Blockchain

İrem Şahar[1]
21050141024

Sema Nur Yılmaz[2]
22050111020

Aybüke Karaçavuş[3]
22050111005

Aglız Nisa Güner[4]
22050151001

ABSTRACT

Blockchain technology has become a powerful force in various industries, offering decentralized and secure solutions for data storage and transaction management. Despite its advantages, blockchain systems face significant challenges, especially in terms of security, interoperability and resilience.This paper presents a comparative analysis of nine recent studies related to blockchain security, interoperability and resilience and their applications in different environments. We focused on systematically review the main contribution of each work, compare their proposed methods, and highlight their strengths and weaknesses. These findings suggest that these paper will provide a comprehensive understanding of the current state and future directions for blockchain research.

CCS Concepts

- ***Computer systems organization→Distributed architectures → Peer-to-peer architectures***
- ***Information systems → Information storage systems → Blockchain-based systems***
- ***Security and privacy → Distributed systems security***

Keywords

Blockchain; security; privacy; interoperability; cryptocurrency; blockchain applications; distributed systems; cryptography.

1. INTRODUCTION

A blockchain is a continuous and organized chain that follows specific rules. As we can understand from the name, this technology is like a chain of blocks linked to each other. Each block contains certain information, its own hash value and the hash of the previous block. This relationship helps to make the chain secure and easily verifiable. If someone wants to change information or data in one block, its hash will change along with it, then all subsequent blocks must also be changed. Also, copies of the blockchain are stored on many different computers, making it even more difficult to attack or change.

The concept of secured chain of blocks is not a new idea. It was presented by Stuart Haber *et al.* in 1991 as a means to digitally timestamp electronic documents to protect against tempering . However, it gained popularity in the recent years when used in Blockchain technology to store transactions of a crypto currency called “Bitcoin” [2]

There are different types of blockchain. Public blockchain - fully open, anyone can join and participate in its management. Private blockchain - closed, available only to invited members of the same organization. Consortium (federated) blockchain - something in between: several organizations manage the network together, and only selected participants get access. Blockchain's capabilities are attributed to its important properties: decentralization, anonymity, transparency, immutability of data, data verifiability, reliability and security.

Although blockchain has become very popular, it still faces significant challenges, especially regarding security and privacy. Therefore, ongoing research is crucial to improve blockchain technologies and find solutions for these open issues. In the following sections, we will discuss the structure, types, applications, and current challenges of blockchain technology in more detail. Moreover, we will analyze different scientific research papers related to this topic and will evaluate their contribution in the development of this technology and to identify whether the solutions to the blockchain problems proposed in these articles are effective.

1.1 Motivation

Blockchain began to enter our lives as the world changed and technology evolved. We first started hearing about this technology in the context of bitcoin and cryptocurrency. But after time it can also be used for many other things, like voting, IoT, keeping medical records, or tracking goods in a supply chain. Researchers, companies, and universities are studying blockchain more and more. They believe it will make a big difference in how we live, work, and communicate. In the future, blockchain could change the way we buy things, sign contracts, and even share personal information online. So, blockchain is a powerful technology that will continue to grow. It has already changed some parts of our lives, and it will probably change even more in the next few years.

Unfortunately, this technology faces challenges such as scalability, high power consumption and a lack of clear legal regulations. These challenges are also motivation to continue research to better understand how blockchain can be developed and applied in different areas.

We can already say that blockchain is our future, so we should already have a better understanding of its architecture, how secure it is in terms of securing information, and examples of how it is already being used in different areas of life.

1.2 Organization

This paper is organized as follows:

Section 2 reviews the major contributions of recent studies on blockchain technology, focusing on aspects such as security, interoperability, and sustainability and usage of blockchain in different areas as Bitcoin, IoT. Section 3 analyzes the methodologies of each paper to to understand the main aspects

and challenges of blockchain, as well as the proposed solutions. Section 4 provides a comparative discussion that highlights the similarities, differences, and unique approaches among the studies. Section 5 presents the summarized results and key insights obtained from the analysis. 6 concludes the paper by discussing overall findings and suggesting future directions for blockchain research. Section

1.3 Contributions

The key contributions of this paper are:

1. Reviewing recent research papers that focus on security, interoperability, and resilience challenges in blockchain technology, as well as its applications in different fields.
2. Analyzing the methods these studies use to address important problems in blockchain systems.
3. Comparing the reviewed papers by highlighting their strengths, weaknesses, and unique ideas.
4. Summarizing the key results and conclusions to help guide future research on blockchain security and resilience.

2. MAJOR CONTRIBUTIONS OF EACH PAPER

This section outlines the primary contributions of each paper, categorizing them into three key areas: surveys of blockchain technology, security and privacy aspects of blockchain, and blockchain technology's applications. By summarizing the core focus of each study, we aim to provide a clear understanding of the diverse research landscape within the field of blockchain technology.

2.1 Survey on Blockchain Technology

2.1.1 A Survey on Blockchain Technology: Evolution, Architecture and Security

This article provides a comprehensive review of blockchain technology by exploring its historical development, technical architecture, consensus mechanisms, development frameworks, and security issues. Unlike previous surveys that tend to focus on isolated aspects such as cryptocurrencies or specific applications, this paper uniquely synthesizes the complete evolution of blockchain—from Blockchain 1.0 (cryptocurrencies) to Blockchain 3.0 (broader applications like IoT and healthcare). It systematically analyzes various types of blockchains (public, private, consortium), compares leading blockchain development frameworks and categorizes consensus algorithms in detail. Moreover, it sheds light on critical security vulnerabilities and open research challenges. The significant contribution of this survey lies in its holistic approach, bringing together technical, architectural, and security dimensions of blockchain in a single resource, thus serving as a valuable foundation for researchers and practitioners aiming to understand or improve upon blockchain technologies.

2.1.2 A survey on blockchain technology and its security

This paper presents research on blockchain with particular relevance to the study and advancement of secure technologies. The authors begin by explaining the fundamental properties of blockchain systems, such as decentralisation, integrity, immutability, verification, anonymity, auditability, transparency and fault tolerance. These properties are provided by a combination of cryptographic techniques and distributed consensus protocols.

The paper then goes on describing the historical path of blockchain technology's development [14] from the early concepts proposed by Chaum in 1982 up to newest discoveries such as Bitcoin, Etherium and Hyperledger. For sure, authors give us technical explanation of the main components of blockchain systems, focusing on coordinated algorithms such as PoW, PoS, DPO, PBFT, DAG and PoET, smart contracts and cryptographic primitives, including public key infrastructure, zero-disclosure proofs and hash functions.These algorithms are evaluated on multiple parameters [15]: throughput (TPS), block confirmation latency, energy efficiency, susceptibility to attacks (e.g. 51%) and scalability. It is indicated which ones are suitable for public blockchains (Bitcoin, Ethereum), enterprise solutions (Hyperledger Fabric) or hybrid systems. The technical limitations of each algorithm are also outlined, such as the high power consumption of PoW or possible centralisation in DPoS.To better understand this real-life technology, the authors describe real-world blockchain applications covering cryptocurrencies, supply chain systems, e-government services (e.g., Smart Dubai), finance, healthcare, identity management, and more.

The central contribution of the paper is a systematic classification of security threats to blockchain systems. The threats are categorised into six categories: Network attacks (e.g. DDoS, BGP hijacking, eclipse attacks); endpoint vulnerabilities (malware-infected wallets, cryptojacking); intentional misuse (51% attacks, Sybil attacks); bugs in smart contract code (logical vulnerabilities, uninitialised variables); data leaks (key compromise, metadata analysis); human error (configuration errors, lack of monitoring). This framework is supported by analyses of more than 20 real incidents: DAO, Parity, Bitfloor, Spankchain and others, with year, vulnerability, attack vector and loss estimates. Now, having analyzed the attacks and possible threats, researchers are evaluating various security tools and frameworks that are aimed at identifying, analyzing, and eliminating blockchain vulnerabilities.

