Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

A Deep Dive into Blockchain Applications, Security Enhancements and Challenges

Sahar Ali Laskar,

Research Scholar, University of North Bengal, Department of Computer Science & Technology, P.O. - NBU., District-Darjeeling, PIN-734013, West Bengal, India.

Sk Jahir Abbas,

PG Student, University of North Bengal, Department of Computer Science & Technology, P.O. - NBU., District-Darjeeling, PIN-734013, West Bengal, India.

J K M Sadique Uz Zaman,

(Corresponding Author), University of North Bengal, Department of Computer Science & Technology, P.O. - NBU., District-Darjeeling, PIN-734013, West Bengal, India.

Article History:

Received: 08-10-2024

Revised: 23-11-2024

Accepted: 09-12-2024

Abstract

Bitcoin is one type of cryptocurrency that operates independently in a decentralized manner for digital payment. Blockchain technology is used in transaction of Bitcoin. It functions as a secure, transparent, and traceable ledger that enables decentralized transactions. While blockchain applications are expanding across various aspects of daily life, implementing this technology presents significant challenges. This paper provides an overview of blockchain's working principles and recent applications, with particular focus on its challenges. This work represents a continuation with some new applications and broader exploration of concepts introduced in the authors' earlier publication. The research examines how blockchain technology is being utilized in traffic management systems—an area where conventional centralized control through roadside units has been standard practice. Despite the difficulties in designing blockchain-based decentralized vehicle networks, this technology is increasingly being applied to traffic control.The paper compiles key blockchain applications to highlight the importance of this emerging field. Additionally, it discusses potential future developments of blockchain technology and its implications across various sectors.

Keywords: Bitcoin, Blockchain, Consensus, Cryptography, Decentralized, Hash function, PoW, Smart contract.

1. Introduction:

Today, cryptocurrency is a widely discussed topic in both industry and academia. Among the various cryptocurrencies, Bitcoin stands out as one of the most successful, reaching a market capitalization of $10 billion in 2016. A specially designed data storage system is used in Bitcoin that makes it more successful than others. In transaction network, no involvement of third parties is required for transactions of Bitcoin. Blockchain is the core and important technology that powers Bitcoin.

The blockchain was first developed by Satoshi Nakamoto at the end of November 2008 and was implemented the following year in 2009. Blockchain is a decentralized and distributed ledger which maintains an ever-expanding list to store records, known as blocks. Each block contains five key elements:

i. Header: It stores header Information.
ii. Previous block address: It stores the address of preceding block.
iii. Timestamp: It indicates the creation time of the block.
iv. Nonce: A 4-byte number used to meet the required proof-of-work.
v. Merkle root: It represents total hash value for all transactions within a block.

The term "blockchain" refers to the concept of an endless chain of these interconnected blocks, where order of transactions is maintained according to block number. The blockchain was designed to solve a specific problem known as the "double-spending problem". According to Satoshi Nakamoto, the inventor of Blockchain, a Bitcoinmust have five key characteristics [1]. These characteristics canbe defined as follows:

i. Allowing direct peer-to-peer transactions without relying on trusted third parties.
ii. Ensuring that transactions are irreversible once confirmed.
iii. Lowering credit-related costs for small transactions.
iv. Reducing overall transaction fees.
v. Preventing the risk of double-spending.

It is important to note that the identity of Satoshi Nakamoto remains unknown, as no verifiable information is available in either print media or on the internet. The Bitcoin whitepaper was published in 2008 and since 2012, there has been no trace of Nakamoto. Numerous journalists have attempted to uncover Nakamoto's identity, but their efforts have been unsuccessful. It is also possible that Nakamoto is not an individual, but rather a collective or a group of people [2].

The first Bitcoin block was mined in 2009, initiating both Bitcoin and Blockchain operations [3]. Since then, the system has run without interruption, with a growing global user base. In Japan, the 2014 collapse of a crypto exchange drew public attention and by 2015, interest in Blockchain technology had grown, boosting the rise of FinTech for financial services.

Significance of this Research activity: In the current scenario, many people—both from academic and non-academic backgrounds—still lack a clear understanding of how blockchain works, how it is applied, and the risks involved. However, blockchain is becoming increasingly important for ensuring security in digital communication, and its role is growing rapidly. This technology is now used in many areas such as money transfers, sharing personal information, voting systems, healthcare, government services, IoT networks, data storage, and management. These examples show how important blockchain has become. Keeping this in mind, the goal of this paper is to explain blockchain in a simple way, using clear examples, so that more people can understand and use this technology in their daily lives.

In this article, the literature review is presented in Section 2, which focuses the application areas of blockchain technology. Section 3 briefly explains the working principle of blockchain. Section 4 highlights a few key applications, while Section 5 discusses the challenges associated with the technology. In Section 6, the conclusion and future scope is discussed.

2. Literature Review

Blockchain is the main and core technology behind the digital payment system of Bitcoin cryptocurrency. It operates as an immutable, transparent and traceable ledger that enables decentralized transactions. The use of blockchain is quickly expanding into various areas of everyday life. However, its implementation still faces several challenges. This section provides an overview of the working principle and recent applications of Blockchain, along with its limitations. In modern society, traffic management remains a major issue. Traditional transportation systems rely on a centralized roadside unit to manage the network. While building decentralized vehicle ad-hoc networks using Blockchain is complex, recent studies show that Blockchain is now being applied in traffic management systems as well. This review highlights the working principles, key applications and challenges of Blockchain to emphasize the growing importance of this technology.

In 2020, Sanjeev Kumar Dwivedi et al. published a research article [4] demonstrating the use of blockchain technology in traffic control systems for smart cities. They proposed a decentralized architecture based on blockchain to enable sharing of event information efficiently among roadside units, supported by a cloud server. The study also introduced an authentication protocol to ensure vehicle authorization and improve message reliability. A consensus algorithm was proposed for validating newly created blocks, along with a novel smart contract procedure tailored for the system. Their security analysis showed that the algorithm is resilient against attacks and meets key requirements such as integrity and authentication. Also in 2020, Chun-An Lin et al. designed a blockchain-based accountable system capable of operating on IoT devices [5]. While their approach assists developers in making design choices for B-IoT systems, they noted that additional constraints and optimization challenges still exist. Similarly, M. A. Khan and K. Salah [6] explored the application of blockchain technology in enhancing IoT security. Earlier, in 2017, Ali Dorri et

al. proposed the use of blockchain to ensure security and privacy in smart home IoT systems [7].

