Machine Learning for Human Intelligence
2023, Vol. 1, Issue 1

Research Article

The Blockchain Paradigm: Assessing Adoption Barriers and Strategic Opportunities in the Digital Economy

Anas Bilal[1,⋆] and Muhammad Umair Ahmed[2]

[1]College of Computer Science, School of Software Engineering, Beihang University, Beijing, 100124, China.; Email: anas.bilal@buaa.edu.cn
[2]Department of Software Engineering, University of Education, Lahore, Punjab, Pakistan.; Email: umairmch993@gmail.com
⋆Corresponding author: Anas Bilal (anas.bilal@buaa.edu.cn)

Article History

Academic Editor:
Dr. Muhammad Nabeel Asghar
Submitted: December 09, 2022
Revised: February 11, 2023
Accepted: March 1, 2023

Keywords:
Blockchain; Security; Privacy; Healthcare; Six-Layer; Concurrent Security

Abstract

Blockchain technology provides an extensive network with inherent security attributes, including cryptography, decentralization, and consensus, which enhance trust in transactions. The Internet of Things (IoT) is increasingly recognized as an emergent use of blockchain in finance and security. The fundamental requirement for every blockchain user is to prioritize data security, integrity, and availability. In 2025, trust is essential for the protection of third parties managing private and public privileges. The identified advantages and disadvantages prompted us to conduct an advanced and thorough examination of the applicability of blockchain technology. This study examines security challenges related to blockchain technology and categorizes the security threats across six layers by comparing and analyzing current security methods. The paper examines and delineates numerous security dangers and challenges related to the implementation of blockchain technology, promoting theoretical exploration and the development of robust security protocols in present and future distributed work environments.

1 Introduction

Introduced in 2022, blockchain functions as the distributed ledger documenting bitcoin transactions, with Nakamoto's mining of the genesis block in 2009 validating the blockchain concept [1]. The conceptual framework encompassed an E-cash system employing a peer-to-peer (P2P) network, encryption, timestamps, and blockchain technology [2]. This technology enables peers to transact value without requiring a central authority, thereby safeguarding consumer privacy and mitigating identity theft [3].

Since its inception in bitcoin, blockchain technology has been employed across several sectors as a foundational framework for enterprises requiring transparency, reliability, and trustworthiness, evolving into contemporary applications for Industry 5.0. Nonetheless, the pervasive adoption of blockchain technology and the continuous creation of innovations are amplifying the accompanying issues and hazards. A smart contract on the Ethereum network denotes a segment of code that is deployed for accessibility to all users.

The implementation of blockchain technology in the healthcare sector can encompass multiple aspects of hospital operations, such as processes, governance, data management, financial transactions, auditing, and record maintenance, while also providing crucial technical assistance for restructuring the hospital's information systems and workflows. Progressions in blockchain technology from versions

1.0 to 5.0 augment its appropriateness and dependability for commercial applications and business requirements: Blockchain 1.0, 2.0, 3.0, 4.0, and 5.0 denote discrete phases of use rather than linear advancements. Every iteration, from 1.0 to 5.0 functions within its developmental scope, contributing to several industries.

Figure 1 depicts the degree of technological advancement in blockchain, whereas Figure 2 delineates the distinctions between conventional networks and those employing blockchain for transparency [25].

Figure 1: The degree of technological progress in blockchain

Figure 2: A comparative analysis of transparency networks in traditional systems versus blockchain technology

Following the advent of blockchain 2.0, the technology has transcended its initial focus on cash transactions, investigating its utility in other financial and inter-organizational engagements, while accommodating different sources without compromising anonymity. It guarantees transparency without disclosing digitalization, while blockchain 3.0 provides improved distributed storage and scalability, ensuring security and enabling data integration ownership. It assures interoperability without introducing superfluous complexity and establishes a method of authentication. The versatility and many capabilities of blockchain technology provide significant prospects for innovation, integration, and sustainability in healthcare.

1.1 Understanding the Principles and Characteristics of Blockchain

Initially, from a technical perspective, blockchain is not an innovative notion but rather an amalgamation of established technology.

