NAVIGATING THE BLOCKCHAIN REVOLUTION: DECENTRALIZATION, FINANCE, AND BEYOND

Editors:
Monica Bhutani
Monica Gupta
Kirti Gupta
Deepali Kamthania
Danish Ather

Bentham Books

Navigating the Blockchain Revolution: Decentralization, Finance, and Beyond

Edited by

Monica Bhutani, Monica Gupta & Kirti Gupta
Department of Electronics and Communications
Bharati Vidyapeeth's College Of Engineering
New Delhi, India

Deepali Kamthania
School of Information Technology
Vivekananda Institute of Professional Studies-Technical
Delhi, India

&

Danish Ather
Department of IT and Engineering
Amity University in Tashkent
Tashkent, Uzbekistan

Navigating the Blockchain ,Revolution: Decentralization Finance, and Beyond

Editors: Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather

ISBN (Online): 979-8-89881-150-1

ISBN (Print): 979-8-89881-151-8

ISBN (Paperback): 979-8-89881-152-5

Published by Bentham Science Publishers Pte. Ltd. Singapore, in collaboration with Eureka Conferences, USA.

First published in 2025.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
No. 9 Raffles Place
Office No. 26-01
Singapore 048619
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

Blockchain is among the disruptive technologies of the 21st century owing to its impact on redesigning the systems of data protection, finance, and other distributed architectures. Of the many global significance that this technology has, this is the most important one because of the potential of this technology to change the different sectors, including the banking sector, supply chain management, the health sector, and the government. **Navigating the Blockchain Revolution:** This work aims to present the readers with an understanding of the core concept of blockchain technology, the various possibilities offered by this technology, and the problems that this sector encounters as it navigates into the global market.

First, the book aims to acquaint the reader with the basic idea of blockchain through the process of creating Bitcoin, Ethereum, and smart contracts. The early chapters create the basis for realizing that blockchain is much greater than cryptocurrencies' underlying technology. Further sections show that different sectors explained how blockchains are introduced and used to unmask certain issues—whether to secure the monetary operations, enhance the supply chain traces, or, among others, defend healthcare information.

Being aware of the problems related to the adoption of blockchain, this book also tackles the major concerns of scalability, power usage, and regulations issues. Readers will be able to get a realistic picture of the future of blockchain technology just by analyzing the current solutions and further advancements being made.

Furthermore, this book discusses some of these applications when overlaying blockchain with other promising technologies such as IoT and AI. The last chapters shed light on the future, presenting further developments like blockchain connection and decentralized autonomous organisms, which can change numerous branches and how companies work.

Thus, this book aims to be a source of practical information and inspiration for professionals, academics, and enthusiasts. Regardless of whether you are approaching the subject from scratch or enhancing your prior knowledge, this book is set to offer inspiring perspectives on blockchain's broad and growing applications in our new digital world. Our intention with this guide is to provide the necessary insights for readers to go forward into the continuous advancement of blockchain technology.

Monica Bhutani, Monica Gupta & Kirti Gupta
Department of Electronics and Communications
Bharati Vidyapeeth's College Of Engineering
New Delhi, India

Deepali Kamthania
School of Information Technology
Vivekananda Institute of Professional Studies-Technical
Delhi, India

&

Danish Ather
Department of IT and Engineering
Amity University in Tashkent
Tashkent, Uzbekistan

List of Contributors

Ayush Arya	School of Information Technology, Vivekananda Institute of Professional Studies-Technical Campus, Delhi, India
Amardeep Pandit	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Aparna Singh	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
Dhiraj Pandey	Department Of Information and Technology, JSS Academy of Technical Education, Noida, India
Deepali Kamthania	School of Information Technology, Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India
Garima Saini	Institute of Information Technology & Management (IITM), GGSIPU, Delhi, India
Gaurav Kumar	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Harsh Taneja	Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India
Jaya Sinha	Department of Computer Science and Engineering, ITS Engineering College, Greater Noida, India
Kiran Deep Singh	Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
Kajal Dubey	Department Of Information and Technology, JSS Academy of Technical Education, Noida, India
Mohit Mittal	School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India
Mumukshu Tyagi	Department of IT, Maharaja Surajmal Institute of Technology, New Delhi, India
Mukta	School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India
Nivedita Palia	School of Engineering and Technology, Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India
Nikhil Kumar	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Ojasvi Singh	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Prerna Ajmani	School of Information Technology, Vivekananda Institute of Professional Studies-Technical Campus, Delhi, India
Prabh Deep Singh	Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India
R. Sujithra Kanmani	School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Rohan Raj	Department of Information Technology and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India
Richa	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Sweeti Sah	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Shweta Sharma	Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India
Shiksha Kumari	School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India
Sherry Verma	School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India
Sonika Malik	Department of IT, Maharaja Surajmal Institute of Technology, New Delhi, India
Siddharth Bisht	Department of IT, Maharaja Surajmal Institute of Technology, New Delhi, India
Sachin Gupta	Department of Computer Science Engineering (CSE), Maharaja Agrasen Institute of Technology, Delhi, India
Surbhi Sharma	School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
Tanusri Gururaj	Ernst & Young Associates LLP, Gurgaon, Haryana, India
Tanu Shree	Department of Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida, India
V. Gayathri	Department of ECE, Bharati Vidyapeeth's College of Engineering, New Delhi, India
Yash Gupta	Department of IT, Maharaja Surajmal Institute of Technology, New Delhi, India

CHAPTER 1

Comprehensive Introduction to Blockchain Technology: Principles, Applications, and Future Prospects

Nivedita Palia[1,*] and **Deepali Kamthania**[2]

[1] *School of Engineering and Technology, Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India*

[2] *School of Information Technology, Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India*

Abstract: Blockchain is an immutable digital ledger system that eliminates the need for centralized storage and authority, enabling decentralized financial transactions. It is made up of timestamped, immutable information blocks that are managed by a collection of nodes rather than by any one node. Using cryptographic methods, every block is connected and secured. Blockchain provides a secure and transparent solution by redefining faith, possession, and identity in financial systems. This chapter thoroughly reviews blockchain technology, focusing on why we need it. Next, the chapter discusses blockchain technology's characteristics, type, architecture, and work. Further, the chapter presents some areas of application and challenges it faces.

Keywords: Blockchain, Blockchain technology, Bitcoins, Cryptocurrency, Decentralization, Public blockchain, Private blockchain, Smart contracts, Security, Transparency.

INTRODUCTION

In the past few years, the word blockchain has changed from a specialised thing to an enormous transforming power with the potential to revolutionize several sectors. It has transformed contracts, financial transactions, and records into digital form. Blockchain technology (BT) was initiated in 2008 with Satoshi Nakamato's introduction of Bitcoin [1]. It introduces the idea of blockchain and initiates the use of cryptocurrency in financial transactions where previously cash was used. The introduction of smart contracts started 2nd generation of blockchain and provides efficiency, security, and transparency to financial transactions.

* **Corresponding author Nivedita Palia:** School of Engineering and Technology, Vivekananda Institute of Professional Studies-Technical Campus, New Delhi, India; E-mail: nivedita134@gmail.com

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

Alternatively, 3rd generation depends on areas other than finance where blockchain is used, such as healthcare, government, science, *etc.* We are in the fourth generation of blockchain with Artificial Intelligence. In less than a decade, Blockchain has seen three generations. Fig. (**1**) summarizes the generations of blockchain.

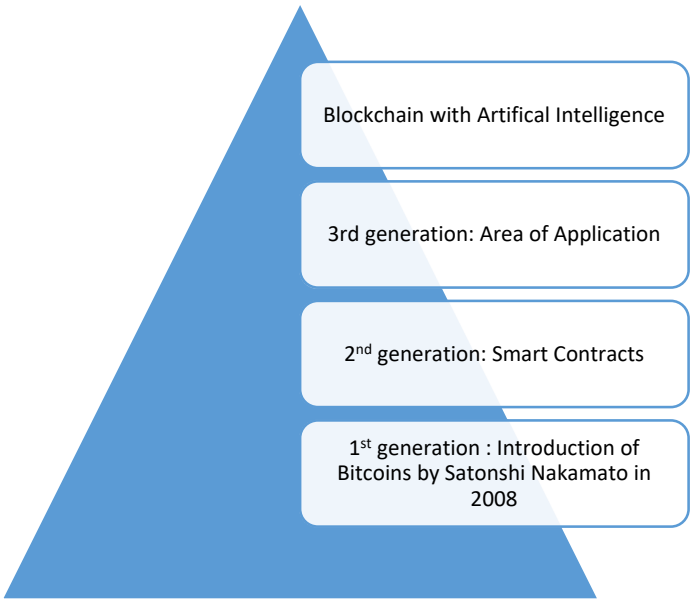

Fig. (1). Generations of blockchain technology.

Blockchain has great potential to transform the financial sector digitally, but some pros and cons remain. In this chapter, we provide a brief survey of the BT, its types, the timeline of blockchain, its characteristics, different algorithms used, and areas of application, followed by a discussion of other challenges and future scope.

TIMELINE OF BLOCKCHAIN TECHNOLOGY

The emergence of the Bitcoin cryptocurrency in 2008 hyped the term "blockchain," but its fundamental ideas and principles have been applied since the 1980s. David Chamu [2] in 1983 proposed the concept of blind signatures for digital transactions. It is a cryptographic technique designed for a safe, automated payment system for enhancing user privacy. Stuart Haber and W. Scott Stornetta 1991 [3] introduced a method for timestamping digital documents by ensuring the validity and integrity of the time of creation. Their pioneering work set the foundation for further development in BT. Reusable Proof of Work (RPoW) was introduced by Hal Finney in 2004 [4] to improve the idea of proof of work, which

was initially implemented to combat spam in the digital world. In 2008, Satoshi Nakamoto [1] gave the concept of bitcoin (BTC) in the paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" defining the decentralized, secure, and transparent transaction system without intervening central authority. On 12th January 2009 [5, 6], the first Bitcoin transaction of 10 BTC occurred between Santoshi Nakamoto and Hal Finney. This historic transaction initiated the era of global cryptocurrency. The world's first bitcoin exchange, "Bitcoin Market" was set up in 2010 [7]. It enables users to transact Bitcoin for U.S. dollars. The first BTC ATM [8] was installed in a Waves Coffee House in Vancouver, Canada, in 2013. It was operated by Robocoin, which allowed users to convert cash for BTC and vice versa. Vitalik Buterin in the year of 2013 presented the idea of a smart contract in his Ethereum white paper [9]. He set up the foundation for the decentralized platform, which can handle decentralized applications (dApps). Officially, in the year 2014, Ethereum launched Blockchain Technology [10]. Concurrently in the same year, the Linux Foundation initiated the Hyperledger project. Free software supports enterprise-grade BT in supply chain management, healthcare, finance, education, *etc* [11]. The establishment of the R3 consortium and the launch of Ethereum's first live release: "Frontier" are the two significant events that took place in the year 2015, which will influence the evolution of BT [12, 13]. The Decentralized Autonomous Organization project was developed on the Ethereum Blockchain and raised US$ 150 million in 2016 [14]. In 2017 Digital Trade Chain platform was announced. Seven European banks collaborated to create the platform. Later it was renamed as we. Trade [15]. Table **1** summarizes the significant events that occurred in the evolution and global spread of BT [1 - 23]. Since 2008, BT has drawn interest from all over the world. Many nations are implementing this technology in various areas such as healthcare, supply chain, finance, agriculture, *etc.* This chapter briefly explained the different aspects of the BT, its area of applications, challenges, and future scope.