It is observed that blockchain technology is used in the field of medical healthcare domain also. Two papers are published in this domain in 2019 - one by H. D. Zubaydiet al [8] and other by A. Saha et al [9]. Few articles discuss the basic ideas about the blockchain technology. M.N.M. Bhutta et al published a paper in 2021 [10] which focuses on the security and architecture of blockchain. B. Mona et al discusses blockchain technology in 2019 [11]. Decentralization of digital currency or Bitcoin is discussed by F. Tschorsch and B. Scheuermann in 2016 [12]. S.K. Dwivedi and others discussed a secured information sharing mechanism in the field of supply chain based on blockchain technology in 2020 [13]. A blockchain-based technique for information sharing in management system of medical supply chain is presented in this article. It provides key management scheme in smart-contract and block validation protocols are also designed here. The article claims that the proposed mechanism is secured from all types of possible attacks. In 2016, A. Kosba and others published an article that discusses application of blockchain in cryptographic field and also in privacy-preservation of smart contracts [14].

Several articles pointed out the challenges and opportunities that are related to the blockchain technology. In 2018, Zibin Zheng and colleagues conducted a comprehensive survey on blockchain [15]. They identified various challenges that could impact the growth of blockchain technology and summarized current strategies to address these issues. Similarly, U. D. Rajguru published a related paper in 2018 [16]. In 2017, E. B. Hamida et al. explored the application of blockchain in the industrial field [17], examining both the technical aspects of blockchain and providing a classification of its applications and use cases. Earlier, in 2016, K. Biswas and a colleague published an article on the use of blockchain technology to enhance the security of smart cities [18].

3. Working Principle of Blockchain Mechanism

Working principle of blockchain mechanism is discussed below to help the readers in gaining a better understanding of the subject. This section is organized into five subsections:

- Blockchain Architecture
- PoW (Proof of Work) Procedure in Blockchain Mechanism
- Mastercoin and Smart Contracts
- Hash Function
- Digital Signature

Short descriptions of these five principles are given below.

3.1. **Blockchain Architecture**

A blockchain is a series of so many blocks that stores transaction records, functioning like a public ledger. Each and every block is securely linked to its previous block through a hash reference, ensuring both continuity and integrity. In a blockchain, the first block is known as the genesis block. It is to be noted that the genesis block has no parent block. In Ethereum, there are also uncle blocks, which are blocks mined alongside the main parent block but not included in the main chain; however, their hash values are recorded for reference. As an example, structure of a blockchain is shown in Figure 1. Each block typically consists of five key parts:

- Header
- Previous block address
- Timestamp
- Nonce
- Merkle root

Arrangement of the five parts of a block are shown in Figure 1.

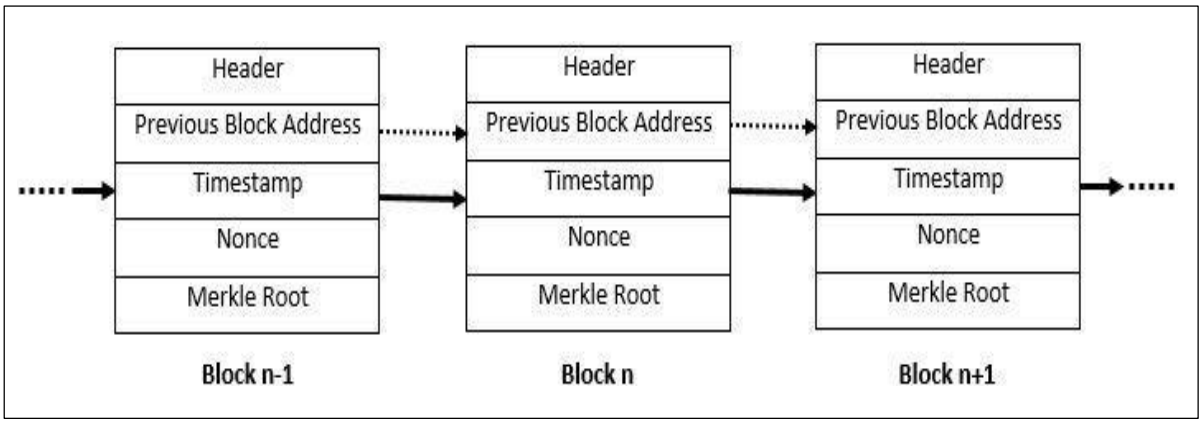

Figure 1: Flow diagram of blocks in Blockchain

- **Header:** It stores header Information and indicates the set of validation rules that the block must follow.
- **Previous block address:** It stores the address of preceding block. The address is a 256-bit hash value that points to the previous block in the blockchain.
- **Timestamp:** Represents the time when the block was created or when a transaction was recorded.
- **Nonce:** It is a 4-byte randomly generated number that miners adjust to change the output of hash value of the block header during the mining process.
- **Merkle root:** It is used within the block to improve the efficiency and security of validating large amounts of data. It is derived from the Merkle tree, where each transaction is verified before reaching consensus. A Merkle root is represented by the root node of a Merkle tree, as shown in Figure 2.