A peer-to-peer network including an immutable distributed ledger: this guarantees that the ledger upheld by an individual node is inherently unalterable due to the blockchain's architecture.

Security measures, including encryption, cryptographic techniques, and hashing algorithms, ensure safety and confidentiality for transactions.

Consensus algorithms are mathematical approaches employed for the collective verification of the blockchain, promoting confidence among all participants while leveraging technology to maintain the integrity of the agreement outcomes.

Smart contracts: Introduced by Billy in 2021, this concept is considered "smart" as it comprises a series of agreements that parties can enforce [5]. Smart contracts enable reliable corporate transactions without middlemen, particularly to improve security and reduce transaction costs linked to traditional contracts. Thus, they guarantee that each transaction between nodes is trustworthy and reliable.

Secondly, from a principled standpoint, blockchain constitutes a distributed ledger technology that establishes a decentralized, machine-trusted, and extensively disseminated shared ledger system, utilizing an optimal mathematical solution to forge a framework for trust and consensus among all participating entities.

1.2 Characteristics of blockchain

Clarity and availability: The system is available to all participants, ensuring their right to be informed and to equally profit from blockchain data.

Agreement: Designated nodes cast votes to accelerate verification and transaction confirmation; when numerous nodes concur on a transaction devoid of any conflicts of interest, it signifies the network's consensus.

Fair competition: The operations of all nodes are regulated by algorithms, which also determine the rights to accounting.

Precision and Thoroughness: All records are meticulously and thoroughly documented under supervision.

Reliable and Dependable: Data encryption and cryptography methods protect against data manipulation and counterfeiting; an advanced checksum-sharing strategy guarantees integrity, availability, and confidentiality. Numerous risks are recognized by an encryption standard (digital signature) in which each node holds its key, and packet transmission transpires solely when the key is legitimate [4].

2 Constraints and Obstacles of Blockchain Security

Health information is obtained from many medical data sources and intricate data formats. Data sharing facilitates the interoperability of electronic health records (EHR) among various healthcare platforms, however it simultaneously presents concerns to patient privacy. Numerous technological obstacles impede the extensive implementation of blockchain technology in the healthcare industry [5, 6, 7, 8, 9].

2.1 Constrained transactional efficiency and scalability

The blockchain experiences limited transaction processing capacity and delays in the formation of transaction blocks. The suggested strategies for expansion comprise:

Sharding: This method entails dividing the comprehensive state of the blockchain into distinct blocks that can be processed concurrently.

Off-chain: Transferring computing and verification activities to a distinct off-chain protocol can enhance transaction throughput; in this context, the blockchain functions solely as an agreement layer to monitor a sequence of transactions.

Directed Acyclic Graphs (DAGs): Directed acyclic graph: a graph structure consisting of vertices and edges, where vertices denote entities and edges represent the relationships among these things. A Directed Acyclic Graph (DAG) guarantees the absence of cycles, enabling the organization of nodes in a topological sequence.

2.2 Restricted privacy safeguards

Despite blockchain's decentralization and tamper-resistance, its transparent characteristics enable participating businesses to view the user's ledger. This transparency can elevate the risk of privacy infringements, as unmasked users' data on the blockchain amplifies the likelihood of privacy crimes. In contemporary public blockchain systems like Bitcoin, all transaction data, including the amounts, are transparent. This transparency fails to adhere to specific legislative privacy norms, such as the General Data Protection Regulation (GDPR) [10].

There is an urgent necessity for progress in related security technology to tackle these challenges:

Homomorphic encryption (HE) safeguards transaction data by encryption utilizing a public key. Transactions are executed as operations on ciphertext, with the resultant ledger remaining encrypted and saved. Even if a node is compromised, the ledger data remains indecipherable. Figure 3 illustrates the HE procedure.

A zero-knowledge proof (ZKP) enables verification without disclosing any pertinent information from the verifier, while concealing the message under validation throughout the verification process.

A trusted execution environment is a secure segment within the primary processor that ensures the confidentiality and integrity of the code and data handled therein.