Of course, as in many studies, the authors of this paper provide a broad overview of blockchain applications in the real world[16]: cryptocurrencies, supply chains (VeChain), electronic voting, medical data storage, copyright, digital identity, IoT and government services (e.g. Smart Dubai initiative). This emphasises the growing role of blockchain beyond the financial sector and the relevance of security issues across industries.

The paper concludes by highlighting current challenges and emerging research directions such as scalability, secure software development, privacy preservation, quantum computing threats, anomaly detection and global standardisation.

2.1.3 The good, the bad and the ugly: An overview of the sustainability of blockchain technology

This study makes a significant contribution to the literature by analyzing the sustainability of proof-of-work (PoW) based blockchain technology. It evaluates the social, environmental, and economic dimensions of blockchain in three phases: the good, the bad, and the ugly. Good blockchain refers to how the technology can enhance society, Bad blockchain addresses the environmental pollution that may result from crypto mining, Ugly blockchain examines how mining may affect the future and very nature of blockchain technology.

The study references the United Nations' Sustainable Development Goals report[23], which emphasizes that by providing decentralized, incorruptible, and transparent records, blockchain technology can help to reduce fraud (goals 8, 10), improve food trust (goals 2, 3, 12), and enhance carbon emission trading and facilitate clean energy trading (goals 7, 13).

The article discusses how cryptocurrencies such as Bitcoin, which are based on the PoW algorithm, have led to increasing energy consumption and carbon emissions over time. Mining activities require progressively more computational power, which in turn leads to industrial concentration.

As PoW-based coins continue to operate, the blockchain grows longer with each transaction over the years, thus requiring ever greater system resources. The difficulty experienced by computers in solving cryptographic problems between 2011 and 2019 is visualized in a graph [24]. These growing challenges discourage individual mining, push miners to organize into mining pools, and overall contribute to centralization. Mining pools significantly increase electricity demand and lead to increased use of coal-fired power plants, which have been shown to exacerbate global environmental pollution.

While blockchain is cryptographically immutable, if an actor gains control over more than 51% of the system, this immutability principle is broken. The article statistically demonstrates that with growing centralization, a significant share of computational power is concentrated in the hands of a few actors engaged in mining, creating a risk of 51% attacks. From this perspective, the environmental sustainability and security of current mining practices are questioned.

As an alternative, the Proof-of-Stake (PoS) algorithm is proposed due to its lower energy consumption and its lack of reliance on computational concentration. However, since PoS has not yet been fully proven secure in cryptographic terms, the PoW algorithm retains its economic relevance. In conclusion, the article argues that further research is needed to examine the long-term implications of blockchain technology with respect to sustainability, security, and systemic impact.

2.1.4 A Survey on Consensus Protocols and Attacks on Blockchain Technology

This paper presents a comprehensive survey on consensus protocols in blockchain technology, focusing on how they operate, differ, and face varying degrees of vulnerability to cyberattacks. The primary goal of the paper is to educate readers on the landscape of consensus mechanisms and to highlight the importance of improving these systems to mitigate increasing threats. The authors collect and review over thirty consensus protocols, categorizing them based on their operational structure and suitability for permissioned or permissionless blockchains.

The study is structured in a comparative format that analyzes each protocol on metrics such as scalability, energy consumption, consensus latency, block finality, and the underlying mechanism for achieving trust. Protocols such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and newer models like Proof of Elapsed Time (PoET), Proof of Authority (PoA), and Directed Acyclic Graphs (DAG) are dissected for their strengths and shortcomings.

Beyond consensus mechanics, a significant portion of the paper is devoted to cataloging the security attacks that threaten blockchain systems. Attacks are divided into four main categories: core architectural attacks (e.g., 51% attacks, selfish mining), network-based attacks (e.g., DDoS, Sybil, eclipse), transaction-level attacks (e.g., double-spending, transaction malleability), and client-level threats (e.g., wallet theft, DNS hijacking). Each attack is presented with technical details on how it is executed, its potential impact, and examples from existing blockchain incidents.

A valuable feature of the paper is the use of tabular comparisons and structured matrices, which make it easy to observe trade-offs between protocols and link them to their corresponding vulnerabilities. This visualization strategy enhances clarity and is particularly useful for researchers or developers comparing different blockchain models.

The authors emphasize that as blockchain networks become more integrated into critical infrastructure and industry applications, the risk profile expands. To future-proof blockchain systems, the paper advocates for hybrid cryptographic approaches, layered consensus mechanisms, and real-time anomaly detection systems embedded into the protocol stack.

However, the paper's scope remains within the theoretical and analytical domain; it does not include experimental simulations, performance benchmarking, or empirical validations. While this is a limitation in terms of proving the effectiveness of the proposed ideas, the breadth and depth of the literature review make it a cornerstone reference for those researching blockchain consensus and security.

2.2 Security and Privacy of Blockchain

2.2.1 SoK: Security and Privacy of Blockchain Interoperability.

The paper "SoK: Security and Privacy of Blockchain Interoperability" examines the security and privacy challenges in cross-chain blockchain systems, focusing on bridges, asset transfers, and data sharing. Analyzing 212 sources, the authors classify 57 interoperability mechanisms across four security layers and define key security and privacy properties. They identify 45 vulnerabilities, 4 privacy leaks, and 92 mitigations, linking them to 18 major bridge hacks exceeding $3 billion in losses—mostly in systems using weakly secured permissioned networks. The paper highlights a research gap in privacy and evaluates techniques like zero-knowledge proofs and trusted execution environments, concluding with 17 insights and best practices for more secure, privacy-aware cross-chain solutions.

2.3 Blockchain Technology's Applications

2.3.1 Tides of Blockchain in IoT Cybersecurity

This paper presents a detailed study on the integration of blockchain technology with Intrusion Detection Systems (IDS) to improve the security posture of IoT and Industrial IoT (IIoT) networks. Recognizing the increasing frequency and complexity of cyber threats in interconnected environments, the authors argue that traditional IDS approaches are insufficient when operating in isolated or centralized architectures. Instead, they propose a blockchain-enhanced IDS framework that leverages the key properties of blockchain—immutability, transparency,

decentralization, and distributed consensus—to ensure trust and resilience in threat detection systems.

The study begins by outlining the pressing cybersecurity challenges in IoT, such as limited device processing capabilities, weak encryption, fragmented protocols, and the absence of secure identity management. To counter these vulnerabilities, blockchain is positioned as a decentralized trust layer capable of ensuring the integrity of log data, securing peer-to-peer communications, and enabling tamper-proof incident tracking.

The paper explores how the combination of blockchain and AI can lead to more dynamic and adaptive IDS solutions. Specifically, it discusses the role of machine learning and deep learning algorithms in identifying anomalies within large datasets generated by IoT devices. These AI techniques, when paired with the immutable data storage and access control offered by blockchain, can enhance detection accuracy while reducing false positives.

Consensus mechanisms such as Proof of Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) are recommended for use in private or consortium IoT networks due to their relatively low resource consumption and fast finality. The authors also examine the potential of smart contracts to automate IDS responses, such as isolating compromised nodes or triggering alerts across distributed systems.

In conclusion, the paper provides a strong case for blockchain's role in future-proofing IoT security systems. While primarily conceptual, the proposed framework and literature-backed analysis form a valuable reference point for further development and real-world experimentation.

2.3.2 Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network

Chosen article represents the study of the potential of blockchain technology application in the security architecture of Internet of Things (IoT) systems. Since the number of connected devices is growing quickly, it is important to find ways to protect them from cyber threats. Unlike other articles that focus only on one topic, like privacy or one type of blockchain, this paper gives a full overview, covering topics such as the fundamental blockchain architecture[12], threat classification and types[13], as well as industry use cases and practical risk mitigation tools. Each type of attack is not only defined but also contextualized with relevant examples from Bitcoin, Ethereum, and other blockchain ecosystems. These explanations provide insight into how these threats exploit weaknesses in consensus algorithms, peer-to-peer communication, or smart contract execution environments.

