Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
DOI : 10.47974/JIOS-1980

Blockchain for secure computing : Technologies, challenges, and future scope

Ashish Singh *
School of Computer Engineering
Kalinga Institute of Industrial Technology
Bhubaneswar 751024
Odisha
India

Pradeep Kumar Roy †
Decision Science and Information Systems Area
Indian Institute of Management Nagpur
Nagpur 411008
Maharashtra
India

Abstract

Secure computing is critical across a wide array of domains, such as finance, healthcare, Internet of Things (IoT), cloud computing, and online services. Blockchain technology has emerged as one of the most transformative frameworks for the development of a secure computing environment. Despite the growing adoption of blockchain in secure computing, most prior research does not offer a comprehensive and systematic review of the various blockchain-based security models, their challenges, and their impact on different computing environments. This paper presents a systematic review of existing blockchain technologies focusing on how blockchain enhances secure computing. We have employed a structured methodology, beginning with the identification of key research questions, followed by an extensive search and filtration of relevant studies, and concluding with a comparative analysis and final report. A detailed comparative study of blockchain systems is conducted to address the security and privacy aspects of the blockchain-based secure computing

* *ORCID-ID:* 0000-0001-5974-0415
† *ORCID-ID:* 0000-0001-5513-2834

* *E-mail:* ashish.singhfcs@kiit.ac.in (Corresponding Author)
† *E-mail:* pradeep@iimnagpur.ac.in

environment. Despite its advantages, this paper also presents several challenges, which represent opportunities for future research and development.

Subject Classification: *68M14, 68M15, 94A60.*

Keywords: *Blockchain, Secure computing, Decentralization, DLT, Cryptographic security, Smart contracts, Consensus algorithms, Privacy and security.*

I. Introduction

In the current digital era, blockchain is a technology for enhancing secure computing across various domains, including finance, healthcare, and supply chain management. Table 1 shows the number of B2B cross-border transactions will reach 745 million by 2025 [1]. The digital nature of these transactions exposes potential security threats. Blockchain technology is a security solution with peer-to-peer (P2P) automated access control in a decentralized network [2]. It offers a robust robust cryptographic foundation for enhancing security. It enables secure interactions between network nodes without relying on trusted intermediaries. The transactions are accurate without any fraud, transparent, verified by the peers in the network, and immutable (can't be changed over time). The strong encryption mechanisms [3, 4], smart contracts [5, 6], decentralized finance (DeFi) [7, 8], and Non-Fungible Tokens (NFTs) [9, 10] extend new capabilities and opportunities for addressing the goals of secure computing. Bitcoin was first proposed in 2008 and implemented in January 2009 [11, 12]. The size of the Bitcoin blockchain is exponentially growing by nearly one gigabyte every few days, and in 2024, size will be close to reaching 5450 gigabytes [13]. A blockchain is a distributed database that

Table 1

B2B cross-border transactions on blockchain in various regions worldwide (in millions)

Year	North America	Latin America	Europe	Far East & China	Rest of the world
2020	20.60	1.10	33.30	45.80	21.40
2021	39.20	2.60	81.30	109.30	46.80
2022	64.10	5.00	152.10	240.30	80.70
2023	100.70	9.70	233.60	371.30	127.80
2024	159.60	18.70	337.50	536.30	190.20
2025	254.30	36.20	466.50	744.70	265.60

differs from traditional ones by storing information in a chain of blocks. Each of these blocks is linked/chained together to form a distributed database, which is visible and accessible to all network participants. When new data is to be written on the blockchain, it must be verified by other network members. These other users are called nodes.

Satoshi Nakamoto [11] outlays the design of a completely P2P payment system. No intermediary entity is needed in this payment system other than the payment network itself. In electronic payments, a central authority was always required to remove trust issues between the parties and verify the transactions. The main problem with the electronic payment system was double-spending. As the name suggests, double spending means spending the digital cash twice or more when proper mechanisms were not in place [14, 15]. Bitcoin replaced the trust-based model with cryptographic proof. It allowed any two individuals to send and receive money between them without needing a reliable central authority like a bank [16, 17]. It introduced a timestamp-based chronological ledger of transactions. Chronological means a record of events in which they occur. Thus, transactions were recorded as they happened with the timestamp

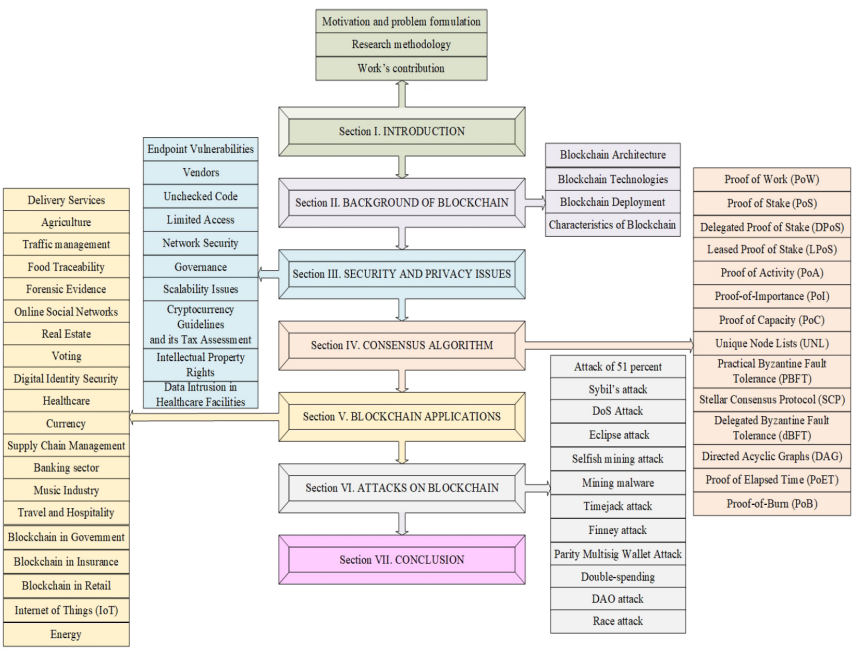

Figure 1

The structure of the paper

[18]. In the blockchain, once a transaction is done, it is verified and checked by consensus, which means most of the network members should agree that the transaction is valid . Once transaction data is written on the blockchain, it almost becomes immutable, meaning it can't be changed easily. Thus, the blockchain contains a definite record that can be verified of every transaction ever made. Table II provides a comprehensive comparative analysis of various survey papers on blockchain technology. It focuses on topics such as objectives, security, privacy, limitations, and applications across different domains.

A. *Motivation and problem formulation*

The growing dependence on online transactions necessitates secure computing environments. The blockchain system provides promising features to protect it from malicious attacks and provide security solutions. Despite its promising features, adopting blockchain technology in secure computing is not without challenges. Several issues, such as scalability, vendors, privacy concerns, and the network security associated with blockchain networks, pose significant hurdles. Additionally, integrating blockchain with existing systems and developing standardized protocols for secure computing remain critical challenges. This research aims to systematically investigate how blockchain can be leveraged to create secure computing solutions that can overcome emerging threats and provide reliable protection for sensitive information. All the above-discussed research findings highlight the importance of blockchain in multidisciplinary applications. Also, from the literature, we have found that most articles do not cover all the aspects of blockchain. Thus, this article's primary objective is to develop a systematic review that contains all the aspects of blockchain for secure computing.

B. *Research methodology*

The primary objective of this survey is to analyze the current state of blockchain technology in secure computing environments. The following steps outline the research methodology.

Step 1: The first step in this research is to identify the core research questions, like how is blockchain technology applied to enhance secure computing in various domains?, what are the challenges and limitations of using blockchain in secure computing environments?, how does

blockchain address specific security risks?, and what are the emerging trends and future directions in blockchain-based secure computing?

Step 2: The following search strings: "Blockchain for secure computing", "Blockchain technology in cybersecurity", "Blockchain-based security models", and "Blockchain challenges in secure computing" were searched in widely used academic databases and search engines such as Google Scholar, IEEE Xplore, and ScienceDirect.

Step 3: Databases like IEEE, Springer, Elsevier, and Scopus were selected for their broad scope and reliable academic sources.

Step 4: After gathering the search results, we applied to filter the relevant works like only English-language publications considered, short papers, articles lacking comprehensive experimental or theoretical backing, and older works were excluded.

Step 5: Once the relevant papers were identified, their reference lists were further scrutinized to identify any missing but important works.

Step 6: The next phase involved categorizing the selected papers based on critical factors such as Blockchain applications, Challenges and limitations, security model, and risks and mitigation techniques,

Step 7: The categorized papers were thoroughly reviewed to extract relevant information.

Step 8: A comparative analysis and final report of the relevant information offer a clear perspective on the state of blockchain in secure computing.

C. *Contributions*

This research enriches the field by presenting a comprehensive analysis of existing blockchain literature. It identifies significant security and privacy challenges, examines consensus mechanisms, and highlights potential avenues for future development, thereby supporting advancements in secure computing solutions. The following are the key contributions of the paper.

- This survey conducts an extensive review of existing literature, offering a comparative analysis that highlights the strengths and limitations of previous survey papers on blockchain technology.

Table II

Comparative analysis of our survey paper with the previous survey papers

Survey paper	Year	Topic discussed	Main Focused area	Objective	Limitations	Blockchain Overview	Consensus Algorithm	Attacks Analysis	S & P Issues	Challenges & Open Issues
Feng et al. [19]	2019	Privacy-preserving techniques, applications, Identity and transaction privacy, Privacy threats, Future research challenges	Addressing privacy challenges in blockchain networks	To give a critical comparative analysis of cryptographic defence mechanisms for the privacy of blockchain.	Limited to privacy concerns, does not cover attacks or consensus algorithms comprehensively.	General privacy-focused overview	No detailed coverage	Not covered	In-depth privacy analysis	No discussion on challenges
Xie et al. [20]	2019	Technology, Smart city components, Blockchain features, Smart city applications, Challenges	Blockchain adoption for smart city infrastructure and its challenges	To explore the use of blockchain in smart city infrastructure and its challenges.	Limited to smart city applications, no comprehensive attack or security analysis.	Overview of blockchain in smart cities	No detailed coverage	Not covered	General security concerns in smart cities	Smart city-specific challenges

Contd...

Viriyasitavat et al. [21]	2019	Business opportunities for blockchain and IoT, Blockchain challenges in IoT, Research context and key contributions of blockchain and IoT integration, IoT characteristics and Service-oriented Architecture (SoA)-based IoT architecture	Using blockchain and IoT for business applications	To examine how blockchain and IoT can be leveraged for business solutions.	Limited business applications and lacks detailed privacy/ security analysis.	General business applications of blockchain	Brief mention of PoS	Not covered	Business-related security concerns	Business-related challenges
Hughes et al. [22]	2019	Blockchain principles, Blockchain benefits, Blockchain applications, blockchain's future	Applications of DLT and blockchain in various sectors	To explore the various applications of DLT and blockchain in different sectors.	Limited focus on consensus algorithms and blockchain attacks.	General overview of DLT and blockchain	Not extensively covered	Not covered	General security concerns	No detailed future scope
Kowalski et al. [23]	2021	Blockchain technology, Blockchain's role in enhancing trust relationships, security in transactions and data exchanges, Challenges and limitations of blockchain technology	Trust management in blockchain-based trade finance	To analyze blockchain technology and trust relationships in trade finance.	Focuses only on finance, lacks broader applications and security issues in other sectors.	Overview focused on finance and blockchain	Limited to PoS	Not covered	Financial privacy concerns	Financial service challenges

Contd...