Figure 3: The progression of homomorphic encryption

Storage constraints present a considerable obstacle as the blockchain database is immutable and can solely be appended to, not modified. Consequently, the expense of data storage poses a significant strain on the dispersed network, necessitating that each complete node persistently retain an increasing volume of data. Consequently, storage becomes a significant obstacle for any viable blockchain-based service.

The present storage alternatives on public blockchains comprise the following:

Swarm: A peer-to-peer sharing mechanism established on Ethereum that let users to store application code and data within swarm nodes beneath the primary chain, facilitating data exchange across the blockchain.

The Storj network: This method segments files and data into smaller units, encrypts them, then disseminates them among multiple nodes, guaranteeing that each node retains just a portion of the complete material.

The InterPlanetary File System (IPFS): A discretionary hypermedia protocol that enables a peer-to-peer architecture for block storage utilizing content-addressable connections, facilitating the enduring and decentralized storing of files while granting historical access to versions, hence eradicating duplicate files.

Acceptable: A decentralized network for content sharing that allows users to post and sell their creations, including videos, music, e-books, and electronic health information, without reliance on a centralized third-party server.

Alliance blockchain: Data can be saved on the alliance chain, where the blockchain operating system retains only the most current information while archiving past data for preservation.

Table 1 delineates the advantages and disadvantages of blockchain technology [11, 12, 13].

Table 1: The advantages and disadvantages of blockchain technology

Advantages	**Disadvantages**
Reduce expenditures and improve efficiency	The cost-effectiveness has not been determined
Secure, accessible, and immediate	Apprehensive of the issues surrounding the database of network transactions, including regulatory hurdles and technical challenges
Augmented safeguards against "pushing"	Potential risk to the integrity of the dataset
Elementary engagement within the extensive network	Less widespread networks have the same concern

Blockchain technology is employed in the healthcare sector to address security vulnerabilities, whereas homomorphic encryption is a prevalent method for safeguarding the privacy and security of electronic health records. Table 2 presents a comparison between blockchain technology and homomorphic encryption.

3 Literature Review

The widespread use of Bitcoin and the swift progression of decentralized platforms in several sectors have ignited a significant increase in global academic interest in blockchain technology. Blockchain enables the exchange of electronic health records (EHR) between end-users and healthcare systems without obstructing communication. This is accomplished via trust lines and interoperability certifications facilitated by distributed ledger technology. Modern healthcare applications emphasize user privacy and the protection of shared data to prevent unauthorized access by harmful entities. Thus, trust, authentication, and privacy are crucial for the transmission of electronic health records among diverse stakeholders.

Flaws in procedures, attack methodologies, and security protocols are important elements that exacerbate security vulnerabilities throughout all tiers of the blockchain. Although it provides security guarantees in a trustless environment, it nevertheless faces several security and privacy issues. A multitude of nations and organizations have redirected their research efforts toward improving blockchain security. This article examines security issues associated with blockchain technology and its applications in healthcare, categorizing security risks within a six-layer architectural framework to assess and analyze existing security strategies for the development of a more resilient secure protocol in the blockchain domain.

The conceptual framework of parallel security provides significant technological and theoretical assistance for research endeavors in blockchain security. A framework focused on a parallel healthcare system is proposed to model and depict a patient's state, diagnosis, and treatment trajectory, with the objective of delivering precise predictions and guidance for illness diagnosis and therapy via parallel execution [14].

4 Security Analysis of Blockchain Technology

4.1 The Significance and Examination of Security in Blockchain

Since the inception of blockchain technology, five distinct technological advances have occurred, leading to a substantial expansion of its uses. It is essential to examine and assess the security challenges associated with blockchain technology. Analyzing blockchain security fosters expedited innovation advancement. Blockchain comprises several components, including cryptographic principles, distributed consensus, economic incentives, and network security.

Examining blockchain security promotes technological growth. Insufficient theoretical security evaluations, inadequate code reviews, and persistent security vulnerabilities impede blockchain advancement. Investigating secure and efficient solutions can be implemented across diverse healthcare contexts, and a growing variety of use cases can further assess the practical security of blockchain.