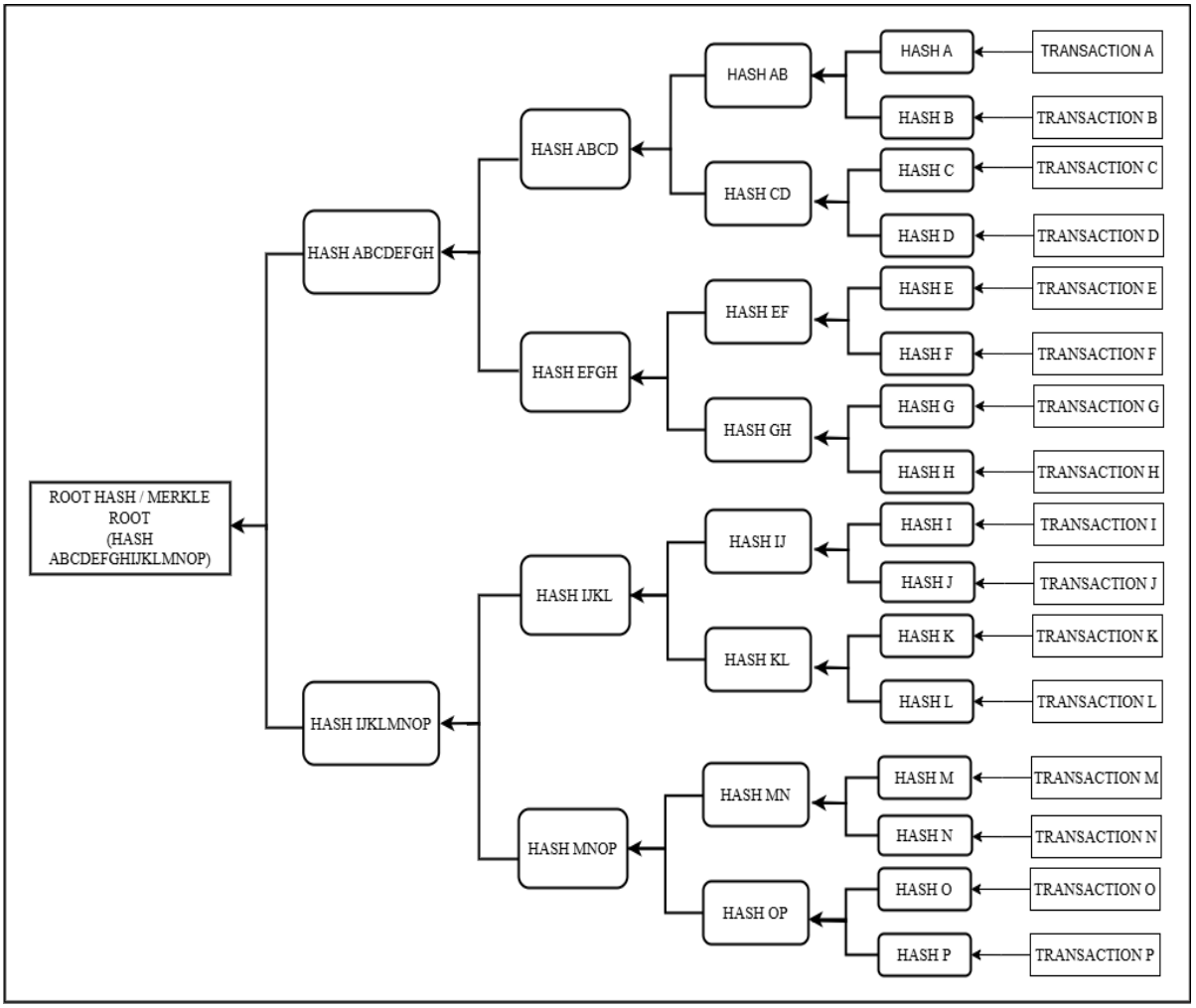

Figure 2: Merkle root in a Merkle tree

3.2. PoW (Proof of Work) Procedure in Blockchain Mechanism

PoW (Proof-of-Work) procedure was described first time in a research paper written by two researchers, Markus Jakobsson of Bell Labs and Ari Juels of RSA Laboratories. PoW is a consensus technique used in blockchain to provide secured transactions and add new blocks to the blockchain networks. In cryptography, several types of PoW mechanisms have been developed, but only a few are implemented in cryptocurrencies. For instance, Bitcoin uses the SHA-256 algorithm, while Litecoin employs the Scrypt algorithm. The significant differences between Bitcoin and Litecoin lie in their hashing functions and popularity. Bitcoin uses a larger hashing function compared to Litecoin and is more widely adopted.

3.3. Mastercoin and Smart Contracts

Blockchain stores trusted agreements which are called smart contracts. The smart contracts are executed automatically if the previously fixed conditions are met. For example, if user 'A' orders a product online — through a website such as abc.com — and makes a payment, the payment is not immediately transferred to the authority of abc.com. Instead, the amount is held by the smart contract until user 'A' confirms receipt of the product. Figure 3 illustrates the working procedure of smart contracts.

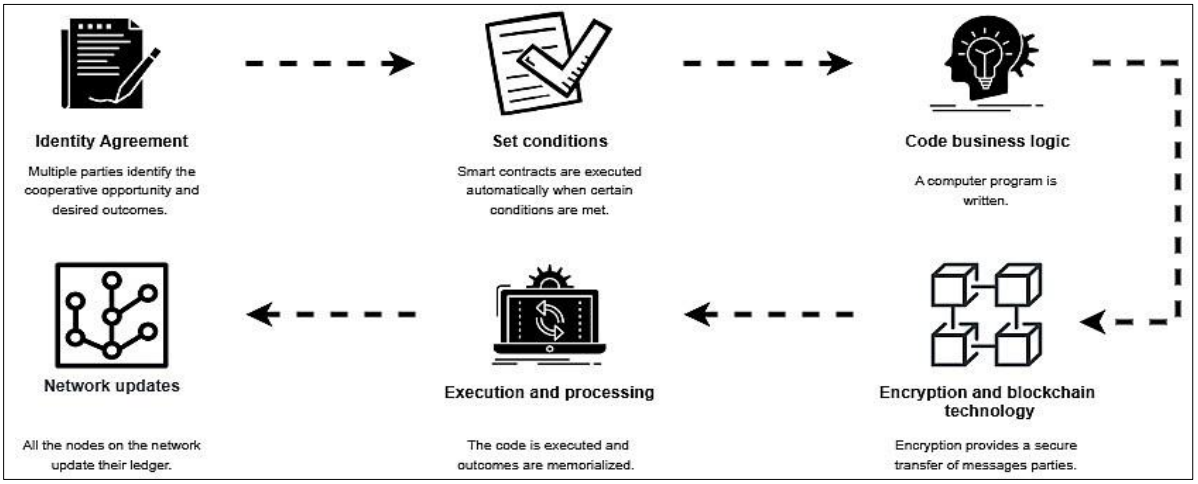

Figure 3: Working procedure of smart contracts

3.4. Hash Function

A hash function uses mathematical operations to produce a fixed-length output from an input of any length. The input can be any type of data, such as a file, image or text. In blockchain, hashing ensures that transmitted data remains unchanged, as even a small modification in the input data produces a completely different output value as hash. Hashing is crucial for the security of blockchain systems and offers the following properties:

