JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 10 Number 1 | June 2025: 177-195
DOI: 10.15575/join.v10i1.1545

Reviewing the Blockchain's Framework and its Role in Sustainable Industries

N. Nasurudeen Ahamed[1], Tanweer Alam[2], Mohamed Benaida[3]
[1]College of Information Technology, United Arab Emirates University, Abu Dhabi, UAE
[2,3]Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah, Saudi Arabia

Article Info

Article history:

Received December 31, 2024
Revised April 16, 2025
Accepted April 17, 2025
Published May 10, 2025

Keywords:

Blockchain
Bitcoin
Cryptography
Cryptocurrency
Supply Chain

ABSTRACT

Blockchain technology is often regarded as a highly advanced and pioneering breakthrough in modern times. Blockchain technology is a distributed ledger that uses encryption to prevent security breaches and securely stores data across many systems. This facilitates collaborative transactions by providing a solitary, dependable reference point, revealing the purported trust intermediaries. This study aims to investigate the core principles of blockchain technology and assess its potential to support sustainability across various sectors. It seeks to examine how blockchain technology enhances reliability, effectiveness, and transparency in industries such as supply chain management and the energy sector. This study addresses these concerns by assessing the valuable applications, advantages, and drawbacks of blockchain in promoting sustainable industrial practices. Bitcoin and other cryptocurrencies rely on hashing as the foundation of their blockchain technology. Blockchain is a digital ledger that documents and tracks financial transactions. Blockchain technology has become prevalent across several sectors, encompassing artificial intelligence, machine learning, and the Internet of Things. Therefore, once the blockchain is prepared for dissemination, the data cannot be modified by anyone. This implies that it is immutable. Hyperledger offers a neutral platform for facilitating collaborative operations among organisations that frequently engage in competitive activities. Hyperledger is specifically designed to provide explicit support for blockchains as a means of business agreements. Authorisation is a prerequisite for a framework, ensuring that only those with proper authorisation can join the organisation. The ability of the manager to impose limitations on user access to the blockchain enhances security measures. Moreover, instead of being universally accessible through online platforms, trades are maintained secretly, limiting access to only essential participants. Using distributed code bases and open-source record upgrades facilitates enhanced efficiency in corporate activities. The fast expansion of blockchain technology has led to its widespread adoption across several industries worldwide. Illustrations encompass various domains, including logistics, copyright, finance, medicine, and supply chain management. Furthermore, we offer an introductory overview of blockchain technology, encompassing topics such as different types of blockchains and their utilisation across many sectors.

Corresponding Author:

Tanweer Alam
Department of Computer Science, Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah, Saudi Arabia
Email: tanweer03@iu.edu.sa

1. INTRODUCTION

During the era of computerization, various domains, such as Machine Learning, Artificial Intelligence, the Internet of Things, and Blockchain Technology, have experienced rapid advancements. This paper examines the concept of Blockchain innovation. It is a rapidly evolving concern among legislators, private investors, and technology developers. The most widely acknowledged modern use of Blockchain technology. Due to the growing interest in Blockchain and its implementation in various sectors and industries, many sectors focus on key areas for Blockchain applications [1], including finance, business, technology, voting, and other educational and medical applications. Regardless, Blockchain is an additional technological advancement. While there is considerable enthusiasm regarding its anticipated benefits, there is also substantial misinformation and risk regarding the overall utility of the Blockchain. Blockchain is a highly advanced technology that combines the principles and advancements of the Internet of Things (IoT) and artificial intelligence (AI) conflicts [2]. The Blockchain model integrates blockchain technology with a consensus mechanism. Cryptography refers to utilizing the Blockchain network as a foundational framework for establishing a security system in various domains [3]. Consequently, the Blockchain framework employs the SHA256 hash to prevent data leakage in each transaction [4]. On the other hand, the Consensus Mechanism pertains to the communication between the client and the server, wherein each transaction can be updated based on evolving standards within the transaction. Additionally, this represents the foundational phase or procedure within the Blockchain network. Blockchain frameworks inherently rely on cryptographic techniques to ensure the integrity and confidentiality of the data [5], [6]. The term "trustworthiness" refers to the ability to identify or prevent the alteration of information in this particular context. In the absence of pre-established trust, this quality appears to be one of the key characteristics of the system [7]. In addition, the security of Blockchain relies on the necessity of public-key cryptography. Public-key testaments are utilised to obtain characters, such as clients and exchange personalities. Ensuring secure key management is crucial for any Blockchain. Losing private keys in this security system results in a loss of access. In every scenario, losing access to Blockchain applications, such as digital currency, results in an instantaneous and irreversible financial impact. Confidential keys authenticate transactions securely, ensure integrity, and prevent unauthorized client data modification. The Blockchain facilitates the exchange of information through a centralised ledger, wherein replication occurs using a shared communication protocol, ensuring transparency and data availability. This exchange occurs through the transfer of information between hubs in the form of blocks, which are collectively hashed and verified. The subsequent sections of the paper are succinctly summarised as follows: Section 1 provides an overview of the paper, Section 2 delves into the fundamental principles of blockchain technology, Section 3 explores the taxonomy and functionalities of blockchain, Section 4 presents a consensus algorithm for blockchain, and Sections 5 and 6 delve into the analysis of the study and the application of blockchain in various industries. Finally, a conclusion is provided.

Definition of Research Questions:

Research Question 01: What are the benefits of this work for future researchers?

Blockchain has emerged as a prominent and transformative technology in contemporary society. This paper examines the integration of blockchain technology in various major industries and its operational mechanisms, including examples such as managed supply chains, Intellectual Property Rights, and the Energy Industry.

Research Question 02: What makes our survey superior to others?

This survey aims to provide comprehensive information regarding Blockchain and Blockchain Platforms, such as Hyperledger. Within this Hyperledger Framework, we extend our focus beyond Hyperledger Fabric only. This paper examines various Hyperledger frameworks, including Hyperledger Indy and Hyperledger Burrow, and their applications in the industrial sector.

2. METHOD

2.1. Blockchain Description

The Blockchain is a decentralised innovation or a circulated record on which transactions are securely recorded anonymously. By 'partitioning' informational collections among various get-togethers, Blockchain essentially dispenses with the requirement for go-betweens who were as of late expected to go about as trusted in outcasts to affirm, record, and bear trades, by working with the move from a concentrated to a decentralised and disseminated framework (Centralized, Decentralized, and Distributed).

- Centralized – Single Master.
- Decentralized – Each node has its own Master.
- Distributed – Each node connects with a single task (No Master Required).

2.2. *History of Blockchain*

Blockchain emerged in the mid-1990s. The concept was introduced in 2008 and implemented in 2009. Following the adoption of technology, the industry experienced rapid growth after 2009. For instance, individuals have been engaging in digital transactions and using cryptocurrencies within the financial markets. Ultimately, Blockchain assumes a significant role in the industry.

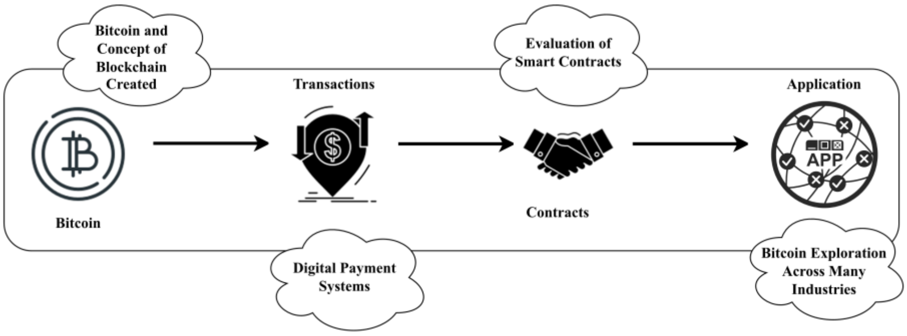
Bitcoin and Concept of Blockchain Created
Transactions
Evaluation of Smart Contracts
Application
APP
Bitcoin
Contracts
Digital Payment Systems
Bitcoin Exploration Across Many Industries

Figure 1. History of Blockchain

2.3. *Blockchain Architecture*

Blockchain is an organisation of squares (hubs) that are associated with each other, rather than a central server, based on geographical proximity. It can store the exchanges in the record and affirm straightforwardness, security, and suitability (Figure 2).