Pal et al. [24]	2021	Blockchain in business management, marketing management, human resource management, supply chain management, manufacturing and operations management, Applications, Challenges, and Future potential	Exploring the use of blockchain in business management	To study the applications of blockchain in business management.	Primarily business-focused, lacks detailed technical analysis of blockchain security, consensus algorithms, and attacks.	General overview of blockchain in business	No detailed coverage	Not covered	Business security concerns	Business-related challenges
Guo and Yu [25]	2022	Blockchain overview, Consensus algorithms, Applications, security risks and attacks, Challenges and future research trends	Addressing security and privacy issues in blockchain systems	To address security challenges and privacy issues of blockchain technology.	Comprehensive security analysis but lacks detailed coverage of specific applications and consensus algorithms.	In-depth overview of blockchain security	Discussed PoW, PoS, PBFT	Attack analysis included	Detailed security analysis	No detailed future challenges

Contd...

Boakye et al. [26]	2022	Blockchain technology in finance, Crowdfunding and equity crowdfunding, Digital currencies, Smart contracts and decentralized, Research trends, Future directions	Reviewing blockchain applications in the finance industry	To review the use of blockchain in finance, focusing on privacy, security, and applications.	Focused on finance and lacks broader applications or attack analysis.	Overview focused on finance	Brief mention of PoW	Not covered	Financial privacy and security issues	Financial service challenges
Hanafizadeh & Alipour [27]	2024	Blockchain applications and adoption in different industries, Challenges and opportunities, Future research directions	Theories and applications of blockchain in business and management	To review theories used in blockchain for business and management and identify gaps.	Focus on operational, strategic, and economic considerations, lacks in-depth security and attack analysis.	Overview of blockchain in business & management	No detailed coverage	Not covered	No significant focus on security	Business and management challenges
Our survey paper	--	**Covered almost all the aspect of blockchain**	**Blockchain for secure computing across different sectors**	**To systematically review blockchain technology for secure computing across various domains.**	N/A	**Comprehensive overview across industries**	**Comprehensive coverage of PoW, PoS, DPoS, PBFT, DAG, PoET**	**Detailed analysis of blockchain attacks like 51%, Sybil, DoS, etc.**	**In-depth analysis of security and privacy across multiple domains**	**Comprehensive coverage of challenges and future scope across industries**

- It provides a thorough examination of the current state of blockchain technology, specifically focusing on its applications in secure computing.
- The paper systematically analyzes key aspects of blockchain, including security and privacy concerns, consensus mechanisms, use cases, and potential vulnerabilities, providing insights into its viability for secure computing solutions.
- The comprehensive analysis of challenges and future opportunities offers valuable guidance for ongoing innovation and the development of more secure blockchain technologies.

The structure of the paper is summarized in Figure 1. Figure 1 creates a building block of this survey in the reader's mind that helps to understand the current taxonomy of this paper. The remaining section of the paper is structured as follows: Section II discusses the background of the blockchain. The security and privacy issues are given in Section III. Section IV discusses the consensus algorithm, which is used for the decision-making process. The blockchain application is given in Section V. Attack on the blockchain is given in Section VI. Finally, Section VII concludes our work.

II. Background of Blockchain

This section includes the fundamentals of blockchain, which is essential for establishing secure computing environments.

A. *Blockchain architecture*

Blockchain [11, 28] is a distributed database that acts as a public ledger, recording digital events that are executed and shared among participating parties. This ensures transparency and fairness for secure computing. An architecture of the blockchain is given in Figure 2. In this architecture, each block is linked to a single parent block. The next block in the line stores the hash of the previous block. This design maintains the integrity of the chain of records, which is essential for secure computing systems. The first block in a blockchain is known as the genesis block. The term "Genesis block" refers to the starting point of the blockchain and does not have a parent block. A block in a blockchain consists a block header and the block body. The block header contains several key components: block version, Merkle tree root hash, timestamp, nonce, and parent block hash. The block body contains the transactions selected by

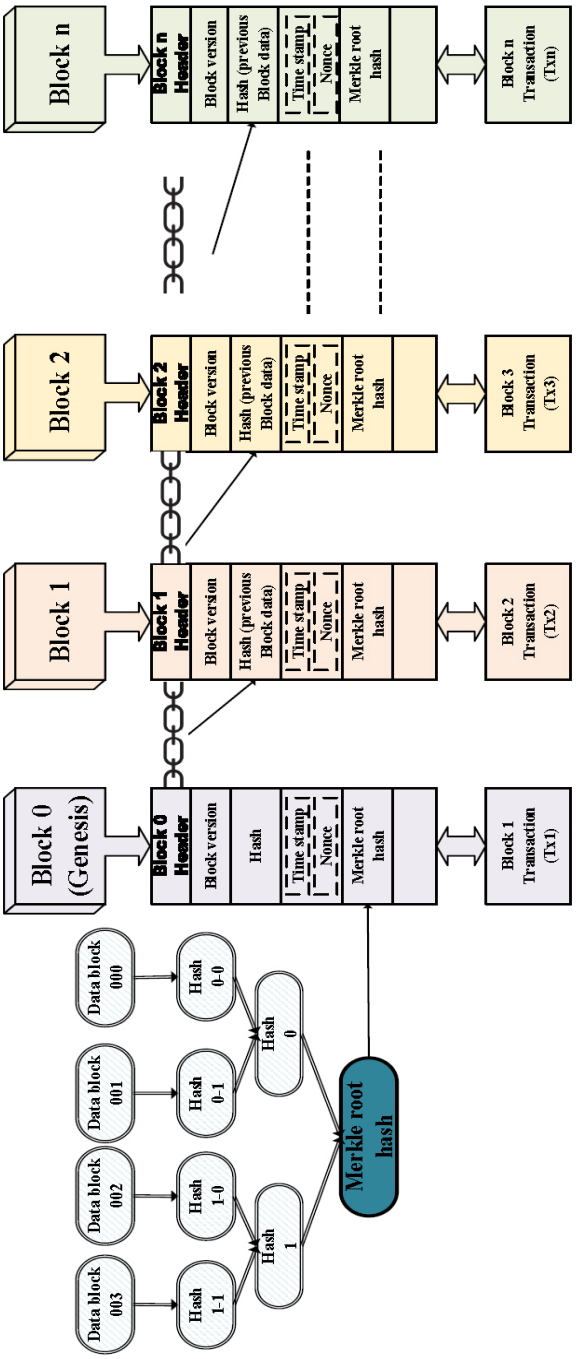

Figure 2
Blockchain architecture [29, 30]

the miner for inclusion in the block. Transactions in a blockchain contain the addresses of both the recipient and the sender, along with the values being transferred. These transactions are ordered and bundled into blocks by specific nodes, such as miners, and distributed across the network.

B. *Blockchain technologies*

This subsection includes some important technologies that enable decentralized, secure, and transparent blockchain systems.

(1) **Blockchain platforms:** Bitcoin is a digital currency stored on a public ledger [31]. Ethereum runs on the Ethereum blockchain [32], supporting smart contracts and decentralized applications. Hyperledger is an enterprise blockchain project providing tools and frameworks for building permissioned networks where participants are known.

(2) **Consensus algorithm:** It is a process used by a group of users to reach an agreement on the best decision for the group, even if some individuals disagree [3, 34]. In the decentralized blockchain system, consensus algorithms maintain the integrity and security of the network operations by ensuring all transactions are legitimate and that all participants agree on the current state of the ledger.

(3) **Cryptographic hashing:** It is a process that converts data into a unique, fixed-size string of characters [35]. It's essential for verifying data integrity and security. In this process, a tiny change in the input produces a completely different hash. The blockchain-based system links blocks together to prevent tampering by ensuring that any alteration is easily detectable [36].

(4) **Smart contracts:** Smart contracts [37] are self-executing programs on a blockchain that automatically enforce and carry out the terms of an agreement when predefined conditions are met. They eliminate the need for intermediaries. It also ensures that transactions or agreements are completed exactly as programmed.

(5) **DLT:** DLT is a system where data is stored across multiple locations or nodes rather than in a single or a central database [38]. This decentralized approach increases security and transparency. It ensures that all participants have access to the same data, and changes are only made through consensus among the nodes.

C. *Blockchain deployment*

(1) **Public blockchain:** This type of blockchain is open to everyone without any restrictions. Anyone with an internet connection can join the network, start mining blocks, and validate transactions without needing permission [39, 40].

(2) **Private blockchain:** In secure computing systems, private blockchains allow the company to control the network and its rules. Participants can join only through a verified invitation. All members are known and trusted. The key aspect is permissions, which ensure that participants see only permissible items and can't make unauthorized transactions [41, 42].

(3) **Permissioned blockchain:** In a permissioned blockchain, nodes are pre-selected and authorized to participate. This type of blockchain allows a specific community or group to record transactions and events securely [43].

(4) **Hybrid blockchain:** A hybrid blockchain combines elements of both public and private blockchains [44]. Hybrid blockchains are flexible, allowing seamless integration between private and public blockchains. Transactions within the private part of a hybrid blockchain are usually validated within that network, but they can also be sent to the public blockchain for additional verification [45]. This enhances the security and transparency of the overall blockchain network.

D. Characteristic of Blockchain

The characteristics of Blockchain are as follows:

- **Immutability:** Data on the blockchain is immutable, meaning it cannot be easily changed [46]. The key benefit is data permanence—once written, the data cannot be altered.
- **Decentralized Public Ledger:** Decentralized public ledgers combine traditional record-keeping with modern technology to create a new system for storing and secure sharing of data [47, 48]. This is a record-keeping system that contains a record of all the transactions. This is maintained and updated by independent nodes that work together based on a protocol's ruleset.
- **P2P Network:** In blockchains, the P2P design offers greater security compared to the client-server model [32]. DoS attacks are nearly

impossible because there is no central point of failure and numerous nodes are distributed across the network.

- **Enhanced Security:** Blockchain removes the need for a trusted third party or central authority to oversee transactions, It uses SHA-256 encryption to add an extra layer of security. All data on the blockchain is hashed using cryptography, which processes the data through an algorithm to produce a fixed-length output that is distinct from the original input [49].
- **Distributed Ledgers:** Distributed ledgers are significantly harder to compromise than centralized ones because an attack would need to target a majority of nodes simultaneously [50]. Additionally, distributed ledgers reduce operational failures, speed up transactions, and operate continuously, lowering costs for users.
- **Consensus:** Consensus plays a crucial role in blockchain technology by determining who has the right to add the next block to the chain [51, 52]. It allows information to be shared with all users in an orderly manner without a third party's involvement.
- **Faster Settlement:** Blockchain enables faster transactions compared to conventional banking systems. It allows users to transfer money more quickly and save time in the long run.