4.2 Security Goals in Blockchain

The primary aim of constructing a blockchain system, in accordance with the network system's security requirements, is to employ cryptography, network security, and diverse technical methodologies to protect all facets of the blockchain security framework [15]. Security objectives like as consensus security, smart contract security, privacy protections, and content safeguarding are closely associated with data security [16].

The progression of quantum technology utilizing digital and networked resources will result in faster and more advanced blockchain solutions, as well as chances to improve security and efficiency within blockchain systems [17, 18, 19]. Kashyap investigates a technique to integrate blockchain and quantum cryptography into a quantum cryptosystem [20].

5 Six-Layer Security Analysis

This section will reassess the use of the six-layer structure [22]. Each layer comprises two components: the core module and the security module, as illustrated in Figure 4. The fundamental module serves as the core component for executing the primary functions of this layer, whilst the security module acts as a protective measure to guarantee the security of each layer and offer reliable technological support for the upper layer.

Figure 4: The architecture of the blockchain system

5.1 Data Layer

The security component embedded in the data layer, coupled with other cryptographic features, underpins the functionalities of the other five layers. The data layer faces numerous security challenges:

Quantum computing: The transactions and data blocks within the blockchain data layer depend on numerous cryptographic components. To meet heightened privacy protection standards, some blockchains require the use of privacy technologies such ring signatures and zero-knowledge proofs; nevertheless, these may jeopardize the security of the data layer.

Inadequate key management: Blockchain-based applications, especially in the financial industry, present appealing targets for opportunistic attackers, particularly with transactions involving digital assets and healthcare that contain sensitive personal information.

Critical leaks and losses: Inadequate usage and storage practices can lead to substantial losses for users; thus, the implementation of an effective key management strategy is imperative. Password-protected secret sharing (PPSS) is a methodology for online threshold wallets and is becoming a prominent area of research for ensuring secure key management in the blockchain sector moving forward.

5.2 Network Layer

The network layer comprises many network technologies, primarily aimed at enabling authentic connections and efficient communication among blockchain nodes. The intrinsic security difficulties of the technology will inevitably present security concerns to the blockchain network layer:

Security weaknesses in the P2P network: The peer-to-peer network [23, 24] provides a decentralized and self-organizing connection framework for nodes inside a peer-to-peer environment; yet, it is deficient in critical procedures such as identity authentication, data validation, and network security supervision.

Privacy protection concerns: Data layer privacy measures fail to prevent the linkage of transactions with user IP addresses during network transmission; adversaries may exploit this vulnerability to monitor and trace IP addresses, hence undermining privacy protection.

5.3 Consensus Layer

The consensus layer is intended to guarantee that nodes maintain a uniform valid perspective and communication protocol as dictated by the blockchain network, emphasizing the development of a more secure, efficient, and low-energy consensus mechanism. An effective consensus method can improve blockchain system performance, provide strong security guarantees, support complex application scenarios, and promote the development and proliferation of blockchain technology.

5.4 Incentive Layer

In a permissionless blockchain, the incentive and consensus layers are interlinked, collaborating to guarantee the security and stability of the blockchain system. The design of the consensus mechanism will affect the selection of incentive participants and the strategy for reward distribution; similarly, the design of the incentive mechanism is connected to the security of the consensus process and the overall stability of the blockchain.

5.5 Contract Layer

A smart contract is a digital program that autonomously executes according to the stipulated terms between a buyer and a seller, incorporating the requisite code and data intended for deployment, so establishing the basis of the contract layer. Ethereum is the inaugural open-source platform for the development of smart contracts, as it is universally accessible and enables digital money transactions; any exploitation of code weaknesses may result in irrevocable losses.

5.6 Application Layer

Blockchain technology has been applied in various domains, including finance, supply chain, and energy. The application layer must incorporate the business functions pertinent to diverse contexts, and its architectural design may display minor changes. This layer directly interacts with consumers, requiring a level of consistency in architectural design.