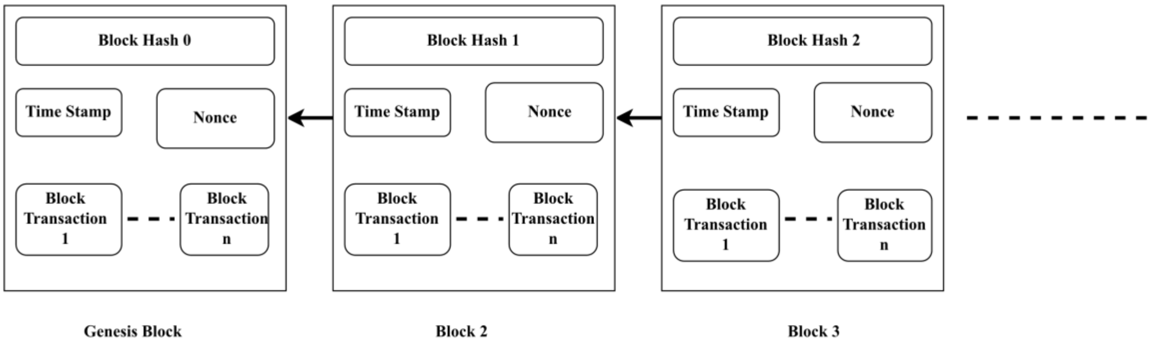

Figure 2. Basic Blockchain Diagram

A basic Blockchain Diagram comprises many Components recorded below:

- **Block:** In the Blockchain innovation, a block is a decentralized hub/excavator equipped with an information base containing a computerized snippet of data. Blocks are connected, containing the hash value of the previous square within the current square. [First Square (Genesis)], the block design can be visualized into a block header and a rundown of transactions [8]
- **Time Stamp:** The hour the square was created. (4 Bytes).
- **Nonce:** Registers the various hashes. (4 Bytes)
- **Block Transaction:** Generated the Transaction. Working as Merkle Tree.
- **Merkle Tree:** A hash of each transaction in a block. (32 Bytes)

- **Merkle Root**: The hash worth of many exchanges in the square.

Figure 3 shows the working Merkle root, which is created from the exchange's hash upsides. The first hash is the hash value of the past square, and the Merkle root is used to verify the exchange's legitimacy. Blockchain utilizes a decentralized cryptography system to confirm transaction validation. Given flawed cryptography, a computerized signature is used in a deceptive context.

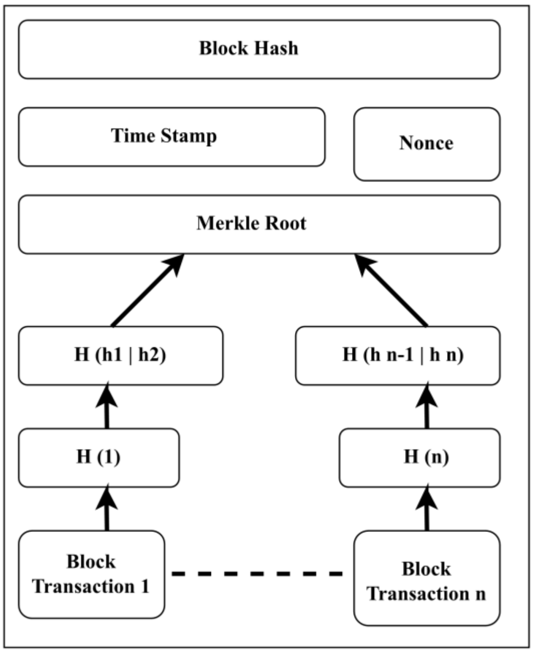

Figure 3. Merkle Tree Structure.

2.4. *Blockchain Cryptography*

Blockchain is a distributed ledger technology that securely records transactions over many nodes [9]. Cryptography safeguards against unauthorized data alterations while also facilitating the process of approving and appending new blocks to the Blockchain. Next, we briefly demonstrate a sophisticated (digital) signature.

2.5. *Digital Signature Algorithm (DSA)*

A computerized signature is a notable technological advancement that ensures authentication, which is significant in cryptography. A basic cryptographic algorithm, known as a digital signature, guarantees transmitted messages' integrity, authenticity, and non-repudiation. People have recognised additional types of symbols and incorporated symbols in a broader range of domains. For example, within the domain of. Blockchain. Upon signing, everyone can verify. This suggests that the Signature is associated with a particular archive. The item cannot be reordered to a different report. The randomised algorithm in digital signatures was referenced in Equation (1)

$$\begin{aligned}&\text{Valid} = \text{Verify}(pk,msg,sg)\\&\text{Sg} = \text{Sign}(sk,msg) \qquad sk,pk = \text{generatekeys}(keysize)\end{aligned} \tag{1}$$

Where,

- sk = Secret Signing Key.
- pk Public Verification Key.
- msg=Message.
- sg=Signature.

Every user is expected to hold a pair of private and public keys. The private key authenticates the transactions. The digital transactions are distributed throughout the organization and accessed by public keys, visible to all organization members. Figure 4 depicts the automated signature employed in the Blockchain. According to equation (1), the advanced mark (signature) is involved in two distinct stages: the marking and confirmation stages.

If User A is required to sign a transaction, User A first generates a hash value derived from the transaction. Subsequently, User A uses User A's private key to obfuscate the hash value and transmits another hash, encoded by User B, that contains the initial data. Sway verifies the received transaction by comparing the unscrambled hash (using User A's public key) with the hash value obtained from the received data using the same hash function as User A. The ECDSA algorithm is effectively employed in Blockchain technology [10].

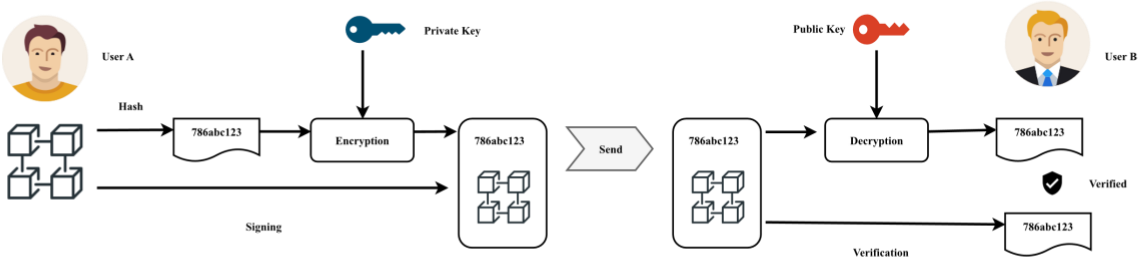

Figure 4. Block Verification Using Digital Signature

2.6. *Elliptic Curve Digital Signature Algorithm (ECDSA)*

Every user is expected to hold a pair of private and public keys. The private key authenticates the transactions. The digital transactions are distributed throughout the organization and accessed by public keys, visible to all organization members. Figure 4 depicts the automated signature employed in the Blockchain. According to equation (1), the advanced mark (signature) is involved in two distinct stages: the marking and confirmation stages.

The signature computation is employed to verify the authenticity of a device or a message transmitted by the device. Consider Two Users, A and B, as an example. User A sends a message to User B, instructing them to utilise their encrypted private key. According to [11], User B receives the message from User A, instructing them to use their decrypted public key. To transmit a marked message from A to B, both parties must agree on the bounds of the Elliptic Curve area. The Elliptic Bend Advanced Mark Calculation is similar to the DSA technique when applied to the elliptic bend. When User A transmits the transaction to User B, it is necessary to include the signature at the time of transaction creation, as depicted in Figure 5.