III. Security and Privacy Issues

Blockchain has become crucial in addressing privacy protection and security issues across various sectors, which has contributed to its success. There are several security risks in blockchain technology [57, 58, 59], ranging from web applications and APIs to smart contracts. An online community, Open Worldwide Application Security Project (OWASP), listed the top 10 web application security risks [60], which are also applied in blockchain technology. The analyzed result of the OWASP Top 10 is summarized in Table III [61]. The user's wallets are also an important component because they contain user credentials and can track digital assets associated with the account. Thus, several attacks like Bitfloor [62], Instawallet [63], Australian Bitcoin bank [64], and other security risks have been reported in the past few years. The smart contract vulnerabilities and criminal activities hamper the different events and processes. A list of the top 10 smart contract vulnerabilities is given in [65, 66].

Table III

Comparison of web application risks

Risk Name	Description	Impact	Prevention	Example Attack Scenarios
A01:2021 — Broken Access Control [53]	Access control failures lead to unauthorized access, modification, or destruction of data and perform unauthorized business functions. This includes failures like bypassing access controls, elevation of privileges, and allowing unauthorized users to access sensitive data.	Leads to unauthorized data access and manipulation.	Enforce access control in server-side code, deny by default, log access control failures, and invalidate sessions appropriately.	Modifying the account number in a URL to access someone else's account details. Force browsing to administrative pages.
A02:2021 — Cryptographic Failures [54]	Failures related to cryptography, such as weak encryption, improper key management, or failure to encrypt sensitive data. These can lead to exposure to sensitive information like passwords, credit card numbers, and other confidential data.	Sensitive data exposure, potentially leading to identity theft or financial loss.	Use strong, up-to-date encryption algorithms, manage keys securely, and enforce encryption for data in transit and at rest.	A site not using TLS allows an attacker to steal session cookies via a man-in-the-middle attack.
A03:2021 — Injection [55]	Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query, allowing the attacker to execute arbitrary commands or access unauthorized data. This includes SQL injection, NoSQL injection, and command injection.	Allows attackers to manipulate the database, access sensitive data, or execute commands on the server.	Use parameterized queries, validate and sanitize inputs, and employ ORM tools.	SQL injection via a manipulated input field leads to data leakage or database corruption.
A04:2021 — Insecure Design [56]	Represents weaknesses due to missing or ineffective control design. This is not about insecure implementation but the lack of appropriate security measures in the design phase.	Can lead to the development of inherently insecure applications that are vulnerable to attacks even with perfect implementation.	Use secure design patterns and threat modelling, and integrate security controls from the beginning of the development lifecycle.	Using "security questions" for password recovery, which are vulnerable to guessing attacks.

Contd...

A05:2021 — Security Misconfiguration [25]	Vulnerabilities due to improperly configured security settings in applications, servers, or databases, such as using default settings or enabling unnecessary features.	Leaves systems open to attack due to misconfigured settings, exposing sensitive data or functionality.	Implement a hardening process, remove unused features, and regularly update configurations.	Leaving sample applications on a production server, which attackers exploit to gain access.
A06:2021 — Vulnerable and Outdated Components	Risks associated with using outdated or unmaintained software components, which may have known vulnerabilities that can be exploited.	Exposes the system to known vulnerabilities, leading to potential security breaches.	Regularly update and patch components, monitor for vulnerabilities, and remove unnecessary dependencies.	Exploiting a known vulnerability in an outdated library to execute arbitrary code.
A07:2021 — Identification and Authentication Failures	Failures in user identification and authentication mechanisms, such as weak passwords, improper session management, or lack of multi-factor authentication.	Allows unauthorized access, leading to potential data breaches or unauthorized actions.	Implement strong multi-factor authentication, avoid default credentials, and secure session management.	Credential stuffing attacks using common passwords to gain unauthorized access.
A08:2021 — Software and Data Integrity Failures	Inadequate verification of the integrity of software updates, libraries, or CI/CD processes, leading to potential unauthorized changes or introduction of malicious code.	Allows attackers to introduce malicious code or unauthorized changes, compromising the system.	Use digital signatures, secure CI/CD pipelines, and verify software integrity.	The SolarWinds attack, where malicious updates were distributed to thousands of organizations.
A09:2021 — Security Logging and Monitoring Failures	Insufficient logging and monitoring make it difficult to detect and respond to security breaches, often allowing attacks to go unnoticed.	Prolonged exposure to breaches due to lack of detection, leads to greater damage.	Implement comprehensive logging, establish monitoring processes, and ensure timely incident response.	A data breach goes undetected for years due to a lack of monitoring, leading to massive data loss.
A10:2021 — Server-Side Request Forgery (SSRF)	Occurs when a web application fetches a remote resource without validating the user-supplied URL, allowing attackers to coerce the application into sending a crafted request to an unexpected destination.	Allows attackers to access internal systems, potentially leading to further exploitation.	Validate URLs, segment resource access, and apply deny-by-default policies.	Attacker uses SSRF to access and exfiltrate sensitive data from an internal server.

- **Endpoint Vulnerabilities:** The most common problem with this kind of technology lies outside the blockchain network [67, 68]. These vulnerabilities can be catastrophic because they occur where the blockchain and its clients interact, such as user devices or interfaces.
- **Vendors [56]:** When new products enter the market, a security risk known as vendor risk also emerges. Many vendors have limited resources and may focus on only a few security risks, such as untested or poorly coded elements, potentially leaving their code vulnerable to bugs or relying on outdated infrastructure. This raises concerns about how they can effectively protect user data from hacker intrusions.
- **Unchecked Code [69, 70]:** Blockchain is still considered highly experimental because its full capabilities are not yet fully understood. Most tech experts agree that every product associated with blockchain technology should be tested in different environments with tough scenarios before being released to the public. The cyber risks associated with blockchain can be significant and long-lasting, especially when blockchain-based technologies are launched without being fully tested on live blockchains. Some developers prioritize profit and release flawed products without adequate testing. Due to the irreversible nature of blockchain, the risks involved are also substantial.
- **Limited Access:** Limited access to digital assets is crucial in blockchain solutions. The security of assets and information relies on digital signatures, which are protected by private keys [71, 72]. These keys are used to sign transactions, which verifies the sender's identity and ensures that the transaction has not been altered. Companies must prioritize the protection and safe usage of these keys to safeguard users and their transactions.
- **Network Security:** The miners maintain the security and stability of the blockchain [73, 74]. But this holds true primarily when there is a large and decentralized group of miners. The problem arises when these miners consolidate their computational power, potentially leading to a 51% attack. In such an attack, the combined miners can gain control over the majority of the network and manipulate the blockchain network, which hampers the integrity of the system.
- **overnance:** The absence of governance within the blockchain network creates challenges, such as when adding new members or modifying existing policies. An on-chain voting mechanism provides

audit trails for governance-related documents and secure access to the processing of these documents.

- **Scalability Issues:** Scalability remains a prominent issue within blockchain technology. One solution is sharding, a method that involves dividing hashing power and storage capacity into segments across the P2P network [32]. However, sharding also has drawbacks, such as reducing the hashing power of nodes, making them more vulnerable to data breaches by hackers, and potentially leading to permanent data loss.
- **Cryptocurrency Guidelines [75] and its Tax Assessment:** For such a vast market of blockchain, certain rules and regulations must be followed. The controlling and judicial panels are facing trouble due to several new modifications and burgeoning transaction techniques.
- **Intellectual Property Rights [76]:** The creator of the blockchain keeps the basis of their work as proof of existence using its block hash value and the time of creation. In academic research, timestamps and reliable proof of research findings must be kept to ensure that the original researcher is credited even if others later modify or build upon the work.
- **Data Intrusion in Healthcare Facilities:** Despite having a lot of benefits in maintaining the patients' records using blockchain, it still poses a threat to the healthcare society [77, 78]. In the USA, data intrusion occurs now and then at a surprising rate of 40%. Most of these data intruders are medical staff working in this health facility. This implies that the more insider people access these records, the more they are encouraged to engage in data intrusion.

IV. Consensus Algorithm

The consensus mechanism plays an important role in achieving the best decision for everyone by setting the rules for how participants in the blockchain contribute. Different consensus algorithms like Proof of Authority [79], Tendermint [80], Proof of Bandwidth (PoB) [81, 40], Ripple [82], Scalable Byzantine Consensus Protocol (SCP) [83], and many more work on various principles is available to ensure the network's security and reliability. Most of the important consensus mechanisms are described in this section. A detailed comparative analysis of all consensus algorithms is illustrated in Table IV.

Table IV
Comparison of Consensus Algorithms

Con. Algo.	Setup	Mechanism	Incentives	Strengths	Weaknesses	Energy Efficiency	Scalability	Resilience to Attacks	Secure Computing Applications	Real-world Examples
PoW [84], [88]	Public/Private Blockchain	Miners solve complex computational problems to validate transactions.	Miners receive new coins and transaction fees.	High security, widely used.	High energy consumption and slower transactions.	Very Low	Low	Resistant to 51% attacks but vulnerable to double-spending.	Prevents DDoS attacks and ensures transaction integrity.	Bitcoin, Ethereum (before 2.0)
PoS [89]	Public/Private Blockchain	Validators are chosen based on the number of coins they hold.	Transaction fees and loss of stake if fraudulent.	Lower energy consumption than PoW.	Potential centralization, nothing-at-stake problem.	High	Medium	Reduced 51% attack probability.	Efficient transaction validation in a secure manner.	Ethereum 2.0, Cardano
DPoS [87]	Public/Private Blockchain	Stakeholders vote for delegates who validate transactions.	Delegates earn transaction fees and loss of reputation/ income if dishonest.	High transaction speed, more energy-efficient than PoS.	Potential for centralization, reliance on delegates.	High	Medium	Reduced 51% attack probability.	Swift and adaptive, suitable for scalable secure environments.	EOS, Lisk
LPoS [90], [91]	Public/Private Blockchain	Token holders lease their coins to validators.	Validators share rewards with those leasing coins.	Increased participation and lower entry barriers.	Relies heavily on validator performance.	High	Medium	Improves network security through distributed staking.	Facilitates broader participation in secure networks.	Waves
PoA [92]	Public/Private Blockchain	Combines PoW and PoS for mining and validation.	Miners and validators receive rewards based on mining and staking contributions.	Balanced security and energy efficiency.	Requires control over both mining and staking.	Medium	Medium	Highly resistant to 51% attacks.	Dual approach enhances secure computing reliability.	Hybrid (Theoretical)
PoI [93]	Public/Private Blockchain	Importance score based on wealth and activity.	Higher importance leads to higher rewards.	Promotes network activity and decentralization.	Favors wealthier participants.	High	Medium	Reduces Sybil attacks by considering activity.	Balances wealth and activity for secure computing.	NEM

Contd...

