future internet

Review

A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things

Yunus Kareem [1,*], Djamel Djenouri [1] and Essam Ghadafi [2]

[1] Department Computer Science and Creative Technologies, University of the West of England, Bristol BS16 1QY, UK; djamel.djenouri@uwe.ac.uk

[2] School of Computing, Newcastle University, Newcastle-Upon-Tyne NE1 7RU, UK; essam.ghadafi@newcastle.ac.uk

* Correspondence: yunus.kareem@uwe.ac.uk; Tel.: +44-7502-583-020

Abstract: The adoption of blockchain platforms to bolster the security of Internet of Things (IoT) systems has attracted significant attention in recent years. Currently, there is a lack of comprehensive and systematic survey papers in the literature addressing these platforms. This paper discusses six of the most popular emerging blockchain platforms adopted by IoT systems and analyses their usage in state-of-the-art works to solve security problems. The platform was compared in terms of security features and other requirements. Findings from the study reveal that most blockchain components contribute directly or indirectly to IoT security. Blockchain platform components such as cryptography, consensus mechanism, and hashing are common ways that security is achieved in all blockchain platform for IoT. Technologies like Interplanetary File System (IPFS) and Transport Layer Security (TLS) can further enhance data and communication security when used alongside blockchain. To enhance the applicability of blockchain in resource-constrained IoT environments, future research should focus on refining cryptographic algorithms and consensus mechanisms to optimise performance and security.

Keywords: blockchain; Internet of Things (IoT); cryptography; consensus algorithm; ethereum; algorand; IoTeX; IoTA; multichain

Citation: Kareem, Y.; Djenouri, D.; Ghadafi, E. A Survey on Emerging Blockchain Technology Platforms for Securing the Internet of Things. *Future Internet* **2024**, *16*, 285. https://doi.org/10.3390/fi16080285

Academic Editor: Christoph Stach

Received: 5 June 2024
Revised: 1 August 2024
Accepted: 3 August 2024
Published: 8 August 2024

1. Introduction

The Internet of Things (IoT) is one of the fastest-growing technologies with billions of devices connected to the internet for both personal and business purposes. IoT systems enable communication and information sharing between devices across diverse locations. The necessity for specially designed devices with sensing capabilities to exchange information over the internet gave rise to IoT, which has been embraced for numerous use cases and innovative applications such as smart healthcare [1,2], smart grid and building energy optimization [3,4], smart buildings [5,6], and smart transportation [7], among others. A summary of the IoT adoption statistics report published on the DataProt website reveals that the number of active IoT devices surged to 10 billion in 2021 and is projected to exceed 25.4 billion by 2030 [8]. Similarly, another projection estimated the rise of IoT devices from a million in 1992 to 50.1 billion in 2020, as shown in Figure 1 [9]. The market size for IoT was forecasted to reach 1.1 trillion dollars in 2023, marking the highest among other researched emerging technologies such as Artificial Intelligence and Edge Computing [8]. IoT applications span from the use of devices like smart light bulbs, smart locks, and security cameras in various homes and offices to more complex implementations in smart cities, traffic systems, and industrial IoT systems.

An IoT system can be classified as a product device that has a sensor, actuator, and communication medium, or a collection of multiple IoT devices with other components like application software, back-end services (cloud, API, etc.), and networking devices (gateway, access point, etc.) [10]. Abdmeziem et al. [11], Abou-Nassar et al. [10], and

Antao et al. [12] proposed different categorisations of IoT system components, including three-, four-, and five-layer models, respectively. However, all three models concur on the existence of fundamental components within the IoT system, such as the Application, Network, and Perception/device-sensing layers. Additional models may include layers such as the middleware layer and the business layer, as shown in Figure 2.

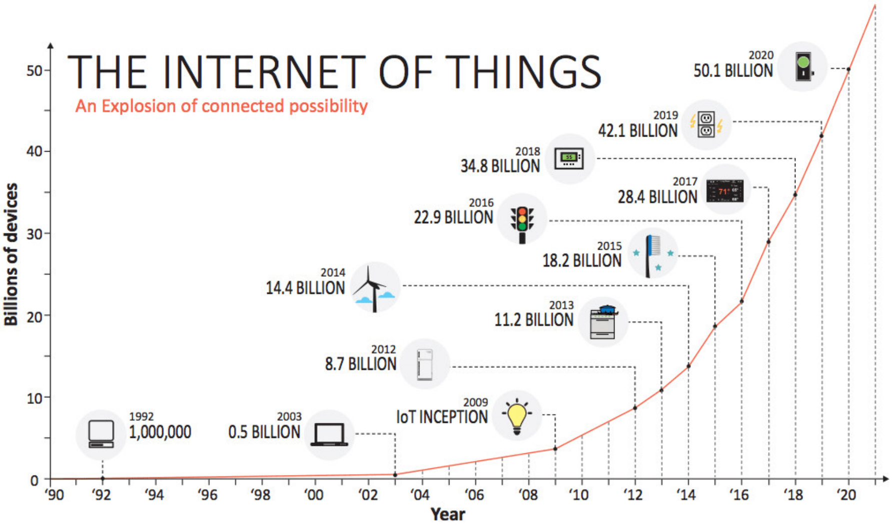

Figure 1. Rise in connected devices [9].

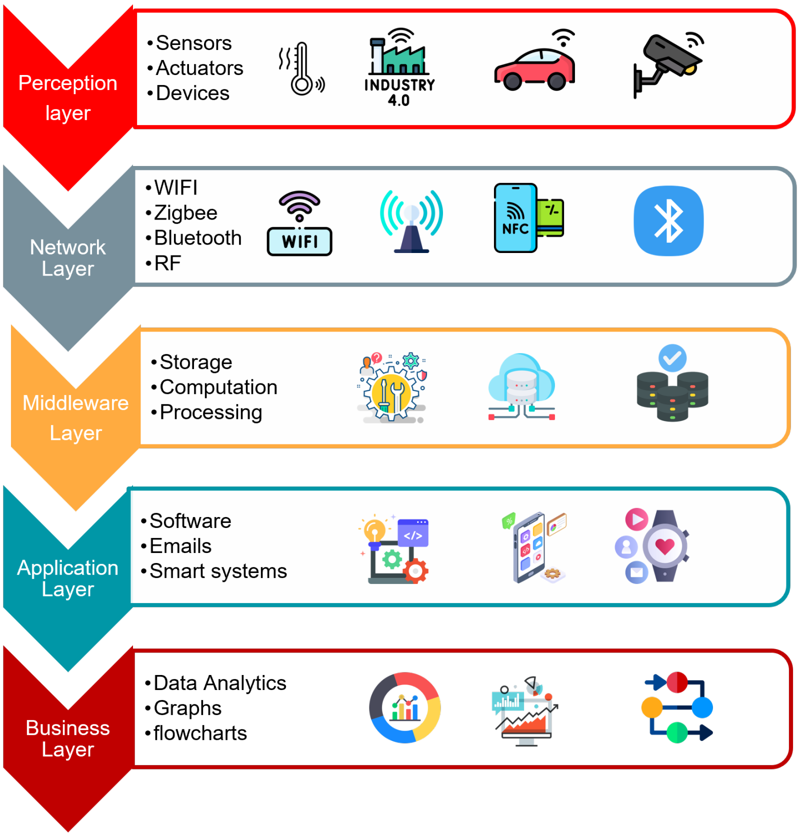

Figure 2. IoT system layers.

IoT systems face several challenges. Harit et al. [13] categorised these challenges into privacy and security, interoperability, scalability, heterogeneity, naming, and addressing. Among these challenges, privacy and security stand out as the primary concerns in IoT, with many of them manifesting at the network layer [13]. In 2021, statistics on IoT attack revealed a disturbingly high frequency of cyber attacks, numbered in the billions. This underscores the need for stringent measures to safeguard IoT networks and protect user information [14]. Mamdouh et al. [15] classified attacks on IoT systems into Goal-oriented, performer-oriented, and layer-oriented. These attacks have been a significant source of insecurity in IoT systems. Various technologies including artificial intelligence and blockchain have been deployed to address these threats [15]. The current work focuses on blockchain.