i. **Pre-image resistance:** Hashing technique is unidirectional. It means that generating the original input from the hash is impossible.
ii. **Second pre-image resistance:** This property indicates that no two different inputs will produce the same hash value as output. Even, if both the input and corresponding hash value are given – yet finding of another input that will produce the same hash value is extremely difficult.
iii. **Collision resistance:** According to this property the generation of similar hash output, which is always a fixed-size alphanumeric string, from two different inputs is highly impossible. Most blockchain technologies implement the Secure Hash Algorithm (SHA), specifically SHA-256, which produces a 256-bit output. Other hashing algorithms like Keccak and RIPEMD-160 are also used in blockchain applications. Figure 4 presents a flow diagram demonstrating the calculation of a hash value from a given message, plaintext, or image, using the SHA-256 algorithm as an example.

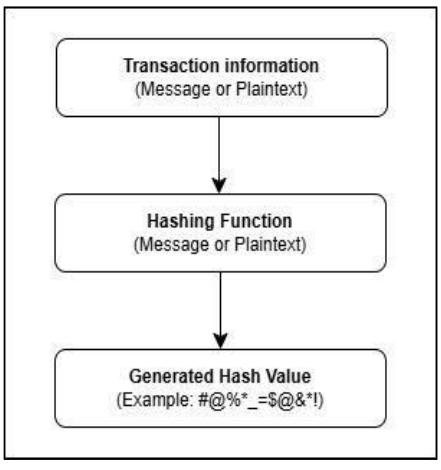

Figure 4: Flow diagram for calculating a hash value

3.5. Digital Signature

In asymmetric cryptography, every user possesses a pair of private and public keys. In digital communication the private key is kept secret. This key is used to sign documents or messages. For example, let a person Alice is interested to send her message to another person Bob. Then first of all, Alice uses her private key to encrypt (or signature) her message. After that, she sends the resulting encrypted message along with the right information to Bob. For authenticity verification of the message, Bob uses public key of Alice for decryption. ECDSA (Elliptic Curve Digital Signature Algorithm) is the mostly used algorithm in blockchain technology to put digital signature.

4. Few Applications of Blockchain Technology

Blockchain technology can store data history efficiently and is being used in many different areas with more applications emerging every day. This section discusses eighteen important application areas to help the readers for understanding how blockchain is being used in the real-world situations. The areas covered are:

i. Money transfer
ii. Lending
iii. Insurance
iv. Real estate
v. Financial exchange
vi. Secure personal information
vii. Voting system (Election)
viii. Government benefits
ix. Applications in Healthcare
x. Artist royalties
xi. Secure Internet of Things (IoT) networks
xii. Data storage
xiii. Gambling
xiv. Copyright management sector
xv. Eco-friendly management sector
xvi. National Security and Defence Operations
xvii. Media & Content distribution
xviii. Legal Metrology

Short discussions of the aforesaid important areas where blockchain is used are given below:

i. Money transfer

Blockchain technology offers a fast, cost-effective and secure method for transferring money between accounts. Intermediaries are present in traditional banking process, so it is a slow process and it needs higher transaction fees. On the other hand, peer-to-peer transactions are allowed in blockchain technology with minimal processing time and reduced costs. Blockchain technology is tamper-proof in nature, hence – if a transaction is recorded, it cannot be reversed or modified. This makes money transfers not only efficient but also highly secure and trustworthy.

ii. Lending

Blockchain technology enables more efficient and transparent lending processes by using smart contracts. Smart contracts are self executing which automatically introduce the terms of

a loan agreement such as initiating service payments, issuing margin calls, or processing full loan repayments once predefined criteria are matched. This automation reduces the requirement of intermediaries, speeds up the overall process, lowers operational costs, and allows lenders to offer more competitive interest rates. Additionally, blockchain's decentralized and immutable nature enhances the trust between lenders and borrowers.

iii. Insurance

The use of smart contracts in blockchain technology can significantly enhance transparency between insurance providers and customers. By automating policy terms and claim conditions, smart contracts ensure that claims are processed fairly and efficiently. Once a claim meets the predefined criteria, the contract can automatically trigger payment to the claimant, reducing delays, minimizing paperwork, and lowering administrative costs. This improves the customer experience and increases trust in the insurance process.

iv. Real estate

Real estate transactions typically involve extensive paperwork for verifying the financial details to confirm ownership, transfer deeds or titles to the new owners. Implementing blockchain mechanism in this field can streamline the process by securely recording and verifying transactions on a decentralized ledger. This enhances the accuracy and accessibility of ownership records, reduces the risk of fraud, minimizes paperwork and significantly speeds up the transfer process, ultimately saving time and reducing transaction costs.

v. Financial exchange

In recent years, numerous companies have emerged offering decentralized cryptocurrency exchanges. These platforms leverage blockchain technology to facilitate faster and more cost-effective transactions. Unlike traditional centralized exchanges, decentralized exchanges allow investors to retain control of their assets without needing to deposit them with a third party. This enhances both security and user autonomy. While these exchanges focus primarily on cryptocurrencies, the underlying concept holds potential for broader application in traditional financial markets as well.

vi. Secure personal information

Blockchain technology provides a highly secure method for storing important personal information, such as date of birth, social security numbers and other identifiers, on a public ledger. Unlike traditional systems, blockchain's decentralized nature and cryptographic techniques ensure that access to this information is tightly controlled and tamper resistant. It can also improve the accessibility of personal data for authorized users in various industries, including travel, healthcare, finance, education making it easier to verify identities while enhancing privacy and security.

vii. Voting system (Election)