PoC [39], [94]	Public/Private Blockchain	Miners allocate storage space for mining.	Rewards based on storage allocated.	Energy-efficient, cost-effective.	Favors miners with large storage.	High	Medium	Potential centralization due to storage requirements.	Cost-efficient secure computing.	Burstcoin
UNL [95]	Public/Private Blockchain	Validators choose trusted lists of other validators.	Validators receive transaction fees.	Customizable, prevents network infiltration.	Depends on the integrity of chosen validators.	High	Medium	Strong defense against coordinated attacks.	Decentralized trust model enhances security.	Ripple
PBFT [96], [97]	Private Blockchain	Validates transactions through mutual agreement among nodes.	No financial incentives, used in permissioned networks.	High security, fast finality.	Communication overhead, low scalability.	Medium	Low	Resistant to Byzantine faults.	Ensures secure and reliable transactions.	Hyperledger Fabric
SCP [51], [52]	Public Blockchain	Federated Byzantine Agreement with node quorum slices.	Validators receive transaction fees.	Fast block creation, proven security.	Requires careful node selection.	High	High	High resilience when quorum is correctly configured.	Fast and secure block creation.	Stellar
dBFT [98], [99]	Public/Private Blockchain	Delegates are chosen to confirm transactions.	Delegates receive transaction fees.	Streamlined, low energy consumption.	Relies on a small group of nodes.	High	Medium	Resistant to general BFT attacks.	Efficient and secure transaction processing.	NEO
DAG [100], [101]	Public/Private Blockchain	Stores data topographically, uses side chains.	No direct financial incentives, participation required for network security.	Reduces transaction time and energy consumption.	Complex implementation, not yet widely tested.	Medium	High	Minimizes double-spend risks.	Efficiently handles complex transactions.	IOTA
PoET [102], [103]	Private/ Permissioned Blockchain	Random wait times to add blocks.	Validators receive transaction fees.	Energy-efficient, fair block creation.	Requires trusted execution environments.	High	Medium	Fair and secure prevents monopolization.	Energy-efficient and fair in permissioned networks.	Hyperledger Sawtooth
PoB [40], [81]	Public/Private Blockchain	Burns coins to increase staking power.	Stakers receive transaction fees and long-term rewards.	Discourages attacks and stabilizes the network.	Irreversible loss of coins, risk of centralization.	Medium	Medium	Enhances security by increasing attack costs.	Stabilizes and secures long-term network operation.	Slimcoin, Counterparty

(1) **Proof of Work (PoW):** It is the first and foremost consensus rule that was introduced for the blockchain network [84]. The responsibility of verifying the aggregated information lies with the miners, who sequentially verify each node. This process is known as mining. Miners are given complex arithmetic problems that require a lot of computational power to solve. PoW is widely used because it protects against DDoS attacks. A survey conducted in South Korea in 2022 illustrated that 45 % of companies developing or providing blockchain-based platforms use the PoW consensus algorithm [85].

(2) **Proof of Stake (PoS):** PoS was developed to address the limitations of PoW like the high energy consumption and time inefficiencies [86]. In PoS, miners must validate a block before it is added to the blockchain. However, unlike in PoW, miners in PoS can participate in the mining process based on the number of coins they hold.

(3) **Delegated Proof of Stake (DPoS):** It is a type of proof-of-stake with some specific changes by introducing delegates. In PoS, there are miners, while in DPoS, there are delegates [87]. In this system, stakeholders vote for a small number of delegates responsible for validating transactions and creating new blocks on behalf of the entire network. DPoS is a strong option if you're seeking a swift, productive, and distributed consensus rule.

(4) **Leased Proof of Stake (LPoS):** The Waves platform introduced LPoS as a new consensus mechanism aimed at reducing energy consumption [91]. The traditional PoS system had limitations, where only a select group of validators with a certain quantity of coins could participate in validation. With LPoS, even those with fewer resources can lease their coins to validators, allowing them to participate in the mining process and earn rewards.

(5) **Proof of Activity (PoA):** It is a hybrid consensus mechanism that combines elements from both PoW and PoS, which provide additional security against attackers and more energy efficient [104, 86]. The mining process begins with miners using PoW to mine the block header, which includes the address for the prize. However, the block is not complete at this point. Once the block header is mined, the system shifts to PoS, where a random stakeholder identified in the header is chosen to validate the transactions and finalize the block.

(6) **Proof-of-Importance (PoI):** The PoI concept was introduced by the New Economy Movement (NEM), evolving from the PoS model [86]. PoI calculates an importance score for each node based on the amount of XEM held, the number of transactions made, and the overall network activity. In this system, a node's eligibility to participate in the blockchain network depends on the frequency of harvesting activities.

(7) **Proof of Capacity (PoC):** This consensus rule is an enhancement of the PoW mechanism. The frequency of successful mining increases based on the solutions (plots) stored on the miner's system. Before mining begins, hard disk storage and computational power need to be allocated, making this process faster than PoW [39, 94]. It also addresses some of the limitations of PoW related to hashing.

(8) **Unique Node Lists (UNL):** Each validator in the blockchain network selects its own list of trusted validators, known as UNLs. Validators in this network do not trust every participant individually. Instead, they trust that the entire list of chosen validators will not collude maliciously [95]. Each validator independently selects its UNLs. An attacker cannot simply form a group to carry out an attack. They must first be included in a validator's UNL, which is possible only based on their performance.

(9) **Practical Byzantine Fault Tolerance (PBFT)**: PBFT is viewed as an improved and more practical algorithm based on Byzantine Fault Tolerance (BFT). PBFT consists of three main parts: i) Normal Case Operation: This allows the client's requests to be processed in a specific order. ii) Garbage Collection: This systematically recovers system log files in the event of any trouble. iii) View Change: It will be carried out when the primary node becomes faulty or unresponsive, allowing the replicas to choose a new primary [96].

(10) **Stellar Consensus Protocol (SCP)**: This consensus mechanism is used by Stellar Cryptocurrency, which is based on public blockchain technology [51, 52]. The majority configuration is essential for verifying the security and liveliness of SCP. SCP is a better option compared to other consensus rules for creating blocks in less time. SCP is also an extension of the Federated Byzantine Agreement (FBA) consensus rule.

(11) **Delegated Byzantine Fault Tolerance (dBFT):** dBFT was created by the Chinese company NEO, which is also known as China's

Ethereum. It streamlines the consensus process, reduces energy consumption, and enhances transaction processing speed compared to traditional BFT mechanisms [98, 99]. It uses a small group of trusted nodes, called delegates or consensus nodes, to validate and confirm transactions.

(12) **Directed Acyclic Graphs (DAG):** In most blockchains, blocks containing data are connected through a virtual chain and stored topographically. It uses the concept of 'side chains,' allowing multiple transactions to occur simultaneously on different chains, reducing both creation time and energy consumption. This structure reduces the risk of double-spend attacks by verifying the current transaction against previous transactions.

(13) **Proof of Elapsed Time (PoET):** It is a consensus rule mainly used in permissioned blockchains where users require permission to join the network [102]. The permissioned network decides the rights of miners or voting principles. For a system to run efficiently, the PoET consensus rule relies on trusted execution environments to ensure that the random wait times are genuine which ensures network transparency.

(14) **Proof-of-Burn (PoB):** This is an important consensus rule that burns a portion of coins to protect the PoW cryptocurrency. The process of burning coins occurs when users send them to an "Eater address [81, 40]". These coins cannot be spent under any circumstances by the Eater address. An Eater address doesn't have a private key, making it inaccessible because no one can spend these coins once they are inside.

V. Blockchain Applications

Blockchain is a most popular use case technological instrument used in many application areas. As of 2021 in Figure 3, 45 percent of respondents stated that their companies were working on blockchain technology to secure information exchange. Figure 4 shows distribution of the global blockchain market value worldwide. This data shows banking industry capture market share of almost 30 percent global spending on blockchain solutions. This section discusses some of the important blockchain applications with recent studies.

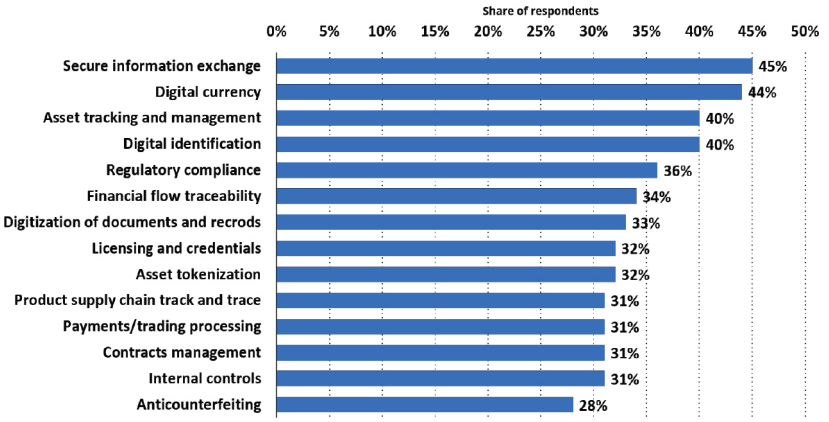

Figure 3

Blockchain technology use cases in organizations [105]

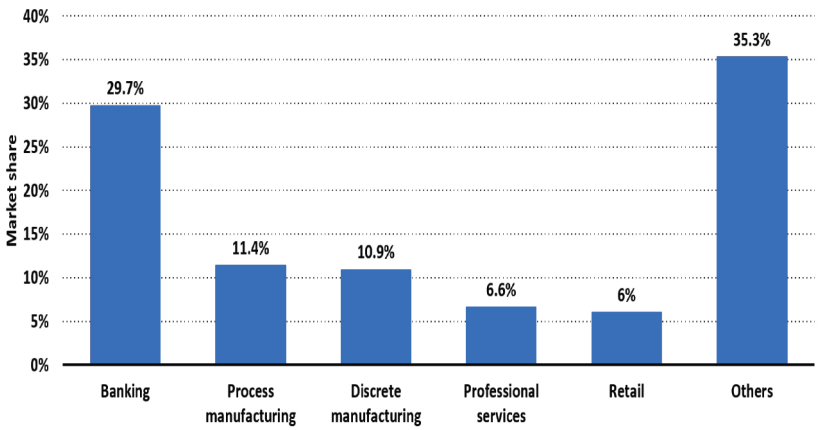

Figure 4

Distribution of blockchain market [106]

- **Delivery Services:** Blockchain technology significantly improves delivery services by enhancing traceability, lowering the risk of fraud, and producing transparent and unchangeable supply chain records. Ferrag et al. [107] present an intrusion detection system and DeliveryCoin a delivery framework based on blockchain.
- **Agriculture:** The use of blockchain technology in agriculture improves supply chain transparency, guarantees food safety, and makes smart farming and crop insurance more feasible. Ferrag et al.

[108] presented a categorization of threat models to green agriculture based on IoT into five different types. In [109], the authors present Agri-Block-IoT, an agricultural traceability solution for food supply management.