Blockchain is generally referred to as a tamper-proof distributed ledger that is immutable and securely linked by cryptographic hashing [16]. Each block contains a unique value called a nonce, which can only be used once. It also includes data, which represent the transactions saved on the blockchain, and a hash, which is a mathematical function that converts a variable-length (generally large) input string into a fixed-length output string. Blockchain technology has revolutionised the security and privacy of applications and devices by creating an interconnected and decentralised system that uses blocks to store information [17,18]. Figure 3 shows the components of a blockchain. Blockchain transactions are managed using a wallet and are protected by digital signatures. These transactions are temporally saved in the mempool until it is nominated and agreed upon via consensus to be added to the blockchain. Blockchains provide a new mode of distributed data storage, point-to-point transmission, consensus mechanisms, and encryption, with features such as decentralisation, openness, tamper-proofing, anonymity, and traceability [19].

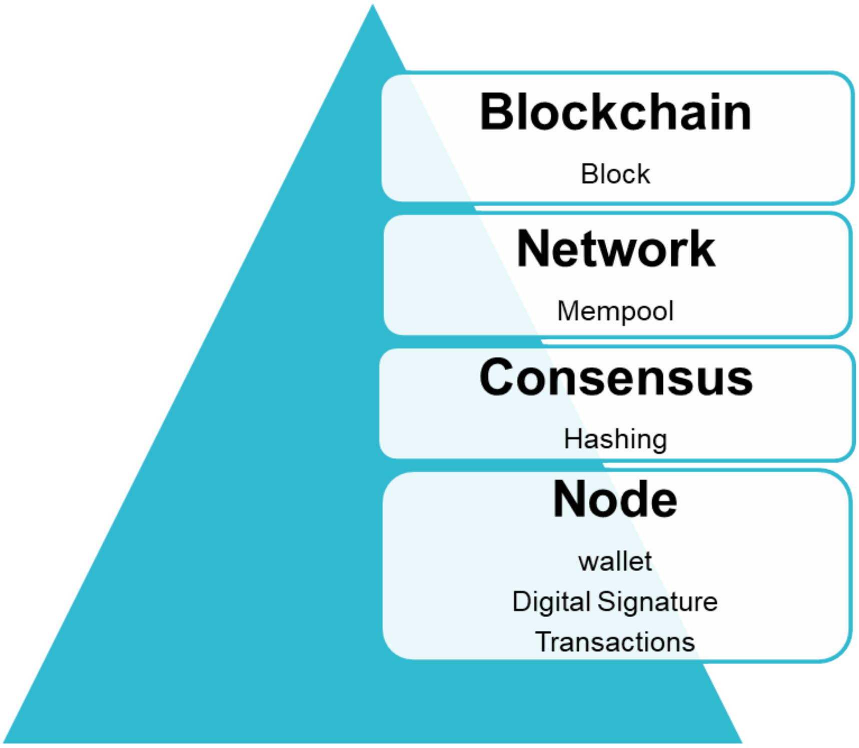

Figure 3. Blockchain framework components.

The effectiveness of blockchain technology in ensuring security, privacy, and reliability is well-established, which has led to its adaptation in various fields, including finance, e-government, IoT, public services, and supply chains. Numerous studies have delved into security and privacy issues in blockchain technology. Determining the most suitable blockchain type for an IoT ecosystem continues to pose a significant challenge in the field. This difficulty arises primarily from the inherent resource limitations of certain IoT devices, which require a careful consideration of the technology's adaptability. Consequently, the industry has witnessed the emergence of specialised solutions such as lightweight blockchain for IoT and half-node (pruned) blockchain for IoT [20]. These innovative approaches entail the deployment of either full-node (which takes part in all blockchain activities and stores all blocks) or pruned node (which only stores recent blocks and removes old blocks to manage storage space) blockchain structures within the IoT systems or the gateway of the IoT network, facilitating the seamless integration of blockchain technology with IoT devices [21]. As a result of this integration, the designated blockchain nodes are capable of collecting pertinent data from the IoT environment, which are then securely shared among the interconnected nodes within the blockchain network, enhancing the system's overall efficiency, security, and reliability. This has also invariably led to high resource consumption of such IoT systems [22].

This paper surveys emerging distributed ledger/blockchain platforms adopted to enhance security in IoT. It explore how these platforms can address vulnerabilities by securing data exchange between devices, managing device identities with tamper-proof mechanisms, and ensuring the integrity of transactions throughout the interconnected world of IoT. This is achieved by examining the frameworks, blockchain types, methodologies employed to ensure security at each layer of IoT, consensus algorithm, cryptography technology, and their limitations and strengths. The paper addresses the following research questions:

1. What are the emerging blockchain technologies/platforms/frameworks used in IoT security, their components, and how have they been modified for resource-constrained IoT devices?
2. Which of the components above can work across all IoT devices without impacting security?
3. What other technology can boost the security of IoT when added to the blockchain with less or no impact on performance?

To address these concerns, this study conducted a thorough search of related work on large database platforms via a digital library (Primo and Science Direct) and indexers (Google Scholar and SciSpace AI search assistance). A total of 14,745 journals were found using "IoT Security using blockchain". The results were filtered by removing duplicates, considering research work from high-profile research platforms (IEEE Xplore UK, ACM Digital Library US, Springer US, Elsevier Netherland, and MDPI Switzerland). The search was further screened by filtering with the following keywords: "Blockchain", "IoT", "Blockchain IoT", "Blockchain IoT Security", "Blockchain Cryptography in IoT Security", "survey of blockchain IoT security", "review of IoT security with blockchain", and "Consensus Mechanism in Blockchain IoT security", obtaining 1246 works. The results were assessed using their abstracts and methodology to select the 146 papers used in this work. Due to the systematic approach of this research, which considered works based on a definite blockchain platform used in IoT security, 46 works were examined under six blockchain platforms, 15 related works consisting of review and survey papers, and the rest of the papers were used to complement the research finding at different section of the paper. The methods are represented using the PRISMA literature search flow, as shown in Figure 4. The rest of the paper is organised as follows: Section 2 presents the related work. It analyses 15 selected reviews and survey papers on blockchain-based IoT security and positions the paper's contribution with a comparison table to reveal the existing gap. Section 3 presents the different blockchain platforms and discusses their usage in the IoT security literature. Section 4 provides an analysis and discussion. Finally, Section 5 concludes the paper with recommendations for future works.

