transactions processed by the system.
- **PHP (PHP 5.6.40)**: The server-side scripting language used for the development of the web application. PHP is commonly used for creating dynamic web pages and is compatible with various databases.

The prototype web application was developed to integrate with an existing cyber-physical system. Transactions from all stakeholders were directed to the Blockchain module. After successful validation within this module, the transactions were recorded on the blockchain. Importantly, this process did not interfere with or affect the existing system. The order processing script in the application managed various types of transactions, including:

- **Purchase of Raw Material**: Handling transactions related to the procurement of materials necessary for manufacturing.
- **Posting Transaction Related to Manufactured Material**: Recording and managing data pertaining to the production process.
- **Sale of Material Produced**: Tracking transactions involved in the selling of the finished products.

One of the critical aspects of this implementation was ensuring that the validation process by the Blockchain module was efficient enough to support real-time validation. The results indicate that the delay introduced by the blockchain validation was minimal, thereby having a negligible impact on the overall performance of the system.

The following section will discuss the results of the test cases performed to assess the effectiveness and efficiency of this integrated system, particularly focusing on how the blockchain module enhances the transaction process without compromising system performance.

6.5 Results

Proposed system was implemented as a proof of concept and results are discussed below.

Performance measurement of the Blockchain Module was conducted to evaluate its efficiency and effectiveness. The module comprises two primary scripts:

1. **Order Processing Transactions Script**: This script is responsible for handling and processing various types of transactions such as the purchase of raw materials, posting transactions related to manufactured materials, and sales of produced materials.
2. **Monthly Transaction Report Generation Script**: This script generates reports summarizing the transactions that occurred over a month.

To measure the performance of these scripts, each was executed 10 times. The focus was on determining the average execution time for both scripts, which serves as a key indicator of the module's operational efficiency. This repeated execution and time recording approach provides a reliable measure of the module's performance under typical operating conditions.

The average execution time is an important metric, as it reflects the real-world usability of the Blockchain Module in a business environment. Ideally, the execution times should be short enough to ensure that the module can handle transactions and generate reports promptly, thereby not causing any significant delays in the overall business process. The results of these performance measurements would provide valuable insights into the feasibility and practicality of implementing the Blockchain Module in a real-world setting, especially in terms of its impact on the efficiency of business operations.

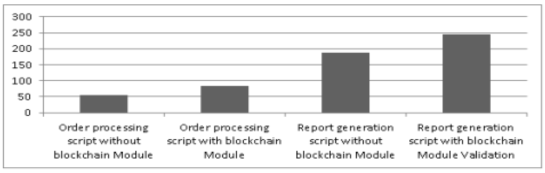


Fig 20. Average Execution Time of 10 transactions for four test cases

The study aimed to evaluate the cost-effectiveness of implementing a blockchain solution in Padmavati Ferrous Limited's (PFL) Management Information System (MIS) operations. The focus was on comparing the running times of basic MIS operations with and without the integration of blockchain technology. The results were aimed at determining the impact of blockchain on performance, particularly in terms of execution time.

The findings, as displayed in Figure 20, encompassed four test cases:

1. **Case 1 (Order Processing without Blockchain)** and **Case 3 (Report Generation without Blockchain)**: These cases represented the baseline execution times for order processing and report generation in the MIS without the use of blockchain technology.
2. **Case 2 (Order Processing with Blockchain)** and **Case 4 (Report Generation with Blockchain)**: These cases demonstrated the execution times for the same operations but with the integration of a distributed blockchain-based ledger, adding traceability and trust to the system.

The results indicated that integrating blockchain into MIS operations had a minimal impact on performance. Specifically, the order processing script with blockchain implementation took an additional 29 milliseconds, and the report generation script with blockchain took 58 milliseconds more.

Additionally, the effectiveness and performance of the blockchain in detecting manipulations in the database were tested. This test was crucial for evaluating the blockchain's capability to trace the source of transaction manipulations. Four test cases were conducted with varying numbers of manipulations (0, 1, 2, and 5) made in the database data post-transaction. All cases were executed successfully, and the results aligned with the expected outcomes. The execution times recorded were 387, 432, 451, and 485 milliseconds, as shown in Figure 21.

This feature is particularly significant for business managers who are concerned about the risk of data manipulation post-transaction, which can lead to serious operational losses. The ability to audit and ensure traceability of manipulations in transactions with a single click adds a layer of security and accountability, thereby enhancing the overall reliability of the MIS. The integration of blockchain technology in this context demonstrates its potential in not only maintaining data integrity but also in improving the overall effectiveness of business operations.