Table 1. Major events occurred [1 - 24].

Year	Work Done
1983	Blind signatures for automated payments proposed by David Chaum
1991	Timestamped documents introduced for securing digital documents
2004	Reusable Proof of Work (RPoW) introduced by Hal Finney
2008	The Bitcoin whitepaper was published, outlining a peer-to-peer electronic cash system
2009	1st Bitcoin transaction occurred
2010	World's first Bitcoin exchange, "Bitcoin Market", established
2013	The first Bitcoin ATM was launched
2013	Smart contracts in the Ethereum whitepaper proposed by Vitalik Buterin

CHAPTER 2

Blockchain in Supply Chain Management, Traceability, Transparency, and Provenance

Prerna Ajmani[1,*], **Garima Saini**[2] and **Ayush Arya**[1]

[1] *School of Information Technology, Vivekananda Institute of Professional Studies- Technical Campus, Delhi, India*

[2] *Institute of Information Technology & Management (IITM), GGSIPU, Delhi, India*

Abstract: Blockchain technology is changing how supply chains work by making things faster, more open, and secure, while also making complicated tasks easier and solving old problems. Blockchain is distributed technology that is safe and secure and once the information is entered into this chain, it cannot be modified. Thus, Blockchain ensures trust and traceability, making it useful for many applications. Blockchain ensures higher security and protects data from any tampering. It also provides the facility of smart contracts for easy workflow. Additionally, Blockchain helps brands show that their products meet industry standards, which builds trust with customers. Overall, this technology is important for making sure goods and services are safe and reliable, while also simplifying how supply chains work. In this chapter, we will explore how Blockchain helps track products in the supply chain, explain smart contracts in detail, and look at some case studies to better understand these ideas.

Keywords: Blockchain technology, Cyber threat protection, Decentralized ledger, Efficiency, Process automation, Product provenance, Security, Smart contracts, Supply chain management, Traceability, Transparency.

INTRODUCTION

Back in 2008, a person who loved technology came up with something new called Blockchain. We do not know who this person is because they stayed anonymous. They made Blockchain to fix some problems with Bitcoin. One big problem was how to send money directly between people without using banks or other middlemen, and another issue was stopping people from spending the same money twice. Today, technology is growing super-fast and helping solve many real-world problems, and Blockchain is one of the ideas that made a big difference.

[*] **Corresponding author Prerna Ajmani:** School of Information Technology, Vivekananda Institute of Professional Studies- Technical Campus, Delhi, India; E-mail: prerna.ajmani@vips.edu

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

Over time, Blockchain technology gained significant attention from industries, academics, and researchers alike. By 2018, it was recognized as one of the top five emerging technologies. Blockchain has evolved through three major phases. The first generation, Blockchain 1.0, emerged in 2009 with a primary focus on supporting digital currency, particularly Bitcoin. As the technology's potential became clearer, the second generation, Blockchain 2.0, appeared in 2014, emphasizing the use of Smart Contracts in various applications, notably through Ethereum. By 2017, Blockchain 3.0 was ushered in, driven by the Hyperledger initiative, leading to the development of decentralized applications across a wide range of industries.

Today, Blockchain's applications extend beyond finance and cryptocurrency, impacting fields such as education, healthcare, agriculture, the Internet of Things (IoT), and even governance. Additional uses include electronic voting, autonomous vehicles, trading systems, supply chains, smart grids, and networking, among others.

TRACEABILITY AND TRANSPARENCY IN SUPPLY CHAIN MANAGEMENT

Traceability and "transparency" are two terms that people often mix up in supply chain management, but they mean different things, even though they are connected. Transparency is about how much you can see what's happening in the supply chain. It means that everyone involved can easily get the info they need about a product, without anything missing or getting messed up. According to a study [1], transparency means all the people in the supply chain can quickly and easily find the info they need. Traceability, on the other hand, is more about being able to find specific details about any part of the supply chain [2, 3].

Researchers also interchange the term traceability with tracking [4 - 6]. Tracking is following the product from where it starts to where it ends up while tracing is about going backward and finding where the product originally came from.

A study breaks transparency down into three parts: history-based transparency, operations transparency, and strategy transparency [7]. History-based transparency, which is achieved through tracking and tracing, refers to a complete and verifiable record of a product's journey. In essence, traceability enables transparency by providing the necessary tools for tracking and tracing.

Several studies have integrated traceability into different supply chain scenarios to enhance transparency. For instance, a study [8] developed a system for creating transparency in the meat supply chain. This system allows consumers to trace the history of meat in the market, suppliers to track its movement, and government

agencies to monitor its quality. Another example is the introduction of GPS [9]. LAB, a Global Positioning System (GPS)-enabled traceability system designed to ensure transparency in global supply chains by managing production planning and supply chain events.

However, these centralized traceability systems have limitations, particularly when it comes to data manipulation. Centralized systems often struggle with transparency and trust issues [10]. A study describes centralized traceability systems as monopolistic, asymmetrical, and opaque, which can lead to problems like corruption, falsification of data, and system failures [11].

On the other hand, Blockchain technology offers decentralized, immutable, transparent, secure, and auditable ledger [12]. Blockchain's traceability, security and decentralized features make its usage worthier in supply chain management [13]. Any transaction that occurs in the supply chain can be recorded in blocks, that can be arranged in chronological order in the Blockchain. To ensure complete transparency, these records are further verified by all authorized participants of Blockchain. A study suggests that Blockchain serves as a trustworthy, transparent, and verifiable resource for all the stakeholders in a particular supply chain [14].

As compared to a centralized system, in Blockchain, each block is linked cryptographically with others thus abolishing data tampering. Blockchain can be further classified as: public, private, and consortium types [15]. Researchers in a study [16] highlighted that Blockchain can mitigate various supply chain risks such as information delays, lack of transparency, security issues, and IT platform incompatibility. Further, the amalgamation of IoT and smart contracts has increased the acceptance and effectiveness of Blockchain-based traceability supply chain systems [17, 18].

An Insight into Blockchain Powered Traceability Solutions in Supply Chain Management

Blockchain technology has already been integrated into numerous supply chains to establish traceability, with the goal of enhancing transparency. This section explores various real-world applications of Blockchain-based traceability solutions as reported in academic literature. Each case is examined to understand the purpose of implementing Blockchain for traceability, including its strengths, limitations, and the methodologies used to develop these solutions. Additionally, the supply chain models employed in these solutions are analyzed, specifically in relation to distribution network designs. As noted in a study, there are six key distribution network designs, and the level of order visibility plays a crucial role in determining the most suitable design [19]. Visibility, in this context, refers to the ability to access and share information across the supply chain. A high level of

CHAPTER 3

Enhancing Electronic Health Records and Patient Data Management through Blockchain Technology

Prabh Deep Singh[1,*], **Kiran Deep Singh**[2] and **Harsh Taneja**[1]

[1] *Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India*

[2] *Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India*

Abstract: Blockchain technology has the potential to help deliver more efficient health services, improving patients' experience from end to end. In this chapter, a blockchain platform is analyzed, which adopts a protocol that is designed to both regulate access to data and information, digitize health data, and enable an untrusted reader to ask for the execution of arbitrary algorithms on the peer's private databases, whose contents must remain hidden to those who are not authorized to access them, and obtaining an efficient and scalable response. The chapter uses blockchain technology to enhance electronic health records and patient data management. Several standardized technologies and models are available in the market for electronic health records, but the users, *i.e.*, patients and hospitals, trust and believe in those services that provide enhanced security to their data. Blockchain can be utilized for securing EHR by deploying attributes of a public or private blockchain, enabling permission access by hospitals and granting access easily to patients and family members.

Keywords: Big health data, Blockchain, Centralization, Chain methods, Electronic health record, Electronic medical record, Encryption, Health care, Medical-chain, Patient data management.

INTRODUCTION

This research proposes that electronic health records (EHR) and patient data management can be drastically enhanced by adopting public blockchain technology. A public blockchain's innovation overcomes the weak points of every other electronic model in terms of disintermediation, crucial security, ownership, data integrity, and data sharing. It is expected that after the widespread adoption of EHR, large-scale blockchain technology will be deployed to support and

[*] **Corresponding author Prabh Deep Singh:** Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India; E-mail: ssingh.prabhdeep@gmail.com

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

enhance this demotion in the health industry. With an open transparent platform, it will also provide a cost-effective secure way for general 'people' to take control of their own health data [1].

The problem of electronic health records (EHR) security, data integrity, secure patient data sharing, and privacy is huge and unsolved. Large-scale data breaches made by hacking, stealing, and insider attacks are increasingly common with EHRs. In addition, corrupted and/or unreliable data in a patient's EHR, the data integrity problem, may result in inappropriate patient care. Furthermore, large-scale data sharing may result in misunderstanding and possible misuse of health information. The new powerful electronic model in management has the potential to address many longstanding and billowing problems, including multi-organization environments, because of its innovative features such as disintermediation and public and private key cryptography.

Background and Significance

In addition to highlighting the lack of industry standards and policy regulations, research related to the adverse impact of inadequate data and electronic health records (EHR) management has proven valuable for several reasons. EHR typically refers to health-related information based on sharing and storage in the electronic format that is maintained by the patient or an organization. Utilizing the data, such as administrative data, extracted from such an electronic form of patient payment, treatment, and outcomes has facilitated healthcare professionals to improve their decision-making. As these data capture that billing systems have been changing rapidly as a result of their ad hoc basis, many of the current issues are related to security, privacy, and compliance regulations protecting sensitive healthcare data from unauthorized disclosure, particularly as the result of a large amount of data breaches [2]. This has led to organizing data in a more secure manner surrounding the establishment of standards designed to guide the more comprehensive use of electronic health data.