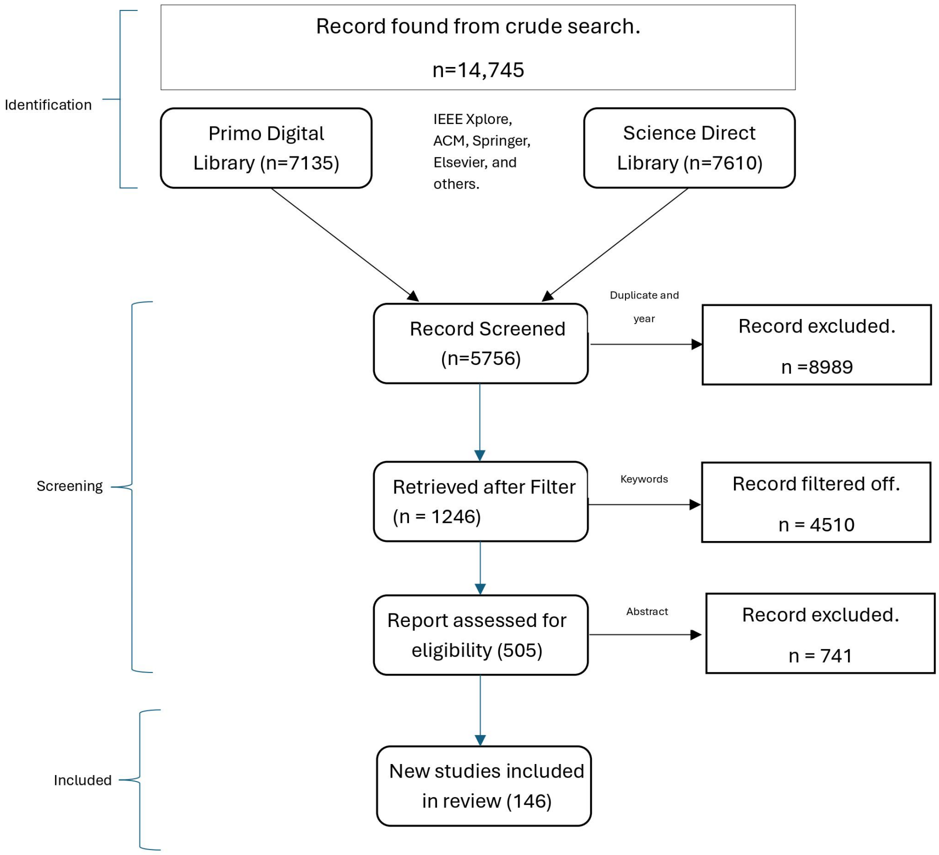
Identification
Record found from crude search.
n=14,745
Primo Digital Library (n=7135)
IEEE Xplore, ACM, Springer, Elsevier, and others.
Science Direct Library (n=7610)
Screening
Record Screened (n=5756)
Duplicate and year
Record excluded.
n =8989
Retrieved after Filter (n = 1246)
Keywords
Record filtered off.
n = 4510
Report assessed for eligibility (505)
Abstract
Record excluded.
n = 741
Included
New studies included in review (146)

Figure 4. PRISMA literature search flow.

2. Related Work

This section provides a summary of existing works and a table to compare 15 review and survey papers, comprising four journal articles and 11 conference papers. Most of these papers delve into fundamental aspects of blockchain and IoT, examining intersections and contemporary research directions. Many of these papers expand on their analyses by concentrating on specific areas or topics (tagged Focus) within IoT-BC systems.

Adaptation of Blockchain (BC) in IoT, its challenges, and solutions are a major focus of [23–25] . Wang et al. [24] additionally focused on Industrial IoT (IIoT). These papers discuss the basic structure and main features of blockchain and its application in the IoT and IIoT. Abdelmaboud et al. [25] reviewed the use of blockchain in IoT applications and provided a taxonomy that covers various aspects such as platforms, recent advances, challenges, and future research directions. Their work gave insights into several blockchain platforms and the contribution they can make to IoT networks. Lao et al. [26] provided an overview of IoT blockchains, including their architectures, communication protocols, applications, and traffic models. They discussed the network structures and protocols of popular IoT blockchain systems, compared different consensus algorithms, and analysed the traffic distribution in P2P and blockchain systems. They also emphasised the need for regulation and development policies to guide the integration of IoT and blockchain technology.

Overviews and reviews of IoT-BC integration and use-cases can be found in [27–29]. Sultan et al. [29] and Kumar et al. [30] additionally investigated issues encountered after IoT blockchain integration, focusing on aspects like system efficiency in terms of resource limitations and scalability. Chowdhury et al. [27] reviewed blockchain-based platforms from the perspective of IoT use cases. They introduced an evaluation framework to select a suitable blockchain platform for a given IoT application based on its specific requirements. They discussed different IoT use cases and their functional and non-functional requirements, emphasising the need for a clear understanding of the requirements to identify an appropriate blockchain platform. Sadawi et al. [28] discussed the integration of blockchain with IoT networks. They evaluated current research in this area and proposed an architectural framework that is structured around a system comprising three distinct layers: the device layer, the dew-blockchain layer, and the cloudlet-blockchain layer.

Security perspectives surrounding IoT-BC integration are seen in [30–34]. Darla and Naveena [34] conducted a critical review of blockchain-based wireless sensor networks (WSN), focusing on the security concerns in WSN and the adoption of blockchain in comparison with other research reviews. Kumar et al. [30] and Shammar Zahary and Al-Shargabi [33] reviewed security problems in IoT, the proposed solutions using blockchain, the status of blockchain adoption in IoT, and their challenges.

Table 1 provides a comparison of selected state-of-the-art surveys and review papers related to IoT security using blockchain. These papers were carefully looked at, considering their key focus (which represents the authors' research focus), reviewed work count (which is the number of works reviewed by their author), limitations, and recommendations for future work. There was a clear gap in the security perspective of IoT-BC in the work; also, the components of BC that enhance security in IoT are given less attention and, in some works, not discussed. These are part of the issues addressed in this work. While the existing reviewed papers focused on a few concepts of security benefits in blockchain IoT, the current paper goes in depth. The existing review identifies six emerging distributed ledger platforms, including five blockchain platforms and one DAG platform. These platforms were presented by conducting a detailed review of the works that use them in IoT systems security, emphasising security components.

Table 1. Comparison of survey and review papers from 2020 to 2024.

S/N	Work	Reviewed Work Count	Focus	Limitation	Recommendation
1.	[35]	98	Lightweight blockchain	No discussion on BC-IoT security	Recommend further research on security and efficiency
2.	[36]	N/A	Data transfer and storage in IoT-BC. Attacks and designs spaces in IoT-BC network	Work is more of a definition and explanation of network-related questions on BC-IoT	Not provided
3.	[32]	N/A	Security threat in IoT and solutions using BC	Blockchain solutions are not discussed in detail	Addressing open issues in IoT security
4.	[30]	8	IoT-BC architecture for IoT Security	No detailed reference to existing IoT-BC work and their challenges	A new, lightweight framework for IoT-BC
5.	[29]	7	IoT Issue and characteristics of BC that can solve them	No detail information on previous work and challenges	Practical implementation of IoT-BC system
6.	[31]	13	Summary of selected work	No technical discussion on integration and challenges	More framework and methods should be introduced for IoT-BC integration
7.	[24]	19	Application of BC in IoT and Industrial IoT	No element of security discussed	No recommendation

Table 1. *Cont.*

S/N	Work	Reviewed Work Count	Focus	Limitation	Recommendation
8.	[25]	20	Security and privacy issues and challenges in IoT-BC Integration.	Lacks detailed explanation on how the security and privacy are achieved	Future work can discuss in depth how to achieve privacy and security in IoT-BC
9.	[23]	7	IoT-BC application	Nothing on security	Not provided
10.	[37]	37	IoT challenges and performance of IoT-BC solutions	Security components in IoT-BC not covered	Proposes adopting dew and cloudlet layer architecture for IoT-BC
11.	[33]	81	Issues and trends in IoT-Blockchain security perspective	Focus on IoT security works using BC from 2017 to 2021	Explores how BC, edge computing, and IoT integration can improve security
12.	[27]	10	Brief review of selected IoT applications and IoT-BC use-cases	Unable to identify a most efficient platform for low resource device	To develop an architecture suitable for all IoT devices irrespective of their size
13.	[26]	N/A	Architecture, consensus, and traffic modelling	Security and platform choice	Security, regulation, and policy development should be addressed for IoT-BC
14.	[28]	15	Summary of works on IoT challenges and BC applications to IoT	Security perspective of IoT-BC not covered	None
15.	[38]	100	Paper review and Hyperledger Saw-tooth for Industrial IoT	Regulatory and compliance for IoT-BC not addressed	Cross-chain for IoT-BC, industrial standardization, distributed preservation, and privacy issues
16.	This	61	IoT-BC Platform and Security components	Limited to works from 2020 to 2024	Improvement on security component in IoT-BC integration

3. Blockchain Platforms

Six distributed ledger/blockchain platforms found to be the most used technology for enhancing security in the Internet of Things (IoT) were analysed in this work, following a thorough assessment of 146 studies. Figure 5 depicts the extent of their usage across the entirety of the works that were reviewed.