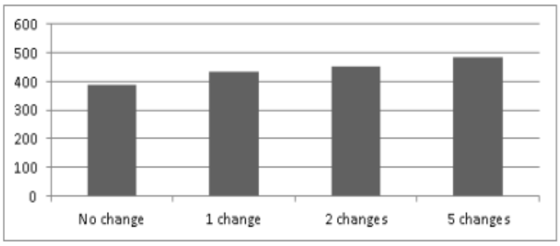


Fig 21. Execution Time of four test cases

7. Performance Evaluation

Performance evaluation of the proposed solution in the research findings is related to the corresponding attributes and co-relating parameters for the study under a network weighted transaction.

To measure the performance in the given social networking environment setup, the system traces a random generation of file loads under a sharing protocol model. The system also ensures the connectivity and the responses of correlating the threshold value existence. In general, the proposed system at the operation mode performs the interconnection into multiple threshold validation. We consider the given random file load to be 500 files independent of the various thresholds set and recorded by the paradigm. We assume the set threshold is 100 to each of the nodes in the array of activation. Then the processing nodes evaluate the parameter for identifying and resolving the interconnected paradigms in the system.

In the NWT, the evaluation of performance is also dependent on the process of allocating the resources and server services as discussed in the early session of the chapter. The server allocated need to be responsive in nature and thus, the same is evaluated in the process. The aim of proposed model is to assure and consolidate the interconnected nodes and data to a secure and safe location of storage.

For the selected files in which the data are stored and saved in the paradigm, the system needs to be provided with sufficient permissions and operation authentication. There could be a permission entreating or misbalancing of the actions of nodes.

Table 2: Simulation Parameters for Social Link

	Real Trace
Environment Parameters	NS-2
Area of Simulation	600m
Number of nodes	100
Range of Communication	50-100m
Size of a file (kb)	10-15

Number of files in each node	100
Querying period	1300s
TTL of each request	200s

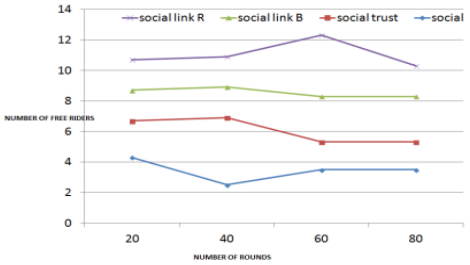


Fig 22. Accumulated Number of Free Riders

Social ordering in the linkage is dependent on the order of trust-based evaluation in the system and thus, the same is demonstrated in Figure 22 and Figure 23 for the correlative analysis. Here the trust factor of the node connectivity depends on the path of maximum distance or length to that of the order of querying file system. This resolves the most ambiguous scenario of operation under node 24 selection and node consideration and misalignment.

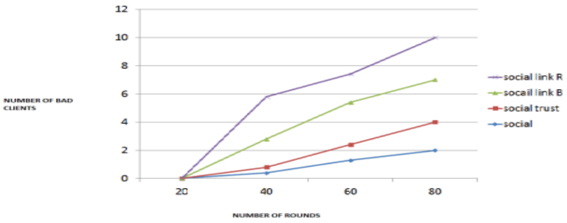


Fig 23. Accumulated Number of Bad Clients

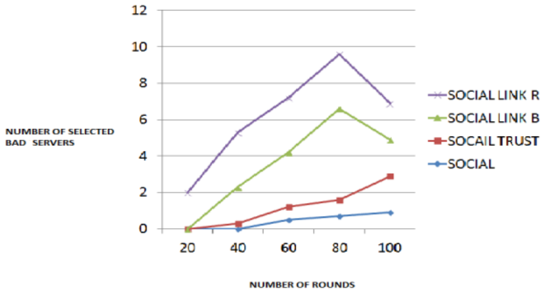


Fig 24. Number of Bad Servers

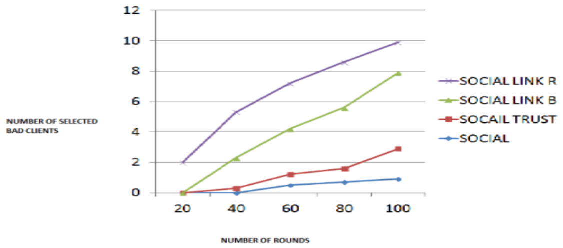


Fig 25. Number of Bad Clients

During the course of an experiment, we discovered that the outcome of Social Link between the Social Trust increased over the course of several rounds (Figure 25). As can be seen in Figure 26, the cumulative number of chosen poor customers will be arranged in the following order: Social Link-B < Social Link-R \ Social Trust.