The National Institute of Standards and Technology (NIST) defines blockchain technology as a decentralized digital ledger that records transactions across multiple computers. This allows parties to safely and securely exchange information, including individual user data, through distributed applications. Blockchain has often been equated with Bitcoin, in that it was initially developed to serve as the accounting method for cryptocurrency, but the technology has evolved and come to the forefront as a multi-faceted peer-to-peer and secure technology [3]. The technology's unique characteristics suggest that it could be leveraged, and has the potential to work, to improve data management issues in healthcare and medicine including the inefficiencies and revenue loss related to

claim and billing management, slow and cumbersome settlements, and patient data privacy breach [4].

Purpose and Scope

The scope of this paper is to analyze the advantages and disadvantages of the current EHR and BD systems and propose a new blockchain-based EHR and data management system in which the patient data is stored in a secure, transparent, and elegantly structured way. It provides control to the patient over their data. It also provides more benefits to the BD managers, such as transparency and security. In addition, it focuses on a Patient Hash tree-based approach with separate data and index distribution to resolve the limitation of using the Merkle tree to generate a large number of hashes. The main scope focuses on comparing the efficiency of current and proposed data on the blockchain and finding the benefits or demerits of the current existing proposed problem. It currently uses IPFS and the medical chain, but many different blockchain-based EHR systems and new EHR networks can also be used. This can also be implemented using other blockchain-based networks. As a result, the proposed system not only brings about the improvement of the patient transaction system but also the storage and control problem of medical blockchain-based EHR problems. Data management is at the heart of this.

In this paper, a patient manages patient transaction information, and a tamper-proof patient data structure is provided. The proposed system adopts IPFS for data storage and management of transaction information. Blockchain (Medical-chain) is adopted to keep patient data and encryption key to be used to generate a Merkle tree. As a result, detailed transaction information is protected in the system. The proposed system not only brings about the improvement of the patient transaction system but also the storage and control problem of medical blockchain-based EHR problems. It is possible to enhance functionality such as revealing others who want to know your information. You will be able to provide protection if you do not want to share your data with others or those who are not authorized. It is expected that patients will help them in a healthier and more effective way to build EHR and BD-based EHR.

Electronic Health Records (EHRs)

For data analysis, a tremendous volume of patient data and evidence-based knowledge, *i.e*. clinical practice guidelines, are analyzed to benefit clinical decision-making, and patient treatment, and enable metrics of patient engagement, satisfaction, and treatment outcomes. A central EHR database is centralized with many independent but EHR-aware healthcare applications. They can establish a connection with EHRs by querying EHR-Aware regulations. The processing of

CHAPTER 4

Blockchain: The Challenges of Scalability and Their Solutions

Amardeep Pandit[1], Sweeti Sah[1,*], Shweta Sharma[1,*], Ojasvi Singh[1], Gaurav Kumar[1] and **R. Sujithra Kanmani[2]**

[1] *Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India*

[2] *School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India*

Abstract: Blockchain technology offers incredible value and opportunity in delivering secured, decentralized transactions but faces significant challenges as it relates to scalability, which hinders adoption and use. As in the maturation of blockchain technology, challenges related to its scalability are important for latest technologies as they can affect scalability and efficiency. These types of challenges to scalability generally emerge through increased user and transaction volumes and cause losses in performance and efficiency as they pertain to a congested network, storage of data, and speed in processing time. Additionally, traditional consensus mechanisms, like proof of work, seamlessly create challenges as they pertain to amounts of computational power, and other resources allow allocation associated with work completion. As we can imagine, potential solutions have already emerged that help to mitigate overcoming these challenges. Solutions related to Layer 2 scaling, such as side chains or payment channels, add an alternative layer to the transaction applications and, theoretically, increase throughput and financially through decreased network congestion. Sharding, which splits the blockchain into smaller, more manageable segments, also improves operational efficiency. Moreover, advancements in consensus algorithms, including Proof of Stake and hybrid models, aim to boost scalability while optimizing resource use. This research explores the primary scalability challenges faced by blockchain systems. It reviews the cutting-edge solutions being developed to improve their performance, ensuring that blockchain technology can effectively support the increasing demands of a decentralized digital world.

Keywords: Architecture, Blockchain, Consensus, Decentralization, Ethereum, Forking, Interoperability, Latency, Ledger, Management, Network.

[*] **Corresponding authors Sweeti Sah and Shweta Sharma:** Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India; E-mails: sweetisah3@nitkkr.ac.in; shweta.sharma@nitkkr.ac.in

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

INTRODUCTION

Blockchain, an increasingly popular form of decentralized innovation, has a bright future ahead of it. The concept of the blockchain data structure was introduced by Haber and Stornetta and received serious consideration when Nakamoto developed a light bulb idea concerning a cryptocurrency-based payment system in 2008 with Bitcoin [1, 2]. Blockchain technology has been proven to be a transformative force within various industries by offering decentralized, secure, and transparent transaction mechanisms. Even after numerous plus pointers, there too exist some of the major hindrances, one of which is scalability challenges. These challenges have been marked out to be very common during the expansion in user base and transaction volume. This work brings views on the scaling challenges that slow down blockchain performance, specifically focusing on transaction throughput, latency, and storage capacity.

The "Blockchain Trilemma" represents one of the major challenges for cryptocurrencies and their widespread use and acceptance. It is a trade-off presented by a blockchain that attempts to achieve an ideal balance of decentralization, security, and scaling at the same time [3]. Blockchain technology is distinguished by several fundamental features that collectively ensure its security, transparency, and reliability. The most prominent feature is data immutability, which guarantees that once data is documented on the blockchain, it cannot be changed without the unanimous agreement of all nodes in the network. This is because each node retains an entire copy of the ledger, making any unauthorized changes practically impossible. The decentralized qualities of blockchain further reinforce its security, as there is no central authority, government, or individual controlling the system. Instead, a network of nodes collectively manages all transactions, ensuring that the system remains robust and resistant to manipulation [4]. Fig. (**1**) depicts the characteristics of blockchain.

LITERATURE REVIEW

As blockchain technology grows in importance, addressing its scalability challenges becomes crucial. Key issues such as data storage, throughput, and monetary costs are central, with off-chain methods emerging as promising solutions to enhance performance. The impact of consensus methods and blockchain types on scalability is significant, while privacy and security remain critical factors that influence both scalability and system efficiency, highlighting the need for further research in these areas [5].

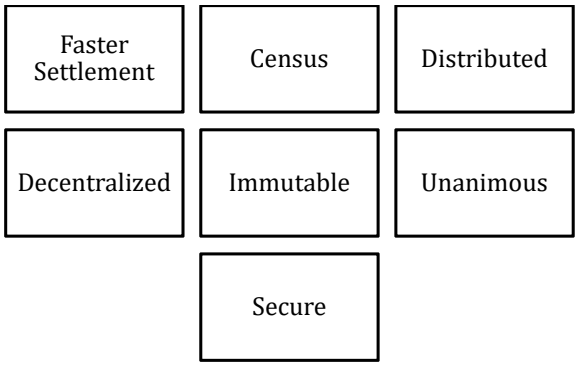

Fig. (1). Characteristics of blockchain.

Blockchain technology has the potential to transform peer-to-peer (P2P) energy trading but faces challenges related to scalability, security, and decentralization. While blockchain offers several advantages, issues such as complex smart contracts, infrastructure changes, and regulatory hurdles complicate adoption. Economic concerns, including cryptocurrency volatility, add further challenges. Collaboration among energy companies, regulators, and technology providers, along with the development of regulatory frameworks, is essential for secure and scalable blockchain-based energy trading. Recent advancements in blockchain technology have focused on optimizing performance metrics [6]. A notable approach has achieved a 40% deduction in transaction verification times and a 60% advancement in throughput through efficient Delegated Proof of Stake (DPoS) consensus, Interplanetary File System (IPFS), and sharding. The model also illustrated cost-effectiveness with a 30% deduction in gas prices and a 25% decline in ether consumption. Scalability has been improved by 70% as compared to traditional Proof of Work (PoW) systems. Future improvements focused on refining consensus mechanisms, advancing cryptography, and implementing dynamic sharding. Cross-chain interoperability could further enhance the interconnectedness of decentralized ecosystems [7].

The amalgamation of blockchain and AI in healthcare holds transformative potential for improving data efficiency and patient care. However, challenges persist in scalability (19%), interoperability (24%), and power consumption (28%). Sharding appears promising for scalability, despite its complexity and potential security risks, while forking could lead to network fragmentation. Future research focused on improving consensus mechanisms to enhance transaction performance and power efficiency, sustaining the broader adoption of blockchain technology in healthcare [8]. As blockchain networks expand, managing data size and storage becomes increasingly challenging. Techniques such as design

CHAPTER 5

A Study on Blockchain Ecosystem Security

Mukta[1,*], Shiksha Kumari[1], Sherry Verma[1] and **Mohit Mittal[1]**

[1] *School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India*

Abstract: Blockchain Technology is one of the leading technologies nowadays. Its unique characteristics such as decentralized, trackable, temper-resistant, reliable, and secure nature make the blockchain popular from the traditional database. Blockchain has a wide range of applications, not limited to the financial sector but also includes healthcare, education, supply chain management, smart cities, and the transportation sector, providing more features and resilience. Various academic and industry sectors have adopted this technology for the past few years due to its secure nature. However, due to its wide range of applicability in both sectors, security has become one of the major issues that need to be addressed. This article focused on the security in the blockchain ecosystem containing the various components integrating to form the blockchain network. The study includes security regarding blockchain protocol, smart contracts, nodes, wallets, decentralized applications, and collaboration between the different elements of the blockchain ecosystem.

Keywords: Block, BlockChain attacks, Blockchain, Consensus algorithm, Cryptocurrency, Cryptography, Hacking, Hyperledger, Intellectual property, Ledger, Weaponization.

INTRODUCTION

Satoshi Nakamoto coined the term Bitcoin having its underlying technology blockchain. Bitcoin is the first cryptocurrency used for funds transfer between the two parties without the involvement of any centralized authority. The blockchain ecosystem is growing faster with the rapidly growing technology. Blockchain is a distributed ledger that records all the transactions and provides transparency, trust, and security to all the transactions. Blockchain [1] is a more secure and resilient technology, making it popular in diverse applications, but it is not completely secure and cyber-attack proof.