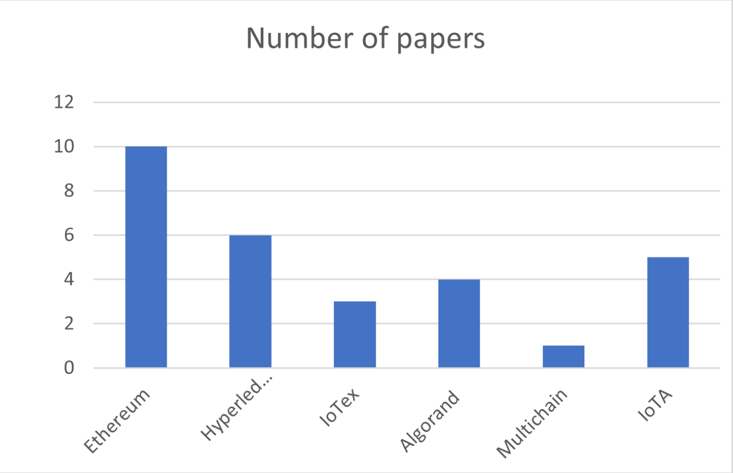

Figure 5. Blockchain platform used in research papers covered in this study.

3.1. Ethereum Blockchain

Ethereum, introduced in late 2015 by Vitalik Buterin, is one of the most distinguished blockchain platforms and frameworks for developing decentralised applications (DApps). The enhancement of security in IoT systems and the necessity for decentralised IoT systems resulted in the integration of Ethereum into IoT ecosystems. This integration was evident in various research studies, showcasing its utilisation across industries like Supply Chain, Healthcare, Transportation, Finance, and Agriculture. Ethereum's robust security stems from its carefully chosen components, including the consensus algorithm, smart contracts, encryption methods, and decentralised network. The consensus algorithm, transitioning to Proof of Stake with Ethereum 2.0, ensures transaction validation and network security. Smart contracts, which are self-executing agreements coded into the blockchain, enhance security by automating contract enforcement. Strong encryption methods like public-key cryptography safeguard data privacy. The decentralised network structure, powered by globally distributed nodes, eliminates single points of failure, bolstering security and resilience against potential threats. These elements collectively contribute to Ethereum's reputation as a secure platform for decentralised applications and digital transactions.

Numerous investigations and initiatives have delved into the application of the Ethereum blockchain in bolstering the security of Internet of Things (IoT) systems. The essence of these endeavours lies in utilising a decentralised, unalterable distributed ledger technology to facilitate secure and openly accessible data management for IoT gadgets. This strategy cultivates a state of affairs devoid of reliance on trust within the IoT environment, promoting transparency and guaranteeing data integrity, culminating in a more robust and dependable communication network among devices. Jabbar et al., Hussein et al. and Bawanar et al. [39–42] are examples of work that tend toward harnessing the security benefit of IoT–Ethereum integration. Rateb et al. [39] used this integration to secure vehicle communication through their proposed decentralised cloud computing platform. Patil et al. [43] adopted this integration to solve a major problem in the vehicle rental system. Other works such as [44–46] experimented on ethereum integration with IoT systems. The modification and addition of technologies were also discussed in some works such as [47], whose work adopted PoA for consensus in place of PoS/PoW. Fog computing and Interplanetary File systems were also introduced in [48] and [49], respectively.

3.2. Hyperledger

Hyperledger occupies a significant and influential position in blockchain technology and provides a broad spectrum of tools and frameworks tailored to cater to the distinct requirements of corporations and institutions. Some of its frameworks include Hyperledger Fabrics, Sawtooth, Indy, and Besu [50]. Like ethereum, Hyperledger's components include encryption (Digital signature and Hashing), chaincode, and Zero Knowledge of Proof (ZKP). Hyperledger is one of the most diversified blockchain frameworks. It redefined blockchain ecosystems by introducing lots of flexibility, such as choosing a custom consensus mechanism, two ledgers for blockchain queries, cryptography to secure transactions, decentralised identities, support for SDKs and APIs, and network monitoring [51]. Its notable influence has been seen in many studies lately for IoT security with blockchain.

Alshehri and Bamasag [52] identified insecurity with IoT access control and proposed a solution using Hyperledger Fabric. This solution employs attribute-based access control, where several attributes were determined based on the sensitivity of the data. The authors report the performance of the proposed system by testing it with the iFogSim simulator. Another work [53] dealt with protecting IoT system devices against attacks associated with firmware updates of embedded IoT devices. Their system uses blockchain as a trusted network to ensure the authenticity and integrity of firmware updates. CATP-Fabric was proposed as a new blockchain platform to solve issues around conflicting transaction problems in Hyperledger Fabric for delay-sensitive IoT applications. This work divides transactions into diverse groups for parallel processing, filters stale transactions, and prioritises read-only transactions to reduce overhead. The results illustrated show that

CATP-Fabric achieves a high throughput of successful transactions while maintaining a lower aborting transaction rate compared to benchmark blockchain systems.

To counter the latency issue that is common with IoT blockchain systems, Lee et al. [54] proposed a latency distribution model for Hyperledger Fabric (HLF) using probability distribution fitting and showed that the latency can be modelled with the gamma distribution. The paper further presents three significant parameters of high-level features and examines their effects on latency. It offers an approach to reduce the average latency of HLF. The model and analysis put forward in this study can be employed to predict the latency of HLF before the actual implementation of blockchain Internet of Things (BC-IoT) networks, thereby addressing the outstanding issue of latency estimation in [50]. Pajooh et al. [50] leveraged smart contracts in HLF to propose a model addressing the scalability, processing power, and storage limitation of IoT edge devices in the blockchain network. HLF is a permission blockchain that has been successfully proposed as a solution to several IoT system issues. Its flexibility has been leveraged in several works.

3.3. IOTA Blockchain

IOTA is a distributed ledger platform that employs a Directed Acyclic Graph (DAG) structure, as opposed to a traditional blockchain. Its intended use is for the Internet of Things (IoT) ecosystem, with an emphasis on scalability, low fees, and secure data transfer between devices [55]. The IOTA platform comprises numerous key features and components, including Tangle Technology, Zero Fees, Decentralised Consensus, MAM (Masked Authenticated Messaging), IOTA Tokens (MIOTA), Smart Contracts (IOTA Smart Contracts—ISCP), Qubic, and Decentralised Identity (DID) [56].

The technology uses a DAG-based structure called the Tangle, allowing for parallel processing and scalability, while Zero Fees ensures a feeless environment. Decentralised Consensus is achieved through a process called “Tip Selection”, thus eliminating the need for miners or validators [57]. The MAM protocol enables private communication and data integrity. IOTA Tokens (MIOTA) are utilised for value transfer and data transactions within the Tangle. IOTA is developing smart contract functionality through the IOTA Smart Contracts Protocol (ISCP), which enables developers to create decentralised applications and automate agreements on the IOTA network [58]. The IOTA development caught the attention of some researchers such as [55,56,58]. They all focused on identifying the gaps in IOTA to further improve it.

Khan et al. [38] adopted IOTA with Edge computing (EC) to tackle the obstacles of real-time processing, resource allocation, and storage provision in IoT devices. They conducted an in-depth survey to identify recurring problems with IoT systems and provided a counter solution to it using EC and IOTA blockchain. Additionally, IOTA explores decentralised identity solutions for secure and private identity management. IOTA has partnered with various companies and organisations to explore real-world applications of its technology, including supply chain management, smart cities, energy management, and more.