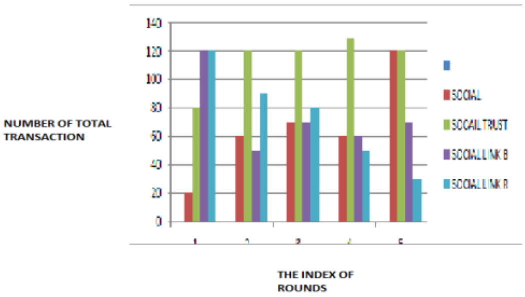


Fig 26. Number of Total Transactions

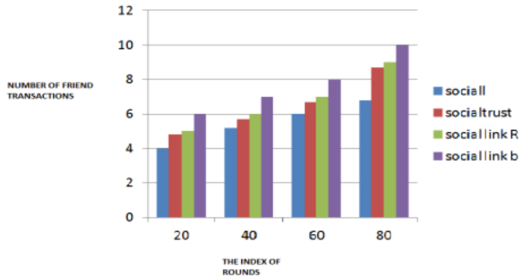


Fig 27. Number of Friend Transactions

The complete node connection will be withdrawn from the network when a new node is added to the network, according to Social connection-B. There will be suspicious transactions carried out by Social Link-R (Figure 27), which will have a reported score of the undesirable nodes that are identified by the server using the settings that have been applied.

The research objective of this chapter is to define and propose a novel approach for secure and reliable file sharing over a peer to peer connected networking environment. The proposed scheme or technique is based on the reputation prediction and detection of the neighbouring nodes in retrieving the mutual relationship and its augmented properties for a secure communication process. The process is provided over a social media platform forming a reliable and un-bounded stream of relationships between the nodes and the network for communication or the transaction to becompleted.

Table 3: Summary of NWT Techniques

	NON NP-TRUST	NP-TRUST
Network Weighted Graph Ratio	7.4	9.6
Performance Ratio	8.3	8.9

Ratio of Nearness	6.2	9.87
Positive Feedback Ratio	5.9	8.45
Attack Resistance	6.89	8.23

The discussed schema proposes a Network Weighted Transaction (NWT) model to predict and evaluate a social link connection over a secure file sharing without any prior need of permissions and acknowledgements. The social link manages weighted information for the successful transaction using most likely used mutual friend or the node for communication. The proposed schema also evaluates (Table 3) on the different types of attacks such as Sybil and whitewashing and has extended its approaches to validate and verify the resistance while attackers are in place. The system has shown a effective productively in connection simplification and performance in a real-time scenario of validation.

8. Conclusion

Blockchain technology, a relatively recent innovation, has been gaining prominence but also facing increased cyber threats due to prevalent misunderstandings and misconceptions. The aim of this article was to assess the security of Blockchain systems and provide a framework for evaluating their security. The study commenced with an exploration of Blockchain as a technological advancement, revealing that its primary application is for decentralization rather than security.

The research included the compilation and analysis of 78 real-world hacking and heist incidents involving Blockchain. These incidents were categorized based on the nature of the exploitation or attack surface: Platform Breach, dApps Exploit, Access Point Attack, or Endpoint Hacking.

A detailed breakdown and examination of the data led to several key findings:

1. **Increasing Financial Losses**: There has been a significant rise in monetary losses due to cyberattacks over the years.
2. **Evolving Hacker Techniques**: Blockchain technology is increasingly targeted by hackers as their methods become more sophisticated.
3. **Inadequate Response and Security Repair**: Blockchain systems have been slow and insufficient in responding to security breaches, often suffering from repeated types of hacks over the years.
4. **Vulnerability of Cryptocurrency Systems**: Cryptocurrency systems have been particularly susceptible to the catastrophic impacts of hacking.
5. **Closure of Blockchain Enterprises**: Several Blockchain businesses have shut down due to hacking and heists.
6. **Authentication as a Key Security Component**: Since decentralised systems primarily rely on user authentication for security, over half of the cyberattacks target this process.

Two specific cyberattacks, on the Ethereum Blockchain system and the Bitfinex cryptocurrency exchange system, were chosen for in-depth analysis using Causal Analysis using System Theory (CAST). The investigation revealed several flaws in Blockchain systems:

- **Overreliance on Inherited Security Features**: Many Blockchain security controls depend heavily on the inherent security features of the technology.
- **Need for Transparency and Openness**: Blockchain systems require openness due to their autonomous nature, including disclosure of security challenges and incident response actions.
- **Lack of Centralized Security Administration**: In decentralized systems, the absence of a single entity overseeing security leads to slow and ineffective incident responses and inadequate post-incident security fixes.

The article also addressed common misconceptions about Blockchain security, clarifying that Blockchain is not immutable, does not guarantee anonymity, its openness does not equate to security, and it is not immune to hacking. This comprehensive analysis underscores the need for continuous development and robust security measures in Blockchain systems.