The authors continue the discussion by showing how these problems can happen in real-life Internet of Things (IoT) situations. For example, they explain that privacy problems with transactions and Sybil attacks can damage the trust needed for large, decentralized IoT systems. In addition, the researchers discuss how regulatory uncertainty and governance challenges are affecting blockchain technology adoption in sectors as finance, healthcare, and energy trading. In addition, the paper discusses industry applications and blockchain implementations for secure electronic health record (EHR) management, privacy-preserving location sharing, smart grid electricity transactions, and decentralized certificate authorities.

I would like to note that in addition to listing the threats, the paper provides an organized overview of strategies and tools to mitigate the challenges. This paper evaluates a set of existing tools for analyzing and verifying blockchain security, including Oyente, Mythril, Remix, and SmartCheck, mapping each of them to the specific vulnerabilities they are designed to detect, such as reentrancy, timestamp dependency, and improper exception handling.

Last but not least, the authors outline several open research directions. These include the need for privacy-preserving consensus mechanisms in resource-constrained IoT devices, the development of regulatory-compliant blockchain architectures, and the creation of interoperability standards between blockchain platforms and legacy systems. By presenting a unified framework that brings together threats, solutions, applications, and research gaps, this paper not only contributes to the academic debate but also serves as a valuable reference for practitioners developing secure blockchain-IoT infrastructures.

2.3.3 A Review of Blockchain in Internet of Things and AI

This paper provides a comprehensive review of the integration of blockchain technology with the Internet of Things (IoT), addressing several persistent challenges in conventional centralized IoT architectures[20]. The authors begin by explaining the vulnerabilities of current IoT systems—such as single points of failure, poor scalability, and weak data integrity—due to their dependence on centralized cloud infrastructure. They argue that blockchain's distributed and immutable ledger structure can mitigate these problems by enhancing data security, promoting decentralization, and eliminating reliance on a central authority.

The review categorizes various blockchain benefits for IoT, such as tamper-resistance, transparency, and increased trust among devices. A major contribution of the paper is the introduction of the concept of Blockchain as a Service (BaaS)[21] for IoT applications, which allows lightweight and scalable blockchain services to be deployed on resource-constrained IoT devices. This makes it feasible to embed blockchain features without significantly altering hardware or requiring powerful computation.

In addition to IoT and blockchain, the paper explores the integration of Artificial Intelligence (AI), positioning it as a tool to further improve IoT systems by enabling autonomous decision-making, real-time analytics, and predictive maintenance. The authors describe how AI algorithms, when supported by the security and integrity of blockchain infrastructure, can create intelligent, self-managing IoT environments capable of reacting dynamically to new conditions.

The paper is structured in a way that progresses from basic technology overviews to applied scenarios. It discusses existing studies and platforms where blockchain has been successfully integrated with IoT systems, particularly in areas like smart cities, healthcare, logistics, and supply chains. The paper also explores potential blockchain frameworks, including Ethereum, Hyperledger, and IOTA, and their suitability for various IoT contexts[22].

The authors conclude by proposing future research directions, emphasizing the need for: (1) developing lightweight consensus mechanisms tailored for IoT, (2) improving interoperability

between heterogeneous IoT devices and blockchain networks, and (3) designing AI models that operate efficiently in decentralized environments. Despite its lack of experimental validation, the paper's detailed analysis and structured synthesis provide strong foundations for academic and industrial researchers aiming to develop next-generation IoT systems secured and enhanced by blockchain and AI technologies.

2.3.4 Bitcoin and Blockchain: Security and Privacy.

This paper provides a comprehensive and systematic analysis of Bitcoin's security architecture and its inherent privacy limitations, while also offering a broad comparative overview of wallet infrastructures, network-level threats, and altcoin improvements. The central contribution of the study lies in bridging theoretical models with practical vulnerabilities through a quantitative and qualitative exploration of blockchain-based digital asset systems.

From a security standpoint, the paper extensively dissects the double-spending attack—one of the most critical threats in Bitcoin. It introduces formal probabilistic models (including binomial walks and Poisson distribution) and calculates the profitability threshold for attackers with varying hash power. This analysis reveals key insights into when an attack becomes economically irrational, offering merchants and miners a framework for balancing transaction confirmation times against attack risk.

Additionally, the paper maps out a comprehensive classification of network-level threats such as Sybil attacks, eclipse attacks, DoS, and BGP-based routing attacks, detailing how they target Bitcoin's peer-to-peer infrastructure and proposing countermeasures such as subnet masking, anchor nodes, and hardened peer selection. These are supported by protocol-specific insights that draw from real-world attack scenarios and research-backed models.

The study also includes a full taxonomy of wallet types (Type 0, Type 1, and HD wallets) and their associated key generation mechanisms, including hierarchical deterministic (HD) key trees, chain codes, and hardened derivation protocols (BIP32, BIP39). These are further categorized based on user environment (web, desktop, mobile, hardware, and signing-only wallets), illustrating the trade-offs between usability and cryptographic resilience.

On the privacy front, the authors challenge the notion of Bitcoin's anonymity, introducing the "linking problem", and cataloging attack vectors through which Bitcoin addresses can be de-anonymized. The paper reviews state-of-the-art mixing protocols (e.g., TumbleBit, CoinSwap), joint transaction methods (e.g., CoinJoin, JoinMarket), and network-level anonymizers (e.g., Tor), evaluating their effectiveness and limitations. Notably, it explains how sophisticated correlation techniques can still compromise anonymity, especially when change addresses or centralized mixers are involved.

To expand its relevance beyond Bitcoin, the paper also surveys security and privacy-enhancing innovations in altcoins, detailing the implementation of alternative consensus mechanisms such as Proof-of-Stake (PoS), Proof-of-Burn (PoB), and Proof-of-Activity (PoA), along with novel cryptographic protocols like zk-SNARKs, CryptoNote, and Mimblewimble. These are discussed in terms of their resistance to 51% attacks, energy efficiency, decentralization, and capability to obscure transaction metadata.

Finally, the study outlines future research directions, emphasizing the need for secure smart contract design, privacy-preserving identity management, and secure integration with IoT and e-voting systems. The authors highlight the role of blockchain-based transparency in healthcare, supply chain traceability, and digital governance, while noting the unresolved risks associated with the immutability of flawed contracts and the lack of global privacy standards.

Overall, this paper stands out by providing both granular technical assessments and a broader systemic understanding of Bitcoin and blockchain security. It serves as a bridge between theoretical frameworks and applied cryptography, offering valuable guidance for researchers, developers, and policymakers aiming to enhance the resilience and trustworthiness of blockchain ecosystems.

3. ANALYSIS OF METHODOLOGY OF EACH PAPER

3.1 SoK: Security and Privacy of Blockchain Interoperability.

The methodology of this paper is structured around a two-phase systematic literature review aimed at consolidating fragmented knowledge in the field. In the first phase, the authors collected academic publications from 2015 onward using keyword searches on Google Scholar, followed by snowballing and forward reference tracking. In the second phase, they expanded their dataset with gray literature, including audit reports, bug bounty disclosures, and security blogs, to capture real-world vulnerabilities and attacks. In total, 212 documents were analyzed—58 academic and 154 from gray literature. This broad and inclusive approach allowed them to classify 57 interoperability mechanisms, identify 45 vulnerabilities and 4 privacy leaks, and examine 18 major bridge hacks. Their analysis is supported by a new taxonomy and a security/privacy model that evaluates interoperability mechanisms across multiple technical dimensions. The use of both scholarly and industry sources ensures the findings are comprehensive and relevant to both research and practice.