3.4. IoTeX Blockchain

The IoTeX blockchain platform was custom-built to cater to the specific needs of the IoT ecosystem. It was developed to overcome the obstacles and constraints faced by current blockchains in meeting the distinct demands of IoT devices and applications. The IoTeX blockchain platform encompasses several critical facets and elements [59].

The architecture of IoTeX consists of multiple interconnected blockchains, including the Root Chain and multiple sub-chains customised for specific use cases. The Root Chain serves as the main blockchain responsible for network consensus and security. The consensus algorithm employed by IoTeX is Roll-DPoS, which enhances security, scalability, and decentralisation. Various token standards, such as IOTX, XRC20, and XRC721, are supported by IoTeX, and tailored for IoT use cases [59].

IoTeX achieved high scalability using sub-chains, which allows for parallel processing and reduces congestion on the main chain. The platform also incorporates advanced privacy features like secure data transfers and lightweight encryption. A decentralised identity framework is offered by IoTeX, which enhances security and control over personal data. The Internet of Trusted Things concept was introduced by IoTeX, focusing on building secure and trusted interactions between devices and users [59].

IoTeX employs innovative cryptography methods to generate secure and unpredictable random numbers, which is essential for certain use cases in IoT. The platform is designed to be compatible with other blockchains, enabling cross-chain communication and interoperability. A growing ecosystem of developers, partners, and community members is working together to build and expand the platform's capabilities and use cases.

The specialised focus of IoTeX on IoT and its architecture were designed to address IoT-related challenges and distinguish it from other general-purpose blockchain platforms. The platform strives to provide a secure and scalable foundation for various IoT applications, including supply chain management and data marketplaces [60]. Fan et al. [61] found that works on IoTeX have shown the strength of the technology in addressing the key challenges in integrating IoT with blockchain. Fan and his team published a paper after developing a user-centric Blockchain-based secure IP camera, which was built on the IoTeX platform. Other works were seen from different domains, such as Wearables [62] and Mobile Payment [63].

3.5. Algorand

Algorand was introduced in 2019 by Silvio Micali and specifically engineered to prioritise reduced latency, security, and decentralisation [64]. This is achieved by employing inventive consensus mechanisms and cryptographic methodologies. Security components in the Algorand blockchain are cryptographic Sortition (Verifiable Random Function), PoS consensus mechanism, and other encryption mechanisms (Hash Function and Edwards-Curve Digital Signature (EdDSA)). Algorand is suitable for various blockchain applications, including financial services, supply chain management, and IoT [65]. The Algorand Blockchain is gaining prominence as a promising technology for the Internet of Things (IoT) owing to its self-sustaining and decentralised characteristics [66]. It has been implemented in low-powered IoT devices such as the Raspberry Pi 4 Model B and the STMicroelectronics STM32MP157A-DK1 [66]. A multi-level blockchain structure and consensus algorithm have been put forth to enhance the security and dependability of IoT data management [24,67]. Additionally, blockchain-based data verification schemes can safeguard data integrity in IoT by employing distributed data authentication and lightweight mining processes, as proposed by Wadhwa et al. [65] in their work. Cardamone et al. [68] used Algorand together with Messaging and Queues Telemetry Transport (MQTT), and Transport Layer Security (TLS), to solve a major authentication issue in an IoT electrical energy system.

3.6. Multichain

Multichain is an example of a cross-chain platform, which supports over 26 blockchains including Ethereum and Bitcoin. Cross-chain refers to integrating various forms of blockchain technologies into interrelated blockchains within a unified network or ecosystem. Although there are few works in this domain, there are some works exploring this concept in the IoT ecosystem. Multichain comes with its components, such as blockchain networks, Nodes (Full Node, API Node, and Mining Node), Assets, Streams, Permissions, Mining controls, etc. This is the building block of the Multichain blockchain. Multichain comes with the flexibility to choose from different consensus mechanisms, with support for PoW, PoS, DPoS, Round Robin, Byzantine Fault Tolerance and Custom Consensus Mechanism. This can selected during the network set-up. Multichain networks in IoT were adopted by [69,70] who aimed at reviewing the existing work and experimenting with multichain integration in IoT. Sawant et al. [70] developed a prototype system using Raspberry Pi and Savoir Rapper for multichain. Umran et al. [71] explored multichain to secure IoT in the petroleum application. They reviewed existing work in the domain and proposed a new architecture comprising an IoT system, multichain, and an interplanetary file system (IPFS). Synergy chain is a multichain framework for IoT blockchain. To address the data-sharing and access controls, Chang et al. [72] proposed this.

4. Analysis and Discussion: IoT Security and BC Components

IoT insecurity can best be summarised in terms of authentication, privacy, data storage, and update delivery. Blockchain is a trust- and privacy-inclined technology, with every component contributing to the security and privacy of IoT in one way or another.

4.1. Technology

This work focuses on six trending and emerging blockchain technologies used in IoT security. We have seen Ethereum as the choice of most researchers. Ethereum is the most used technology, as illustrated in Figure 6. Another technology that has gained much momentum in adoption is Hyperledger. Other platforms include IoTA, IoTeX, and Algorand. From our findings, we observed large community support on both Ethereum and Hyperledger from individuals and organisations who are actively improving the framework. This may justify their popularity within the research community. Also, we noticed that the adoption of Ethereum in the IoT space started quite recently. This can be attributed to the adoption of a new consensus mechanism (PoS), which reduces power consumption significantly without impacting its security. Table 2 is a summary of selected works from the six blockchain technologies reviewed, their area of applications, additional technology used to support their development, and their choice of consensus algorithm. From this table, it is observed that there is a trend towards supporting IoT-BC integration with cloud services, external BC file storage such as IPFS, and creating web interfaces for easy management. Cloud storage has helped IoT systems in terms of data storage but does not guarantee security. Blockchain storage Technology such as IPFS has been a good replacement. Other security enhancement technologies introduced to support resource-constrained IoT-BC integration include the TLS protocol and Pebble Tracker.

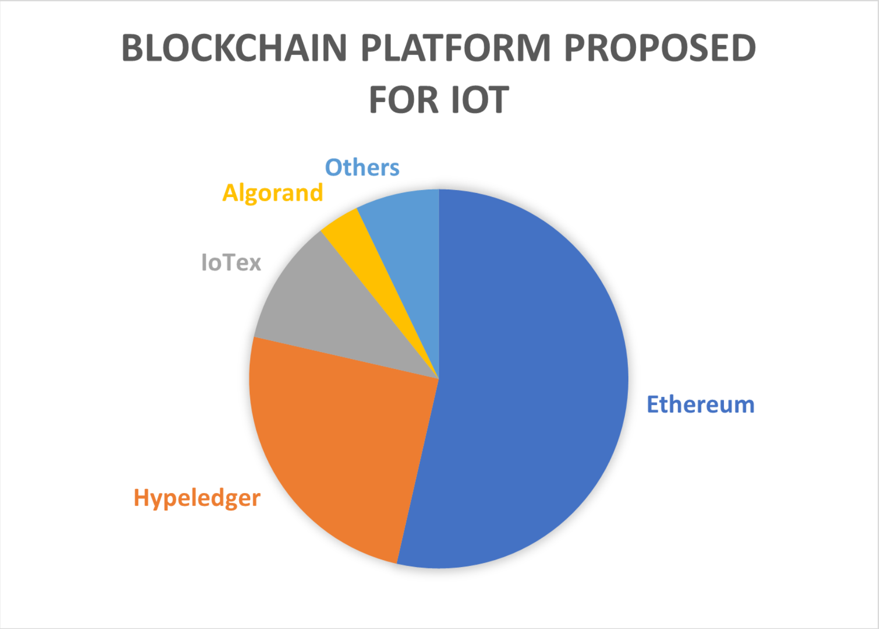

Figure 6. Blockchain platform for IoT.