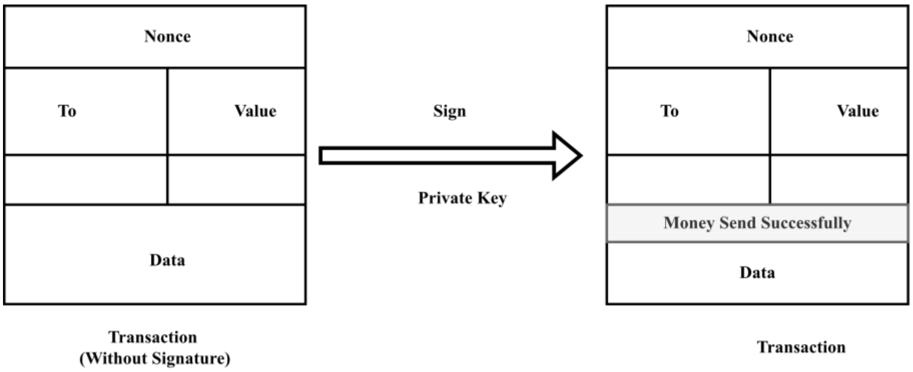

Figure 5. Launch a Transaction

These exchange objects should be endorsed to become marked exchanges. To do this, the elliptic bend advanced mark calculation will be used [12]. First, the hash of the exchange is calculated, and then the hash is agreed upon to obtain the mark, which is supplemented into the unsigned exchange object to complete the formation of the market exchange. Currently, it is prepared to present the exchange to the exchange pool, as shown in Figure 6.

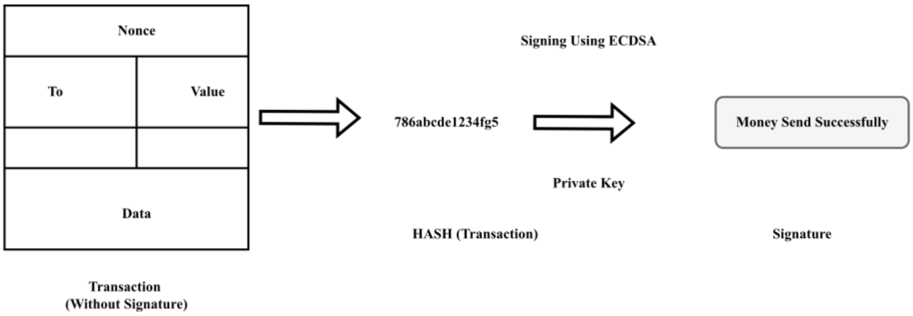

Figure 6. Transaction Using Signature

2.7. *Curve Parameter*

The boundary points a and b, which are different boundaries, should be concurred upon by the two players associated with the got and believed correspondence utilizing the Elliptic Curve. The accompanying Table 1 characterizes a few documents.

Table 1. Format Symbols and Their Description

Format Symbol	Description
A	private key
B	public key
N	modulus
S	digital signature
W	hamming weight
E	elliptic curve
F	finite field
G	group of points
P	prime field
Fp	Finite prime field
Mod	Modular
M	message
K	random integer
k-1	inverse of k
H	hash value
h()	hash function

An outline of the ECDSA (Elliptic Curve Digital Signature Algorithm) process is presented in Table 2 below.

ECDSA Sign Generation

User A signs the message m with a digital signature to generate the signature in Table 2.

Table 2. Signature Generation

Step 1	Select a random integer k, [1, n-1]
Step 2	Calculate h, has value and hash function[h()], example: SHA
Step 3	Calculate r = x(mod n) where, (x,y)= kG , if r=0 goto step 1 [reselect random integer]
Step 4	Calculate s=k-1(h+ra)(mod n) , if s=0 goto step 1 [reselect random integer]
Step 5	Signature Pair (r,s), [User A sends the message in the pair(r,s) verified by user B]

gn Verification

After receiving the message M from user A to user B, the public key (i.e., b = aG) is used in Table 3.

Table 3. Signature Verification

Step 1	Verify the signature pair r and s In the interval of [1, n-1], on the off chance that not, the mark is invalid
Step 2	Calculate h=h(M)
Step 3	Calculate u=hw(mod n) and v=rw(mod n)
Step 4	Calculate (x,y)=uG+vb [r1=x(mod n)]

Step 5	The Signature is valid when r = r1; otherwise, it's invalid.

2.8. Hash Function

A significant part of Blockchain innovation is the utilisation of cryptographic hash capacities for some activities. Hashing is a strategy for applying a cryptographic hash function to data, which computes a unique result for any contribution, regardless of size. Hashing is arguably the primary component of Blockchain innovation. It authorizes safety efforts on hubs, confirms transactions, and adds blocks to the Blockchain through hash functions. Hashing is a significant numerical activity utilized in Blockchain stages. Figure 8 shows the data before hashing.

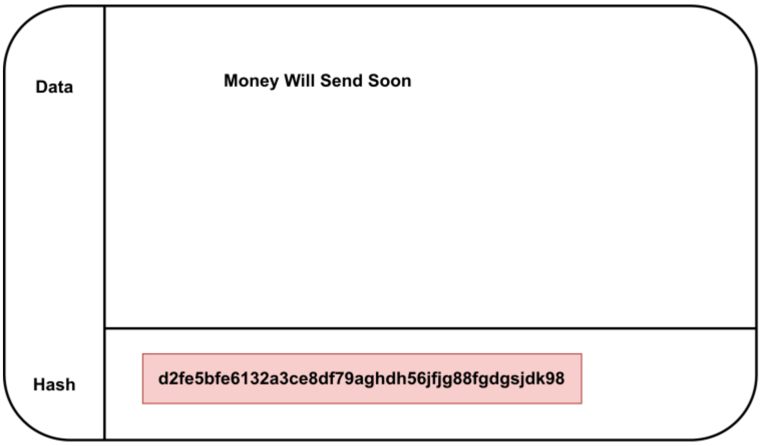

Figure 7. Before Hashing Data

Hashwork is a numerical planning activity involving a set of whole numbers with a dynamic size and a set of fixed size. Applying hash capacity to information is called hashing. Hashing is deterministic and is utilized in applications such as information verification, data analysis, and performing other data calculations or operations [13].

Given input information to various frameworks to calculate the hash value, all frameworks will provide the same service. Hashing can be utilized in multiple ways for storing sensitive data; a model is key checking. Hash functions are designed in an irreversible and novel way to fortify the protection and security of stored information. This implies that the hash values created by a PC with specific details can't be used to retrieve the original information. This is because the approved PC (client) will receive a duplicate of the information and, subsequently, compute its hash value to make a correlation with the first. This correlation, nonetheless, affirms the legitimacy of the given information.

2.9. SHA 256 Hashing

The SHA256 calculation takes information with a length of less than 2^64 bits. A specific cryptographic hash work used in various Blockchain executions is the Secure Hash Algorithm (SHA), with a result size of 256 pieces (SHA-256). The SHA-256 method is illustrated in Figure 8.

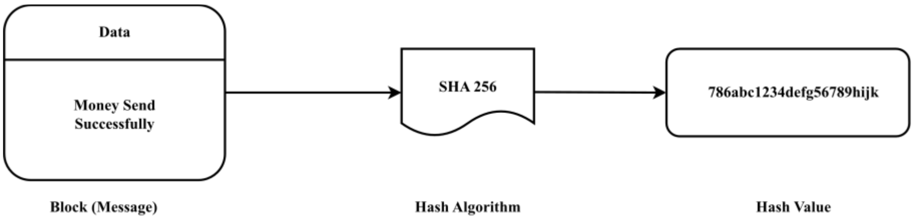

Figure 8. SHA 256 Method

Numerous PCs support this calculation in equipment, making it quick to register. SHA-256, which is derived from 32 bytes (each byte comprising 8 bits, and 32 bytes comprising 256 bits), is typically displayed as a 64-character hexadecimal string. Figure 9 shows the data after hashing.