3.2 A Survey on Blockchain Technology: Evolution, Architecture and Security

The methodology in "A Survey on Blockchain Technology: Evolution, Architecture and Security" is based on a structured literature review that traces the evolution of blockchain across three phases—cryptocurrencies, smart contracts, and broader decentralized applications. The authors systematically analyze architectural models, consensus mechanisms, development frameworks, and security issues, supported by comparative tables and taxonomies. A key strength of this approach is its comprehensive scope and clear organization, offering a unified view of diverse aspects of blockchain technology. However, the absence of empirical data or case studies limits the practical validation of its findings. Nonetheless, the methodology effectively lays a solid foundation for future research and development in the field.

3.3 A survey on blockchain technology and its security.

The methodology applied in this review paper, as the authors themselves write to us, is a systematic study and analysis of various scientific papers aimed at building a holistic picture of the state of blockchain technologies and their vulnerabilities [19]. First, the authors defined key terms for searching for scientific publications: blockchain, consensus algorithm, smart contract, blockchain security, risk, vulnerability. They used these to collect a corpus of publications from leading academic conferences and journals in the information security field, including IEEE Symposium on Security and Privacy, USENIX Security Symposium, ACM CCS, and IEEE Transactions journals.

The authors then performed a thematic categorisation of the collected data into five main areas: architecture and evolution of blockchain systems; consensus algorithms and cryptography; smart contracts and their vulnerabilities; practical applications of blockchain; and security risks and protection mechanisms. For each of the topics, they performed a detailed review of existing solutions, including comparative analyses and synthesis of findings from different sources.

One of the most important steps was to analyse the security risks of blockchain, which was done in stages. First, the threats were compared to known vulnerabilities from the OWASP Top 10 [18] to show that blockchain inherited typical web application problems such as XSS, injection and weak access control. They then looked at specific threats to blockchain: protocol bugs (e.g., BGP attacks, Eclipse), smart contract vulnerabilities (e.g., reentrancy, number overflow), misconfigurations, and key theft. The researchers then tabulated actual attacks from 2010 to 2020 [17] - with name, year, risk type, vulnerable component, damage and cause. This helped them understand how threats evolved over time. Once they knew about the attacks, they compared more than 10 smart contract inspection tools (e.g. Mythril, ZEUS, Securify), examining what vulnerabilities they found and how effective they were. It turned out that many contracts are vulnerable, and for better protection you need to use several tools at once.

It turned out that many contracts are vulnerable, and for better protection, you need to use several tools at once.It is worth noting that the methodology includes not only analyses but also forecasts of future threats and research directions. It seems to me that this paper takes into account problems that have not yet been solved - for example, the inability to update already deployed contracts, as well as new risks: quantum attacks, scalability and privacy issues. Promising solutions such as off-chain channels (Perun), quantum-safe algorithms (SPHINCS, XMSS), Zero Trust and AI to find anomalies in transactions are considered. In summary, We can conclude that the methodology used makes the research useful for both novices and experienced professionals.

3.4 Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.

In this study, the authors used a method based on a detailed analysis of previous studies. They studied a variety of scientific articles, technical reports, and case studies from 2016 to 2020. These studies covered various blockchain systems such as Bitcoin, Ethereum, and private blockchains such as Hyperledger. One of the strengths of the article is that it clearly distributes this large amount of information on the main topics.: how the blockchain works, types of attacks, security issues, solutions, and real-world applications.

Instead of retelling old studies, the authors of this work have created a detailed comparison table, which shows how their work differs. For example, if previous articles talked only about how the blockchain is used or how it works in general, then this article focuses more on attacks and ways to prevent them. This makes their work more unique and relevant. In addition, each type of attack is explained in the context of how the blockchain works — for example, during the verification of blocks, signing transactions or launching smart contracts. The authors also explain the impact of these attacks on Internet of Things systems, such as network hacking using BGP interception or data leakage using poorly written smart contracts. Despite the fact that there are no real experiments or test systems in the article, it is still interesting because it contains detailed technical explanations and real examples, such as the hacking of the DAO in 2016, BGP attacks or malware that steals secret keys.The paper's methodology is also notable for its structured visual presentation. Diagrams like the "roadmap of literature" (Fig. 1)[10], and comparative matrices (Tables I, II, III and VIII)[11], help the reader quickly absorb trends and gaps across multiple studies. These tools support cognitive mapping—allowing complex relationships between threats, sectors, and solutions to be visualized effectively. However, this methodology also has clear limitations. The study does not include quantitative analysis, statistical synthesis (e.g., meta-analysis), or empirical testing of any of the proposed defense mechanisms.

As a result, this method is good because it uses extensive literature, but by applying real tests or doing your own experiments to prevent the most popular attacks, it would be even more useful for fans and researchers of blockchain technology, as well as more innovative.

3.5 Tides of Blockchain in IoT Cybersecurity

The paper adopts a structured and formal systematic review methodology guided by the PRISMA framework, enabling the authors to collect and analyze scholarly articles published between 2019 and 2024. The review focuses on studies that explore the integration of Artificial Intelligence (AI) and blockchain technologies within Intrusion Detection Systems (IDS) tailored for Internet of Things (IoT) and Industrial IoT (IIoT) environments. The literature is filtered through predefined inclusion criteria that ensure the relevance and quality of selected works.

The authors categorize the existing body of research into themes such as anomaly detection using AI, blockchain-based identity management, decentralized decision-making, and privacy preservation. In evaluating the collected studies, the paper identifies trends and limitations in the field, such as the challenges of computational overhead, real-time processing, and device heterogeneity in IoT ecosystems. A conceptual blockchain-IDS framework is proposed to address these issues by leveraging the immutability and transparency of blockchain for log auditing, along with AI's predictive capabilities for real-time threat detection.

Furthermore, the paper includes case-based illustrations of how such a framework can be implemented, detailing scenarios in which smart contracts are triggered to autonomously respond to detected anomalies. Despite this practical outlook, the framework remains theoretical and has not yet been tested through large-scale or empirical validation. Nevertheless, the structured approach to

data collection and the clarity in thematic synthesis strengthen the reliability of the study's findings and provide a strong foundation for future experimental development in blockchain-enabled IoT security.

3.6 A Review of Blockchain in Internet of Things and AI

The methodology employed in this paper is a systematic literature review, which involves the careful selection, categorization, and analysis of a wide spectrum of research articles and technical reports on blockchain integration with IoT. The authors gather and examine studies from both foundational and recent works to construct a comprehensive understanding of how blockchain technologies are applied to resolve challenges in IoT ecosystems.

The review begins by laying down a foundational understanding of IoT and blockchain technologies, ensuring clarity for readers from varying technical backgrounds. The authors use this foundation to explore key architectural differences between centralized and decentralized IoT models, emphasizing how blockchain's immutability, decentralization, and cryptographic strength can address traditional issues such as single points of failure, poor data transparency, and privacy vulnerabilities.

To structure the discussion, the authors organize the literature into major themes: benefits of integration (e.g., improved data trust and transparency), architectural changes (including permissioned vs. permissionless ledgers), and technical limitations (such as high computational demands and scalability constraints). Notably, the review introduces the concept of Blockchain as a Service (BaaS), which enables deployment of blockchain functions like smart contracts or distributed ledgers on lightweight devices without heavy overhead.

Further into the analysis, the paper expands into the role of Artificial Intelligence in IoT-blockchain systems, evaluating AI's ability to manage real-time analytics, make autonomous decisions, and facilitate predictive maintenance when supported by blockchain-secured data streams. Several AI models such as machine learning and deep learning algorithms are discussed in terms of how they can improve system reactivity and threat detection.

The methodology is enriched with visual illustrations (figures showing IoT architectures and blockchain layering) and a structured framework of how blockchain and AI together support next-generation IoT applications in domains like smart cities, agriculture, logistics, and healthcare. However, while the review provides rich conceptual discussion, it does not include quantitative analysis, experimental validation, or performance evaluation of the technologies discussed. This theoretical nature is a limitation, although the breadth and clarity of analysis offer valuable insights and future research directions for academia and industry.