Blockchain technology can improve voting systems by ensuring that only eligible voters are allowed to cast their votes, preventing multiple votes from the same person and ensuring that votes cannot be tampered or altered. With its decentralized and secure nature, blockchain makes it nearly impossible for anyone to manipulate the voting process. It also allows for more accessible voting, as people could vote securely from their smartphones, making the process simpler and more convenient. Additionally, using blockchain can significantly lower the costs of elections by reducing the need for paper ballots, physical polling stations, appointment of polling personnel and manual vote counting. Thus blockchain makes elections more efficient and cost-effective.

viii. Government benefits

Blockchain technology can be utilized for management of government benefits, like Social Security, welfare programs and Medicare, by securely storing digital identities. This approach helps reduce fraud due to transparency and tamper-resistant nature of blockchain. It can also lower operational costs by streamlining processes and removing the need for intermediaries. Additionally, blockchain allows beneficiaries to receive funds more quickly through digital disbursement, improving efficiency and accessibility.

ix. Applications in Healthcare

In healthcare system, blockchain mechanism enhances data transparency, data security and interoperability that revolutionizing Electronic Medical Record (EMR). In EMR, blockchain-based solutions like MedRec and FHIRChain ensure secure data sharing, privacy and interoperability, reducing inefficiencies in patient record management [19-20]. RPM (Remote Patient Monitoring) system is benefitted from blockchain's encrypted, tamper-proof storage safeguarding IoT-based health data. The pharmaceutical supply chain leverages blockchain for drug authentication and regulatory compliance, preventing counterfeit medicines through traceable supply chains like Modum.io AG [21]. Health insurance claims gain transparency and fraud prevention via MIStore, which secures medical records and automates claim processing through smart contracts [22]. Despite these benefits, scalability, interoperability and security risks remain key challenges. Future research must optimize blockchain frameworks for biomedical research, drug development, and secure patient data management to enable widespread adoption.

x. Artist royalties

Distribution of musical and film related files through internet system can also be done by using blockchain technology ensuring that payment are made to the artists for their work. As blockchain was designed to prevent duplicate copies of the same file, it can also help reduce piracy. Additionally, by using blockchain mechanism for tracking repeat on streaming platforms and implementing smart contracts to manage payments, it provides transparency and ensures that artists receive their royalties.

xi. Secure Internet of Things (IoT) networks

The IoT (Internet of Things) has made human lives more convenient, but it also introduces risk on security issues, such as illegal access to personal data or to others secret system. Blockchain mechanism can enhance the security of IoT systems by keeping passwords and other sensitive data on a decentralized network. Additionally, blockchain’s immutable nature provides strong protection against data tampering, which ensures that the information will remain secured.

xii. Data storage

Blockchain mechanism can significantly increase the security and integrity of data storage systems. By enabling decentralized storage, blockchain makes it much harder for malicious actors to hack or erase data entirely, unlike centralized systems that may have only a few points of redundancy. Additionally, decentralized storage improves data accessibility, as access is not dependent on a single entity’s infrastructure. In some cases, the decentralized data storage process of blockchain mechanism may also offer cost advantages over traditional centralized providers.

xiii. Gambling

The gambling industry can leverage blockchain technology to offer enhanced transparency and security to players. One of the main advantages of blockchain-based casinos

is the ability to prove fairness, since all transactions and game outcomes are stored on the blockchain. Hence, players can verify data integrity of the system independently. Additionally, blockchain eliminates the need for players to share personal or banking information, lowering entry barriers and preserving user privacy. This also enables anonymous participation, which may help bypass certain regulatory limitations, as decentralized platforms are more resistant to centralized government restrictions or shutdowns.

xiv. Copyright management sector

Blockchain mechanism can play an important role in the copyright management sector by providing transparent and tamper-proof records of ownership. It enables the tracking of intellectual property rights and helps prevent forgery and unauthorized use. Additionally, this mechanism can be used to digitize event tickets, to reduce the risk of unauthorized resale and fraud. It also helps prevent the illegal duplication and distribution of digital content such as computer software and video games. These capabilities significantly strengthen copyright protection and rights enforcement.

xv. Eco-friendly management sector

Blockchain technology, when integrated with Artificial Intelligence, Big Data and IoT, can significantly improve how we monitor and manage environmental factors such as water and air pollution. These advanced systems enable more accurate tracking and decision making for eco-friendly initiatives. While blockchain has many more applications across various sectors, this article focuses only on selected areas due to time and space constraints.

xvi. National Security and Defence Operations

Blockchain technology is redefining defence operations by introducing decentralized, cryptographically secure systems that enhance communication, logistics, and cyber resilience. In military communications, consensus protocols like PBFT and Federated Byzantine Agreement (FBA), along with elliptic curve cryptography, provide robust multilayer encryption and fault-tolerant message validation. For logistics, Merkle tree structures and zero knowledge proofs ensure verifiable, tamper-proof tracking of assets, preventing fraud and improving supply chain transparency. Smart contracts automate key processes like inventory control and resource allocation, optimizing operational efficiency. Furthermore, quantum-enhanced blockchain systems, including Quantum Key Distribution (QKD) and Quantum Byzantine Agreement protocols, resist both classical and quantum cyber threats. Sharded blockchain architectures enhance scalability and real time visibility of assets, supporting secure and efficient decision making. Altogether, blockchain delivers strategic benefits in defence by securing data, automating operations, and reinforcing resilience in increasingly complex threat environments [23].

xvii. Media & Content distribution

Blockchain is changing the media industry by solving problems like fake news, ad fraud, copyright issues and data privacy. In news media, platforms like Civil and NewsDog use blockchain to check who published the news and keep the content safe from tampering. This helps people trust the news more. Some platforms also let creators earn money directly from their content, giving them more control and fairness [24]. In digital ads, platforms like AdEx and Brave use blockchain to stop fake clicks and protect user privacy. Everyone – advertisers, publishers, and users – gets a fair share without middlemen. For copyrights, companies like Microsoft, EY and Po.et use blockchain to confirm ownership and make sure creators get paid properly. Content sites like Steemit provide reward to users with crypto, while social

networks like Minds and FORESTING give users control of their data. Overall, blockchain helps make media safer, fairer, and more transparent.

xviii. Legal Metrology

In the legal sector, decentralized systems offer new ways to enhance transparency and trust. One key benefit is creating a decentralized audit trail, where blockchain can log every action in a secure, tamper-proof way. This could help maintain the chain of custody for evidence or ensure transparent auditing in legal processes. Smart contracts also play a major role by automating updates or ensuring compliance, as seen in measuring instruments. These same features can be applied to legal document handling or compliance tracking. Additionally, blockchain-based Public Key Infrastructure (PKI) can improve how digital identities and signatures are verified, making legal communication more secure and trustworthy. Blockchain is also useful for building transparent billing systems, like in electricity metering. In law, this can support automated payment systems. While the focus here is on legal metrology, these use cases hint at broader legal applications such as smart contracts, property records, IP rights management, and even dispute resolution, offering improved transparency, security and efficiency in legal systems [25].