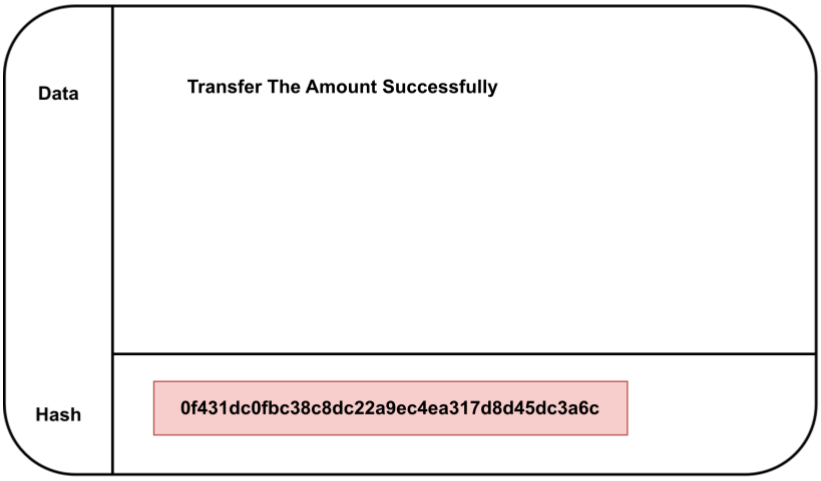
Data
Transfer The Amount Successfully
Hash
0f431dc0fbc38c8dc22a9ec4ea317d8d45dc3a6c

Figure 9. After Hashing Data

3. RESULT AND DISCUSSION

3.1. *Blockchain Taxonomy*

Currently, there are three types of Blockchain networks in use. They are,

- Permissionless Blockchain.
- Permissioned Blockchain.
- Hybrid Blockchain.

Permissionless Blockchain: A Permissionless Blockchain is essential, with no limitations on passage to utilise it. As the name suggests, anyone and anything can be a part of it without authorization. Permissionless Blockchain, in which the approval of exchanges relies upon agreement. Generally, it is disseminated, where everyone distributes the new blocks and recovers blockchain content. In a public Blockchain, each node is permitted to keep a copy of the Blockchain, which supports the new blocks. {Example: Bitcoin.}.

Bitcoin: Bitcoin is a Blockchain innovation that relies on Cryptocurrency (e-cash or digital money), which is a decentralized, shared network in nature, with no intermediaries like banks or a single authority. **Ethereum:** Ethereum is a Public/Permissionless type of Blockchain, which is a decentralised registering stage that runs 'Brilliant agreements usefulness' and 'Digital money exchanging' safely, without the need for an outsider [14].

Permissioned Blockchain: It requires authorization from the specific association or proprietor to access any portions of the Blockchain. Assuming a hub will accompany it, it must be an individual from that single association [15]. This new hub must send a unique exchange and is expected to participate in the agreement component. The private Blockchain is helpful and generally preferred for individual business solutions, tracking data movement between various offices. {Example: Hyperledger}. Hyperledger: Hyperledger is a multi-project, open-source collaborative effort presented by The Linux Foundation, established primarily for the cooperative development of blockchain-based distributed records and the advancement of cross-industry collaboration. It doesn't uphold Bitcoins or other digital forms of money [16], [17].

Hybrid Blockchain*:* A Hybrid Blockchain combines a public and private section. It is additionally permissioned; however, rather than a single entity controlling it, multiple associations could each work as a node within such an organization. A pre-chosen gathering of hubs controls the agreement interaction. However, different hubs might be permitted to create and evaluate new exchanges.

Blockchain Works: A Blockchain is a square chain containing information or data. Every square in the Blockchain stores some conditional data alongside the hash of its past square. A hash is an exceptional numerical capacity that has some restricted intel about a particular block [18]. The association of squares through remarkable hash values makes the Blockchain safer. The hubs of Blockchain approve every single exchange that occurs in it. These hubs are designated as "excavators."

Blockchain is a standard, distributed ledger among a network of partners that cannot be altered; no one can update it. It must be refreshed with the understanding of organisation members, and all changes to the disseminated record are auditable in Figure 10.

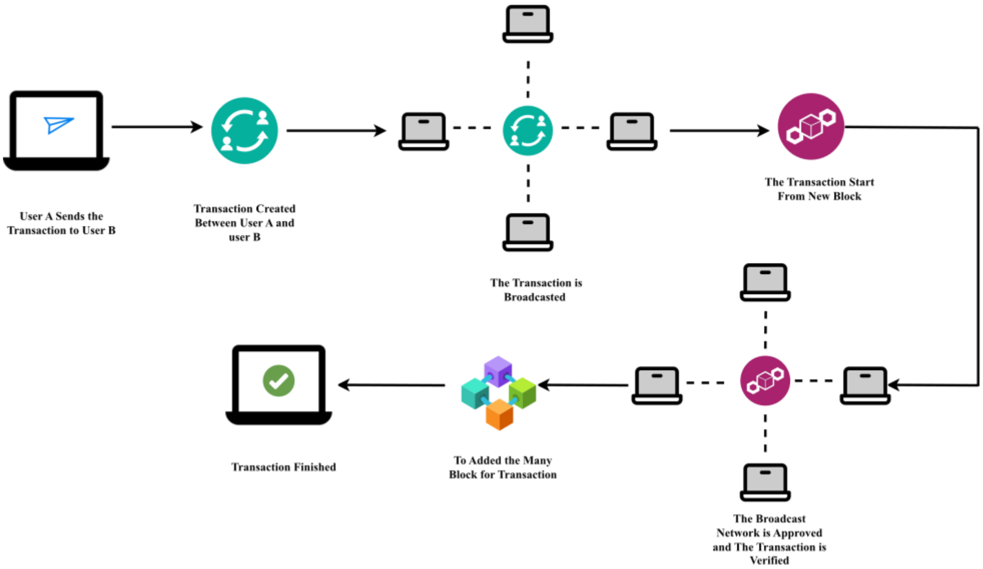
User A Sends the Transaction to User B
Transaction Created Between User A and user B
The Transaction is Broadcasted
The Transaction Start From New Block
The Broadcast Network is Approved and The Transaction is Verified
To Added the Many Block for Transaction
Transaction Finished

Figure 10. Blockchain Transaction Works

An exchange is considered substantial if it matches the hash of its preceding block. Only after it is validated is it added to the chain. Assuming that the programmer attempts to adjust the information in the square or hack the organization, the hash value associated with that block also changes. Subsequently, the break in the Chain organisation will be recognised, as the altered hash will not match the genuine one.

3.2. Blockchain Attributes

a) Information straightforwardness

Blockchain innovation incorporates components to guarantee that stored records are accurate, tamper-proof, and from an unalterable source. Accordingly, rather than various gatherings maintaining and updating duplicates of their dataset, each partner now has controlled access to a shared dataset, creating a single source of truth.

b) Security

Conventional records typically provide a comprehensive layer of security, which, once compromised, allows access to all stored information. In a Blockchain-based framework, the security instruments ensure that individual transactions and messages are cryptographically signed. This ensures fundamental security, providing a more practical approach for the board to manage the current high risks of hacking, data breaches, and data compromise.

c) Resource the Board.

Blockchain innovation can be utilized to address the ownership of digital assets and facilitate resource transfers. For instance, it is often used to follow the responsibility for (e.g., land titles and precious stone authentications) and to protect freedoms (e.g., copyright and mineral rights).

d) Savvy contracts

Manual cycles ordinarily governed by formal agreements can be automated with a self-executing computer program called a smart contract. A savvy contract is part of a Blockchain-based framework that can naturally implement partner-concurred rules and interaction steps. When sent off, brilliant agreements are entirely independent; when agreement conditions are met, pre-indicated and concurred activities happen consequently.

3.3. Blockchain Consensus Algorithm

Agreement (Consensus) calculations are critical for Blockchain P2P (Peer-to-Peer) organisations. Numerous agreements can be calculated to build Blockchain agreement instruments, which can be arranged into any gathering [19].