3.7 Bitcoin and Blockchain: Security and Privacy

The methodology of this paper combines conceptual explanation, mathematical modeling, and comparative security analysis. It begins by offering a detailed technical breakdown of Bitcoin's architecture—including the blockchain, mining, transaction validation, and wallet types—laying a clear foundation for the reader.

A standout feature is the quantitative modeling of double-spending attacks using probabilistic tools such as Poisson and binomial distributions. The authors simulate different attack scenarios and evaluate not just the likelihood of success, but also the economic profitability based on mining costs, equipment depreciation, and electricity usage.

The paper also analyzes key network-level threats (e.g., Sybil, DoS, Eclipse attacks) and explains how Bitcoin defends—or sometimes fails to defend—against them. The section on wallet infrastructure is particularly technical, exploring hierarchical deterministic (HD) wallets and security flaws linked to key derivation.

Lastly, the paper reviews privacy techniques and consensus mechanisms used by alternative cryptocurrencies (altcoins), offering a comparative view of security trade-offs beyond Bitcoin.

Although the paper doesn't conduct simulations or real-world experiments, its methodological strength lies in bridging theory with real-world concerns—especially through attack modeling, system-wide risk evaluation, and infrastructure-level insights.

3.8 The good, the bad and the ugly: An overview of the sustainability of blockchain technology

The methodology used in this paper is fundamentally conceptual and narrative-driven, offering a structured reflection on the sustainability of Proof-of-Work (PoW)-based blockchain technology. Rather than relying on original data collection or experimental validation, the author builds their argument through a thoughtful synthesis of existing academic literature, institutional reports, technical statistics, and real-world developments.

The analysis is organized around three metaphorical yet analytically meaningful categories: "The Good" explores blockchain's potential contributions to the UN Sustainable Development Goals, such as financial inclusion, food supply transparency, and clean energy exchange. "The Bad" highlights the environmental costs of PoW-based cryptocurrencies like Bitcoin, particularly their high electricity consumption and carbon emissions. "The Ugly" addresses the growing centralization of mining power, quantitatively illustrated using the Four-Firm Concentration Index (FFCI), and discusses its implications for decentralization and network trust (i.e., the risk of 51% attacks).

The author employs descriptive and comparative methods, referencing secondary data sources such as Blockchain.com, Digiconomist, and UNEP reports. Graphs, figures, and mining pool concentration data are used to support key arguments and provide real-world context.

What sets this methodology apart is its interdisciplinary nature: by combining insights from technology studies, environmental economics, and governance, the paper doesn't just critique PoW blockchains from a technical standpoint, but also from a systemic and ethical one. While it lacks quantitative modeling or empirical testing, its interpretive depth and integration of cross-sector

perspectives make it a strong contribution to blockchain sustainability discourse.

As a result, the paper takes a narrative-analytical approach, appropriate for exploring broad, long-term questions of viability and trust in blockchain systems. Yet to strengthen its claims, especially regarding environmental impact, future work might consider adding empirical methods or simulation-based analyses.

3.9 A Survey on Consensus Protocols and Attacks on Blockchain Technology

This paper adopts a structured survey-based approach, reviewing a diverse set of peer-reviewed research studies from established academic sources, including IEEE, Springer, Elsevier, ACM, and Hindawi. The study organizes the reviewed literature around consensus protocols, classifying them based on their operational models and their applicability to permissioned and permissionless blockchain systems.

The paper opens with a foundational overview that reintroduces the concept of decentralization as articulated by Satoshi Nakamoto in the Bitcoin whitepaper. It emphasizes the continuing relevance of decentralized architecture in blockchain systems, particularly in the context of growing cybersecurity challenges.

The authors group the 30 examined consensus protocols into five categories: (i) proof-based methods like Proof of Work (PoW), Proof of Stake (PoS), and Proof of Elapsed Time (PoET); (ii) voting-based approaches such as Practical Byzantine Fault Tolerance (PBFT); (iii) reputation-based models including Proof of Authority (PoA); (iv) time/resource-based protocols like Delegated Proof of Stake (DPoS); and (v) structure-based designs such as Directed Acyclic Graphs (DAG) and Holochain. Each category is evaluated with respect to key parameters including scalability, latency, and resilience.

A significant portion of the paper is dedicated to cataloging threats to blockchain networks. Attacks are grouped into four domains: core protocol-level (e.g., 51% attacks), network-level (e.g., DDoS, Sybil), transaction-level (e.g., double spending), and client-level threats (e.g., crypto-jacking, wallet theft). The paper supplements its explanations with comparative tables that aid in visualizing these attack vectors alongside the consensus protocols they affect.

The authors conclude by emphasizing the need for more resilient consensus models and hybrid cryptographic techniques. While the paper does not include empirical validation or simulations, it serves as a valuable reference for understanding the consensus-security landscape in blockchain research.

4. COMPARISONS OF PAPERS

5. RESULTS

6. CONCLUSION

7. REFERENCES

[1] A. Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang, and T. Hardjono, "SoK: Security and Privacy of Blockchain Interoperability.", *Conference: 2024 IEEE Symposium on Security and Privacy (SP)*, https://scholar.google.com.tr/citations?view_op=view_citation&hl=en&user=mSzH4DQAAAAJ&citation_for_view=mSzH4DQAAAAJ:Fu2w8maKXqMC

[2] M. N. Mumtaz 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 (Volume:9) 2021,* https://ieeexplore.ieee.org/abstract/document/9402747

[3] H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022*, https://www.sciencedirect.com/science/article/pii/S2096720922000070

[4] S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.", *IEEE Access (Volume: 9) , Page(s): 13938 – 13959, 14 January 2021, E- ISSN: 2169-3536,* https://ieeexplore.ieee.org/abstract/document/9323061

[5] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity.", Sensors 2024, https://www.mdpi.com/1424-8220/24/10/3111

[6] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI.", *Big Data Cogn. Comput. 2020,* https://www.mdpi.com/2504-2289/4/4/28

[7] E. Zaghloul, T. Li, M. W. Mutka, J. Ren, "Bitcoin and Blockchain: Security and Privacy.", *IEEE INTERNET OF THINGS JOURNAL, VOL. 7, NO. 10, OCTOBER 2020,*https://www.egr.msu.edu/~renjian/pubs/Blockchain-IoT.pdf

[8] C. Schinckus, "The good, the bad and the ugly: An overview of the sustainability of blockchain technology", *Energy Research and Social Science, volume 69, pages 101614,*https://colab.ws/articles/10.1016%2Fj.erss.2020.101614

[9] A. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman, and A. Yadav, "A Survey on Consensus Protocols and Attacks on Blockchain Technology." *Applied Science 2023, 13(4),* https://www.mdpi.com/2076-3417/13/4/2604

[10]

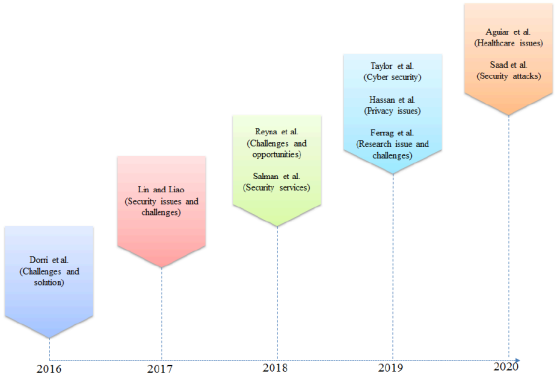


FIGURE 1. Roadmap of different literature on security issues, attacks, and solutions in blockchain technology between 2016 and 20

S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.", *IEEE Access (Volume: 9) , Page(s): 13938 – 13959, 14 January 2021, E- ISSN: 2169-3536,* https://ieeexplore.ieee.org/abstract/document/9323061

[11]