Industries are adopting this technology for the future perspective to attract more customers and other business enterprises, but security is a major concern that

[*] **Corresponding author Mukta:** School of Engineering and Technology, Sushant University, Gurgaon, Haryana, India; E-mail: mukta.mittal2006@gmail.com

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

needs to be focused on. People participating in blockchain networks can be faulty leading to a serious impact on security which violates the law and regulations of the country. Blockchain technology has many applications, including the financial area, the Internet of Things (IoT), education, supply chain management, transportation, and the medical sector. It is more secure and resistant compared to traditional databases having features such as, **i**) there is no single point of failure, which makes this network more resilient; **ii**) the consensus algorithm ensures the security and integrity of the network on the same state of the network; **iii**) provides the immutability and integrity due to permanent storage of the data in the ledger. Having a lot of benefits of using blockchain technology, still it suffers from various security challenges [2] that need to be addressed: 51% of attacks are one type of attacks in which the attacker gains access to more than 50% of computational power; another one is the smart contract, which a self-executing code runs on the blockchain leading to security threats due to bugs or flaws in the code. Moreover, blockchain uses cryptographic techniques to secure data thus poor key management is also one of the security threats. This article highlights the security threats and challenges of the blockchain ecosystem.

COMPONENTS OF BLOCKCHAIN

With the advent of technology and the internet, several methods were proposed and used for storing data. However, each had limitations of security and accountability in case of fraud or data leakage. Blockchain ecosystem on the other hand is a combination of several interconnected entities that collaborate in providing the most secure and decentralized way of storing critical information. All the components work together to ensure the coherence of the data. It has transformed the mode of financial transactions in the most secure, unanimous way, especially in an untrustworthy medium. Additionally, transparency adds a trust factor amongst the users of this niche technology. One needs to understand the participants of this complex yet safe network to harness the power of this new-age approach. Fig. (**1**) depicts the composition of the blockchain network.

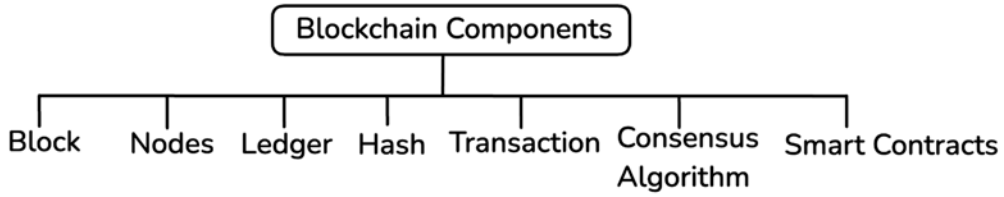

Fig. (1). Blockchain ecosystem [3].

Block

It is a kind of immutable data structure that stores records of several transactions. Every block has a unique ID called hash and it also stores the previous block's hash, thereby creating a chain of blocks we address as blockchain. Each block consists of a body and a block header. The body has records of transactions. The header is the very crucial part of the block. It has metadata comprising a Merkel root, a predecessor block hash, a timestamp, and nonce. This metadata ensures linear and cryptographic linkage of blocks in the chain. Merkle root [4] is a single hash value for all the transactions in the block. It is created by pairing and hashing all the transactions. This process ensures that tampering in any transaction will result in a different hash value and Merkle root for the block. Therefore, any tampering in the transaction can be easily detected. It makes the integrity and verification of all transactions simpler by not requiring every single transaction to be checked. The timestamp tells the time the block was created. Fig. (**2**) depicts the chain of blocks along with the structure of the individual block. The hash of the predecessor block is used to compute the current block's hash by hashing the metadata present in the header of the block. The first block has no parent block and is called a genesis block.

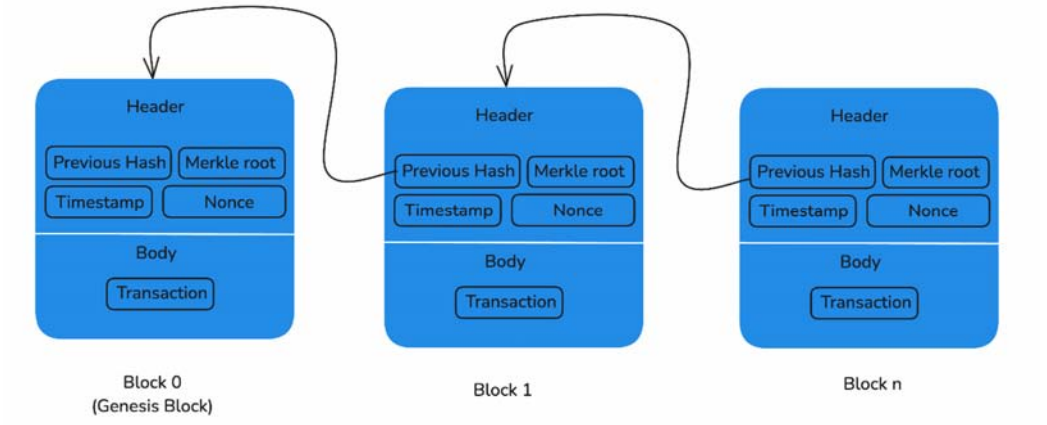

Fig. (2). Structure of block in blockchain [5].

Nodes

They are the most basic structure of the network. Nodes are the devices that run specialized blockchain software and record the transactions' history as digitized and secure ledgers. The fundamental responsibility of the node is to authenticate the legitimacy of each group of transactions called block. They are also accountable for assigning unique identification to each transaction, making them different. It further shares the transaction history or the ledger with other nodes to

CHAPTER 6

Blockchain-Enabled Algorithmic Trading: Quantitative Techniques and Regulatory Compliance in India

Sonika Malik[1,*], Siddharth Bisht[1], Mumukshu Tyagi[1] and **Yash Gupta[1]**

[1] *Department of IT, Maharaja Surajmal Institute of Technology, New Delhi, India*

Abstract: Indeed, this paper will discuss various strategies, and approaches of algorithmic trading with a view to making profits through data analysis. It introduces the way of operations in terms of mathematical models and logical approaches to gather and evaluate the information about investment potentialities. Hence, another contribution of this study is the analysis of these models and techniques in the context of the Indian market with regard to SEBI regulation. The paper also expands on the role of adopting blockchain technology within algorithmic trading to reduce opacity, increase security, and optimize its running. This study informs on how blockchain can transform trading strategies in India's regulatory environment when used through smart contracts, DEXs, tokenization of assets, write-once ledgers, and real-time clearing. The results highlight the radical evolution of applying algorithmic trading coupled with blockchain to the new generation of more complex financial platforms for India.

Keywords: Algorithmic trading, Backtesting, Blockchain technology, CAGR, Calmar Ratio, Delta variations, Data analysis, Data scrubbing, Derivative market, Risk-to-reward ratio.

INTRODUCTION

Traders and investors have traditionally relied on securities and stock market assets to achieve financial gains. The fundamental principle guiding these activities has often been to "Buy Low, Sell High," a strategy that underpins many conventional trading approaches. That said, as both the theory and practice of financial markets have become more intricate, this rather straightforward approach has been augmented, and in some cases, overshadowed by vehicles of greater complexity. This shift leads us to the topic of our study: To be precise, it involves Quantitative Trading as well as Algorithmic Analysis. Today's traders whether small or big investors are using sophisticated tools and techniques for the

[*] **Corresponding author Sonika Malik:** Department of IT, Maharaja Surajmal Institute of Technology, New Delhi, India; E-mail: sonika.malik@msit.in

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

investment so as to make perfect decisions for maximum profit. Quantitative trading is one of the drives that mark significant progress in this endeavor. It refers to the involvement of mathematical models and computational tools as well as applying them in order to perform a huge number of transactions of stocks and any other sorts of financial assets. Quantitative trading, on the other hand, can be defined as an advanced form of trading that differentiates between 'buy' and 'sell' based on some established algorithms rather than employing conventional instinct and subjective judgment of the market trends. This change has made quantitative trading even more achievable, making more institutional investors approach this method of trading in addition to the availability of new technologies and tools needed for quantitative trading, individual traders can now easily obtain them, which were originally widely used only in large financial businesses [1, 2]. The main feature of quantitative trading complemented the statement made above is that data is used quite extensively. Gain charts identify that accurate quantitative traders work with computer languages and even numerical methods to gather and assay previous records of the stock exchange. This information is then employed in the construction of theoretical and prognostic modes of operation with the goal of predicting market shifts. The reliability of these models to a large extent, is predicated on the veracity of the data that have been entered into the system in the past. Credible historical data help the trader understand trends in the market that can help him in his trading. Basically, backtesting is one of the most important aspects used in quantitative trading. Backtesting is the process of analyzing the current market to historical data in order to devise a trading strategy. Such a process affords a way for traders to assess their techniques free from risk environment as well as validate their credibility before using them under real trading conditions. Looking at how the strategy would have operated in the past creates a way through which the trader can evaluate the possibility of its success and make changes as deemed necessary. Backtesting is a process that lets out possible loopholes in the strategy and modifies facets to increase its strength and efficiency. It can therefore be concluded that the role of the regulation has been pivotal in defining the prospects of algorithmic trading in India. In India, the Securities and Exchange Board of India (SEBI) was quite active in regulating algorithmic trading with a perspective of keeping the market as clean as possible and would not allow algorithmic trading in case it presented a threat of disrupting the market [3].

First, SEBI enacted rules to standardize the market because developers are using third-party algorithms with custom APIs access. This shift intended to control the market and the lack of it, concerning such algorithms as uncontrolled and not having a head moderator who would create and introduce them. The year under review has also witnessed severe disruption due to the COVID-19 pandemic affecting various aspects of the economy and business regulation. Earlier, SEBI

had imposed certain stringent norms and after a decade of implementation, SEBI eased some of these norms to provide more flexibility and choice to traders regarding algorithmic trading tools. Significantly, the allowed rate of transactions per second changed from 20 to 120, which stoked new opportunities for the traders to work out and apply the self-coded algorithmic platforms. This relaxation was in light of the increased popularity of algo-trading in India as well as the changing dynamics of the market that required an amendment to the rules to suit the traders and investors. The possibility of translating blockchain into the growing field of algorithmic trading brings more prospects for increasing its transparency and security, as well as optimization of its work. Quantitative trading can benefit from blockchain technology as follows. Some of the advantages of the concept of blockchain include: the ability to provide accuracy and security on data that is analyzed quantitatively from historical records. This feature is very essential for the preservation of trading models and the appropriate decision-making to be based on valid data. One interesting feature of the actualization of trading strategies that can be derived from smart contracts, which are widely used in the sphere of blockchain technology, is the possibility of automatization of trades provided that certain conditions are met. Such automation reduces the number of third-party participants in trading and lowers the interval between the actions thus improving the effectiveness of trading transactions. Smart contracts can be used to develop trading algorithms that allow certain trades to be carried out in a precise way without any human interference. This capability is especially useful in trading that occurs frequently in a manner with high velocity.