1. Types of Blockchain Consensus Algorithm

A Blockchain network is a complex and critical undertaking. New exchange records would be added to the blockchain as all hubs in the organization verify the new block [20]. It should be noted that whenever blocks are confirmed, they cannot be altered or erased. The construction of Blockchains is intended to be legitimate in a trustless and untrustworthy organisation with ill-disposed clients. Different strategies are planned and created as agreement calculations [21]. As indicated by blockchain development, the number of these calculations is increasing daily.[22]. Nonetheless, in this part, we will present the main agreement algorithms generally utilised in Blockchain networks.

a) **Proof–of–Work (PoW):** The most notable consensus strategy is Proof of Work (PoW), which was proposed by Nakamoto and is utilized in Bitcoin. Proof of Work has been around for a long time as a suitable strategy for cryptocurrency. In this strategy, the PC does numerous calculations to tackle a mathematics puzzle [22]. This puzzle-tackling is done through the Hash work. Hash is an arbitrary and complex numerical algorithm used to verify the transactions stored in blocks. In short, each square comprises the hash of the previous square, a background marked by transactions, nonce, and the current square hash. An excavator, the PC attempting to settle the hash, will try to observe a particular worth as a nonce so that the hash esteem meets a pre-characterized condition.

b) **Proof–of–Stake (PoS):** The PoS calculation relies on the principle that the maker of the subsequent square ought to be chosen utilizing various mixes of arbitrary determination, stake supply, and maturity, which can offer great adaptability.

c) **Delegated Proof of Stake (DPoS):** The number of representatives is limited, which makes it possible to organize the network more efficiently. Each agent can determine the optimal time to distribute each block. This strategy has been utilised in Bitshares. In any case, this restriction on the number of representatives would make the organisation more incorporated.

d) **Proof of Elapsed Time (PoET):** It is similar to Proof of Work (PoW), where every excavator is expected to address a hash issue. Each square approver (miner) is chosen in the briefest anticipated time [23] and for a solid capacity because of square creation.

e) **Practical Byzantine Fault Tolerance (PBFT):** The Byzantine Generals Problem exists in Blockchain since Blockchain P2P networks are decentralized, and there are no central or trusted hubs in Blockchain P2P organizations. This agreement technique is used to address the Byzantine General problem. The present vindictive attacks on programming have become increasingly common. The growing reliance of businesses and states on internet-based data services will make malicious attacks more appealing and increase the severity of the consequences. Furthermore, the number of programming errors has increased due to the growing size and complexity of the product. Since malicious assaults and programming blunders can be an aftereffect of erratic (Byzantine) conduct of flawed hubs, the significance of the Practical Byzantine Fault Tolerance calculation can be perceived [24].

f) **Delegated Byzantine Fault Tolerance (DBFT):** This technique adheres to the guidelines of the PBFT; however, it does not require the support of all hubs during the democratic phase to add another square. Various hubs are chosen as agents of different hubs and given a progression of rules, follow a consensus process similar to the PBFT strategy. In this technique, a select group of expert hubs cast a vote to record exchanges for all hubs.

g) **Proof of Weight (PoWeight):** In a Blockchain view of Proof of Weight, a weight is associated with every client. The weight is determined by various factors, which prompt different agreement calculations based on evidence of weight.

h) **Proof of Burn (PoB):** Confirmation of consumption is optional for reaching consensus in a Blockchain network. The idea behind it is that miners should not expend energy or time demonstrating that they have accomplished something difficult.

i) **Proof of Capacity (PoC):** Miners use the free space on their hard disk to mine free coins. The leading digital money that used this calculation was Burstcoin, established in 2014. The PoC calculation comprises plotting the hard drive, which means processing and putting away arrangements on your hard circle before the mining starts [25]. A few arrangements are quicker than others. Assuming a hard drive has stored the quickest (nearest) answer for the new square's riddle, then it wins the square.

j) **Proof of Importance (PoI):** The Proof of Importance (PoI) is another agreement calculation that was first introduced in the NEM project to address criticisms of the Proof of Stake calculation. Each record or hub is assigned a significance score, which affects the likelihood of the air conditioner count receiving a small monetary reward in return for adding clients' transactions to the organization.

k) **Proof of Activity (PoA):** Verification of Activity (PoA) depends on the combination of Proof of Work (PoW) and Proof of Stake (PoS). It is a practically safe calculation against potentially reasonable assaults on Bitcoin and has a low penalty regarding organizing communication and additional space.

l) **Directed Acyclic Graphs (DAG):** DAGs are fundamentally an information structure and are not genuine Blockchain networks; we chose to include them in this paper as they are generally utilized in effective digital currencies. Likewise, being familiar with the elements of DAG can assist perusers with bettering comprehending the Blockchains [26]. Figure 11 shows the Blockchain Structure in DAG.

$$\boldsymbol{(DAG)G = (B,P)} \tag{2}$$

Where,

- B- Blocks.
- P- Points.

To such an extent, squares of B highlight each other with pointers P and an extraordinary square.

$$gb \in B \tag{3}$$

Where,

- gb – Genesis Block.
- B - Blocks.

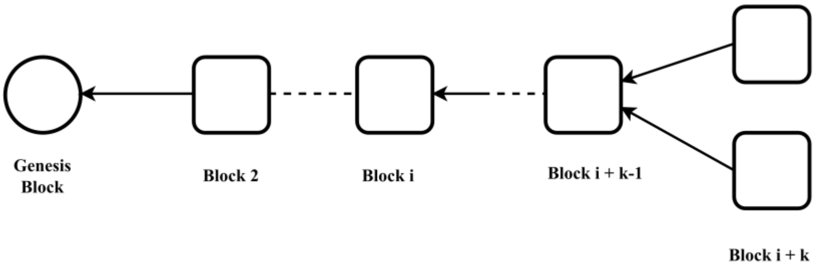

Figure 11. Blockchain Structure in DAG

The above equation (2) is called the genesis block, distinct from any other block. The very first block is called the genesis block. In genuine Blockchain networks, transactions are stored in a chain of blocks, whereas in DAGs, transactions are stored topologically in a graph.

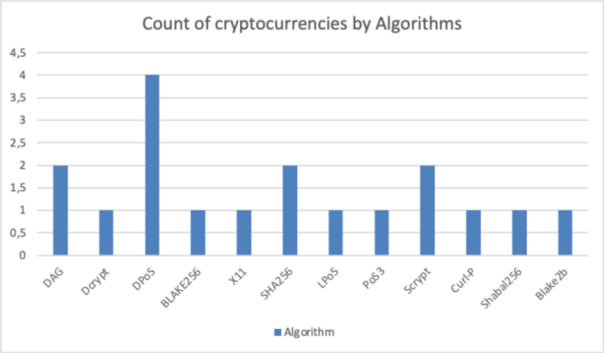

Figure 12(a): Comparison of Algorithm Based on Cryptocurrencies.

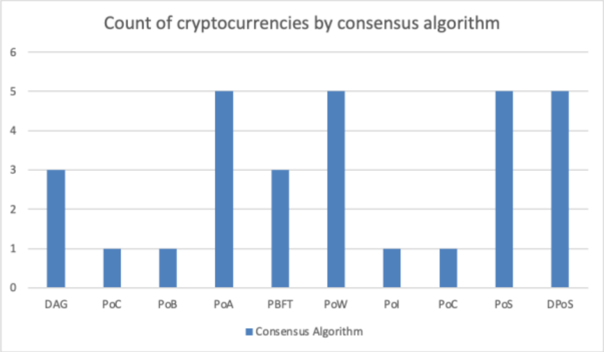

Figure 12(b): Comparison of Consensus Algorithm Based on Cryptocurrencies.

Figures 12 and 13 above illustrate the incorporation of a few digital currencies as examples of each approach and then compare them according to specified standards. A permission structure probably centralizes the blockchain, whereas an unrestricted setup decentralizes the network by allowing more diverse nodes. However, securing an anonymous blockchain and validating the nodes and transactions might be difficult. Table 3 below contrasts several cryptocurrencies' authorization systems.

Table 4. Permissioned and Permissionless Consensus Algorithm

Cryptocurrency	Consensus Algorithm	Model
Neo	DBFT	Permissioned
Icon	LFT	
WTC	PoS	
EOS	DPoS	
Ark	DPoS	
Lisk	DPoS	
VeChain	PoA	
Nuls	PoC	
Hashgraph	Asynchronous BFT	
Bitcoin	PoW	Permissionless
Ethereum	PoW	
Litecoin	PoW	
Dogecoin	PoW	
Monero	PoW	
Stellar	PFT	
XRP	NA	
Nano	PoS	
Cardano	DPoS	
Decred	PoS	
Zilliqa	PBFT	
Elastos	DPoS	
IOTA	DAG	

3.4. Study Analysis of Blockchain in Industry

Presently, a day, Blockchain is gaining mass consideration in a limited amount of time. Significant organisations are embracing Blockchain innovation due to its unique features, and [27] they do not want to miss out on the forthcoming disruption in the field of Information Technology.

Blockchain strengthens transaction reliability. It uses hashing technology to secure the data for every recorded transaction. An example is Supply Chain Management (SCM). In classical times, we used paperwork; when Blockchain technology came into the modern world, we could avoid the paperwork and third parties.