- **Traffic management:** The use of blockchain technology in traffic management contributes to increased data transparency, decreased congestion, and the guarantee of safe and decentralized traffic control. Fujihara et al. [110] proposed a distributed system using blockchain for collective traffic information sharing, traffic jams, and accidents. In [111], the authors present a blockchain-based framework called SpeedyChain for smart vehicles.
- **Food Traceability:** Transparency, safety, and quality are all ensured by using blockchain technology in food traceability. It generates immutable records and enables real-time tracking of food products from the farm to the table. Arsyad et al. [112], the authors propose a Blockchain traceability system for the production of cacao and chocolate. It gives a way to connect legal documentation with two-factored blockchain using digital watermarking. One Blockchain traces steps of documentation. The other Blockchain traces watermarking embedding.
- **Forensic Evidence:** In forensic evidence, blockchain technology allows for the creation of immutable records. Li et al. [113] presented LEChain. LEChain is a Blockchain-based rightful legal evidence management scheme to oversee complete evidence circulation. In this paper [114], the authors proposed a framework based on permissioned blockchain to manage vehicle-related data. In [115], the authors propose a blockchain-based solution named Cyber Trust Blockchain (CBT) for smart homes.
- **Online Social Networks:** The application of blockchain technology in online social networks improves data security, protects user privacy, eliminates the possibility of censorship, and promotes decentralized content sharing. Guidi et al. [116] listed several current problems of online social media platforms. As a solution to the problems, the authors propose a new model that utilizes the blockchain concept.
- **Real Estate:** The use of blockchain technology in real estate improves transparency, makes transactions more secure, automates procedures through the use of smart contracts, and eliminates fraud. Morena et al. [117] implemented blockchain technology in a real

estate environment that aims to manage the Trust tool within the Dopo di Noi project. In this paper [118], authors present Lorikeet. It is a model-driven engineering tool that can be used for the implementation of business processes on. It can automatically create well-tested smart contracts.

- **Voting:** Blockchain technology in the voting system ensures transparency and security through immutable and auditable records. In this article [16], the authors present a multichain-based system for voting in which a secure cryptographic hash is generated for every vote based on voter-related information. In this paper [119], the authors present an Auditable Blockchain Voting System (ABVS). This paper [120] presents a new e-voting procedure using blockchain as an unambiguous polling box.
- **Digital Identity Security**: The use of blockchain technology for digital identity protection preserves the integrity of data, inhibits unauthorized access, and enables decentralized, verified identity management. For instance, Digilocker, a government-verified application, allows users to store digital copies of important documents that are recognized nationwide. In [121], the authors propose a Sora Identity Mobile Application based on Blockchain technology that can make identity management more secure.
- **Healthcare:** The healthcare sector uses blockchain technology for various purposes, like storing patient data and recording information across different hospital departments [122]. In this paper [123], the authors present an application called Med Rec. It is a decentralized record management system that uses blockchain technology to handle patient's digital health records. In this paper [124], the authors have presented a model for 'Ledger of Me.' The system aims to provide well-built consent techniques for data sharing between different apps that the patients use or organizations. In this paper [125], the author discusses the Dovetail consent application that uses blockchain technology. It is a mobile-based application for patients.
- **Currency:** The implementation of blockchain technology in monetary systems ensures the creation of immutable records, the reduction of fraudulent activity, and the facilitation of decentralized control. This contributes to increased confidence and efficiency within digital financial systems [126]. Due to this feature, both merchants and customers are willing to use/accept cryptocurrencies for payments across various industries worldwide. In this paper [127], the author

discusses Libra (now known as Diem). Libra (initiated in June 2019) is a global virtual currency project. Abdullah et al. [128] presented a theoretical framework for developing a national cryptocurrency.

- **Supply Chain Management:** Blockchain technology in supply chain management improves transparency, traceability, and efficiency across the supply chain. In this paper [129], the authors proposed blockchain-enabled supply chain use cases to overcome issues like linking physical products to digital ledgers, linking blockchain-enabled networks to external markets, supporting complicated supply chain structures, and the availability of enough space to store data required by supply chains. Mondal et al. [130] proposed an IoT-based food supply chain monitoring architecture using blockchain. It uses an authentication protocol. It is based on proof-of-object, which contains physical and cyber layers.
- **Banking sector:** The bank uses blockchain technology for faster payments, clearance and settlement systems, fundraising, trade finance, asset transactions, credits and loans, digital identity verification, accounting, and P2P transfers [131, 132].
- **Music Industry:** Blockchain technology is widely used in the music industry [133, 134]. This technology supports copyright management, ensuring secure and accurate payments to the correct individuals.
- **Travel and Hospitality:** Blockchain has significantly transformed the travel and hospitality sector [135]. It handles transactions, verifying identities like passports, confirming reservations, and ensuring travel insurance. It also enhances transparency and manages rewards and loyalty programs.
- **Blockchain in Government:** Governments increasingly use blockchain technology to enhance their operations, schemes, and services [136, 137]. In this article [138], the authors discuss a blockchain-based social governance scheme to achieve real-time data resource sharing, business process optimization, and promotion of public participation.
- **Blockchain in Insurance:** Blockchain significantly benefits insurance companies by solving many of the challenges they face [139, 140, 141]. This technology enhances trust and loyalty between insurance companies and customers by streamlining the entire process, like document verification, payment issues, and mutual trust concerns.

- **Blockchain in Retail:** Blockchain technology enables retailers to track their products at every stage, from manufacturing to delivery [142, 143, 144]. By integrating blockchain into the supply chain, retailers can easily monitor the status of their products, resolve payment issues, and accurately predict delivery times. For example, Walmart collaborates with IBM on food supply management to reduce food waste, improve tracking accuracy, and enhance transparency.
- **Internet of Things (IoT):** In [145], the author presents a blockchain-based distributed access control model for permissions and roles in IoT. In [146], the authors propose a lightweight, scalable blockchain to optimize IoT requirements.
- **Energy:** A Secure Private Blockchain-based framework (SPB) presented by [41]. A Certificate of Existence (CoE) is used to verify smart meters. A security analysis of the SPB is also done in the paper. In this paper [147], a Secure Energy Trading System (SETS) is proposed. It is a blockchain-based decentralized energy trading system using smart grids and smart contracts.

VI. Attacks on Blockchain

There are various attacks on the blockchain network [148, 149]. The security threats and attacks grew over nine times between 2020 and 2021. As per the report [150], the value of crypto stolen in August 2021 accounted for 610 million U.S. dollars. The report [150] also states that between March 2020 and February 2022, 3044 million U.S. dollars were lost due to theft and blockchain attacks, and only 709 million U.S. dollars were recovered back. Some of the important attacks are discussed in this section.

(1) **Attack of 51 percent:** In a 51% attack, attackers or hackers gain control of more than 51% of the computer network or the hash power in a blockchain [151, 152].

This attack is unlikely to affect Bitcoin due to its immense hash power, making it difficult to compromise. To prevent this issue, it's crucial to ensure that no single or multiple attackers can control more than half of the system's resources.

(2) **Sybil's attack:** A sybil attack on a blockchain occurs when an attacker creates multiple fake identities or nodes to gain control over a network [34, 153]. To prevent such attacks, various consensus algorithms are employed [154]. These algorithms make it difficult for attackers to succeed. For instance, Bitcoin uses a rule where the

power to generate a new block must be proportional to the total processing power of the system. This ensures that only those with significant computing power can add blocks to the blockchain.

(3) **Denial-of-Service (DoS) Attack:** In a DoS attack, the attacker targets an online system or website with the intent to disrupt its operations. This attack is a powerful tool used to crash or hack websites by overwhelming them with excessive traffic, making them unable to handle the influx of requests [155, 156].

(4) **Eclipse attack:** In an Eclipse attack, attackers target specific users or nodes within a decentralized system rather than attacking the entire system [157, 148]. This attack exploits the fact that not all nodes in a decentralized network are connected to each other simultaneously. Instead, for efficiency, nodes are connected to specific groups of other nodes, creating isolated segments. Attackers take advantage of this by isolating a particular node or user, controlling its connections, and thereby influencing its view of the network [158].

(5) **Selfish mining attack:** Selfish mining is known as a block withholding attack. It is an attempt to undermine the integrity of blockchain technology [159, 160]. In a selfish mining attack, a miner withholds successfully mined blocks instead of broadcasting them to the network [159]. The selfish miner maintains a private chain, revealing it only when it benefits them, aiming to gain greater rewards based on their contribution to a mining pool. This tactic can involve one or more participants working together to exploit the mining process for personal gain.

(6) **Mining malware:** Cryptocurrency mining malware is a stealthy type of malware that exploits the resources of a system—such as laptops, desktops, smartphones, and other internet-connected devices to generate revenue for cyber attackers [161]. The primary symptom of this malware is a significant slowdown in system performance, as mining requires substantial processing power. If a system is infected with this malware, it will run noticeably slower due to the high demands of the mining process [161]. Table V shows the most frequently detected crypto-mining malware in worldwide regions.

(7) **Timejack attack:** In a Timejack attack, nodes or blocks within a blockchain network rely on other blocks for internal timing, which is derived from the median time reported by nodes. The attacker

Table V
Most frequently detected crypto-mining malware

Characteristic	Americas	EMEA	Asia-Pacific
XMRig	75%	69%	55%
RubyMiner	11%	8%	6%
LemonDuck	4%	5%	13%
Wannamine	1%	1%	7%
Lucifer	1%	2%	9%
Other	6%	16%	10%

typically starts with an Eclipse attack to isolate the target node. Once isolated, the target node cannot accept blocks from the original network because the block times will not align with its manipulated internal clock. This allows the attacker to manipulate transactions with the target node, as these transactions won't be submitted to the original blockchain network.

(8) **Finney attack:** The Finney attack, named after developer Hal Finney. He was the first recipient of a Bitcoin transaction and commented on its source code release [162, 163]. It is similar to a double-spending attack. This attack only works when users or account holders accept unconfirmed transactions. It requires the participation of the miner once a block has been mined. Although merchants or participants cannot entirely prevent a Finney attack by taking precautions, the attack's success depends on the miner's involvement and a specific sequence of events. This makes the Finney attack challenging for attackers to execute [162].

(9) **Parity Multisig Wallet Attack:** In this attack, the attacker sends two transactions to the targeted contracts [148]. The first transaction is designed to gain exclusive ownership of the Multisig wallet, and the second is to transfer all the funds. By manipulating these transactions, the attacker redirects all funds to a special account under their control. It's similar to going to a bank and convincing the manager to transfer ownership of a stranger's account to you, then withdrawing all the money. This is exactly what happened in the Parity Multisig wallet attack. The hacker added their account as an owner in the library contract, effectively becoming a co-owner

of all affected wallets. This allowed the attacker to manipulate transactions and transfer funds easily.

(10) **Double-spending:** Double-spending occurs when the same unit of e-currency is fraudulently spent more than once [164], typically due to the ease of copying e-currency files. However, digital currencies like cryptocurrencies are designed to prevent copying [153, 165]. Attackers may try to trick the network into accepting both transactions and double-spend the same coin before the network confirms the first transaction. To prevent such attacks, developers use cryptographic algorithms based on hash functions within blockchain technology, ensuring the integrity of transactions [33].