Other innovations made possible by blockchain technology are decentralized exchanges also known as DEXs. DEXs enable decentralized trading where individuals are able to deal directly with others without the assistance of a central clearinghouse. This approach strengthens security because there is a lower tendency for exchange hacks and brings out the aspect of minimization of the chances of manipulation. There is also increased efficiency in trading transactions as they occur on public ledgers that can be checked to be accurate [4].

Thus, blockchain as an enabler of asset tokenization may be considered a breakthrough in the financial market. Tokenization is a process whereby traditional assets are created in a digital form only to be traded in blockchain markets. It makes it possible to invest in portions of expensive and illiquid commodities, besides making it possible to buy and sell stakes in such properties. In addition, tokenization gives the following benefits: Trading can be conducted at any time, making trading highly liquid; there is also an option for more algorithms to trade. Through the processes of constant trading and ownership in small shares, the tokenization of assets contributes to the overall accessibility and liquidity of the market to open more opportunities for investment and trading.

CHAPTER 7

The Carbon Footprint of Blockchain: Environmental Impact

V. Gayathri[1,*] and **Tanusri Gururaj**[2]

[1] *Department of ECE, Bharati Vidyapeeth's College of Engineering, New Delhi, India*

[2] *Ernst & Young Associates LLP, Gurgaon, Haryana, India*

Abstract: Blockchain technology is a distributed digital ledger, which is a sequence of interconnected blocks comprising secure and transparent peer-to-peer transaction records. It is a combination of blocks with shared memory, each of which is uniquely identified by a hash value. The distinctive nature of these blocks makes them resistant to falsification and builds trust and resilience in technology. This chapter provides an overview of blockchain technology, its architecture, and diverse applications. It explores the carbon footprint of blockchain technology and examines its environmental impacts through case studies on Bitcoin mining, Ethereum, Chia network, food supply chain, Tezos blockchain, and geothermal energy. It also endeavors to analyze energy consumption and Carbon dioxide (CO_2) emissions and eventually understand high-power usage, which has led to environmental impacts. The carbon footprint, which is the total greenhouse gas (GHG) emitted (including CO_2 and methane), is released at high levels and significantly affects habitats because of its ability to trap atmospheric heat. With the emissions of GHGs at high levels, this chapter also focuses on the mitigation process, namely, renewable energy. The chapter in the conclusion underscores the importance of continued efforts to make blockchains more environmentally sustainable.

Keywords: Bitcoin mining, Carbon footprint, Chia network, Consensus mechanism, Defi, Energy consumption, Environmental impact, Ethereum, Food supply chain, Geothermal energy, GHG, KlimaDAO, Non-renewable sources, Nordic energy market, Tezos blockchain.

INTRODUCTION OF BLOCKCHAIN TECHNOLOGY

Information has always been a vital component of our lives, and today, the most significant portion is digitally maintained. Indeed, this is so as the switch to 'digital storage' offers dire consequences, where any mishap can be the public revelation of millions of personal aspects open to abuse. Privacy and security

* **Corresponding author V.Gayathri:** Department of ECE, Bharati Vidyapeeth's College of Engineering, New Delhi, India; E-mail: ythi.kkl007@gmail.com

issues in recent years have led to the search for better solutions. They established that blockchain technology provides a good solution for these challenges. Unlike most conventional systems that operate in a hierarchy with a major control center, blockchain works as an open ledger digital system that updates correspondingly with all nodes in the network, while maintaining similar data. The data stored in a block can hardly be changed, and any change requires the consensus of the majority [1]. Every block holds information and comes with the digital signature of the preceding block, thereby connecting it. This chain structure also means that if the information in one of these blocks were to be altered in any way, the whole chain would be affected, making the blockchain very secure against such an alteration. Thus, the use of blockchain reduces instances of forgery attempts to minimize bias and enhance data safety.

Key Characteristics of Blockchain Technology

1. ***Decentralized Peer-to-peer Network:*** Unlike traditional systems, in which there is a client and server, a blockchain consists of nodes or peers that communicate directly with each other without the requirement of a central authority [2, 3].
2. ***Security and Transparency:*** Every transaction is recorded in a public ledger or database that is accessible to all nodes. The system is secure because each block stores the hash value of the previous block [2, 3].
3. ***Smart Contracts:*** These are digital agreements stored in a blockchain network and executed when specific conditions are satisfied. For example, a 10th- or 12th-grade mark sheet/certificate can be stored in a blockchain and issued once a person's identity and other details have been verified [2, 3].
4. ***Proof of Work (PoW):*** A new node cannot be added to the blockchain without approving the transaction. Therefore, participants (miners) in the network contended to solve a type of computational challenge. The first person to solve it gets to add the new block and earns cryptocurrency as a reward [2, 3].

Taxonomy of Blockchain Technology

1. ***Public Blockchain***: This is a permissionless open network. This implies that anyone can join or become a member. To add a block to the network, a consensus mechanism must be followed, such as a PoW [2, 3], shown in Fig. (**1a**).
2. ***Private Blockchain***: This is also known as a closed network because members can only be part of it through an invitation. They are typically faster and more secure than public networks [2, 3], as shown in Fig. (**1b**).
3. ***Hybrid Blockchain***: This offers transparency and privacy by combining the features of both private and public blockchain networks [2, 3], as shown in Fig. (**1c**).

4. ***Consortium Blockchain***: This is a type of network that, instead of being managed by one organization, is managed by multiple organizations. This means that various organizations can collaborate in a shared ledger [2, 3], as shown in Fig. (**1d**).

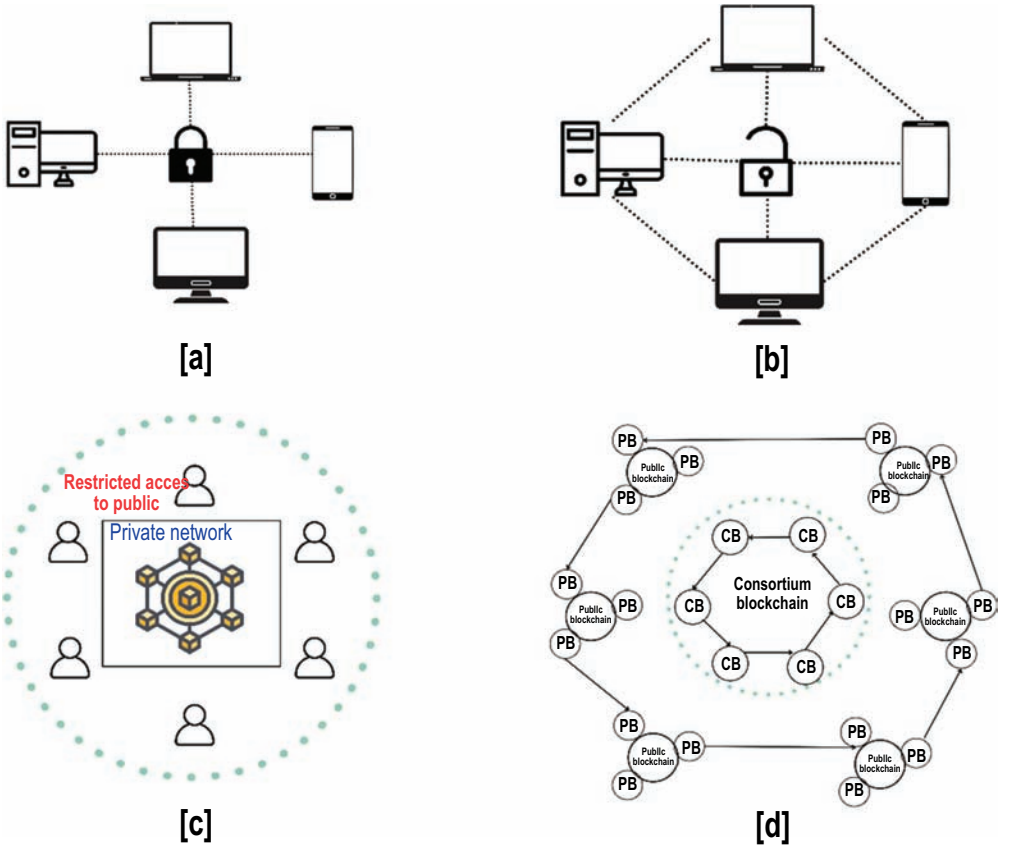

Fig. (1). Taxonomy of blockchain technology; (**a**) Private blockchain; (**b**) Public blockchain; (**c**) Hybrid blockchain; (**d**) Consortium blockchain.

ARCHITECTURE

A blockchain is an order of blocks. This involves maintaining a database of all transactions, similar to a conventional account book. It is a transactional inventory that is immutable, decentralized, secured, consensus, and unanimous. Therefore, a blockchain is a combination of blocks and shared memory. These blocks are the basic structural units of the blockchain systems. A detailed overview of this architecture is provided below [4].

CHAPTER 8

Dissecting Blockchain Technology: An In-Depth Analysis

Nikhil Kumar[1], Richa[1], Sweeti Sah[1,*], Shweta Sharma[1,*] and **R. Sujithra Kanmani[2]**

[1] *Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India*

[2] *School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India*

Abstract: Blockchain is known for being a decentralized ledger with distributed storage. It has changed whole industries across borders by increasing security, transparency, and reliance on intermediaries. Thus, from its initial design for cryptocurrencies like Bitcoin, Blockchain extends its transformative potential for a wide range of fields such as finance, supply chain management, and healthcare. The contribution of this research is an in-depth analysis of blocks, transactions, and consensus mechanisms constituting the anatomy of a blockchain. We have paid particular attention to block-structure research in our work, emphasizing that a block is an indivisible information unit, each containing transactional data and cryptographic hashes that link it to the previous block. One of the most valuable parts of our research consists of an innovative analysis of a consensus mechanism. We explain how different algorithms ensure the validity and sequence of transactions among the network nodes, and review the strengths and weaknesses of algorithms, namely, Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). The key highlights in this work are the case studies of well-established blockchain platforms, including Bitcoin and Ethereum. These manifest our insight into their operational efficiencies and mechanisms for security. Further, we demonstrate empirical results on the processing times for transactions and scalabilities of blockchains under different network conditions. Additionally, the challenges of scalability and energy consumption are put forth, for which novel approaches may be proposed for future blockchain development. The study contributes to the further development of blockchain technology by informing future research directions toward solving the existing limitations and exploring new applications within emergent sectors.

Keywords: Bitcoin, Blockchain, Consensus mechanisms, Decentralization, DeFi, Distributed ledger, Energy consumption, Ethereum, Mining, NFTs, Proof of stake, Proof of work, Smart contracts.