1. Hyperledger Frameworks

Each Hyperledger innovation for the distributed ledger has its benefits in specific applications. The Hyperledger structures are utilised to assemble business Blockchains for a consortium of associations [28]. Hyperledger hatches and advances a scope of business Blockchain innovations recorded below:

- Hyperledger Fabric.
- Hyperledger Iroha.
- Hyperledger Indy.
- Hyperledger Sawtooth.
- Hyperledger Burrow.

Table 5. Talks about the Hyperledger Frameworks and the projects of recent industrial areas [29]

Methodology	Performer	Sector	Consensus Algorithm	Programming Context
Fabric	IBM	Healthcare(Supply et al.).	BFT	Go, Java, JavaScript
Sawtooth	Intel	Logistics	PoET	Any Languages
Burrow	Monax	Computerised Identities	PoET	Solidity
Indy	Sovrin	Banking (National Bank of Cambodia)	RBFT	Python,Node.Js
Iroha	Soramitsu	Create Computerised Information(All Fields)	YAC	C++

2. Hyperledger Tools

Instruments, such as programs that facilitate sending, troubleshooting, and configuration, can significantly impact the convenience of any system for engineers and clients. Hyperledger is continually investing in building innovative support tools. There are a few devices that permit simple and productive admittance to Blockchain. The most utilised instruments are:

- Hyperledger Composer.
- Hyperledger Cello.
- Hyperldger Explorer.
- Hyperledger Caliper.

Table 6. The Hyperledger Tools and projects across various industrial sectors [29]

Frameworks	Projects
Hyperledger Composer.	Business Networks.
Hyperledger Cello.	Service Oriented (Deployment Model)
Hyperldger Explorer.	Web Oriented Application
Hyperledger Caliper.	Measuring the Performance(In Blockchain)

3. Corda

The consortium's joint endeavors have led to the development of an open-source distributed ledger platform called Corda. It is primarily responsible for overseeing complex transactions and limiting access to exchange information. Corda offers privacy and encryption of the client's information.

The current circumstance requires a tremendous amount of work to synchronise the records of various organisations as the conventional records are kept in different arrangements:

- Protection.
- Exchange Finality.

- Personality.
- Adaptability.
- Venture Integration

4. Open Chain

OpenChain is an open-source, standardized record management innovation that enables organizations to address issues and manage digital assets in a structured and transparent manner. Each exchange is connected to the chain, and simultaneously, it is submitted to the organization.

5. Multi Chain

Multichain is a private Blockchain created within or between organizations to build and execute blockchain applications quickly. It should play out a different number of exchanges each second. It is suitable for monetary areas to keep up with, process, and secure information.

6. Ripple

Swell is a Blockchain that enables the secure and rapid exchange of digital money between financial institutions, payment providers, and digital asset exchanges over the Internet. It is a conveyed open Internet convention (XRP) that facilitates the trade and movement of cash for clients through a cryptographically secure exchange.

Table 7. Permissioned Outline Structures

Types of Permissioned Outlines	Types of Consensus	Support Smart Contracts	Open Source Available	Provision / Supremacy	Digital Currency
Hyperledger Fabric	SOLO	Yes	Yes	Linux Foundation	No
Multi Chain	Round Robin	Yes	Yes	Coin Sciences	No
Corda	RAFT	Yes	Yes	R3 Consortium	No

3.5. Blockchain Applications Across Various Industries

Blockchain is one of the most impressive forthcoming innovations, serving as the foundation for Bitcoin [30]. Blockchain innovation has driven different organisations, enterprises, significant associations, and new companies across the globe to investigate innovation's actual capacity and to make progressive turns of events in their particular fields [31].

a) Brilliant Contract:

Business agreements exist between organizations to trade services or products. These have now become advanced and self-executable, and they are referred to as "Brilliant agreements." They are similar to paper-based agreements yet not prone to human errors or alterations [32].

Model: Ethereum, the most popular Blockchain innovation, is utilized to create health-based smart contracts (also known as savvy contracts) in the healthcare sector to maintain consistency in the pharmaceutical supply chain.

b) Casting a ballot

The government can incorporate blockchain innovation into decisions by eliminating the possibility of cheating, such as through fake voters or anti-social components. The customary democratic strategy depends more on human interaction.

Model: "DemocracyEarth" is a Blockchain innovation that aims to establish a shared framework for voting. In light of the straightforward concept of blockchain innovation, individuals in power are responsible for their actions. This will eliminate cheating and ensure transparency and security, thereby protecting citizens.

c) Personality Management

Blockchain innovation is utilized as a solution for online identity management. In Blockchain, a user's identity can be verified as genuine with the assistance of distributed ledger technology. A distributive record utilizes public and private key encryption methods to identify a more specific client.

Model: "City" is the Blockchain capacity used to securely handle the identity of a single client by employing a staggered verification process or biometric authentication.

d) Copyrights

Copyright claims are one significant capacity for any association to guarantee ownership of the items or services it creates and manages. Blockchain enables corporations and other organizations to create a tamper-proof digital signature, which enhances the integrity and validity of their copyrighted items and services [33].

Model: "Initiation" is an idea of Blockchain innovation that utilizes an advanced token framework to distinguish the owner's data of an item, such as the creator, distributor, and interpreter of a book, and to provide fairness in their respective portions.

e) Finance Sector

The banking and financial sectors play a significant role in the nation's economy. Undeniably, organisations and programmers focused on banking and other economic areas are inclined to numerous digital risks. From information breaches to data leaks, banks are impacted every day. Blockchain presents an innovation called SALT (Secured Automated Lending Innovation), which will be particularly useful for any financial institution in reducing bank fraud.

Model: ETHLend has several monetary stages based on blockchain technology. These innovations enable the distribution of lending, savings accounts, insurance, and other financial services.

f) Energy and Power Sector

Blockchain innovation enables the Power to establish direct customer power benefits, Providing Electricity from solar and wind energy. It offers more straightforwardness to their activities. This is the idea of a shared exchange of power without the necessity of a halfway power. Power creation areas play a significant part in the economy of any Country's Government. Likewise, these days, it becomes simpler for programmers to assume responsibility for power generation frameworks because most nations provide power supply frameworks with the internet. Henceforth, it becomes helpless [34].

Model: "PowerLedger" is another concept for a decentralized energy exchange approach that aims to exchange excess energy with residents, predominantly at the loft level, thereby eliminating the need for power plant organizations and decentralizing the energy sector. A Lithuanian startup presents a Blockchain innovation called "Wepower" to invest in efficient power energy projects and exchange inexhaustible energy on a larger scale. "Grid+" is a blockchain-based concept that leverages Artificial Intelligence to optimize energy utilization designs and facilitate energy purchases.

g) Supply Chain Management

The store network industry is confronting many battles, like:

- Time and power utilisation
- Fuel cost rise
- Transportation
- To supply items proficiently to retailers and shoppers with an insignificant expense

Blockchain offers a promising fix to these issues. Implementing the bright agreement concept, which involves manufacturing items only when a specific number of orders is fulfilled, can prevent overproduction and the wasteful use of essential resources, such as water and electricity. Securing the money in a legally binding agreement-based arrangement is feasible, where production will commence only when a particular number has been reached [35]. [36]

Model: VeChain and ShipChain are two Blockchain projects revolutionizing the Supply Chain industry. [37] is intended for an exceptional change in what is to come.

h) Medical Industry

Apart from banking areas, it is also acknowledged that digital threats and attacks frequently target medical care enterprises. In the well-being area, there are high possibilities of information phony, misfortune, and altering of clinical records through cyberattacks. Blockchain in the medical services industry gives two significant benefits. To begin with, it fabricates a trusting relationship between the shopper and the business. Second, it mitigates the digital risks associated with clinical information records. Clinical information records can become safer and more secure with the assistance of Blockchain.