(11) **Decentralized Autonomous Organization (DAO) attack:** The DAO attack is one of the most significant hacks in the history of cryptocurrencies [166, 167]. A DAO is designed to codify rules, make decisions, and eliminate the need for physical documents. In this attack, the attacker identified a portion of the code where a recursive function could be executed without verifying the settlement of the current transaction. By repeatedly calling this function, the hacker was able to drain the DAO of funds by making small deposits and then withdrawing them multiple times before the system could register the transactions, allowing the attacker to siphon off a significant amount of money.

(12) **Race attack:** This attack is a slight variation of the Finney attack and occurs when an attacker creates two conflicting transactions. The first transaction is sent to a participant who accepts the payment without waiting for confirmation. Simultaneously, the attacker broadcasts a second transaction that returns the same amount of cryptocurrency to themselves, rendering the first transaction invalid. This type of double-spending attack relies on the recipient accepting unconfirmed transactions as payment [148, 163].

VII. Conclusion, limitation, and future scope

Blockchain technology is increasingly being adopted across various secure computing environments, including finance, healthcare, IoT, and cloud services. It highlights blockchain's capacity to decentralize trust, provide immutable records, and enable secure P2P transactions without intermediaries. However, due to the decentralized and complex nature of

blockchain applications, proper quantification and management are critical. This paper has provided an extensive exploration of blockchain technology's impact on secure computing environments. This paper presents a systematic review of blockchain's role in enhancing security and privacy across various secure computing environments. It highlighted key blockchain concepts such as architecture, deployment models, consensus, smart contracts, privacy-preserving mechanisms, attacks, and applications, which play a crucial role in securing transactions and data exchanges. This paper offers a comprehensive perspective, examining both technical and operational aspects of blockchain adoption. The paper also examined the various security threats and attack taxonomies related to blockchain technology. The paper also touched on several blockchain applications. The future scopes focused on developing more energy-efficient consensus algorithms and enhancing privacy through advanced cryptographic techniques. Furthermore, this work emphasizes the need for ongoing developments in blockchain technology to address open challenges like combining AI with blockchain, improving scalability and interoperability, reducing implementation costs, energy-efficient consensus algorithms, transparency, and balancing privacy with scalability. The integration of blockchain with IoT devices and healthcare systems offers opportunities for more secure data management and transactions.

REFERENCES

[1] "B2b cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025," https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide/#:~:text=The%20number%20of%20B2B%20cross,blockchain%20will%20reach%20745%20million., [Accessed 19-09-2024].

[2] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *Ieee* Access, vol. 9, pp. 61 048–61 073 (2021).

[3] L. Guo, H. Xie, and Y. Li, "Data encryption based blockchain and privacy preserving mechanisms towards big data," *Journal of Visual Communication and Image Representation*, vol. 70, p. 102741 (2020).

[4] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, "Blockchain mechanism and symmetric encryption in a wireless sensor network," *Sensors,* vol. 20, no. 10, p. 2798 (2020).

[5] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-peer Networking and Applications*, vol. 14, pp. 2901–2925 (2021).

[6] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," *The Review of Financial Studies*, vol. 32, no. 5, pp. 1754–1797 (2019).

[7] Y. Chen and C. Bellavitis, "Blockchain disruption and decentralized finance: The rise of decentralized business models," *Journal of Business Venturing Insights*, vol. 13, p. e00151 (2020).

[8] Y. Chen and C. Bellavitis, "Decentralized finance: Blockchain technology and the quest for an open financial system," *Stevens Institute of Technology School of Business Research Paper* (2019).

[9] M. Mazur and E. Polyzos, "Non-fungible tokens (nfts)," in The Elgar Companion to Decentralized Finance, Digital Assets, and Blockchain Technologies. Edward Elgar Publishing, pp. 280–297 (2024).

[10] F. Valeonti, A. Bikakis, M. Terras, C. Speed, A. Hudson-Smith, and K. Chalkias, "Crypto collectibles, museum funding and openglam: challenges, opportunities and the potential of non-fungible tokens (nfts)," *Applied Sciences*, vol. 11, no. 21, p. 9931 (2021).

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system bitcoin: A peer-to-peer electronic cash system," Bitcoin. org. Disponible en https://bitcoin. org/en/bitcoin-paper, 2009.

[12] B. Bitcoin et al., "Blockchain technology," Tech. Rep2015 (2015).

[13] "Size of the bitcoin blockchain from january 2009 to september 23, 2024," https://www.statista.com/statistics/647523/ worldwide-bitcoin-blockchain-size/, [Accessed 19-09-2024].

[14] S. Masteika, E. Rebždys, K. Driaunys, A. Šapkauskiene˙, A. Mac˘erinskiene˙, and E. Krampas, "Bitcoin double-spending risk and countermeasures at physical retail locations," *International Journal of Information Management*, vol. 79, p. 102727 (2024). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401223001081

[15] K.-Y. Kang, "Cryptocurrency and double spending history: Transactions with zero confirmation," *Economic Theory,* vol. 75, no. 2, pp. 453–491 (2023).

[16] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *International Journal of Electronic Government Research* (IJEGR), vol. 14, no. 1, pp. 53–62 (2018).

[17] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys* (CSUR), vol. 54, no. 8, pp. 1–41 (2021).

[18] M. Pacheco, G. Oliva, G. K. Rajbahadur, and A. Hassan, "Is my transaction done yet? an empirical study of transaction processing times in the ethereum blockchain platform," *ACM Transactions on Software Engineering and Methodology*, vol. 32, no. 3, pp. 1–46 (2023).

[19] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *Journal of network and computer applications,* vol. 126, pp. 45–58 (2019).

[20] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE communications surveys & tutorials,* vol. 21, no. 3, pp. 2794–2830 (2019).

[21] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets internet of things: Characteristics, challenges, and business opportunities," *Journal of industrial information integration*, vol. 15, pp. 21–28 (2019).

[22] A. Hughes, A. Park, J. Kietzmann, and C. Archer-Brown, "Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms," *Business Horizons*, vol. 62, no. 3, pp. 273–281 (2019).

[23] M. Kowalski, Z. W. Lee, and T. K. Chan, "Blockchain technology and trust relationships in trade finance," *Technological forecasting and social change*, vol. 166, p. 120641 (2021).

[24] A. Pal, C. K. Tiwari, and N. Haldar, "Blockchain for business management: Applications, challenges and potentials," The *Journal of High Technology Management Research*, vol. 32, no. 2, p. 100414 (2021).

[25] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: research and applications*, vol. 3, no. 2, p. 100067 (2022).

[26] E. A. Boakye, H. Zhao, and B. N. K. Ahia, "Emerging research on blockchain technology in finance; a conveyed evidence of bibliometric-based evaluations," *The Journal of High Technology Management Research*, vol. 33, no. 2, p. 100437 (2022).

[27] P. Hanafizadeh and M. Alipour, "Taxonomy of theories for blockchain applications in business and management," *Digital Business,* vol. 4, no. 2, p. 100080 (2024).

[28] A. El Bekkali, M. Essaaidi, and M. Boulmalf, "A blockchain-based architecture and framework for cybersecure smart cities," *IEEE Access* (2023).

[29] T. A. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE access,* vol. 7, pp. 176 838–176 869 (2019).

[30] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things," *Journal of Industrial Information Integration*, vol. 21, p. 100190 (2021).

[31] L. Zhao, S. Sen Gupta, A. Khan, and R. Luo, "Temporal analysis of the entire ethereum blockchain network," in Proceedings of the Web Conference 2021, pp. 2258–2269 (2021).

[32] T. Wang, C. Zhao, Q. Yang, S. Zhang, and S. C. Liew, "Ethna: Analyzing the underlying peer-to-peer network of ethereum blockchain," *IEEE Transactions on Network Science and Engineering,* vol. 8, no. 3, pp. 2131–2146 (2021).

[33] N. A. Akbar, A. Muneer, N. ElHakim, and S. M. Fati, "Distributed hybrid double-spending attack prevention mechanism for proof- of-work and proof-of-stake blockchain consensuses," *Future Internet*, vol. 13, no. 11, p. 285 (2021).

[34] M. Platt and P. McBurney, "Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance," *Algorithms*, vol. 16, no. 1, p. 34 (2023).

[35] N. Storublevtcev, "Cryptography in blockchain," in Computational Science and Its Applications–ICCSA 2019: 19th International Conference, Saint Petersburg, Russia, July 1–4, 2019, Proceedings, Part II 19. Springer, pp. 495–508 (2019).

[36] A. Kuznetsov, I. Oleshko, V. Tymchenko, K. Lisitsky, M. Rodinko, and A. Kolhatin, "Performance analysis of cryptographic hash functions suitable for use in blockchain," *International Journal of Computer Network & Information Security*, vol. 13, no. 2, pp. 1–15 (2021).

[37] P. Vats, S. K. Vats, and P. Peddi, "Unveiling crypto analysis secrets: A comprehensive analysis of smart contract security within blockchain network environments," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 4, pp. 1121–1128 (2024).

[38] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," pp. 355–364 (2017).

[39] X. Wang, W. Ni, X. Zha, G. Yu, R. P. Liu, N. Georgalas, and A. Reeves, "Capacity analysis of public blockchain," *Computer Communications*, vol. 177, pp. 112–124 (2021).

[40] Monika and R. Bhatia, "Cross-blockchain decentralized asset transfer protocol for public blockchains," *International Journal of Communication Systems*, vol. 37, no. 6, p. e5709 (2024).

[41] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak, and Z. Y. Dong, "Spb: A secure private blockchain-based solution for distributed energy trading," *IEEE Communications Magazine,* vol. 57, no. 7, pp. 120–126 (2019).

[42] R. Yang, R. Wakefield, S. Lyu, S. Jayasuriya, F. Han, X. Yi, X. Yang, G. Amarasinghe, and S. Chen, "Public and private blockchain in construction business process and information integration," *Automation in construction*, vol. 118, p. 103276 (2020).

[43] C. V. Helliar, L. Crawford, L. Rocca, C. Teodori, and M. Veneziani, "Permissionless and permissioned blockchain diffusion," *International Journal of Information Management*, vol. 54, p. 102136 (2020).

[44] H. W. Marar and R. W. Marar, "Hybrid blockchain," *Jordanian Journal of Computers and Information Technology* (JJCIT), vol. 6, no. 04 (2020).

[45] Z. Ge, D. Loghin, B. C. Ooi, P. Ruan, and T. Wang, "Hybrid blockchain database systems: design and performance," *Proceedings of the VLDB Endowment*, vol. 15, no. 5, pp. 1092–1104 (2022).

[46] I. Tarkhanov, D. Fomin-Nilov, and M. Fomin, "Application of public blockchain to control the immutability of data in online scientific periodicals," *Library Hi Tech*, vol. 37, no. 4, pp. 829–844 (2019).