5. Challenges in Blockchain Technology

From literature it is very clear that blockchain technology is an emerging field. However, it still faces several significant challenges. Among them, three key issues are: scalability, privacy leakage, and selfish mining [15]. These challenges are briefly discussed below.

5.1. Scalability

With the growth in number of daily transactions on blockchain networks scalability becomes a critical concern. Currently, the Bitcoin blockchain has exceeded 100 GB in storage size, as it is necessary to retain all historical transactions for validation purposes. However, limitations in block size and the fixed intervals for generating new blocks restricted the system's throughput. For example, the Bitcoin network can process only about seven transactions per second, which is inadequate for supporting millions of real time transactions. Additionally, due to limited block space, smaller transactions often face delays, if miners try to prioritize those with more transaction charges. While larger block size could improve transaction throughput, it may also produce propagation delay across the network and lead to blockchain forks. As a result, scalability remains a major technical challenge. Researchers have proposed several techniques to address these limitations.

- **Storage optimization:** To address the problem of bulky blockchain, a novel cryptocurrency approach was introduced, which aims to minimize the need for storing extensive transaction histories [26]. In this method, the network eliminates older transaction records and instead maintains the current balances of all active addresses in a data structure known as the account tree. This reduces the storage burden on nodes by eliminating the requirement to track every past transaction to verify legitimacy. Moreover, lightweight clients can contribute to mitigate this issue. A notable solution in this regard is a scheme called VerSum [27], which enables lightweight clients to outsource computationally intensive tasks involving large datasets. By comparing outputs from multiple independent servers, VerSum ensures the accuracy of results while significantly reducing the processing load on individual nodes.

- **Redesigning:** Eyal et al. in 2016, proposed a novel framework called Bitcoin-NG (NG stands for Next Generation) to address the limitations of traditional blockchain structures, particularly regarding scalability and throughput [28]. The core idea behind Bitcoin-NG is to

decouple the block structure in two distinct components: (i) key blocks and (ii) microblocks. Key blocks are used only for leader election through a competitive mining process, while the elected leader is authorized to produce microblocks that record transactions until a new leader is selected. Unlike conventional blockchains, Bitcoin-NG modifies the longest chain rule by assigning significance only to key blocks, thereby excluding microblocks from contributing to the chain's cumulative weight. This architectural redesign offers a more efficient way to increase transaction throughput without compromising the network's security, effectively balancing the trade-off between block size and propagation delay.

5.2. Privacy leakage

Although blockchain is widely regarded as a secure and pseudonymous system where users conduct transactions through cryptographic addresses rather than personal identities, several studies have revealed that transactional privacy is not fully guaranteed. Users often generate multiple addresses to obscure their identities and enhance privacy. However, research by S. Meiklejohn et al. in 2013 [29] and Ahmed Kosba et al. in 2016 [14] highlights that all transaction details, including transfer amounts and the balances tied to each public address, are visible publicly, making the blockchain inherently transparent rather than truly private. Furthermore, for Bitcoin, J. Barcelo in 2014 [30] demonstrated that transactions are traceable and potentially linked back to individuals, thereby compromising anonymity. In addition, A. Biryukov et al. [31] proposed a method to associate user pseudonyms with their IP addresses even when users are protected by firewalls or network address translation (NAT). Their findings showed that a unique client can be identified with the help of nodes it connects, allowing for the potential tracing of transaction origins. To counter these privacy concerns, several anonymity enhancing strategies have been proposed, which generally fall in two main categories.

• **Mixing:** Though addresses of blockchain users are pseudonymous, yet it can be possible to link these addresses to real-world identities, particularly when individuals repeatedly use the same address for multiple transactions. To enhance user privacy, mixing services – known as tumblers – are employed to distract the flow of funds by redistributing coins from various input addresses to different output addresses. For example, if sender (whose address S) sends funds to receiver (whose address R), a direct transaction could potentially reveal their association. To prevent this, sender may use an intermediary, such as Carol. sender sends the funds to Carol, who then forwards the amount to receiver using several input addresses (e.g., c1, c2, c3) and distributes the funds across multiple output addresses (e.g., d1, d2, B, d3). This process makes it significantly more difficult to trace the original transaction path and link for sender and receiver. However, this approach introduces the risk of relying on a potentially dishonest intermediary. The intermediary (Carol) could intentionally leak information about the transaction parties or misappropriate the funds by redirecting them to personal address instead of receiver. To address such concerns, J. Bonneau et al. in 2014 [32] proposed a method where user instructions – such as transaction amount and timing – are encrypted by suitable cryptosystem. Though this technique provides a means to detect fraud, it does not entirely eliminate the possibility of theft.

To further reduce the reliance on trust, G. Maxwell in 2013 proposed CoinJoin [33], that introduces a central mixing server that shuffles transaction outputs, reducing the likelihood of misappropriation. Building upon this idea, T. Ruffing et al. in 2014 published CoinShuffle [34] that utilizes decryption mixnets to perform address shuffling without depending on a centralized server, thereby offering a more decentralized and secure approach to transaction mixing.