Model: The Estonian Government has established an arrangement with GuardTime (Enterprise Blockchain) to provide blockchain services and safeguard the clinical information of its residents.

i) Digital Currency Exchanges

Apart from banking areas, it is also acknowledged that digital threats and attacks frequently target medical care enterprises. In the well-being area, there are high possibilities of information phony, misfortune, and altering of clinical records through cyberattacks. Blockchain in the medical services industry gives two significant benefits. To begin with, it fabricates a trusting relationship between the shopper and the business. Second, it mitigates the digital risks associated with clinical information records. Clinical information records can become safer and more secure with the assistance of Blockchain.

j) Human Resource Management (HRM)

Enlisting the right individuals for your business is a crucial aspect of your organization, as it significantly impacts income growth and net revenue. Blockchain innovation facilitates the management and oversight of Human Resources more efficiently and accurately. Individual Data has been stored in an easily accessible, carefully designed record that can save time utilization. It will enroll a more effective applicant and request all unnecessary HR-related tasks, such as providing a personnel file, benefits, Provident funds, and health benefits [38].

Model: A blockchain concept called "ChronoBank" has been developed, aiming to assist HR experts in identifying and recruiting the ideal and suitable candidates they need.

k) Blockchain as a Service

Numerous advancements are emerging in the current business world and are driving the Information Technology field forward. Numerous associations are implementing blockchain methods to position themselves as trailblazers in programming.

Models "Stratis" and "Passion" have been designed to provide comprehensive solutions for programming improvement.

l) Social Media

Correspondence security plays a vital role in the rapidly evolving tech world. The protection of an individual has become prey to many assaults and dangers. Blockchain fosters trust and safeguards personal protection [39]. [40].Implementing blockchain in correspondence will ensure the possibility of 'Got Encrypted Communication Channels' for informal organisations.

Model: The Blockchain idea is typically adopted by well-known messaging platforms, such as Telegram and Mercury Protocol. These Ethereum-based blockchain stages offer clients a secure end-to-end encryption service during communication.

According to the survey, all relevant literature works are cited in this article to compare the above. We provide a detailed overview of all Hyperledger frameworks and their applications in various industries, including the banking, medical, and power sectors. The figure details the key evaluation metrics and incorporates the types of Hyperledger frameworks [41]. In Figure 12, we set the x-axis contribution level to a maximum of 100. Those Hyperledger frameworks match the performance metrics on the y–axis; we give a contribution level of 100. In the above survey report, despite various types of Hyperledger frameworks, Hyperledger Fabric is one of the major frameworks [42] that incorporates many industries because it provides privacy and Security [43] (Permissioned). Table 7 outlines the permission structures.

3.6. *Challenges in Blockchain*

The present-day blockchain system must contend with numerous internal and external obstacles and potential constraints. The main barriers that the blockchain system confronts can be observed from the viewpoints of designers, customers, and legislators. Problems with low flexibility, restricted compatibility [44], inconsistency, and a shortage of trained programmers arise when implementing blockchain-based solutions. In this section, we discuss a few of the main issues that the field of blockchain is currently facing.

Flexibility: One of the primary obstacles preventing the widespread adoption of the blockchain system is sustainability. Along with other blockchain characteristics, such as speed, delay, transmission time, block size, and block time, versatility is also an issue. The number of operations a blockchain can handle is determined by its flow [45]. It can be expressed mathematically as the product of the number of operations per block and blocks per second.

Utilisation of Energy: It is costly to operate, particularly on open-source blockchains, which results in significant energy consumption and emissions. The SHA-256 hashing method, the foundation of the Proof of Work system, produces a secure hash with a value less than the desired nonce [46]. Mining and creating new blocks for the blockchain is a fiercely competitive activity that requires significant computing power and effort. Finding the correct nonce value requires extensive operations [47], [48] which are the foundation of every step of mining for a valid block. The continual process of block mining encourages miners to extract more blocks, and the entire process uses a significant amount of energy.

Security and Confidentiality: Numerous blockchain-powered businesses and digital currencies have been the target of hacking attacks over the years, which have led to significant monetary losses. [49] and even company closures. Numerous investigations and studies on the safety components of the blockchain system have been published.

A few of the underlying reasons why security risks exist on a blockchain :

- Intelligent Agreement.
- Issues in Conventions.
- Hot Wallet Hack.
- Issues in Application.

Lack of Generally Recognized Procedures and Guidelines: In many nations, the blockchain system is still regarded as invalid. There is no single set of guidelines that everyone agrees upon when using the blockchain system.

Prices and Effectiveness: Blockchain deployment is initially expensive; medium-sized enterprises often struggle to integrate blockchain solutions into their existing systems. Additionally, the public blockchain's transaction accuracy is subpar, directly affecting the organization. Additional studies on the blockchain system could lead to the development of authentication methods that utilize multiple factors, thereby enhancing the security of current approaches.

4. CONCLUSION

The emergence of blockchain technology has demonstrated its inherent capabilities and robust components across several industries and sectors. Several organisations have already begun to implement it. Regardless, Blockchain and Bitcoin are the most prominent terms in technological advancement. While the internet has influenced data transfer, Blockchain has transformed the transfer of values. The utilisation of Blockchain technology is a vital asset for the field of network security and specific organisations. They have showcased their success by surpassing other security systems and are a significant threat to various organizations. Therefore, data security experts must be knowledgeable and up-to-date with the latest developments in Blockchain. Numerous innovations and solutions are being explored to address the challenges of implementing blockchain in sustainable sectors, and real-world use cases are being examined to demonstrate how blockchain effectively promotes sustainability in industries such as the Energy sector and supply chain management. The global implementation and use of Blockchain technology are anticipated to bring significant transformations and enhancements in our daily routines, yielding numerous advantages. Blockchain technology is expected to become increasingly prevalent in the coming years as individuals worldwide become more aware and concerned about various advancements, such as Bitcoin, the Internet of Things (IoT), and Artificial Intelligence (AI). Finally, the future uses and services of Blockchain technology remain limited. Our objective is to analyze

Blockchain security and protection in the future comprehensively. We intend to investigate quantum-resistant blockchains to ensure long-term safety and sustainability in our future work and integrate blockchain with AI, IoT, and Big Data to enhance robotics and decision-making in sustainability projects.

REFERENCES

[1] Yusuf Perwej, "A Pervasive Review of Blockchain Technology and Its Potential Applications," . *Open Science Journal of Electrical and Electronic Engineering*, vol. 5, no. 4, pp. 30–43, 2018.

[2] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," *Internet of Things*, vol. 25, p. 101019, 2024, doi: 10.1016/j.iot.2023.101019.

[3] I. T. , & Q. K. N. Javed, "Role of Blockchain Models for AIoT Communication Systems," *In Artificial Intelligence of Things (AIoT)*, pp. 122–139, 2024.

[4] A. Panwar, V. Bhatnagar, M. Khari, A. W. Salehi, and G. Gupta, "A Blockchain Framework to Secure Personal Health Record (PHR) in IBM Cloud-Based Data Lake," *Comput Intell Neurosci*, vol. 2022, p. 3045107, Apr. 2022, doi: 10.1155/2022/3045107.

[5] Y. Liu, J. Zhang, S. Wu, and M. S. Pathan, "Research on digital copyright protection based on the hyperledger fabric blockchain network technology," *PeerJ Comput Sci*, vol. 7, pp. e709–e709, Sep. 2021, doi: 10.7717/peerj-cs.709.

[6] A. Altarawneh, T. Herschberg, S. Medury, F. Kandah, and A. Skjellum, "Buterin's Scalability Trilemma viewed through a State-change-based Classification for Common Consensus Algorithms," in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2020, pp. 0727–0736. doi: 10.1109/CCWC47524.2020.9031204.

[7] I. Aviv, A. Barger, A. Kofman, and R. Weisfeld, "Reference Architecture for Blockchain-Native Distributed Information System," *IEEE Access*, vol. 11, pp. 4838–4851, 2023, doi: 10.1109/access.2023.3235838.

[8] J. A. Alzubi, "Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare," *Comput Commun*, vol. 170, pp. 200–208, 2021, doi: 10.1016/j.comcom.2021.02.002.

[9] N.-Y. Lee, J. Yang, M. M. H. Onik, and C.-S. Kim, "Modifiable Public Blockchains Using Truncated Hashing and Sidechains," *IEEE Access*, vol. 7, pp. 173571–173582, 2019, doi: 10.1109/access.2019.2956628.

[10] B. K. Kikwai, "Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions," vol. 7, no. 11, pp. 135–138, 2017.