Table 2. Technologies in selected IoT-BC existing works and their areas of applications.

S/N	Work	Areas of Application	Technologies	Blockchain Platform	Consensus
1.	[48]	Healthcare	Cloud and Fog computing	Ethereum	PoS, POW , PoA
2.	[40]	Authentication and Access control	None	Ethereum	POS
3.	[39]	Vehicle communication	Cloud computing	Ethereum	PoW
4.	[41]	Voting System	Web	Ethereum	PoW
5.	[73]	E-Business	None	Ethereum	PoW and PoA
6.	[74]	Embedded System	FGPA	Ethereum	PoW
7.	[42]	Data Counterfeiting	Cloud	Ethereum	PoW
8.	[75]	Decentralised Authentication	web	Ethereum	PoW
9.	[76]	Key Management	TLS Protocol	Ethereum	PoW
10.	[47]	Networks Attacks	None	Ethereum	Proof of Authority
11.	[49]	Data Sharing	Interplanetary File System	Ethereum	PoS
12.	[52]	Access Control	Lightweight cryptography	Hyperledger Fabric	PBFT
13.	[53]	Firmware Update	None	Hyperledger Fabric	PBFT
14.	[63]	Experimental IoT	None	Hyperledger Fabric	PBFT
15.	[50]	Edge Internet	None	Hyperledger	PBFT
16.	[77]	Access Control	None	IoTA	DAG
17.	[78]	TangleSim	None	IoTA	DAG
18.	[55]	Access Control	Lightweight cryptography	IoTA	DAG
19.	[58]	IOTA	None	IoTA	DAG
20.	[62]	Wearable	None	IoTeX	Roll-DPoS
21.	[79]	Data Authorisation	Pebble Tracker	IoTeX	Roll-DPoS
22.	[63]	Mobile Payment	None	IoTeX	Roll-DPoS
23.	[61]	Home IP Camera System	Intel SGX	IoTeX	Roll-DPoS
24.	[68]	Electrical Energy System, Authentication	MQTT, TLS, and CA	IoTeX	Roll-DPoS
25.	[66]	Prototype	Raspberry Pi and STM32	Algorand	Pure PoS
26.	[68]	Electrical Energy System, Authentication	MQTT, TLS, and CA	Algorand	Pure PoS
27.	[69]	None	None	Multichain	N/A
29.	[80]	Authentication	None	Multichain	DAG
30.	[71]	Industrial IoT	IPFS	Multichain	Proof of Rapid Authentication
31.	[70]	Security	None	Multichain	NA

4.2. Consensus

The Consensus mechanism provides trust in the blockchain, ensuring that every block is verified before being added to the blockchain. This has invariably been used in IoT-Blockchain to ensure data integrity in IoT system communication. Achieving consensus follows three processes: proposal (where a node proposes a block to be added), verification (another node validating the proposed block), and agreement (the majority node agrees that the proposed block is valid). This process employs algorithms such as Proof of Work (PoW), Proof of Stake (PoS), Byzantine fault tolerance (BFT), Proof of Authority (PoA), Practical

Byzantine Fault Tolerance (PBFT), and Raft to achieve the agreement. This agreement helps to ensure the right data are added to the blockchain, especially in a large IoT system where several IoT systems depend on each other's data. It also guides against malicious actions by preventing unauthorised tampering and easily spotting malicious nodes. Research has shown that consensus algorithms also have flaws, and some of these are less effective in small IoT networks due to the required resources to carry out the attack.

For IoT security using blockchain, default consensus algorithms are adopted on most platforms based on IoTeX, Algorand, Ethereum, and Hyperledger. A few exceptions also exist where other consensus mechanisms were proposed to support resource-constrained IoT devices. Figure 7 illustrates the consensus algorithms from the perspective of their use in IoT research papers covered in this study. From the reviewed works, the mechanism of achieving consensus by each algorithm was explained, along with some attacks that each algorithm can be vulnerable to. This is summarised in Table 3. Six algorithms are carefully selected as the most used in the IoT blockchain. The comparison of consensus algorithms in Table 3 highlights that many are susceptible to attacks like Sybil attacks, 51% attacks, and long-range attacks. However, these attacks often require significant resources, making them less of a concern for integrating blockchain with resource-constrained IoT devices.

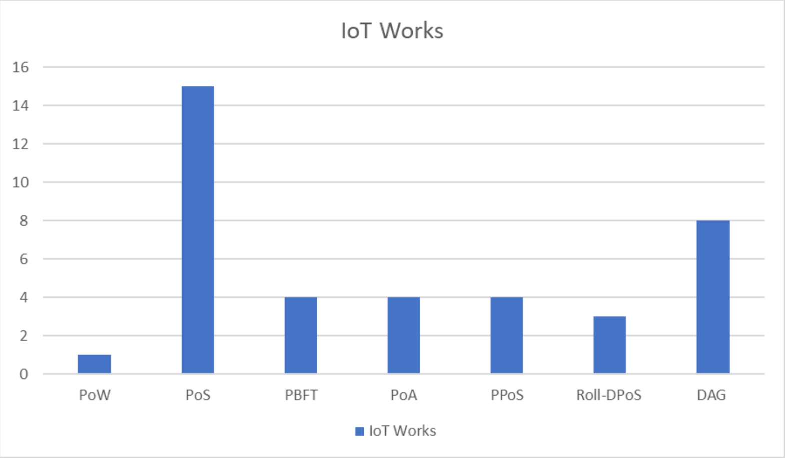

Figure 7. Consensus mechanisms in the studied literature.

Table 3. Consensus algorithm properties and threats.

S/N	Consensus	Blockchain	Mechanism	Threat	Throughput
1.	PoS	Ethereum	Locked assets	Sybil & 51% attack	20 TPS
2.	Pure PoS	Algorand	Random selection	long range attack	6000 TPS
3.	DAG PoW	IoTA	Tip Selection	34% attack	12 TPS
4.	Roll- DPoS	IoTeX	Random selection	Collusion Attacks	10,000 TPS
5.	Round Robins	Multichain	Rotational	Nothing at stake attack	2 million TPS
6.	PBFT	Hyperledger	Voting	1/3 faulty node & DoS	20,000 TPS

4.3. Cryptography

Another key security component for blockchain-based IoT security solutions is cryptography. Cryptography contributes highly to the security of information in blockchain. By employing cryptographic mechanisms including hashing, digital signatures, zero-knowledge proof, and encryption, blockchain systems can foster increased levels of security and trust among users and things. This has been adopted for IoT security in areas of authentication, data encryption during communication, and data validation. Existing blockchain technology has been seen to use different cryptographic settings for digital signatures, e.g., Ethereum uses an Elliptic Curve Digital Signature Algorithm (ECDSA), which is a type of Elliptic Curve Cryptography (ECC); others are the Edward Digital Signature Algorithm (EdDSA) and Rivest–Shamir–Adleman (RSA). ECDSA is adopted in most works, and while some of these works proposed a lightweight ECC to adapt it to resource-constrained IoT devices, this is not recommended as it impacts the security strength of the device. Cryptographic Sortition is another approach used by Algorand. The Winternitz One-Time Signature (WOTS) and Merkle Signature Scheme were also used and are considered quantum resistant. Figure 8 illustrates the percentage breakdown of reliance and security contribution provided by the predominant key tools across the six platforms under examination. The calculation of this percentage involves a standard fixed allocation of 30% for all major security tools, namely, consensus, digital signature, and hashing. The remaining portion is derived from the collaborative security features integrated to augment the overall security framework of the platforms.