[47] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized public key infrastructures atop blockchain," *IEEE Network,* vol. 34, no. 6, pp. 133–139 (2020).

[48] J. Shu, X. Zou, X. Jia, W. Zhang, and R. Xie, "Blockchain-based decentralized public auditing for cloud storage," *IEEE Transactions on Cloud Computing*, vol. 10, no. 4, pp. 2366–2380 (2021).

[49] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustišek, "Towards decentralized iot security enhancement: A blockchain approach," *Computers & Electrical Engineering,* vol. 72, pp. 266–273 (2018).

[50] M. Zachariadis, G. Hileman, and S. V. Scott, "Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services," *Information and organization*, vol. 29, no. 2, pp. 105–117 (2019).

[51] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in 2017 4th international conference on advanced computing and communication systems (ICACCS). *IEEE*, pp. 1–5 (2017).

[52] C. Cachin and M. Vukolic´, "Blockchain consensus protocols in the wild," arXiv preprint arXiv:1707.01873 (2017).

[53] Z. Zhang, F. Zou, J. Hong, L. Chen, and P. Yi, "Detection and analysis of broken access control vulnerabilities in app-cloud interaction in iot," *IEEE Internet of Things Journal* (2024).

[54] R. Anderson, "Why cryptosystems fail," in Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 215–227 (1993).

[55] Z. Li, X. Liu, W. M. Wang, A. Vatankhah Barenji, and G. Q. Huang, "Ckshare: secured cloud-based knowledge-sharing blockchain for injection mold redesign," *Enterprise Information Systems,* vol. 13, no. 1, pp. 1–33 (2019).

[56] E. Zamani, Y. He, and M. Phillips, "On the security risks of the blockchain," *Journal of Computer Information Systems*, vol. 60, no. 6, pp. 495–506 (2020).

[57] D. He, R. Wu, X. Li, S. Chan, and M. Guizani, "Detection of vulnerabilities of blockchain smart contracts," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12 178–12 185 (2023).

[58] A. Hamdi, L. Fourati, and S. Ayed, "Vulnerabilities and attacks assessments in blockchain 1.0, 2.0 and 3.0: tools, analysis and countermeasures," *International Journal of Information Security*, vol. 23, no. 2, pp. 713–757 (2024).

[59] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing security and privacy issues of iot using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 881–888 (2020).

[60] O. T. Ten, "Top 10 Web Application Security Risks," https://owasp.org/www-project-top-ten/#, 2024, [Online; accessed 19-July-2024].

[61] OWASP Top Ten, "OWASP Top Ten | OWASP Foundation," https://owasp.org/www-project-top-ten/, [Accessed 10-09-2024].

[62] S. N. Wolfson, "Bitcoin: the early market," *Journal of Business & Economics Research* (Online), vol. 13, no. 4, p. 201 (2015).

[63] C. K. Elwell, M. M. Murphy, M. V. Seitzinger, and E. V. Murphy, "Bitcoin: Questions, answers, and analysis of legal issues," (2013).

[64] B.Times, "Australian Bitcoin bank hacked: $1m+ stolen," https://www.brisbanetimes.com.au/technology/ australian-bitcoin-bank-hacked-1m-stolen-20131108-hv2iv.html, 2013, [Online; accessed 19-July-2024].

[65] A. Bhardwaj and S. Goundar, "Attack vectors for blockchain and mapping owasp vulnerabilities to smart contracts," in Blockchain Technologies, Applications and Cryptocurrencies: Current Practice and Future Trends. World Scientific, pp. 139–156 (2021).

[66] H. Poston, "Mapping the owasp top ten to blockchain," *Procedia Computer Science*, vol. 177, pp. 613–617 (2020).

[67] M. A. F. Noor and K. Mustafa, "A systematic literature review on endpoint vulnerabilities of blockchain applications," *International Journal of Advanced Technology and Engineering Exploration*, vol. 10, no. 109, p. 1666 (2023).

[68] M. A. F. Noor and K. Mustafa, "A taxonomy of endpoint vulnerabilities and affected blockchain architecture layers," *Concurrency and Computation: Practice and Experience*, p. e8158.

[69] G. Yu, S. Zhao, C. Zhang, Z. Peng, Y. Ni, and X. Han, "Code is the (f) law: Demystifying and mitigating blockchain inconsistency attacks caused by software bugs," in IEEE INFOCOM 2021-IEEE Conference on Computer Communications. *IEEE*, pp. 1–10 (2021).

[70] Z. Wan, D. Lo, X. Xia, and L. Cai, "Bug characteristics in blockchain systems: a large-scale empirical study," in 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR). *IEEE*, pp. 413–424 (2017).

[71] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2020, pp. 1–15 (2020).

[72] S. Thompson, "The preservation of digital signatures on the blockchain," See Also, no. 3 (2017).

[73] Q. Bai, Y. Xu, N. Liu, and X. Wang, "Blockchain mining with multiple selfish miners," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3116–3131 (2023).

[74] Priyanka, B. Keswani, and R. Hussain, "Blockchain-based cryptography model to preserve privacy for smart contracts," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 8, pp. 2279–2289 (2021).

[75] M. Hougan and D. Lawant, Cryptoassets: The guide to bitcoin, blockchain, and cryptocurrency for investment professionals. CFA Institute Research Foundation (2021).

[76] B. Singh and A. K. Tripathi, "Blockchain technology and intellectual property rights." *Journal of Intellectual Property Rights*, vol. 24 (2019).

[77] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, and A. N. Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in iot-enabled healthcare system," *Journal of Parallel and Distributed Computing*, vol. 172, pp. 69–83 (2023).

[78] A. A. Khan, S. Bourouis, M. M. Kamruzzaman, M. Hadjouni, Z. A. Shaikh, A. A. Laghari, H. Elmannai, and S. Dhahbi, "Data security in healthcare industrial internet of things with blockchain," *IEEE Sensors Journal*, vol. 23, no. 20, pp. 25 144–25 151 (2023).

[79] OpenEthereum, "Proof of Authority Chain," https://openethereum.github.io/Proof-of-Authority-Chains, 2023, [Online; accessed 19- August-2024].

[80] J. Kwon, "Tendermint: Consensus without mining," Draft v. 0.6, fall, vol. 1, no. 11, pp. 1–11 (2014).

[81] M. Rodinko, R. Oliynykov, and A. Nastenko, "Decentralized proof-of-burn auction for secure cryptocurrency upgrade," *Blockchain: Research and Applications*, vol. 5, no. 1, p. 100170 (2024).

[82] D. Schwartz, N. Youngs, A. Britto et al., "The ripple protocol consensus algorithm," *Ripple Labs Inc White Paper*, vol. 5, no. 8, p. 151 (2014).

[83] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, "Scp: A computationally-scalable byzantine consensus protocol for blockchains," Cryptology ePrint Archive (2015).

[84] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm," Computer Networks, vol. 214, p. 109118 (2022).

[85] "Distribution of consensus algorithms offered by companies providing blockchain-based platforms in south korea in 2021," https://www.statista.com/statistics/1260566/south-korea-consensus-algorithms-of-blockchain-companies-by-type/, [Accessed 19-09-2024].

[86] S. Fahim, S. K. Rahman, and S. Mahmood, "Blockchain: A comparative study of consensus algorithms pow, pos, poa, pov," *Int. J. Math. Sci. Comput,* vol. 3, pp. 46–57 (2023).

[87] R. Huang, X. Yang, and P. Ajay, "Consensus mechanism for software-defined blockchain in internet of things," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 52–60 (2023).

[88] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of proof of work (pow) blockchains security network on selfish mining," in 2018 International seminar on research of information technology and intelligent systems (ISRITI). *IEEE*, pp. 126–130 (2018).

[89] R. Asif and S. R. Hassan, "Shaping the future of ethereum: Exploring energy consumption in proof-of-work and proof-of-stake consensus," Frontiers in Blockchain, vol. 6, p. 1151724 (2023).

[90] J. Aki, "Leased Proof-of-Stake (LPoS)," https://www.techopedia.com/definition/leased-proof-of-stake-lpos (2023), [Online; accessed 19-July-2024].

[91] U. Pavloff, Y. Amoussou-Guenou, and S. Tucci-Piergiovanni, "Ethereum proof-of-stake under scrutiny," in Proceedings of the 38th *ACM/SIGAPP Symposium on Applied Computing*, pp. 212–221 (2023).

[92] S. Seth, "Proof-of-Activity: What It Is, How It Works, and Example," https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp#, 2024, [Accessed 19-09-2024].

[93] "Proof-of-Importance (PoI) |Finance Magnates," https://www.financemagnates.com/terms/p/proof-of-importance-poi/, [Accessed 19- 09-2024].

[94] X. Wang, G. Yu, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, K. Zheng, and X. Niu, "Capacity of blockchain based internet-of-things: Testbed and analysis," *Internet of Things,* vol. 8, p. 100109 (2019).

[95] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375 (2018).

[96] Y. Li, L. Qiao, and Z. Lv, "An optimized byzantine fault tolerance algorithm for consortium blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2826–2839 (2021).

[97] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, "Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain," *ACM Transactions on Internet Technology* (TOIT), vol. 21, no. 1, pp. 1–17 (2021).

[98] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE access*, vol. 7, pp. 118 541–118 555 (2019).

[99] Y. Zhan, B. Wang, R. Lu, and Y. Yu, "Drbft: Delegated randomization byzantine fault tolerance consensus protocol for blockchains," *Information Sciences*, vol. 559, pp. 8–21 (2021).

[100] B. Wang, M. Dabbaghjamanesh, A. Kavousi-Fard, and S. Mehraeen, "Cybersecurity enhancement of power trading within the networked microgrids based on blockchain and directed acyclic graph approach," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 7300–7309 (2019).

[101] S. Ko, K. Lee, H. Cho, Y. Hwang, and H. Jang, "Asynchronous federated learning with directed acyclic graph-based blockchain in edge computing: Overview, design, and challenges," *Expert Systems with Applications*, vol. 223, p. 119896 (2023).

[102] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in Stabilization, Safety,

and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19. Springer, pp. 282–297 (2017).

[103] A. A. Khan, S. Dhabi, J. Yang, W. Alhakami, S. Bourouis, and L. Yee, "B-lpoet: A middleware lightweight proof-of-elapsed time (poet) for efficient distributed transaction execution and security on blockchain using multithreading technology," *Computers and Electrical Engineering*, vol. 118, p. 109343 (2024).

[104] D. Wang, C. Jin, H. Li, and M. Perkowski, "Proof of activity consensus algorithm based on credit reward mechanism," in Web Information Systems and Applications: 17th International Conference, WISA 2020, Guangzhou, China, September 23–25, 2020, Proceedings 17. Springer, pp. 618–628 (2020).

[105] "Blockchain technology use cases in organizations worldwide as of 2021," https://www.statista.com/statistics/878732/ worldwide-use-cases-blockchain-technology/, [Accessed 19-09-2024].