[*] **Corresponding authors Sweeti Sah and Shweta Sharma:** Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India; E-mails: sweetisah3@nitkkr.ac.in; shweta.sharma@nitkkr.ac.in

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

INTRODUCTION

First mentioned in 2008 by Satoshi Nakamoto as the underlying technology of Bitcoin [1], blockchain evolved to be more than its core function of leading active innovations for various businesses. Among the strong points brought about by the application of a decentralized and distributed ledger system in blockchain are safety, transparency, efficiency, and partly, reduction of reliance on intermediaries [2, 3]. Due to the presence of these features, blockchain-based industries use it confidently since it is designed for more security and efficiency; thus, it was able to extend its functionality to finance, supply chain management, healthcare, and beyond [4]. The recently attained advances in blockchain technology turned out to be one of the ways to cope with new problems and opportunities in the digital economy. The wider use of DeFi platforms completely changed the current face of financial services by allowing users to do their banking and make more by cutting out the middleman altogether [5]. Another point is that the development of the Non-Fungible Token (NFT) market transforms the creative space and allows artists, musicians, and other individuals to create content for alternative ways of monetizing digital projects, and processes of proving their ownership [6]. The fact that these achievements open a very interesting route for illustrating how capable blockchain can be in reforming the economy and changing individual styles of living and business models. Efficiency and effectiveness in blockchain comprise the blocks, transactions, and consensus mechanisms. These will include immutable blocks containing transaction data and store cryptographic hashes securely linking such blocks to prior ones, hence ensuring data integrity [7]. Transactions represent the life of blockchain, carrying out the role of ensuring that assets or information get transferred from one point of the system to another. The consensus strategy employs different kinds of algorithms that ensure the accuracy and timeliness of transactions, hence arriving at a consensus between different parts [8]. We will go deeper into the internals of various consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), whereby their advantages and disadvantages will be brought out in relation to catering to business queries and network volumes.

LITERATURE REVIEW

Blockchain technology has drawn interest in recent times from both academia and industry circles as a game-changer across many industries. A lot of research has been done on its fundamentals, applications, and issues with blockchain. This review narrates the development with respect to consensus mechanisms concerning the most important aspects of blockchain technology: reliability, security, and usability. The first application of blockchain technology in Bitcoin used PoW [1]. Although PoW has been tested for safety and reliability in case of

network attacks; it is, however, very power-consuming and is limited by capacity. Regardless, it has driven further research into other methods [9].

PoS, electing its validators based on the stake candidates have in the network, has recently been considered a quite promising alternative [10]. This is due to its energy efficiency and potential for improved scalability. In this respect, one of the most significant developments is the ongoing transition of Ethereum into PoS through the Casper protocol [11]. Other consensus mechanisms, such as DPoS, Practical Byzantine Fault Tolerance, and Proof of Authority, have also been proposed and implemented in various blockchain platforms, modulo their trade-offs between security, scalability, and decentralization [12]. Specifically, scalability—the ability to handle an increasing number of transactions without compromising on performance—has been traditionally one of the major challenges for blockchain technology. This has driven many researchers into more scalable and energy-friendly alternatives to PoW [13]. Such transitioning of the PoW to the PoS consensus algorithm will hugely improve Ethereum's scalability while reducing its energy consumption [14]. Layer 2 solutions have shown enormous potential for achieving high performance in blockchain without compromising security or decentralization and at a much cheaper cost of transactions [15].

Security is very critical for blockchain applications, especially in financial and sensitive data management. Although immutability and the crypto-based backbone of blockchain are a prima facie case for security, there are still some vulnerabilities that pertain mostly to smart contracts. This has led to research being directed toward developing strong smart contract auditing tools, which can allow attack simulation that facilitates the identification and mitigation of potential risks [16]. In addition, privacy issues concerning the transparency of public blockchains have also driven the need for research into techniques that offer further layers of privacy, such as zero-knowledge proofs and confidential transactions [17]. Interoperability between the different blockchain networks is one of the top priorities within the growing blockchain ecosystem. Full empowerment of this technology's power requires the seamless exchange of data and assets across chains. These studies led to the realization of cross-chain protocols and bridges like Polkadot and Cosmos that have enabled the communication and collaboration of disparate blockchain networks today [18].

METHODOLOGY

This section details the experimental design, sources of data, and analysis methods used in studying the basics of components and consensus mechanisms in blockchain technology. We present our methodology in the current pool of

CHAPTER 9

Decentralized Identification Systems Using Blockchain and Sovereign Identity

Rohan Raj[1] and **Sachin Gupta**[2,*]

[1] *Department of Information Technology and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India*

[2] *Department of Compter Science Engineering (CSE), Maharaja Agrasen Institute of Technology, Delhi, India*

Abstract: This chapter focuses on the intersection of self-sovereign identity and blockchain technology. This review encompasses a number of issues: the role of SSI in augmented identity management, the advantages and challenges of blockchain integration, and real-world applications. It looks at how these technologies can make identification processes more efficient, secure, and reliable. The current review elaborates on the impact of SSI and blockchain on identity management with the use of selected papers from previous years. It is here that the main benefits, as well as practical challenges, are identified with the implementation of the technologies. The provided study concludes that SSI and blockchain technology have enormous potential to make identity management an order of magnitude more acceptable for various application domains. This will help shed more light on further research with an understanding of the benefits and challenges of these technologies.

Keywords: Authentication, Blockchain, Cryptography, Data integrity, Decentralized identity, Decentralized systems, Digital identity, Distributed ledger, Identity management, Interoperability, Privacy, Protocols, Scalability, Security, Self-sovereign identity, Smart contracts, Trust, User control, Verification systems, Zero-knowledge proofs.

INTRODUCTION

Background and Motivation

Conventional systems that are centralized in identity have only one point of control and vulnerability, for which they are enormously capacity-limited to cope with security, privacy, and user autonomy concerns. For example, central systems

* **Corresponding author Sachin Gupta:** Department of Computer Science Engineering (CSE), Maharaja Agrasen Institute of Technology, Delhi, India; E-mail: sachin.gupta@mait.ac.in

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

carry single points of failure that attract data breaches and cyberattacks. Identity management systems, especially centralized ones, are ripe for such high-profile incidents, as attested to by the Equifax breach in 2017, where the personal data of millions of individuals was exposed. A graver issue would be that centralized identity systems leave the control in the hands of very few entities; hence, some concerns over user autonomy and data sovereignty arise. Their data usually lies with third parties, who have control over and commercialize personal data without explicit consent. This growing number of digital interactions is the reason why the demand for more secure identity solutions, which are user-centric and privacy-preserving, is on the rise. Much attention goes to decentralized identification systems through the application of blockchain technology principles and self-sovereign identity. Blockchain itself emerges as an inflexible, decentralized structure that provides security, transparency, and tamper-proof identity management. Self-sovereign identity empowers individuals to own, control, and selectively share their personally owned data. They hold the promise of better security, user control, and privacy and are a very appealing model compared to the conventional ones [1]. The shift towards decentralization in identity management is more or less a technological innovation with a fundamental shift in how digital identities should be managed and protected.

Problem Statement

In addition to this great opportunity, there is now an extensive range of problems associated with the implementation of decentralized systems for identification, including purely technical issues and questions of regulation and conscience. On this basis, perhaps the most significant issue is the capacity of blockchain networks, which must be able to process massive numbers of transactions. It also leaves the point of how these decentralized identity solutions are to interoperate with existing system architecture. Besides, there is one more important aspect; decentralized beings have to negotiate with the rules put in the regulated environment. For example, the General Data Protection Regulation (GDPR) is the regulation of the European Union. Some of them regulate data processing, storage, and user consent, which is quite challenging to reconcile with the principles of blockchain. Protecting users from identity theft, along with ethical considerations and ensuring user obscurity, is crucial for maintaining trust and security in online systems. The integrated ‘openness’ in the blockchain system can be an issue when it comes to privacy; besides, new approaches will be required to address this issue. The ethical issues of digital identity, like the problem of accessibility and inclusiveness of these technological solutions, must be addressed so that these decentralized systems are equally beneficial to all users.

Purpose and Scope

In this chapter, an overview of the decentralized identification system applying blockchain technology and SSI is given, including core principles, technical frameworks, regulatory issues, and practical applications. It is based on a number of research works, which gives a rich source of information on the current state of advances and challenges in the field. Furthermore, it identifies the research trends in the subject under discussion and indicates the gaps to be further explored.

Structure of the Chapter

The chapter will introduce the technology under review in this chapter on blockchain technology and decentralized identity. It starts with an introduction and background, then goes on to state the problem, the purpose, and the scope of the study. Consequently, an overview of blockchain technology, including its key concepts, terminology, benefits, and challenges, is presented. It compares traditional and decentralized identity systems, showing the benefits of decentralized identity, self-sovereign identity (SSI) principles and frameworks, decentralized public key infrastructure, verifiable credentials, and digital identities. The interplay between blockchain and identity is discussed, followed by a discussion of technical architecture and components, security and privacy considerations, regulatory and ethical considerations, legal and regulatory challenges, data protection and privacy laws, and finally, ethical implications and concerns. The chapter then discusses case studies and applications, including real-world implementations and examples, successful case studies, lessons learned, and best practices. Finally, the section on discussion and future directions explores current trends and innovations, open research questions, and potential future developments and concludes with a summary of key findings, implications for research and practice, and future directions.

OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Introduction to Blockchain

Blockchain, the greatest creation of Satoshi Nakamoto in 2008 by inventing Bitcoin, is a distributed and decentralized ledger mechanism intended for the safe and immutable recording of transactions taking place over various computers. Each block of this chain features a cryptographic hash of the previous block, along with the transaction data, thereby representing a continuous chain of linked blocks. This structure gives security to the network and makes it tamper-proof so that once a block is added, it cannot be changed retroactively without altering all these subsequent blocks—a process that needs the agreement of a majority of the network. With this inherent immutability and transparency, the blockchain

CHAPTER 10

Exploring the Spectrum of Blockchain: Private, Public, Consortium, and Hybrid and their Applications

Aparna Singh[1,*], **Jaya Sinha**[2,†], **Tanu Shree**[3,†] and **Surbhi Sharma**[1,†]

[1] *School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India*

[2] *Department of Computer Science and Engineering, ITS Engineering College, Greater Noida, India*

[3] *Department of Computer Science and Engineering, Galgotias College of Engineering and Technology, Greater Noida, India*

Abstract: Blockchain technology, well known for its security and decentralization, has become evident as a revolutionary force among multiple global industries. Initially developed as a foundation for cryptocurrencies like Bitcoin, it is now being used for user authentication, data sharing, record management, access control, and many more. Fundamentally, blockchain is an integration of peer-to-peer networking and cryptography, where each transaction is recorded in the form of blocks. Each block links to the block before the current block through its hash value, thereby forming a chain of blocks. This article delves into the underlying principles of blockchain and its architecture. It also explores the consensus protocols and their application in five key areas: the Internet of Things, finance, healthcare, supply chain management, and the Industrial Internet of Things (IIoT). The four primary forms of blockchain— public, private, consortium, and hybrid —are among the article's main topics of attention.