[11] A. Faz-Hernández, J. López, and R. Dahab, "High-performance Implementation of Elliptic Curve Cryptography Using Vector Instructions," *ACM Transactions on Mathematical Software*, vol. 45, no. 3, pp. 1–35, 2019, doi: 10.1145/3309759.

[12] W. , J. X. , & Z. M. Bi, "A Secure Multiple Elliptic Curves Digital Signature Algorithm for Blockchain."

[13] T. Alam, "Performance evaluation of blockchains in the internet of things," *Computer Science and Information Technologies*, vol. 1, no. 3, 2020, doi: 10.11591/csit.v1i3.p93-97.

[14] A. López Vivar, A. L. Sandoval Orozco, and L. J. García Villalba, "A security framework for Ethereum smart contracts," *Comput Commun*, vol. 172, pp. 119–129, 2021, doi: 10.1016/j.comcom.2021.03.008.

[15] S. P. and M. Venkatesan, "Scalability improvement and analysis of permissioned-blockchain," *ICT Express*, vol. 7, no. 3, pp. 283–289, 2021, doi: 10.1016/j.icte.2021.08.015.

[16] H. Liu, D. Han, and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020, doi: 10.1109/access.2020.2968492.

[17] O. Elijah *et al.*, "A Survey on Industry 4.0 for the Oil and Gas Industry: Upstream Sector," *IEEE Access*, vol. 9, pp. 144438–144468, 2021, doi: 10.1109/access.2021.3121302.

[18] S. Dange and P. Nitnaware, "Secure Share: Optimal Blockchain Integration in IoT Systems," *Journal of Computer Information Systems*, vol. 64, no. 2, pp. 265–277, 2023, doi: 10.1080/08874417.2023.2193943.

[19] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Generation Computer Systems*, vol. 107, pp. 760–769, 2020, doi: 10.1016/j.future.2017.09.023.

[20] F. Asuncion *et al.*, "Connecting supplier and DoD blockchains for transparent part tracking," *Blockchain: Research and Applications*, vol. 2, no. 3, p. 100017, 2021, doi: 10.1016/j.bcra.2021.100017.

[21] M. Uddin *et al.*, "Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records," *Computers, Materials &amp; Continua*, vol. 68, no. 2, pp. 2377–2397, 2021, doi: 10.32604/cmc.2021.015354.

[22] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," 2019, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2019.2936094.

[23] T. Alam, "IoT-Fog: A Communication Framework using Blockchain in the Internet of Things Tanweer Alam. "IoT-Fog: A Communication Framework using Blockchain in the Internet of Things," 2019.

[24] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, and D. Patel, "Secured Energy Trading Using Byzantine-Based Blockchain Consensus," *IEEE Access*, vol. 8, pp. 8554–8571, 2020, doi: 10.1109/access.2019.2963325.

[25] N. C. K. Yiu, "Toward Blockchain-Enabled Supply Chain Anti-Counterfeiting and Traceability," *Future Internet*, vol. 13, no. 4, p. 86, 2021, doi: 10.3390/fi13040086.

[26] F. Wang *et al.*, "An Experimental Investigation Into the Hash Functions Used in Blockchains," vol. 67, no. 4, pp. 1404–1424, 2020.

[27] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, "Overview on the Blockchain-Based Supply Chain Systematics and Their Scalability Tools," *Emerging Science Journal*, vol. 4, pp. 45–69, 2021, doi: 10.28991/esj-2021-sp1-04.

[28] F. Wang *et al.*, "An Experimental Investigation Into the Hash Functions Used in Blockchains," *IEEE Trans Eng Manag*, vol. 67, no. 4, pp. 1404–1424, 2020, doi: 10.1109/tem.2019.2932202.

[29] S. Aggarwal and N. Kumar, "Hyperledger☆," in *Advances in Computers*, vol. 121, Academic Press Inc., 2021, pp. 323–343. doi: 10.1016/bs.adcom.2020.08.016.

[30] T. Alam, R. Gupta, A. Ullah, and S. Qamar, "Blockchain-Enabled Federated Reinforcement Learning (B-FRL) Model for Privacy Preservation Service in IoT Systems," *Wirel Pers Commun*, vol. 136, no. 4, pp. 2545–2571, 2024, doi: 10.1007/s11277-024-11411-w.

[31] Y. Cui and H. Idota, "Improving Supply Chain Resilience with Establishing A Decentralized Information Sharing Mechanism," *ACM International Conference Proceeding Series*, pp. 1–7, 2018, doi: 10.1145/3227696.3227723.

[32] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, "The case of HyperLedger Fabric as a blockchain solution for healthcare applications," *Blockchain: Research and Applications*, vol. 2, no. 1, p. 100012, 2021, doi: 10.1016/j.bcra.2021.100012.

[33] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.095647.

[34] N. Al-Saif, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for Electric Vehicles Energy Trading: Requirements, Opportunities, and Challenges," *IEEE Access*, vol. 9, pp. 156947–156961, 2021, doi: 10.1109/access.2021.3130095.

[35] D. Ivanov and P. Pashkov, "A blockchain-based approach to providing technically expressed trust in the supply chains of the fashion industry," *J Phys Conf Ser*, vol. 2032, no. 1, p. 012086, 2021, doi: 10.1088/1742-6596/2032/1/012086.

[36] S. K. Rana *et al.*, "Blockchain-Based Model to Improve the Performance of the Next-Generation Digital Supply Chain," *Sustainability*, vol. 13, no. 18, p. 10008, 2021, doi: 10.3390/su131810008.

[37] T. H. Pranto, A. A. Noman, A. Mahmud, and A. B. Haque, "Blockchain and smart contract for IoT enabled smart agriculture," *PeerJ Comput Sci*, vol. 7, pp. e407–e407, Mar. 2021, doi: 10.7717/peerj-cs.407.

[38] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities," *IEEE Internet Things J*, vol. 6, no. 5, pp. 7702–7712, 2019, doi: 10.1109/JIOT.2019.2901840.

[39] T. Alam, "Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges," *Computers*, vol. 12, no. 1, p. 6, 2022, doi: 10.3390/computers12010006.

[40] T. Alam, "Blockchain-based Big Data Integrity Service Framework for IoT Devices Data Processing in Smart Cities," *Mindanao Journal of Science and Technology*, vol. 19, no. 1, 2021.

[41] T. Alam, "Blockchain-Enabled Deep Reinforcement Learning Approach for Performance Optimization on the Internet of Things," *Wirel Pers Commun*, vol. 126, no. 2, pp. 995–1011, 2022, doi: 10.1007/s11277-022-09780-1.

[42] Z. Leng, Z. Tan, and K. Wang, "Application of Hyperledger in the Hospital Information Systems: A Survey," *IEEE Access*, vol. 9, pp. 128965–128987, 2021, doi: 10.1109/access.2021.3112608.

[43] T. Alam, "Data Privacy and Security in Autonomous Connected Vehicles in Smart City Environment," *Big Data and Cognitive Computing*, vol. 8, no. 9, p. 95, Aug. 2024, doi: 10.3390/bdcc8090095.

[44] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," *IEEE Access*, vol. 7, pp. 118541–118555, 2019, doi: 10.1109/access.2019.2935149.

[45] T. Aslam *et al.*, "Blockchain Based Enhanced ERP Transaction Integrity Architecture and PoET Consensus," *Computers, Materials &amp; Continua*, vol. 70, no. 1, pp. 1089–1109, 2022, doi: 10.32604/cmc.2022.019416.

[46] T. Alam and R. Gupta, "Reviewing the Framework of Blockchain in Fake News Detection," *Jurnal Online Informatika*, vol. 9, no. 2, pp. 286–296, 2025, doi: 10.15575/join.v9i2.1349.

[47] M. J. Krause and T. Tolaymat, "Quantification of energy and carbon costs for mining cryptocurrencies," *Nat Sustain*, vol. 1, no. 11, pp. 711–718, 2018, doi: 10.1038/s41893-018-0152-7.

[48] C. Mora *et al.*, "Bitcoin emissions alone could push global warming above 2°C," *Nat Clim Chang*, vol. 8, no. 11, pp. 931–933, 2018, doi: 10.1038/s41558-018-0321-8.

[49] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.