Author contributions

Sony Kumari: Conceptualization, Methodology, Software, Field study, Data curation, Writing-Original draft preparation, Software, Validation., Field study. **Dr. Manoj Eknath Patil:** Visualization, Investigation, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund. (2019) "Blockchain technology in healthcare: a systematic review." In Healthcare, Multidisciplinary Digital Publishing Institute, vol. 7, 56, pp. 1-30.

[2] Ahram, Tareq, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba. (2017) "Blockchain technology innovations." IEEE Technology &

Engineering Management Conference (TEMSCON17), IEEE, pp. 137-141.

[3] Akın, Yasin, Caner Dikkollu, Bekir Baran Kaplan, Uğur Yayan, and Esra Nergis Yolaçan. (2019) "Ethereum Blockchain Network-based Electrical Vehicle Charging Platform with Multi-Criteria Decision Support System."1st International Informatics and Software Engineering Conference (UBMYK-19), IEEE, pp. 1-5.

[4] Akyuz, Goknur Arzu, and Guner Gursoy. (2020) "Transformation of Supply Chain Activities in Blockchain Environment." In Digital Business Strategies in Blockchain Ecosystems, Springer, Cham, pp. 153-175.

[5] Alamri, Malak, N. Z. Jhanjhi, and Mamoona Humayun. (2019) "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review." Int. J. Comput. Sci. Netw. Secur 19, pp. 244-258.

[6] Ali Fattaholmanan, Hamid R. Rabiee, Senior Member, IEEE (2015) “A Large-scale Active Measurement Study on the Effectiveness of 134 Piece-Attack on BitTorrent Networks.” IEEE Transaction On Dependable And Secure Computing.

[7] Ali, Imran, and Nadeem Javaid. (2018)"Delay management and Security for States and Actions Involves Gaming Network based on the Blockchain." IEEE Access.

[8] Ali, Muhammad Salek, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, and Mubashir Husain Rehmani. (2018a) "Applications of blockchains in the Internet of Things: A comprehensive survey." IEEE Communications Surveys & Tutorials 21, no. 2, pp. 1676-1717.

[9] Al-Saqaf, Walid, and Nicolas Seidler. (2017) "Blockchain technology for social impact: opportunities and challenges ahead." Journal of Cyber Policy 2, no. 3, pp. 338-354.

[10] Angraal, Suveen, Harlan M. Krumholz, and Wade L. Schulz. (2017) "Blockchain technology: applications in health care." Circulation: Cardiovascular Quality and Outcomes 10, no. 9.

[11] Aras, Supriya Thakur, and Vrushali Kulkarni. (2017) "Blockchain and Its Applications–A Detailed Survey." International Journal of Computer Applications 180, no. 3, pp. 29-35.

[12] Bahga, Arshdeep, and Vijay K. Madisetti. (2016) "Blockchain platform for industrial internet of things." Journal of Software Engineering and Applications 9, no. 10, pp. 533-546.

[13] Bore, Nelson, Samuel Karumba, Juliet Mutahi, Shelby Solomon Darnell, Charity Wayua, and Komminist Weldemariam. (2017) "Towards blockchain-enabled school information hub." In Proceedings of the Ninth International Conference on Information and Communication Technologies and Development, pp. 1-4.

[14] Bozic, Nikola, Guy Pujolle, and Stefano Secci. (2016) "A tutorial on blockchain and applications to secure network control-planes." 3rd Smart Cloud Networks & Systems (SCNS), IEEE, pp. 1-8.

[15] Buccafurri, Francesco, Gianluca Lax, Serena Nicolazzo, and Antonino Nocera. (2017) "Overcoming limits of blockchain for IoT applications." In Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1-6

[16] Cha, Hyun-Jong, Ho-Kyung Yang, and You-Jin Song. (2018) "A Study on Access Structure Management of CP-ABTD Based Blockchain for Medical Information Monitoring System." Advanced Science Letters 24, no. 3, pp. 2026-2030.

[17] Chen, Guang, Bing Xu, Manli Lu, and Nian-Shing Chen. (2018a) "Exploring blockchain technology and its potential applications for education." Smart Learning Environments 5, no. 1.

[18] Choudhury, O., Sarker, H., Rudolph, N., Foreman, M., Fay, N., Dhuliawala, M., Sylla, I., Fairoza, N., & Das, A. K. (2018). Enforcing Human Subject Regulations using Blockchain and Smart Contracts. Blockchain in Healthcare Today, 1. https://doi.org/10.30953/bhty.v1.10

[19] Chung, K., Yoo, H., Choe, D. and Jung, H. (2019) “Blockchain network based topic mining process for cognitive manufacturing.” Wireless Personal Communications, 105(2), pp. 583-597.