[106] "Distribution of blockchain market value worldwide in 2020," https://www.statista.com/statistics/804775/ worldwide-market-share-of-blockchain-by-sector/, [Accessed 19-09-2024].

[107] M. A. Ferrag and L. Maglaras, "Deliverycoin: An ids and blockchain-based delivery framework for drone-delivered services," *Computers*, vol. 8, no. 3, p. 58 (2019).

[108] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE access*, vol. 8, pp. 32 031–32 053 (2020).

[109] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in agri-food supply chain management: A practical implementation," in 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany). *IEEE*, pp. 1–4 (2018).

[110] A. Fujihara, "Proposing a system for collaborative traffic information gathering and sharing incentivized by blockchain technology," in International Conference on Intelligent Networking and Collaborative Systems. Springer, pp. 170–182 (2018).

[111] R. A. Michelin, A. Dorri, M. Steger, R. C. Lunardi, S. S. Kanhere, R. Jurdak, and A. F. Zorzo, "Speedychain: A framework for decoupling data from blockchain for smart cities," in Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, pp. 145–154 (2018).

[112] A. A. Arsyad, S. Dadkhah, and M. Köppen, "Two-factor blockchain for traceability cacao supply chain," in International Conference on Intelligent Networking and Collaborative Systems. Springer, pp. 332–339 (2018).

[113] M. Li, C. Lal, M. Conti, and D. Hu, "Lechain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Generation Computer Systems*, vol. 115, pp. 406–420 (2021).

[114] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 50–57 (2018).

[115] S. Brotsis, N. Kolokotronis, K. Limniotis, S. Shiaeles, D. Kavallieros, E. Bellini, and C. Pavué, "Blockchain solutions for forensic evidence preservation in iot environments," in 2019 IEEE Conference on Network Softwarization (NetSoft). *IEEE*, pp. 110–114 (2019).

[116] B. Guidi, "When blockchain meets online social networks," *Pervasive and Mobile Computing*, vol. 62, p. 101131 (2020).

[117] M. Morena, T. Truppi, A. S. Pavesi, G. Cia, J. Giannelli, and M. Tavoni, "Blockchain and real estate: Dopo di noi project," *Property Management* (2020).

[118] A. B. Tran, Q. Lu, and I. Weber, "Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management." in BPM (Dissertation/Demos/Industry), pp. 56–60 (2018).

[119] M. Pawlak, J. Guziur, and A. Poniszewska-Maran´da, "Voting process with blockchain technology: auditable blockchain voting system," in International Conference on Intelligent Networking and Collaborative Systems. Springer, pp. 233–244 (2018).

[120] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). *IEEE*, pp. 1561–1567 (2018).

[121] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identity on the blockchain," in 2018 ieee 42nd annual computer software and applications conference (compsac), vol. 2. *IEEE*, pp. 582–587 (2018).

[122] J. Andrew, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *Journal of Network and Computer Applications*, vol. 215, p. 103633 (2023).

[123] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare:"medrec" prototype for electronic health records and medical research data," in Proceedings of IEEE open & big data conference, vol. 13, p. 13 (2016).

[124] G. Leeming, J. Cunningham, and J. Ainsworth, "A ledger of me: personalizing healthcare using blockchain technology," *Frontiers in medicine,* vol. 6, p. 171 (2019).

[125] G. Despotou, J. Evans, W. Nash, A. Eavis, T. Robbins, and T. N. Arvanitis, "Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the dovetail digital consent application: A cross sectional exploratory study," *Digital Health*, vol. 6, p. 2055207620924949 (2020).

[126] M. Pineda, D. Jabba, and W. Nieto-Bernal, "Blockchain architectures for the digital economy: Trends and opportunities," *Sustainability,* vol. 16, no. 1, p. 442 (2024).

[127] V. Brühl, "Libra—a differentiated view on facebook's virtual currency project," *Intereconomics,* vol. 55, no. 1, pp. 54–61 (2020).

[128] A. Abdullah, R. M. Nor et al., "A framework for the development of a national crypto-currency," *International Journal of Economics and Finance*, vol. 10, no. 9, pp. 14–25 (2018).

[129] A. Jabbari and P. Kaminsky, "Blockchain and supply chain management," Department of Industrial Engineering and Operations Research University of California, Berkeley (2018).

[130] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired rfid-based information architecture for food supply chain," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 5803–5813 (2019).

[131] Q. Gan and R. Y. K. Lau, "Trust in a 'trust-free'system: Blockchain acceptance in the banking and finance sector," *Technological Forecasting and Social Change*, vol. 199, p. 123050 (2024).

[132] H. O. Mbaidin, M. A. Alsmairat, and R. Al-Adaileh, "Blockchain adoption for sustainable development in developing countries: Challenges and opportunities in the banking sector," *International Journal of Information Management Data Insights,* vol. 3, no. 2, p. 100199 (2023).

[133] A. Taghdiri, "How blockchain technology can revolutionize the music industry," *Harv. J. Sports & Ent. L.*, vol. 10, p. 173 (2019).

[134] B. Rosenblatt, "The future of blockchain technology in the music industry," *Ent. & Sports Law.,* vol. 35, p. 12 (2019).

[135] A. Khanna, A. Sah, T. Choudhury, and P. Maheshwari, "Blockchain technology for hospitality industry," in Information Systems: 17th European, Mediterranean, and Middle Eastern Conference, EMCIS 2020, Dubai, United Arab Emirates, November 25–26, 2020, Proceedings 17. Springer, pp. 99–112 (2020).

[136] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—use cases, security benefits and challenges," in 2018 15th Learning and Technology Conference (L&T). *IEEE*, pp. 112–119 (2018).

[137] H. Hou, "The application of blockchain technology in e-government in china," in 2017 26th international conference on computer communication and networks (ICCCN). *IEEE*, pp. 1–4 (2017).

[138] Q. Wang, F. Geng, P. Zhang, Y. Chen, L. He, and S. Cheng, "A social governance scheme based on blockchain," in Journal of Physics: Conference Series, vol. 1621, no. 1. IOP Publishing, p. 012103 (2020).

[139] H. Kantur and C. Bamuleseyo, "How smart contracts can change the insurance industry: Benefits and challenges of using blockchain technology," (2018).

[140] A. A. Amponsah, F. A. Adebayo, and B. A. WEYORI, "Blockchain in insurance: Exploratory analysis of prospects and threats," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 1 (2021).

[141] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE access,* vol. 7, pp. 36 500–36 515 (2019).

[142] M. H. Miraz, M. G. Hassan, and K. I. Mohd Sharif, "Factors affecting implementation of blockchain in retail market in malaysia," *International Journal of Supply Chain Management* (IJSCM), vol. 9, no. 1, pp. 385–391 (2020).

[143] S. Mukherjee, M. M. Baral, B. L. Lavanya, R. Nagariya, B. Singh Patel, and V. Chittipaka, "Intentions to adopt the blockchain: investigation of the retail supply chain," *Management Decision*, vol. 61, no. 5, pp. 1320–1351 (2023).

[144] R. M. A. Latif, M. Farhan, O. Rizwan, M. Hussain, S. Jabbar, and S. Khalid, "Retail level blockchain transformation for product supply chain using truffle development platform," *Cluster computing*, vol. 24, pp. 1–16 (2021).

[145] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195 (2018).

[146] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Lsb: A lightweight scalable blockchain for iot security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197 (2019).

[147] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "When blockchain meets smart grid: Secure energy trading in demand response management," *IEEE Network*, vol. 34, no. 5, pp. 299–305 (2020).

[148] S. Aggarwal and N. Kumar, "Attacks on blockchain," in Advances in computers. Elsevier, vol. 121, pp. 399–410 (2021).

[149] T. Guggenberger, V. Schlatt, J. Schmid, and N. Urbach, "A structured overview of attacks on blockchain systems." PACIS, p. 100 (2021).

[150] "Total value of cryptocurrency lost to and recovered from theft and other attacks between march 2020 and february 2022," https: // www.statista.com/statistics/1285057/crypto-theft-size/, [Accessed 19-09-2024].

[151] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied sciences*, vol. 9, no. 9, p. 1788 (2019).

[152] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% attack on blockchains: A mining behavior study," *IEEE access*, vol. 9, pp. 140 549–140 564 (2021).

[153] S. Zhang and J.-H. Lee, "Double-spending with a sybil attack in the bitcoin decentralized network," *IEEE transactions on Industrial Informatics*, vol. 15, no. 10, pp. 5715–5722 (2019).

[154] P. Otte, M. de Vos, and J. Pouwelse, "Trustchain: A sybil-resistant scalable blockchain," *Future Generation Computer Systems*, vol. 107, pp. 770–780 (2020).

[155] B. Rodrigues, E. Scheid, C. Killer, M. Franco, and B. Stiller, "Blockchain signaling system (bloss): cooperative signaling of distributed denial-of-service attacks," *Journal of Network and Systems Management*, vol. 28, no. 4, pp. 953–989 (2020).

[156] R. Singh, S. Tanwar, and T. P. Sharma, "Utilization of blockchain for mitigating the distributed denial of service attacks," *Security and Privacy*, vol. 3, no. 3, p. e96 (2020).

[157] G. Xu, B. Guo, C. Su, X. Zheng, K. Liang, D. S. Wong, and H. Wang, "Am i eclipsed? a smart detector of eclipse attacks for ethereum," *Computers & Security*, vol. 88, p. 101604 (2020).

[158] Q. Dai, B. Zhang, and S. Dong, "Eclipse attack detection for blockchain network layer based on deep feature extraction," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 1451813 (2022).

[159] Z. Wang, Q. Lv, Z. Lu, Y. Wang, and S. Yue, "Forkdec: accurate detection for selfish mining attacks," *Security and Communication Networks*, vol. 2021, no. 1, p. 5959698 (2021).

[160] Q. Wang, T. Xia, D. Wang, Y. Ren, G. Miao, and K.-K. R. Choo, "Sdos: Selfish mining-based denial-of-service attack," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3335–3349 (2022).

[161] R. Zheng, Q. Wang, J. He, J. Fu, G. Suri, and Z. Jiang, "Cryptocurrency mining malware detection based on behavior pattern and graph neural network," *Security and Communication Networks*, vol. 2022, no. 1, p. 9453797 (2022).

[162] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID). *IEEE*, pp. 458–467 (2017).

[163] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A

comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008 (2020).

[164] Y. Li and C.-C. Wang, "A search-theoretic model of double-spending fraud," *Journal of Economic Dynamics and Control*, vol. 142, p. 104157 (2022).

[165] A. Begum, A. Tareq, M. Sultana, M. Sohel, T. Rahman, and A. Sarwar, "Blockchain attacks analysis and a model to solve double spending attack," *International Journal of Machine Learning and Computing*, vol. 10, no. 2, pp. 352–357 (2020).

[166] C. Jentzsch, "Decentralized autonomous organization to automate governance," White paper, November (2016).

[167] J. Scharfman, "Decentralized autonomous organization (dao) fraud, hacks, and controversies," in The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks. Springer, pp. 65–106 (2024).

Received October, 2024