Keywords: Bitcoin, Blockchain, Consensus protocols, Cryptocurrency, Decentralization, Ethereum, Finance, Hash, Healthcare, Hyperledger, Industrial internet of things, Internet of things, Mining, Peer-to-peer network, Private blockchain, Proof of stake, Proof of work, Public blockchain, Smart contracts, Supply chain management.

[*] **Corresponding author Aparna Singh:** School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India; E-mail: aparnasingh2211@gmail.com

[†] *These authors have equal contribution.*

INTRODUCTION

Blockchain has become evident as a revolutionary technology in this era of digital applications, significantly transforming how data is generated, transferred, and managed among various industries. Blockchain was initially developed as the underlying technology behind the famous cryptocurrency-Bitcoin, by Satoshi Nakamoto in 2008 [1]. Since then, it has expanded into a significant aid behind applications like healthcare, banking, security, and many other fields. The focal area of blockchain is its distributed ledger system, which, being decentralized, provides enhanced transparency, security, and immutability compared to traditional centralized databases. A recent survey called the Blockchain Hype Cycle survey, done by Gartner, assessed the maturity and ease of acceptance of blockchain technology across a diverse set of industries. It found that while blockchain as a technology had moved past the initial hype, its adoption was still growing steadily, with 60% of enterprises either using or planning to use blockchain in the upcoming two years. The survey also emphasized the shift towards more practical and scalable use cases.

A blockchain is a chain of interconnected blocks, with each block holding a list of transactions. Each block is interconnected to the previous one *via* a cryptographic hash of the previous block, producing a chain that is virtually tamper-proof and immutable. Consensus techniques such as Proof of Work (PoW), Proof of Stake (PoS), or Proof of Burn (PoB) make it even more secure and reliable. “The use of consensus mechanism also ensures that the state of the blockchain is always stable and all the nodes have access to the same chain of blocks” [2]. Additionally, its decentralized nature also portrays that no sole party possesses full authorization, thereby lowering the danger of data breaches or any other interference by an intruder. Each transaction happening in the network is validated by special nodes known as miners.

The increased interest in this ever-growing technology is due to its capability to handle several fundamental difficulties in modern digital systems, such as data security, privacy, and trust. For example, in the banking sector, blockchain aids in the secure and transparent movement of assets without the involvement of middlemen, lowering both costs and risks. Growing financial services without the need for traditional middlemen are provided by Decentralized Finance (DeFi), while Non-Fungible Tokens (NFTs) are moving beyond digital art to include virtual real estate and games. Global research is being done on Central Bank Digital Currencies (CBDCs), which would increase financial efficiency and inclusivity. Interoperability between various blockchains is becoming increasingly important as cross-chain solutions become more prevalent. In healthcare, blockchain can protect the integrity and privacy of sensitive records of patients,

allowing for better data storage and management with seamless system interoperability. In addition, blockchain is essential to Web3 and the metaverse, allowing digital ownership and decentralized apps (dApps). To safeguard privacy and control fraudulent activities, security improvements—including cutting-edge crypto-graphic techniques, are also being integrated with blockchain technology. This article examines the core principles of blockchain technology, including its architecture, types of blockchain, the different categories of consensus mechanisms available in it. We also explored its application areas in multiple domains, along with possible future scope and limitations. Section 2 of this chapter explores some of the significant research works done in this field. Section 3 and Section 4 discuss the architecture and its different types. Section 5 throws light on various characteristics of blockchain that make it a revolutionary force in today's world and a prominent part of most of the current and future industries. Section 6 discusses the various applications of blockchain across multiple domains, with the conclusion briefly summarizing the article and also discussing the future scope of blockchain technology.

LITERATURE REVIEW

This section is used to discuss some of the existing work on this rapidly growing technology, addressing architecture, core components, applications, and associated challenges. The first paragraph covers literature related to surveys conducted on blockchain technology. The second paragraph explores the literature discussing various consensus protocols and the work done, while the third paragraph examines the literature concentrating on blockchain applications in various domains.

Gad *et al.* [3], in their paper, discussed blockchain technology, analyzing existing literature spanning from 2013 to 2020. The paper explored the evolution of blockchain, its current design and state, and its impact on various existing applications. On the same grounds, Dabbagh *et al.* [4], in their paper, conducted an analysis of blockchain technology and provided insight into the existing work on blockchain and its role in enhancing some of the latest technologies. Banerjee *et al.* [5] also presented a survey discussing the integration of blockchain in IoT and explored the available IoT datasets for the same. They highlighted the need for a standard to securely share these datasets and the potential role of blockchain in ensuring dataset integrity and also in making IoT systems more secure. Gorkhali *et al.* [6] provided another comprehensive review of 76 blockchain-related journal publications. It categorized the research into 14 distinct areas, summarizing each category's content and proposing future research directions.

CHAPTER 11

MegaETH: A New Era of Real-Time Blockchain Technology

Kajal Dubey[1,*] and **Dhiraj Pandey**[1]

[1] *Department Of Information and Technology, JSS Academy of Technical Education, Noida, India*

Abstract: MegaETH leads the way in blockchain technology. It created the Real-Time Proof of Stake (RTPoS) consensus method. This new approach tackles regular blockchain networks' main speed and scaling issues in regular blockchain networks. It allows fast transaction processing without giving up security or decentralization. Meg+aETH focuses on high output and can handle thousands of transactions per second (TPS). This opens doors for many decentralized apps (dApps) across different fields. A big plus of the Ethereum platform is how MegaETH fits into the Ethereum ecosystem. It uses smart contract features and works well with the Ethereum Virtual Machine (EVM). This compatibility helps the ecosystem grow and brings new ideas by making it easier for more developers to join in. MegaETH also cares about the environment. Its design uses less energy, meaning it has less impact on nature than proof-of-work systems. MegaETH brings together efficiency, security, and the ability to grow. This sets a new bar for real-time blockchain apps. As a result, it speeds up how the economy takes on decentralized solutions. It also lets developers and companies explore new ways to use this technique.

Keywords: Blockchain revolution, Consensus algorithms, Decentralized applications (dApps), Distributed ledger technology (DLT), Ecosystem growth, Energy-efficient, Ethereum virtual machine (EVM), Finance industry disruption, High throughput, Innovation, Interoperability, MegaETH, Proof of stake (PoS), Rapid transaction processing, Real-time applications, Real-time proof of stake (RTPoS), Scalability, Security, Smart contracts, Supply chain management.

INTRODUCTION

The blockchain space has advanced significantly since its inception, consistently pushing the boundaries of decentralized technologies and digital transactions. Every breakthrough in smart contracts and decentralized finance, from the early days of Bitcoin, has brought us one step closer to achieving the full promise of blockchain technology. Real-time processing is a significant obstacle that has not

* **Corresponding author Kajal Dubey:** Department Of Information and Technology, JSS Academy of Technical Education, Noida, India; E-mail: kajal.dubey@jssaten.ac.in

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

been fully overcome. We are presenting MegaETH, a ground-breaking invention that has the potential to completely transform blockchain technology. By addressing the crucial need for real-time transaction processing and instant updates, MegaETH is poised to completely transform the industry. MegaETH is built to deliver performance that is both quick and effective, bringing in a new era of real-time capabilities in the cryptocurrency industry. Traditional blockchains, on the other hand, frequently suffer from latency and scalability problems [1, 2].

For the first time in the cryptocurrency industry, Web2-level real-time performance is available thanks to MegaETH, an EVM-compatible blockchain. Our objective is to close the gap between blockchain technology and conventional cloud computing servers by pushing Ethereum L2s' performance to the edge of hardware.

High transaction throughput, a large amount of computing capacity, and—most notably—millisecond-level reaction times even under high demand are just a few of MegaETH's unique qualities. Developers are able to create and construct the most complex apps without limits when using MegaETH.

In this chapter, we will examine how MegaETH is expected to change the real-time blockchain technology ecosystem. We will investigate its novel aspects, evaluate its possible influence on different industries, and comprehend how it is establishing new standards for efficiency in the blockchain field [2]. MegaETH might change industry norms and expand the potential of blockchain technology, marking not simply a technological advance but also a fundamental change in how humans engage with digital systems.

WHY ANOTHER BLOCKCHAIN? AN OVERVIEW OF MEGAETH'S ROLE AND FUNCTION

Why is There a Need for New Blockchains?

The creation of new chains, including L1s and L2, is now easier, thanks to the development of blockchain frameworks. As such, a plethora of new chains have surfaced in recent times. As a result, there is currently a boom in the number of blockchain networks, with over 50 L2 projects up and running. Even with this growth of chains, the basic scalability problems remain unresolved by just adding more [2]. The ability of each chain to host decentralized apps (dApps) is still severely limited. As evidenced by the current metrics for gas per second and block timings, significant EVM chains, for instance, have limits regarding transaction throughput and block delays [3].

Limitations of Current Blockchain Frameworks

Recent gas parameter comparisons show that current EVM chains have major hurdles. Their low transaction throughput is one of the main issues. Even with its remarkable gas rate of 100 MGas/s, opBNB, for instance, is still unable to match the capabilities of contemporary Web2 servers [4]. To put this into perspective, modern database systems can process over one million transactions per second, as demonstrated by the TPC-C benchmark. In comparison, 100 MGas/s is equivalent to about 650 Uniswap swaps or 3,700 ERC-20 transfers per second. There is a noticeable performance disparity here [4]. For example, the table below shows the target gas per second and block time of major EVM chains today (Table **1**).

Table 1. Comparison of gas parameters across EVM chains in 2024.

Select EVM Chains	Gas Per Second	Target Gas Per Block(Supply)	Block Time
opBNB	**100.0 mg/s**	**100M**	**0.1s**
BSC	**46.5 mg/s**	**140M**	**3.0s**
Polygon	**7.5 mg/s**	**15M**	**2.0s**
Avalanche C-Chain	**7.5 mg/s**	**15M**	**2.0s**
Arbitrum one	**7.0 mg/s**	**1.75M**	**0.25s**
Base	**5.0 mg/s**	**15M**	**2.0s**
Optimism Mainnet	**2.5 mg/s**	**5M**	**2.0s**
Conduit	**2.5 mg/s**	**5M**	**2.0s**
Ethereum L1	**1.25 mg/s**	**15M**	**12.0s**

This table (Table **1**) distinctly shows that in many aspects, there are still severe limitations in EVM chains. The lack of computing power for sophisticated applications is another issue. For example, n = 10^8 costs about 5.5 billion gas to calculate the n-th Fibonacci number using a standard EVM contract. This calculation in C takes only 30 milliseconds; however, on the opBNB chain, it would take 55 seconds at a rate of 100 MGas/s [5]. This demonstrates the necessity for blockchains to have more processing power, a need that multicore processing can help with by improving performance [5].