• **Anonymous Transactions:** To enhance transactional privacy on the blockchain, cryptographic methods like zero knowledge proofs have been developed. One notable example is Zerocoin [35] which employs a zero knowledge proof mechanism to obscure the link between transaction origin and destination. In this scheme, miners do not verify transactions using conventional digital signatures. Instead, they verify that the coins being spent belong to a pre-approved set of valid coins. This effectively splits the traceable link between the source of the coins and the resulting transaction, thereby reducing the risk of transaction graph analysis. However, though Zerocoin improves anonymity, but still reveals the address of destination and amount of transaction. For addressing these limitations, Zerocash [36] was introduced as an enhancement. Zerocash employs a cryptographic proof zk-SNARK, which enable users for proving the validity of transactions without disclosing any sensitive information. The full form of zk-SNARK is zero knowledge Succinct Non-interactive Arguments of Knowledge. This advanced cryptographic proof ensures that both the value of coins held by users and the transaction amounts remain completely hidden from the public blockchain, offering a significantly higher degree of privacy and anonymity than its predecessor.

5.3. Selfish mining

Blockchain networks are susceptible to certain strategic attacks, one of which is *selfish mining*. Traditionally, it is assumed that only miners controlling over 51% of the network's computational power could compromise the blockchain by reversing transactions or creating forks. Fork is the changing in blockchain protocol that splits the transaction in two different versions of blockchain with different transaction histories. However, research by Eyal and Sirer [37] has shown that even miners with less than 51% of the computational power can disrupt the network through selfish mining tactics. In a selfish mining scenario, malicious miners mine new blocks but withhold them from the public chain, instead maintaining a private fork. They release their private chain only when it offers a strategic advantage typically when it is longer than the public chain, causing the network to adopt it. This tactic makes the honest miners' efforts wasted, as their blocks become part of an orphaned chain. Meanwhile, selfish miners continue mining privately with reduced competition, thereby increasing their mining rewards. Over time, this imbalance inspires the original miners to join the selfish mining pool, potentially pushing the dishonest miners to achieve the critical 51% threshold. Based on this concept, various advanced selfish mining strategies have been proposed:

• **Stubborn mining:** It is described by K. Nayak et al. [38]. It combines selfish mining with eclipse attacks. Eclipse attacks work on network-layer vulnerability and isolates honest nodes – allowing attackers to manipulate consensus more effectively.

• **Trail-stubborn mining:** It allows attackers to keep mining their private chain even when it temporarily lags behind the public one. In certain network conditions, this strategy can provide up to a 13% profit advantage over basic selfish mining.

• **Smaller mining:** Research by A. Sapirshtein et al. [39] reveals that even smaller mining entities can benefit from alternative selfish mining strategies, although their gains are modest compared to larger attackers.

Significantly, studies have shown that even attackers having less than 25% of the network's total computational power can exploit selfish mining under certain conditions. To mitigate such threats, several counter measures have been proposed. Two methods are mentioned here: (i) E. Heilman [40] suggested a method that encourages honest miners to follow the chain with more recent timestamps, using random beacons as a reference.

However, this method may be vulnerable to forged timestamps. (ii) ZeroBlock, introduced by S. Solat and M. Potop-Butucaru [41], imposes a strict maximum time interval for block propagation. If a block is not published and accepted within this timeframe, it is automatically rejected. This mechanism prevents selfish miners from gaining undue rewards by withholding blocks.

These solutions aim to level the playing field and reinforce the fairness and stability of blockchain networks against selfish mining threats.

.

6. Conclusion and Future Scope

The target of this research work is to implement blockchain technology for small devises, so that everyone can use it for their security purpose. Bitcoin requires powerful calculating system and more memory size whereas Litecoin can be executed in less powerful system and it can be executed with small memory. So, future activity of this research will focus on Litecoin. For this purpose, simple hashing technique may be chosen instead of SHA-256. And it is assumed that this idea will be helpful to the new researchers in this field for their future research.

Acknowledgments

This research work was executed in the Department of Computer Science and Technology, University of North Bengal. The team members are thankful to the department for providing such opportunity to carry on the research activity. Authors of this article are also grateful to the HoD and other faculty members of the department for providing necessary infrastructural facilities, resources and valuable suggestions to the research work.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer ElectronicCash System”, 2008, https://bitcoin.org/bitcoin.pdf

[2] Mastering Blockchain Unlocking the Power of Cryptocurrencies- - -, Lorne Lantz and Daniel Cawrey,O’REILLY, 1st Edition, Shroff Publishers and Distributors PVT. LTD. Second Indian Reprint, Sep 2021.

[3] Mastering Bitcoin Programming the Open Blockchain, Andreas M. Antonopoulos, O’REILLY, 2nd Edition, Shroff Publishers and Distributors PVT. LTD., Third Indian Reprint, May 2021.

[4] Sanjeev Kumar Dwivedi et al., “Blockchain-base d secured event-information sharing protocol in internetof vehicles for smart cities”, Computers and ElectricalEngineering, Elsevier, Vol. 86, September 2020, https://doi.org/10.1016/j.compeleceng.2020.106719

[5] CHUN-AN LIN et al, “Design Patterns for Blockchain assistedAccountable Data Dissemination between IoTDevices and Edge Server”, Asian PLoP’20, March 4- 6,2019.

[6] Minhaj Ahmed et al., “IoT security: Review, blockchainsolutions, and open challenges”, Future GenerationComputer Systems, ELSEVIER, Vol 82 (2018), pp 395-409, 2018.

[7] Ali Dorri et al., “Blockchain for IoT Security and Privacy:The Case Study of a Smart Home”, IEEE InternationalConference on Pervasive Computing and CommunicationsWorkshops (PerCom Workshops), 13-17March 2017, DOI: 10.1109/PERCOMW.2017.7917634.

[8] 18. H. D. Zubaydi et al.," A Review on theRole of Blockchain Technology in the Healthcare Domain", electronics, MDPI, 15 June 2019,doi:10.3390/electronics8060679.

[9] Arijit Saha et al. "Review on "Blockchain technologybased medical healthcare system with privacy issues",Wiley, Vol 2 (5), 2019. DOI: 10.1002/spy2.83.

[10] Muhammad Nasir Mumtaz Bhutta et al. "A Survey onBlockchain Technology: Evolution, Architecture andSecurity",IEEEAcess, Vol 9, pp 61048-61073, 2021.

[11] B.Mona, Shaik Yasmeen et al. "Blockchain Technology",Journal of Applied Science and Computations,Vol- VI(I) pp 526 -534, January 2019.