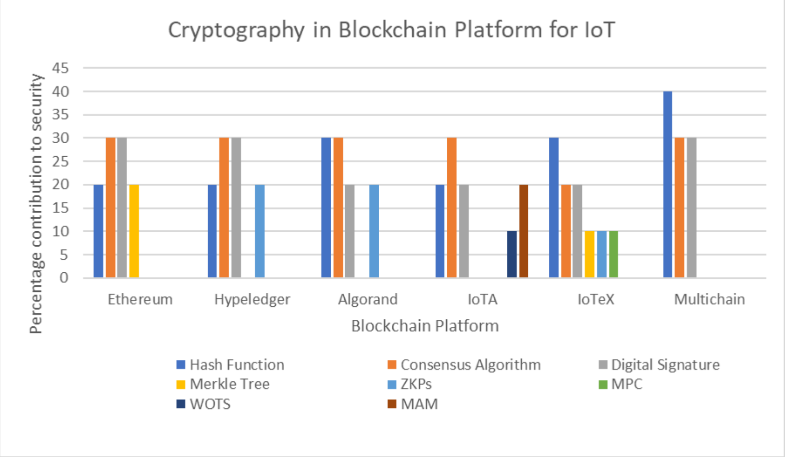

Figure 8. Cryptography in Blockchain platform for IoT.

5. Effect of Blockchain

In an IoT network, devices can communicate and transfer data autonomously. Transferred data may be private and highly confidential in many applications, e.g., healthcare, defence, smart buildings, etc., which amplifies the security risks of such systems. Blockchain technology has revolutionised the IoT system by addressing these security risks (such as weak authentication, insecure communication, and unreliable updates). Through decentralised identity, encrypted transactions, immutable records, and data distribution, blockchain ensures the integrity, authenticity, and protection of IoT systems. Its resistant nature to manipulation further solidifies its role in safeguarding IoT ecosystems. The adoption of blockchain also has both security and performance effects on IoT systems.

5.1. Security Effect

Table 4 presents a few of the most significant security issues that blockchain technology has helped to tackle. It emphasises the technology of blockchain that was utilised to solve the security challenges as well as the research that led to the development of the solution. Considering the security concerns of weak authentication and unrestricted access to systems, decentralised authentication and access control on a permissioned blockchain like Ethereum is an intriguing solution that was proposed in [40]. This method utilises an "authorisation sensitivity factor" stored on the blockchain. This factor determines a client device's access level, eliminating the need for a central authority to manage permissions. This system was tested against distributed denial of service attacks (DDOS) and was found to be secure against them. Another good example is delivering secured firmware update to devices. Bettayeb et al. [53] adopted blockchain as the secure network to deliver the updates to various devices on the chain whose firmware versions are verified for already validated firmware files. Similar to the above, Jeyakkannan et al. [47] enhanced IoT network communication by adopting blockchain as the medium of exchange of information between devices. Data and privacy protection are critical challenges in IoT systems. To address this, researchers in [49] proposed a three-phase approach. This involves establishing secure authentication through decentralised blockchain-based authentication (DBA), safeguarding data with blockchain encryption, and ensuring data integrity through secure decryption. Insufficient privacy protection, which is common in IoT systems, was also addressed in [42] by encrypting the identity of devices on the block and managing access to information using data access control and auditable data provenance of ethereum blockchain. Blockchain offers a secure architecture for IoT applications, but that does not mean it is immune to security challenges. Resource constraints in some IoT devices might limit the feasibility of certain attacks, but others remain a significant concern. These include Sybil attacks, 51% attacks, replay attacks, wallet poisoning, and smart contract vulnerabilities. Carefully evaluating these risks is crucial when choosing a blockchain platform for IoT security.

Table 4. Breakdown of IoT security enhancement with BC-components.

S/N	Security Challenges	Research Works	Blockchain Technologies
1.	Weak Authentication and Uncontrolled Access	[40,55,75]	Immutable Ledger, Decentralised Identity, Digitally signed Wallet
2.	Insecure Network Services and Communication	[47]	Encrypted Communication, Smart Contracts/ Chain-code.
3.	Lack of Secure Update Mechanism	[53]	Immutable Update History, Decentralised Distribution
4.	Insufficient Privacy Protection	[42]	Data Access Control, DBA, Auditable Data Provenance
5.	Data Protection	[49,79]	Blockchain Digital signature, Consensus Algorithm

5.2. Performance Effect

Although performance and scalability are not security issues, it is important to briefly explain their effect in achieving efficiently secured IoT-BC system. While blockchain presents a compelling solution for securing IoT, its adoption comes with performance-related challenges due to the limitations of IoT devices in terms of computation, memory, and power supply. Scalability is also a major hurdle. Integrating public blockchains can lead to slow transaction processing times and high costs, making them unsuitable for resource-constrained IoT devices. Additionally, the complexity increases, potentially requiring specialised knowledge or dedicated blockchain expertise for management. Also, the regulatory landscape surrounding blockchain is still evolving, creating uncertainty for businesses considering its implementation. This ambiguity could hinder wider adoption. This survey will serve as a guide for future research and will allow researchers to build upon previous work to further improve security solutions.

6. Conclusions

The IoT security ecosystem has witnessed a great transformation with the introduction of blockchain, and several research projects have explored this technology. This paper reviewed works from the blockchain platform perspective. This was achieved through a review of literature by identifying the gaps and positioning the contributions. This paper is more security-centric compared to the existing literature. It presents a detailed review of the emerging blockchain platforms used in IoT system security, with more emphasis on cryptography and other security components of the blockchain. The reviewed work presented a greater adoption of private and hybrid blockchains compared to exclusively public blockchains, with 55%, 25%, and 20%, respectively, in the number of works. Technology such as IPFS, cloud technology, TSL, fog, etc. has been identified as promising for complementing security in IoT-Blockchain Integration. Also, there has been an increase in research work in this field in the last few years and we expect more to come.

Potential directions in this domain include the following: Improving the existing consensus mechanism to enhance more adoption of it in the resource-constrained IoT system without compromising security, such as using Proof of Location (PoL). Cryptography: More work should be done to further discover lightweight cryptography algorithms that will be quantum-proof. Innovative identity mechanisms, e.g., decentralised identity, can be adopted in place of full blockchain nodes for very light IoT devices.

Author Contributions: Conceptualization, Y.K., D.D. and E.G.; methodology, Y.K. and D.D.; validation, D.D. and E.G.; formal analysis, Y.K., D.D. and E.G.; investigation, Y.K., D.D. and E.G.; resources, Y.K., D.D. and E.G.; data curation, Y.K. and D.D.; writing—original draft preparation, Y.K. and D.D.; writing—review and editing, Y.K., D.D. and E.G.; visualization, Y.K. and D.D.; supervision, D.D. and E.G.; project administration, D.D.; funding acquisition, D.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Arab–German Young Academy (AGYA) Academy grant number 01DL20003 from BMBF. This research was funded by UWE Bristol: PHD Scholarship from Computer Science Research Centre, College of Arts, Technology and Environment, +CHIST–ERA EU Project grant number EP/Y036301/1 from EPSRC.

Data Availability Statement: No new data were created or analyzed in this study.