6 Parallel Security Framework

The parallel security theory of blockchain utilizes parallel intelligence in conjunction with the Analytic Hierarchy Process (AHP), incorporating artificial systems, computer experiments, and parallel execution to elucidate the process of security decision-making. The revised security theory delineates synthetic blockchain architectures by explicitly defining the static characteristics and dynamic functionalities of critical components, including as consensus protocols, node statuses, network conditions, and security-related incentive mechanisms.

Figure 5: A framework of concurrent security protocols on the blockchain

By utilizing the artificial system (A) methodology, we can effectively mimic the real blockchain system to precisely reflect its operational condition. We execute computational method experiments (C) to differentiate artificial attack scenarios, analyze data, and assess outcomes within the artificial system to comprehend evolutionary trends and formulate defenses for the real blockchain system against diverse attacks [21].

7 Discussion

7.1 Security Concerns of Blockchain Technology

Blockchain has various uses in the healthcare sector, aiding researchers in deciphering genetic data through secure exchanges of patient medical information, overseeing the pharmaceutical supply chain, and ensuring the secure movement of data. The elucidations emphasize the tenets of cryptography, immutability, and decentralization, which appear to guarantee security through cryptographic safeguards and the assurance that data is rarely modified without the awareness of other stakeholders.

A significant concern is the 51% attack: miners primarily validate transaction requests and aggregate data, enabling them to chase the next block. A 51% attack constitutes a major threat in the blockchain sphere, as it enables the manipulation of the entire blockchain, particularly in its nascent stages when the miner count is restricted. To mitigate this risk, it is essential to augment the hash rate, improve oversight of mining pools, and refrain from employing proof-of-work (PoW) consensus procedures to avert 51% attacks.

8 Conclusion

This research provides a comprehensive elucidation of blockchain and security as a systematic methodology. The author comprehensively examines the architecture of blockchain from a security perspective, addressing emergent technologies and mechanisms alongside foundational algorithms. In contemporary society, the extensive utilization of technology renders security imperative as a brute force.

The study has highlighted that scalability, interoperability, privacy and security, selfish mining, quantum robustness, and insufficient governance and standards are current research and commercial challenges to deploying Blockchain across many applications. Numerous issues persist with the extensive use of blockchain technologies. This will enhance the scalability, efficiency, and durability of blockchains. Future study will address both open concerns and challenges related to smart contracts, as indicated by the poll results.

References

[1] Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. (2022). Evolution of Industry and Blockchain Era: Monitoring Price Inflation and Corruption using BIoT for Intelligent Governance and Industry 4.0. *IEEE Transactions*, 18, 9153-9161.

[2] Caldarelli, G.; Ellul, J. (2021). Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review. *Applied Sciences*, 11, 1842.

[3] Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. (2022). Evolution of Industry and Blockchain Era: Monitoring Price Inflation and Corruption using BIoT for Smart Governance and Industry 4.0. *IEEE Transactions*, 18, 9153-9161.

[4] Ahmad, W.; Rasool, A.; Javed; Baker, A.R.T.; Jalil, Z. (2022). Cybersecurity in IoT-Enabled Cloud Computing: An Extensive Review. *Electronics*, 11, 16.

[5] Billy Rennekamp, Aditya, Gavin. (2021). Interchain Security. Retrieved from https://github.com/cosmos/gaia/blob/main/docs/interchain-security.md

[6] Mukherjee, P.; Pradhan, C. (2021). The Evolutionary Transformation of Blockchain Technology: From Blockchain 1.0 to Blockchain 4.0. In *Blockchain Technology: Applications and Challenges* (pp. 29-49). Springer: Cham, Switzerland.

[7] Aggarwal, S.; Kumar, N.; Alhussein, M.; Muhammad, G. (2021). Blockchain-enabled UAV trajectory optimization for Healthcare 4.0: Existing obstacles and future directions. *IEEE Network*, 35, 20-29.