Furthermore, the majority of current chains have lengthy block durations, which renders them inappropriate for applications that need instantaneous updates or input. All chains update their statuses at least once every second, except for Arbitrum One [6]. High-frequency trading systems and autonomous worlds that require instantaneous battle simulations, among other entirely on-chain dApps that require real-time interactions, find this delay problematic. Order execution

CHAPTER 12

MegaETH Solutions for Secure Healthcare Transactions

Kajal Dubey[1] and **Dhiraj Pandey**[1,*]

[1] *Department Of Information and Technology, JSS Academy of Technical Education, Noida, India*

Abstract: The MegaETH blockchain introduces new twists into improving healthcare transactions in efficiency and safety. MegaETH follows the hybrid consensus approach of PoS with BFT for solving some of the big issues in healthcare data management. Its strong encryption and zero-knowledge proof further enable significantly better protection of sensitive patient data, while reducing the risk of data breaches. It manages healthcare transactions fast and reliably, with a remarkable transaction throughput of about 10,000 transactions per second and a block duration of about one minute. Another important virtue of MegaETH architecture is that it uses less energy compared to more conventional Proof of Work systems. The demands of healthcare data are effectively managed with the scalability of the platform, underpinned by layer-2 solutions and sharding. MegaETH also illustrates excellent interoperability, as it will integrate with the existing systems of an institution and strictly abide by the rule of law. Moreover, smart contract executions are rather cheap, which enhances fraud prevention and accelerates administrative processes. The impacts from the adoption of MegaETH will be huge on reducing costs, ensuring data integrity, and finally improving patient care. Among the different options for solving current and future issues in health transaction administration, MegaETH is one of a kind.

Keywords: Blockchain, Byzantine fault tolerance data encryption, Layer-2 solutions, MegaETH, Transaction speed.

INTRODUCTION

The digital transition of the healthcare industry raises many challenging issues in various forms, such as sensitive patient data integrity and security, electronic health records, and networked systems [1]. Data breaches resulting from ineffective data exchange and related regulatory compliance also pose setbacks for this industry [2]. Clearly, these complications demand urgent, innovative solutions to protect patient privacy and improve operations for the healthcare business while raising systemic efficiency.

* **Corresponding author Dhiraj Pandey:** Department Of Information and Technology, JSS Academy of Technical Education, Noida, India; E-mail: kajal.dubey@jssaten.ac.in

Monica Bhutani, Monica Gupta, Kirti Gupta, Deepali Kamthania & Danish Ather (Eds.)

This work discusses potential applications of blockchain in the health sector and gives an overview of the key contributions of Mega ETH [3]. This paper looks at how Mega ETH uses blockchain in the research for improvements in the security and transparency of healthcare transactions to establish how it might apply to solve data management challenges currently present. In this respect, the importance of the investigation to fully understand how decentralized technologies may improve the quality and dependability of healthcare services is well underlined through robust responses to operational inefficiencies and data security concerns dogging the sector [4].

This chapter is designed to comprehensively discuss the healthcare transaction security solutions offered by Mega ETH. First, the paper looks at the issues affecting the health sector and, after that, the benefits of blockchain technology concerning the solving of these problems. Later on, it enumerates specific aspects relating to Mega ETH application, advantages, and implications for healthcare data management. The discussion concludes by measuring the future development and consequences that might be imminent from blockchain technology, to further enlighten how it will keep changing the healthcare industry [5].

BLOCKCHAIN TECHNOLOGY AND ITS RELEVANCE TO HEALTHCARE

Blockchain technology is one of the most promising innovations of the future in network security and data management. In simple terms, a blockchain is a kind of distributed ledger that keeps track of transactions across a fleet of computers in such a manner that it is impossible to alter the transactions [6]. Unlike traditional centralized databases, where the data can be controlled by only one party, this decentralized approach gives so much more flexibility. A “chain” of blocks is formed whenever each transaction or “block” is linked with a previous block. This linkage, with the consensus process, goes a long way toward ensuring that everyone on the network agrees on the present state of the ledger, hence enhancing data security and integrity [7]. Among the key ingredients of this are digital signatures for ensuring the validation of transactions and cryptographic hashing for generating a unique identifier for every block.

Blockchain Architecture: Decentralization, Consensus, and Immutability

Architecture has been built in such a way with blockchain technology that it allows very high degrees of security and transparency (Fig. **1**).

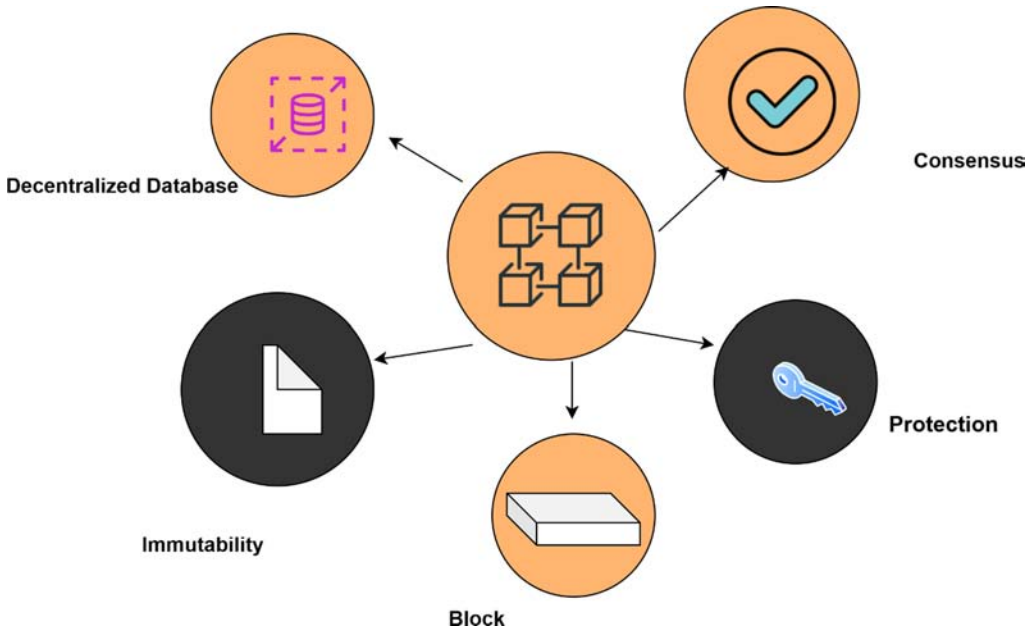

Fig. (1). Blockchain technology architecture.

Decentralization: Decentralization is an intrinsic part of blockchain technology that distributes the core of information from the hands of a single main authority to a network of nodes. Each node has a copy of the blockchain; hence, there would be fewer chances for centralized control and failure due to a single-point mode.

Consensus Mechanisms: The set of consensus mechanisms comes in to verify a new transaction and to validate the agreement of all on the current state of the ledger. Proof of Stake and Proof of Work are common techniques to reach a consensus that prevents fraud and confirms the transaction's validity.

Immutability: Immutability is a characteristic that demonstrates that the majority of the network consensus is needed to change or delete this blockchain. Once data becomes recorded in a block added to the chain, it cannot be changed or removed without concurrently altering all the subsequent blocks. This feature provides guarantees regarding data permanence and integrity.

Fig. (**1**) shows an overview of blockchain architecture. We divide the blockchain architecture into the following layers: a decentralized database, a consensus layer, an immutability layer, and a block.

SUBJECT INDEX

Monica Bhutani

Dr. Monica Bhutani, is an accomplished academician and researcher in Electronics and Communication Engineering and Computer Science. She is an Associate Professor at BVCOE, New Delhi, and a Postdoctoral Researcher at Lincoln University College, Malaysia. With a Ph.D. from IIT Delhi, her expertise spans Optical Wireless Communication, VLC, Li-Fi, Wireless Sensor Networks, IoT, and Machine Learning. She serves as Editor-in-Chief of Scienxt Journal and on the editorial board of Bentham Science. Author of 85+ papers, patents, and books, she is an active IEEE leader, keynote speaker, and mentor, dedicated to advancing STEM education and next-generation communication technologies.

Monica Gupta

Dr. Monica Gupta, Associate Professor at Bharati Vidyapeeth's College of Engineering, New Delhi, earned her Ph.D. from Delhi Technological University in 2022. With over 17 years of teaching experience, her research spans Low Power Memory Design, VLSI, IoT, AI, ML, and Image/Video Processing. She has authored numerous publications, books, and patents, and actively reviews for reputed journals and conferences. In 2022, she co-founded the IOSC-BVP student club with Intel OneAPI, fostering industry-academia collaboration through national events on AI, IoT, ML, and web technologies.

Kirti Gupta

Dr. Kirti Gupta, Professor and Head of Electronics and Communication Engineering at BVCOE, New Delhi, and Vice-Principal (Academics), has over two decades of teaching experience. She holds a Ph.D. in Electronics and Communication Engineering from DTU. Her expertise lies in digital systems, SRAM, and low-power circuit design, with 100+ publications, two books, and two patents. Recognized with multiple Best Researcher Awards, she is also a reviewer for reputed journals, contributing significantly to education, research, and innovation in the academic community.

Deepali Kamthania

Dr. Deepali Kamthania, Professor and Dean at the School of IT, VIPS-TC, has over 20 years of experience in academia and the IT industry. She holds a Ph.D. from IIT Delhi, with research interests in machine learning and hybrid photovoltaic systems. She has published 100+ papers, authored four books, and holds a patent. A session chair, keynote speaker, and editorial board member, she has guided Ph.D. scholars and designed curricula. Recipient of multiple awards, she is a lifetime member of IEEE, CSI, and ISTE.

Danish Ather

Dr. Danish Ather, Associate Professor at Amity University Tashkent, Uzbekistan, has over 18 years of teaching, research, and administrative experience. He holds dual doctorates in Computer Science and Computer Science & Engineering, along with a post-doc from Infrastructure University, Malaysia. An accomplished editor, he led IEEE SMART Series proceedings (2016–2019). He has authored multiple books and 70+ research papers, including 41 Scopus-indexed. A Senior IEEE member, awardee, and specialist in IoT, AI, and programming, he is recognized for academic publishing excellence.