[12] Florian Tschorsch& Björn Scheuermann, "Bitcoin andBeyond: A Technical Survey on Decentralized DigitalCurrencies", IEEE Communications Surveys & Tutorials,Vol 18(3), pp 2084 – 2123, March 2016.

[13] Sanjeev Kumar Dwivedi, "Blockchain based secured information sharing protocol in supply chainmanagement system with key distribution mechanism", Journal of Information Security and Applications, Elsevier, Vol. 54 October 2020. https://doi.org/10.1016/j.jisa.2020.102554.

[14] Ahmed Kosba et al. "Hawk: The Blockchain Modelof Cryptography and Privacy-Preserving Smart Contracts",IEEE Symposium on Security and Privacy (SP),10.1109/SP.2016.55, 2016.

[15] Zibin Zheng et al. "Blockchain challenges and opportunities: a survey", International Journal of Web andGrid Services, Vol.14(4) pp 352-375, October 2018.

[16] Urvi Dilip Kumar Rajguru, "A review on challengesand opportunities in Blockchain Technology ", InternationalJournal of Advance Research and Development,Vol. 3 (10) pp 122-127, 2018.

[17] Elyes Ben Hamida et al., "Blockchain for Enterprise: Overview, Opportunities and Challenges", The Thirteenth International Conference onWireless and Mobile Communications, June 2017. https://www.researchgate.net/publication/322078519

[18] Kamanashis Biswas and VallipuramMuthukkumarasamy,"Securing Smart Cities Using Blockchain Technology", 12-14 December 2016,DOI:10.1109/HPCC-SmartCity-DSS.2016.0198

[19] Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A.: A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference, vol. 13, p. 13 (2016)

[20] Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotech. J. **16**, 267–278 (2018)

[21] Bocek, T., Rodrigues, B.B., Strasser, T., Stiller, B.: Blockchains everywhere – a use-case of blockchains in the pharma supply-chain. In: IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 772–777, May 2017

[22] Zhou, L.,Wang, L., Sun, Y.: MIStore: a blockchain-based medical insurance storage system. J. Med. Syst. **42**(8), 149 (2018)

[23] Kostopoulos, N., Stamatiou, Y. C., Halkiopoulos, C., & Antonopoulou, H. (2025). Blockchain Applications in the Military Domain: A Systematic Review. *Technologies*, *13*(1), 23.

[24] Liu, L., Zhang, W. & Han, C. A survey for the application of blockchain technology in the media. *Peer-to-Peer Netw. Appl.* **14**, 3143–3165 (2021). https://doi.org/10.1007/s12083-021-01168-5

[25] D. Peters, J. Wetzlich, F. Thiel and J. -P. Seifert, "Blockchain applications for legal metrology," *2018 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Houston, TX, USA, 2018, pp. 1-6, doi: 10.1109/I2MTC.2018.8409668

[26] J. Bruce, (2017) The Mini-Blockchain Scheme,http://cryptonite.info/files/mbc-scheme-rev3.pdf

[27] J. van den Hooff et al. (2014) 'Versum: Verifiablecomputations over large public logs', Proceedingsof the 2014 ACM SIGSAC Conference on Computerand Communications Security, New York, NY, USA,pp.1304–1316.

[28] I. Eyal et al. (2016) 'Bitcoin-ng: a scalable blockchainprotocol', Proceedings of 13th USENIX Symposiumon Networked Systems Design and Implementation(NSDI 16), Santa Clara, CA, USA, pp.45–59.

[29] S. Meiklejohn et al.(2013) 'A fistful of bitcoins: Characterizingpayments among men with no names', Proceedingsof the 2013 Conference on Internet MeasurementConference (IMC'13), New York, NY, USA.

[30] J. Barcelo, (2014) User Privacy in the Public BitcoinBlockchain.

[31] A. Biryukov et al. (2014), 'Deanonymisation of clientsin bitcoin p2p network', Proceedings of ACMSIGSAC Conference on Computer and Communications Security, New York, NY, USA, pp.15–29.

[32] J. Bonneau et al. (2014) 'Mixcoin: Anonymity for bitcoinwith accountable mixes', Proceedings of InternationalConference on Financial Cryptography andData Security, Berlin, Heidelberg, pp.486–504.

[33] G. Maxwell, (2013) Coinjoin: Bitcoin Privacy for the Real World, Post on Bitcoin Forum.

[34] T. Ruffing et al. (2014) 'Coinshuffle: Practical decentralizedcoin mixing for bitcoin', Proceedings of European Symposium on Research in Computer Security, Cham,pp.345–364.

[35] I. Miers et al. (2013) 'Zerocoin: Anonymous distributede-cash from bitcoin', Proceedings of IEEE SymposiumSecurity and Privacy (SP), Berkeley, CA, USA,pp.397–411.

[36] E. B. Sasson et al. (2014) 'Zerocash: Decentralizedanonymous payments from Bitcoin', Proceedings of2014 IEEE Symposium on Security and Privacy (SP),San Jose, CA, USA, pp.459–474.

[37] I. Eyal and E. G. Sirer, (2014) 'Majority is not enough:Bitcoin mining is vulnerable', Proceedings of InternationalConference on Financial Cryptography andData Security, Berlin, Heidelberg, pp.436–454.

[38] K. Nayak et al. (2016) ‘Stubborn mining: generalizingselfish mining and combining with an eclipse attack’,Proceedings of 2016 IEEE European Symposium onSecurity and Privacy (EuroSandP), Saarbrucken, Germany,pp.305–320.

[39] A. Sapirshtein et al. (2015) Optimal Selfish MiningStrategies in Bitcoin, arXiv preprint arXiv:1507.06183.

[40] E. Heilman, One Weird Trick to Stop Selfish Miners:Fresh Bitcoins, A Solution for the Honest Miner. CryptologyePrint Archive, Report 2014/007 (2013). https://eprint.iacr.org/2014/007.pdf

[41] S. Solat and M. Potop-Butucaru, (2016) ZeroBlock:Timestamp-Free Prevention of Block-Withholding Attackin Bitcoin, Technical Report, Sorbonne Universites,UPMC University of Paris 6.