TABLE I
COMPARISON OF RELATED SURVEYS

Article	Year	Focused on	Security Attacks	Classification	Opportunities	Applications	Solutions	Security tools
[S1]	2016	Proposing a secure, private, and lightweight architecture for IoT based on blockchain technology	Yes	No	No	No	Yes	No
[S2]	2017	Introducing preliminaries of blockchain and security issues in blockchain	No	No	No	Yes	No	No
[S3]	2018	Investigating the challenges in IoT applications integrated with blockchain.	Yes	No	Yes	Yes	No	No
[S4]	2019	Blockchain-based solutions for security issues.	No	No	No	No	Yes	No
[S5]	2019	Blockchain applications in cybersecurity	No	No	No	Yes	No	No
[S6]	2019	Privacy issues caused by the integration of IoT with blockchain	Yes	Yes	No	No	No	No
[S7]	2019	Surveying existing blockchain protocols used with IoT	Yes	Yes	No	Yes	Yes	No
[S8]	2020	Applications of blockchain in the healthcare domain	No	No	No	No	Yes	No
[S9]	2020	Exploring the attack surface of the public blockchain	No	Yes	No	Yes	Yes	No
This Survey	2020	All of the above	Yes	Yes	Yes	Yes	Yes	Yes

TABLE II
ITEMS AVAILABLE THROUGH CRIMINAL ENTERPRISES

Category	Number of Items	Percentage (%)	Related Information and Title	Money Seized	Reference
Weed	3338	13.7	"From Seeds to Weed, Bitcoin Finds Home Where Commerce Goes Gray" (https://www.coindesk.com/bitcoin-atms-gray-areas)	$141.8 Billion	[75] [76]
Drugs	2194	9.0	"Blockchain in Action: Derailing Drug Abuse & Prescription Drug Fraud" (https://blockchain.wtf/2018/06/series/blockchain-in-action/derailing-drug-abuse/) "Tracing Illegal Activity Through the Bitcoin Blockchain To Combat Cryptocurrency" (https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/#18aa339b33a9)	$72 Billion	[77] [78]
Prescriptions	1784	7.3	"Bitcoin: Economics, Technology, and Governance" (https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213) "Blockchain Aims to Curb Prescription Drug Abuse" (https://hackernoon.com/blockchain-aims-to-curb-prescription-drug-abuse-47fc9cc66379)		[77] [79] [80] [81]
Benzodiazepines	1193	4.9	A class of psychoactive drugs	$3.6 Million	[80]
Cannabis	877	3.6	"Blockchain for Crime Prevention in the Legal Cannabis Space" (https://investingnews.com/innspired/blockchain-crime-prevention-legal-cannabis-space/)		[82] [83]
Hash	820	3.4	"The Future of Blockchain technology and cryptocurrencies" (https://skemman.is/bitstream/1946/30832/1/The%20future%20of%20blockchain%20technology%20and%20cryptocurrencies.pdf) "The Dark Side of Bitcoin" (https://blog.blockonomics.co/the-dark-side-of-bitcoin-illegal-activities-fraud-and-bitcoin-360e83408a32)		[73] [84]
Cocaine	630	2.6	"How the Feds Took Down the Silk Road Drug Wonderland" (https://www.wired.com/2013/11/silk-road/) "Heroin, Cocaine and LSD Sales Transactions Were Stopped Using Digital Currency BitCoin"		[85]
Pills	473	1.9	"Drug Dealers Are Using BitCoins to Fund the Flooding-Fatal Fentanyl Waves in Foreign Countries" "From the Dark Side of Bitcoin: Misusing Cryptography" (https://99bitcoins.com/the-dark-side-of-bitcoin-misusing-cryptography/)	$10 million	[81] [86]

TABLE III
SMART CONTRACT VULNERABILITIES

Vulnerability	Cause	Smart Contract	Level	Reference
Call to the unknown	Call to the unknown	Ethereum	Solidity	[87]
Gasless send	The recipient contract's fallback function *send* is invoked	Ethereum	Solidity	[88]
Field disclosure	Selfish miners published their private chain completely.	Bitcoin	Solidity	[89]
Exception disorder	Inconsistent in terms of exception handling while the call contract will not recognize errors that occur during execution.		Solidity	[90]
Reentrancy	A call that invokes back to itself through a chain of calls.	Ethereum	Solidity	[90]
Dangerous Delegate Call	DELEGATECALL opcode is identical to the standard message call	Wallet contract, Ethereum	Solidity	[90] [91]
Time stamp dependency	Vulnerability favoring a malicious miner by changing timestamp of StartTime, EndTime		Blockchain	[92]
Block number dependency	block.blockhash function associated with block number as parameters for random number is being manipulated			[90]
Freezing ether	Freezing ether contract i.e., no transfer/send/call/suicide code within the current contract itself to transfer ether to other address	Wallet contracts		[90]
Immutable bug	Altered contract that cannot be patched.		EVM	[93]
Ether lost in transfer	Ether sent to an orphan address that did not belong to any particular contract or user	Cryptocurrency, Ethereum	EVM	[93]
Unpredictable state	User cannot predict the state of contract if he or she invokes the particular transaction		Blockchain	[87]

TABLE VIII
TOOLS AND VULNERABILITY

Security tool	Interface	ReEntrancy	Timestamp dependency	Mishandled exceptions	Immutable Bugs	Gas costly patterns	Blockhash usage
Oyente	Command line	✓	✓	✓	✓	.....	.....
Remix	Command line	✓	✓	✓	.....	✓	✓
Gasper		.....	.....	.....	.....	✓	.....
Securify	User interface	✓	.....	✓	.....	-----	.....
S. Analysis		.....	.....	✓	.....	-----	.....
Smartcheck	User interface	✓	✓	✓	✓	✓	.....
Mythril	Command line	✓	.....	✓	✓	-----	.....

S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.", *IEEE Access (Volume: 9) , Page(s): 13938 – 13959, 14 January 2021, E- ISSN: 2169-3536,* https://ieeexplore.ieee.org/abstract/document/9323061

[12]

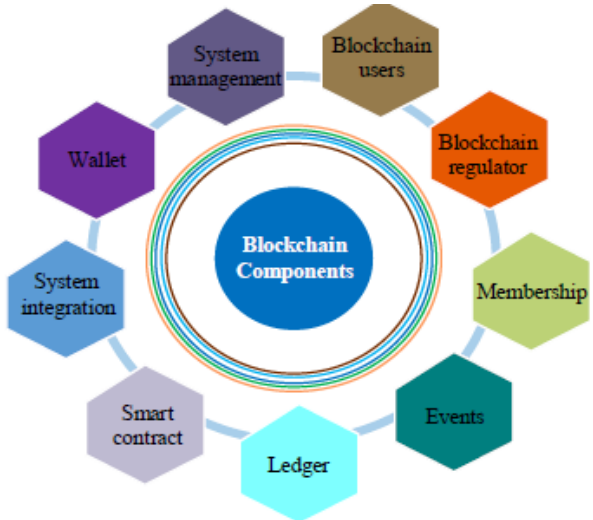


FIGURE 3. Blockchain Components.

S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.", *IEEE Access (Volume: 9) , Page(s): 13938 – 13959, 14 January 2021, E- ISSN: 2169-3536,* https://ieeexplore.ieee.org/abstract/document/9323061

[13]

No.	Type of Attack	Summary
1	**Liveness Attack**	Delays transaction confirmation through a three-phase process: preparation, transaction denial, and blockchain delay. Aimed at slowing down block propagation.
2	**Double Spending Attack**	Allows the same digital currency to be spent more than once. Includes race, Finney, 51%, and Vector 76 attacks. Exploitable if a miner controls majority power.
3	**51% Attack**	An attacker with over 50% mining power can manipulate blockchain by reversing transactions, excluding others' transactions, and halting operations.
4	**Private Key Security Attack**	Involves theft of private keys through malware, making recovery difficult and enabling unauthorized access to funds.
5	**Transaction Privacy Leakage**	Leakage of user data and cryptographic keys due to wallet operations or transaction traceability, leading to possible privacy breaches.
6	**Selfish Mining Attack**	Miners keep discovered blocks private to gain advantage, wasting honest miners' efforts and reducing overall blockchain efficiency.
7	**DAO Attack**	Exploits vulnerabilities in smart contracts (e.g., reentrancy) to drain funds from DAOs, as happened with Ethereum's DAO in 2016.
8	**BGP Hijacking Attack**	Manipulates internet routing (BGP) to intercept and redirect blockchain traffic, affecting mining pools and network integrity.
9	**Balance Attack**	Delays communication between subgroups with equal mining power, allowing attacker to manipulate block acceptance.
10	**Sybil Attack**	Uses fake identities in peer-to-peer networks to gain majority influence; harder in permissioned blockchains requiring identity proof.