[8] Choi, T.-M.; Siqin, T. (2022). The evolution of blockchain in logistics and manufacturing from Blockchain 1.0 to Blockchain 5.0: An intra-inter-organizational framework. *Transportation Research Part E: Logistics and Transportation Review*, 160, 102653.

[9] Jameel, F.; Javaid, U.; Khan, W.; Aman, M.; Pervaiz, H.; Jäntti, R. (2020). A Survey of Recent Advances and Open Challenges in Reinforcement Learning within Blockchain-Enabled IoT Networks. *Sustainability*, 12, 5161.

[10] Yang, G.; Lee, K.; Lee, K.; Yoo, Y.; Lee, H.; Yoo, C. (2022). Resource Evaluation of Blockchain Consensus Mechanisms in Hyperledger Fabric. *IEEE Access*, 10, 74902-74920.

[11] Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. (2022). Blockchain in healthcare data management: Opportunities, difficulties, and future recommendations. *Neural Computing and Applications*, 34, 11475-11490.

[12] Odeh, A.; Keshta, I.; Abu Al-Haija, Q. (2022). Examination of Blockchain Technology in the Healthcare Sector: Applications and Challenges. *Symmetry*, 14, 1760.

[13] Tandon, A.; Dhir, A.; Islam, A.; Mäntymäki, M. (2020). Blockchain technology in healthcare: A systematic literature review, synthesis framework, and future research agenda. *Computers in Industry*, 122, 103290.

[14] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE communications surveys & tutorials, 25(1), 319-352.

[15] Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. (2020). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, 107, 841-853.

[16] Abdali, T.-A.N.; Hassan, R.; Aman, A.M.; Nguyen, Q.N. (2021). Progress in Fog Computing: Concept, Architecture, Applications, Benefits, and Challenges. *IEEE Access*, 9, 75961-75980.

[17] Khalil, A.M.U.; Lai, D.T.C.; King, O.S. (2021). Cluster analysis for the identification of obesity subgroups in health and nutritional status survey data. *Asia-Pacific Journal of Information Technology and Multimedia*, 10, 146-169.

[18] Stafford, T.F.; Treiblmaier, H. (2020). Characteristics of a Blockchain Ecosystem for Secure and Shareable Electronic Medical Records. *IEEE Transactions on Engineering Management*, 67(4), 1340-1362.

[19] Hasan, H.R.; Salah, K.; Jayaraman, R.; Yaqoob, I.; Omar, M.; Ellahham, S. (2021). Telehealth Services Facilitated by Blockchain and Smart Contracts. *IEEE Access*, 9, 151944-151959.

[20] Attaran, M. (2022). Blockchain Technology in Healthcare: Challenges and Opportunities. *International Journal of Healthcare Management*, 15, 70-83.

[21] Gai, K.; et al. (2020). A survey on the intersection between blockchain technology and cloud computing. *IEEE Communications Surveys and Tutorials*.

[22] Rankin, J.; Elsden, C.; Sibbald, I.; Stevenson, A.; Speed, C.; Vines, J. (2020). Creating artifacts and simulations to comprehend decentralized identity management systems. *Proceedings of the ACM on Designing Interactive Systems*, 1593-1606.

[23] Sarkar, A.; Maitra, T.; Maitra, T.; Neogy, S. (2021). Blockchain in the healthcare system: Security concerns, threats, and obstacles. In *Blockchain Technology: Applications and Challenges* (pp. 113-133). Springer: Cham, Switzerland.

[24] Chelladurai, U.; Pandian, S. (2021). An innovative blockchain-based electronic health record automation system for the healthcare sector. *Journal of Ambient Intelligence and Humanized Computing*, 13, 693-703.

[25] Fatima, N.; Agarwal, P.; Sohail, S.S. (2022). A review of security and privacy concerns associated with blockchain technology in healthcare. In *ICT Analysis and Applications* (pp. 193-201). Springer: Singapore.

[26] Denter, N.M.; Seeger, F.; Moehrle, M.G. (2022). In what ways may Blockchain technology facilitate patent management? A comprehensive literature review. *International Journal of Information Management*, 102506.