S. Singh, A. S. M. S. Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network.", *IEEE Access (Volume: 9) , Page(s): 13938 – 13959, 14 January 2021, E- ISSN: 2169-3536,* https://ieeexplore.ieee.org/abstract/document/9323061

[14]

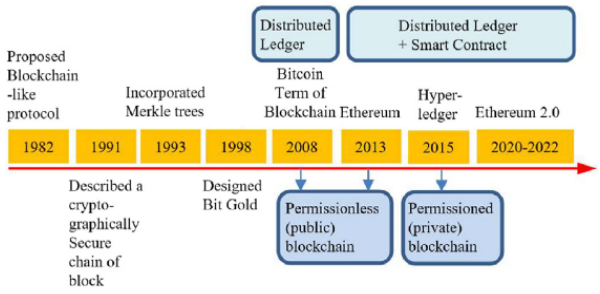


Fig. 1. History of blockchain.

H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022,* https://www.sciencedirect.com/science/article/pii/S2096720922000070

[15]

Table 1
Comparison of consensus algorithms [13,37–40].

	PoW	PoS	DPoS	PoET	PBFT	DAG
Setup	Public permissionless/ Private blockchain	Public permissionless/ Private blockchain	Public/Private blockchain	Private permissioned/ permissionless blockchain	Private permissioned blockchain	Public permissioned non-blockchain
Cost of entry and returns	Relatively high cost of entry, but high returns	Low cost of entry, but low returns	Lower cost and lower returns than PoS	Very low cost of entry, but low returns	All participate with no return	All participate with no return
Incentives	The winning miner receives new coins with the block & transaction fees in the block he/she validates	The winner receives transaction fees with the new block. If a block winner attempts to add an invalid block, he/she loses his/her stake	The threat of loss of reputation & income provides an incentive for delegates to act honestly and keep the network secure	The winning miner receives the transaction fees with the new block he/ she validates.	Nil	Nil
Finality	Probabilistic	Probabilistic	Probabilistic	Probabilistic	Immediate	Probabilistic
Scalability in network	High	Medium	Medium	Medium	Low (quickly grow into a huge communication cost as the amount of nodes scales upwards)	High
Energy efficiency	Very low (energy intensive computations, e.g., Bitcoin consumes around 121.36 terawatt-hours (TWh) a year)	High	High (no miners required)	High	Medium (Some PBFT systems use PoW to prevent Sybil attack, but only after a set number of blocks (i.e., 100) and not for every block)	Medium (A small PoW operation when a node submits a transaction to ensure the network is not being spammed and also validates previous transactions)
Majority or 51% attack	The number of malicious nodes >25% of all nodes for attack	Reduced 51% attack probability	Easier to organize a 51% attack if delegates combine their power	Reduced 51% attack probability	The number of malicious nodes > one third of all nodes for attack	Not tested at scale
Susceptible to Sybil attack	No	Yes	Yes	No	Yes	No
Examples	Bitcoin, Ethereum, Litecoin, Monero, Dash, Zcash, Decred, and more	Ethereum 2.0, Cardano, Polkadot BlackCoin, and Peercoin.	EOS, BitShares, Lisk, Steem, Ark, Nano, Cardano, and Tezos.	Hyperledger Sawtooth	Hyperledger Fabric, Zilliqa	IOTA
Transactions per second (TPS)	Bitcoin: 7 maximum 27	Ethereum: 15	EOS: 3996 BitShares: 3300	Hyperledger Sawtooth: 2300	Hyperledger Fabric: approximately 3500	IOTA: 250 IOTA Pollen V0.2.2: >1000
Block confirmation time (s)	Bitcoin: 6000 Litecoin: 150	Ethereum: 15	EOS: 0.5 BitShares: 3	No actual time is found	In seconds' level (No actual time is found)	120

H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022,* https://www.sciencedirect.com/science/article/pii/S2096720922000070

[16]

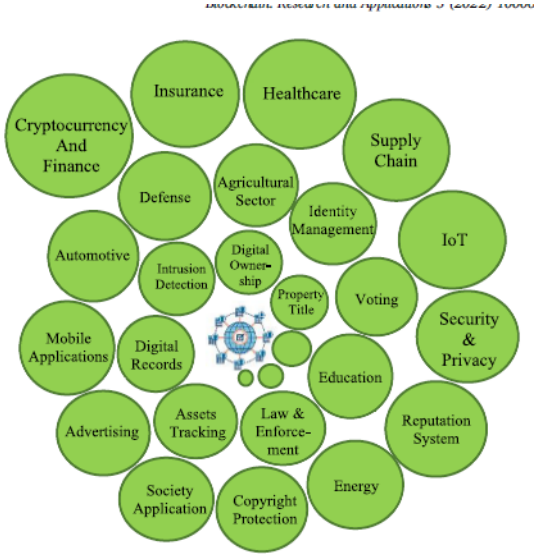


Fig. 5. Blockchain applications.

H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022,* https://www.sciencedirect.com/science/article/pii/S2096720922000070

[17]

Table 3
Top 10 web application security risks on blockchain technology [54].

Top 10 Web Application Security Risks	Assess on blockchain Technology	Analysis Examples
Injection	Poor input sanitization in blockchain technology	Before the EOS mainnet launches, discovered vulnerability of buffer-out-of-bounds EOS smart contract and the potential to run the malicious smart contract
Broken Authentication	A large attack surface exists without proper implementation of authentication functionality	The cryptocurrency LISK is an example of allowing an attack on authentication
Sensitive Data Exposure	High potential for this vulnerability	Vulnerable to data mining efforts—mining the public data on blockchain for useful information; Quantum computing will break the public key cryptography used to e data on the blockchain
XML External Entities (XXE)	Not applicable	
Broken Access Control	One major vulnerability for smart contracts	Two attacks on Parity multi-signature wallets due to access control vulnerabilities
Security Misconfiguration	Affect blockchain security	Attackers exploited a vulnerability to steal cryptocurrency when Ethereum wallets configured to receive external commands from port 8545
Cross-Site Scripting (XSS)	Affect blockchain in some ways	Blockchain explorers under XSS attack could display untrusted transaction data; Bo blockchain explorers and wallets under XSS attack could allow access to a private l user and control over his/her account
Insecure Deserialization	May compromise of blockchain systems	If malicious users control transaction data, blockchain systems may be compromise vulnerable deserialization code
Using Components with Known Vulnerabilities	Very common to reuse code for Ethereum smart contracts	More than 90% of smart contracts in Ethereum did reuse code, and may contain kr vulnerabilities
Insufficient Logging & Monitoring	The log owners may un-monitor their logs	May smart contracts lack of monitoring and hackers may exploit their vulnerabilities being detected

H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022*, https://www.sciencedirect.com/science/article/pii/S2096720922000070

[18]

Table 4
Blockchain security risk categories at low level in Ref. [29].

S/N	Category
1	51% vulnerability
2	Criminal activity
3	Private key security
4	Transaction privacy leakage
5	Double-spending
6	Criminal smart contracts
7	Under-priced operations
8	Smart contract's vulnerabilities
9	Under-optimized smart contract

Table 5
Blockchain security risk categories at high level.

Risk	Description
Network Attacks	As shown in Table 1, blockchain has a limited number of transactions per second, DoS attacks may submit more transactions than the blockchain's capability and cause the blockchain unavailable. Besides DoS, BGP (Border Gateway Protocol) attacks, routing attacks, eclipse attacks, stealthier attacks, DNS attacks, and remote side-channel attacks are also under this category.
Endpoint Security	Endpoints can be heterogeneous which have more options to exploit the vulnerabilities. Endpoints can be also homogeneous which a flaw in one system can exist in all systems.
Intentional Misuse	As shown in Table 1, the attackers may control more nodes to launch like 51% type of attacks.
Code Vulnerabilities	Code vulnerabilities can come from smart contracts that anyone can write or the underlying platform code. The vulnerabilities have a wide-reaching impact due to the distributed network and the code cannot be modified once deployed. Intentionally write malicious smart contracts.
Data Protection	Data protection relies upon the blockchain instead of data owners to provide data integrity and availability.
Human Negligence	The log owners may un-monitor their logs.

Table 7
Attacks, years, categories, exploit values and root causes.

Attack	Year Category	Exploit Value	Root Cause
Mt. Gox	2011 C1	Several thousand BTC	Deficiencies in network protocols
Bitfloor	2012 C2	24,000 BTC (250,000 USD)	Bitfloor's server was hacked to leak an unencrypted backup of the wallet keys
Instawallet	2013 C4	35,000 BTC	Instawallet was hacked
Bitcoin Foundation	2013 C6	–	A generation bug with old pseudo random number
Sheep Marketplace	2013 C4	5400 BTC	One site vendor exploited a vulnerability
Mt. Gox	2014 C4	650,000 BTC (450 million USD)	A bug in software that allows users to modify transaction IDs
Dell SecureWorks	2014 C1	83,000 USD	BGP hijack
DAO	2016 C4	50 million USD	Code weakness: subtle game-theoretic weaknesses
Bitfinex	2016 C2 & C4	119,756 BTC (65 million USD)	Hackers stole BTC.
Ethereum network	2016 C1 & C4	–	DDoS attack: calling EXTCODESIZE opcode roughly 50,000 times per block
Gold HKG	2017 C4	–	A bug with contract code that reads "=+" instead of "+="
Parity Wallet	2017 C4	30 million USD	Addresses were comprised (Delegate call + exposed self-destruct)
SmartBillions	2017 C4	400 ETH (120,000 USD)	Broke into smart contract Broken caching mechanism
Parity Wallet	2017 C4	300 million USD	An undiscovered bug of not proper initialization (Delegate call + unspecified modifier)
Cryptojacking	2017–2018 C2 & C4	–	Hacked and inserted crypto mining script or cryptojacking code
PoWH	2018 C4	888 ETH	Integer overflow
Spankchain	2018 C4	165.38 ETH	Reentrancy attack
IOTA	2019 C2	3.94 million USD	A phishing attack to collect the users' privacy keys
IOTA	2020 C4	–	Custom-made hash-function was broken
Cashaa	2020 C2	More than 336 BTC	Suspect a piece of malware was installed onto the system
2gether	2020 C2	1.3 million USD	2gether's servers were hacked

Note: C1: network attacks, C2: endpoint security, C3: intentional misuse, C4: code vulnerabilities, C5: data protection, C6: human negligence; DAO: decentralized autonomous organization; PoWH: Proof of Weak Hands.

H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022*, https://www.sciencedirect.com/science/article/pii/S2096720922000070

[19]

Table 9
Summaries of various survey works.

Work	Blockchain Category	Consensus Protocols		Applications	Scalability	Blockchain Security	Quantum Computin
		Qualitative Comparison	Quantitative Comparison				
[26]	Yes	Yes					
[27]	Yes	Yes			Yes	Partial	
[55]						Partial	
[2,28]	Yes	Yes		Yes	Yes	Partial	
[3]	Yes	Yes	Partial	Yes	Yes	Partial	
[150]				Yes			
[29]		Yes				Partial	
[30]		Yes					
[31]	Yes	Yes	Partial		Yes	Partial	
[32]				Yes			
[45]	Yes	Yes	Partial	Yes	Yes		
[44]				Yes		Partial	
[146]	Yes	Yes		Yes		Partial	
[147]		Yes	Partial			Partial	
[148]				Yes	Yes	Surveyed on vulnerabilities	Yes
[149]		Yes		Yes	Yes	Examined security in process, data and infrastructure levels	Yes
This paper	Yes	Yes	As many as possible	Yes	Yes	Comprehensive blockchain security risk categories, real attacks, bugs & root causes, recent security measures	Yes

H. Guo and X. Yu, "A survey on blockchain technology and its security.", *Blockchain: Research and Applications, ISSN: 2096-7209, Vol: 3, Issue: 2, Page: 100067, 2022,* https://www.sciencedirect.com/science/article/pii/S2096720922000070

[20]

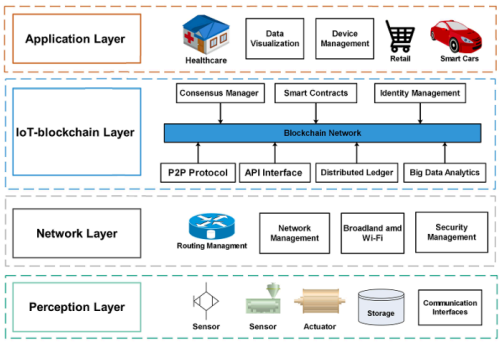


Figure 5. Architecture of IoT with blockchain.

H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI.", *Big Data Cogn. Comput. 2020,* https://www.mdpi.com/2504-2289/4/4/28

[21]

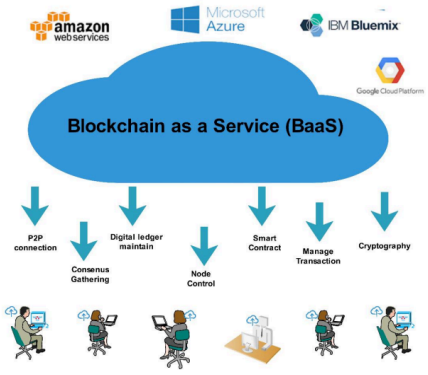


Figure 6. Typical Architecture of BaaS.

H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI.", *Big Data Cogn. Comput. 2020,* https://www.mdpi.com/2504-2289/4/4/28

[22]

Table 4. Comparison between Ethereum, Hyperledger and IOTA.

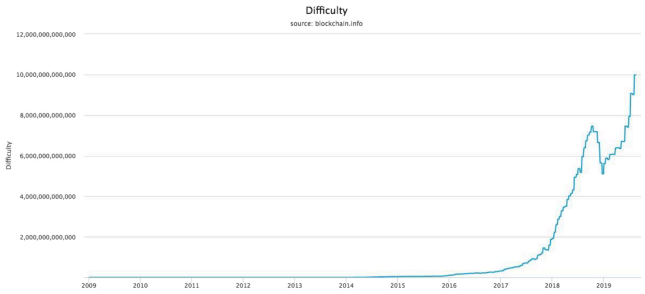
Item	Ethereum	Hyperledger	IOTA
Transaction Time	10–15 s	0.05–100 ms	120 s
Consensus Mechanism	Proof of Work (PoW)	Practical byzantine fault tolerance (PBFT)	N/A
Network Usage	Less usage	High usage	Less usage
Computation Cost	High computation cost	Less computation cost	Less computation cost
Smart Contracts	Yes	Yes	No

H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI.", *Big Data Cogn. Comput. 2020,* https://www.mdpi.com/2504-2289/4/4/28

[23]

C. Schinckus, "The good, the bad and the ugly: An overview of the sustainability of blockchain technology", *Energy Research and Social Science, volume 69, pages 101614,*https://colab.ws/articles/10.1016%2Fj.erss.2020.101614

[24]



C. Schinckus, "The good, the bad and the ugly: An overview of the sustainability of blockchain technology", *Energy Research and Social Science, volume 69, pages 101614,*https://colab.ws/articles/10.1016%2Fj.erss.2020.101614