Acknowledgments: Sincere appreciation to the reviewers for their insightful comments.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
BC	Blockchain
PoW	Proof of Work
PoS	Proof of Stake
PoL	Proof of Location
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
TPS	Throughput Per Second
DoS	Denial of Service
ECC	Elliptic Curve Cryptography

References

1. Khan, M.N.U.; Cao, W.; Tang, Z.; Ullah, A.; Pan, W. Energy-Efficient De-Duplication Mechanism for Healthcare Data Aggregation in IoT. *Future Internet* **2024**, *16*, 66 . [CrossRef]
2. Wang, H.; Huang, J.; Wang, G.; Lu, H.; Wang, W. Contactless Patient Care Using Hospital IoT: CCTV-Camera-Based Physiological Monitoring in ICU. *IEEE Internet Things J.* **2024**, *11*, 5781–5797. [CrossRef]
3. Bagheri, N.; Bendavid, Y.; Safkhani, M.; Rostampour, S. Smart Grid Security: A PUF-Based Authentication and Key Agreement Protocol. *Future Internet* **2024**, *16*, 9. [CrossRef]
4. Lasla, N.; Doudou, M.; Djenouri, D.; Ouadjaout, A.; Zizoua, C. Wireless energy efficient occupancy-monitoring system for smart buildings. *Pervasive Mob. Comput.* **2019**, *59*, 101037. [CrossRef]
5. Marin, O.; Cioara, T.; Anghel, I. Blockchain Solution for Buildings' Multi-Energy Flexibility Trading Using Multi-Token Standards. *Future Internet* **2023**, *15*, 177. [CrossRef]
6. Djenouri, D.; Laidi, R.; Djenouri, Y.; Balasingham, I. Machine Learning for Smart Building Applications: Review and Taxonomy. *ACM Comput. Surv.* **2019**, *52*, 1–36. [CrossRef]
7. Djenouri, Y.; Belhadi, A.; Djenouri, D.; Srivastava, G.; Lin, J.C.W. A Secure Intelligent System for Internet of Vehicles: Case Study on Traffic Forecasting. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 13218–13227. [CrossRef]

8. Jovanovic, B. Internet of Things Statistics for 2023—Taking Things Apart. Technical Report; DataProt. 2023. Available online: https://dataprot.net/statistics/iot-statistics/ (accessed on 1 May 2024).
9. Rasheed, A. IoT Explosion Connected Possibility. 2016 . Available online: https://www.linkedin.com/pulse/iot-explosion-connected-possibility-abdul-rasheed (accessed on 1 May 2024).
10. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.Y.; Bashir, A.K.; El-Latif, A.A. DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access* **2020**, *8*, 111223–111238. [CrossRef]
11. Abdmeziem, M.; Tandjaoui, D.; Romdhani, I. Architecting the Internet of Things: State of the Art. In *Robots and Sensor Clouds*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 55–75. [CrossRef]
12. Antão, L.; Pinto, R.; Reis, J.P.; Gonçalves, G. Requirements for Testing and Validating the Industrial Internet of Things. In Proceedings of the 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Västerås, Sweden, 9–13 April 2018. [CrossRef]
13. Harit, A.; Ezzati, A.; Elharti, R. Internet of things security: Challenges and perspectives. In Proceedings of the ACM International Conference Proceeding Series, Association for Computing Machinery, Tacoma, WA, USA, 18–20 August 2017. [CrossRef]
14. Cyrus, C. IoT Cyberattacks Escalate in 2021, According to Kaspersky. 2021 . Available online: https://www.iotworldtoday.com/security/iot-cyberattacks-escalate-in-2021-according-to-kaspersky (accessed on 1 May 2024).
15. Mamdouh, M.; Elrukhsi, M.A.; Khattab, A. Securing the Internet of Things and Wireless Sensor Networks via Machine Learning: A Survey. In Proceedings of the 2018 International Conference on Computer and Applications, ICCA 2018, Beirut, Lebanon, 25–26 August 2018; pp. 215–218. [CrossRef]
16. Nathan, C.; Leandros, M.A.; Ioanna, K.; Nestoras, C.; Amine, F.M. Blockchain Technology: Security and Privacy Issues. In *Blockchain Technology and Innovations in Business Processes*; Srikanta, P., Wang, T.S., Tao, S., Kumar, P.S., Eds.; Springer: Singapore, 2021; pp. 95–107. [CrossRef]
17. Zhong, S.; Huang, X. Special Focus on Security and Privacy in Blockchain-Based Applications. *Sci. China Inf. Sci.* **2020**, *63*, 130100. [CrossRef]
18. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv.* **2019**, *52, 1–34.* . [CrossRef]
19. Huang, H.; Kong, W.; Zhou, S.; Zheng, Z.; Guo, S. A Survey of State-of-the-Art on Blockchains. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 44. [CrossRef]
20. Chen, Z.; Cui, L.; Palanisamy, B.; Zhang, L.J. (Eds.) Blockchain—ICBC 2020. In *Lecture Notes in Computer Science*; Springer International Publishing: Cham, Switzerland, 2020; Volume 12404. [CrossRef]
21. Shaikh, M.; Shibu, C.; Angeles, E.; Pavithran, D. Data storage in blockchain based architectures for internet of things (IoT). In Proceedings of the 2021 IEEE International IOT, Electronics and Mechatronics Conference, IEMTRONICS 2021, Toronto, ON, Canada, 21–24 April 2021. [CrossRef]
22. Amitha, A.K.; Pamba, R.V. A Solid Waste Management System Using Smart Bins in a Decentralized Manner in Ethereum Blockchain Network for Incentivization. In Proceedings of the ICCSC 2023—Proceedings of the 2nd International Conference on Computational Systems and Communication, Thiruvananthapuram, India, 3–4 March 2023. [CrossRef]
23. Shah, R. A Systematic Review on Blockchain in IoT. In Proceedings of the 4th International Conference on Energy, Power, and Environment, ICEPE 2022, Shillong, India, 29 April–1 May 2022. [CrossRef]
24. Wang, Q.; Zhu, X.; Ni, Y.; Gu, L.; Zhu, H. Blockchain for the IoT and industrial IoT: A review. *Internet Things* **2019**, *10*, 100081. [CrossRef]
25. Abdelmaboud, A.; Ahmed, A.I.A.; Abaker, M.; Eisa, T.A.E.; Albasheer, H.; Ghorashi, S.A.; Karim, F.K. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* **2022**, *11*, 630. [CrossRef]
26. Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 18. [CrossRef]
27. Chowdhury, M.J.M.; Ferdous, M.S.; Biswas, K.; Chowdhury, N.; Muthukkumarasamy, V. A survey on blockchain-based platforms for IoT use-cases. *Knowl. Eng. Rev.* **2020**, *35*, e19. [CrossRef]
28. Sadawi, A.A.; Hassan, M.S.; Ndiaye, M. A Review on the Integration of Blockchain and IoT. In Proceedings of the ICCSPA 2020—4th International Conference on Communications, Signal Processing, and Their Applications, Online, 16–18 March 2021. [CrossRef]
29. Sultan, A.; Mushtaq, M.A.; Abubakar, M. IoT security issues via blockchain: A review paper. In Proceedings of the ACM International Conference Proceeding Series, Wuhan, China, 12–13 July 2019; Volume Part F148153, pp. 60–65. [CrossRef]
30. Kumar, S.; Vidhate, A. Issues and Future Trends in IoT Security using Blockchain: A Review. In Proceedings of the IDCIoT 2023-International Conference on Intelligent Data Communication Technologies and Internet of Things, Bengaluru, India, 5–7 January 2023; pp. 976–984. [CrossRef]
31. Sallam, A.; Qahtani, F.A.; Gaid, A.S. Blockchain in Internet of Things: A Systematic Literature Review. In Proceedings of the 2021 International Conference of Technology, Science and Administration, ICTSA 2021; 22–24 March 2021. [CrossRef]
32. Alam, S.R.; Jain, S.; Doriya, R. Security threats and solutions to IoT using Blockchain: A Review. In Proceedings of the Proceedings—5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021, Madurai, India, 6–8 May 2021; pp. 268–273. [CrossRef]

33. Shammar, E.A.; Zahary, A.T.; Al-Shargabi, A.A. A Survey of IoT and Blockchain Integration: Security Perspective. *IEEE Access* **2021**, *9*, 156114–156150. [CrossRef]
34. Darla, S.; Naveena, C. Survey on Securing Internet of Things through Block chain Technology. In Proceedings of the International Conference on Electronics and Renewable Systems, ICEARS 2022, Tuticorin, India, 16–18 March 2022; pp. 836–844. [CrossRef]
35. Stefanescu, D.; Montalvillo, L.; Galan-Garcia, P.; Unzilla, J.; Urbieta, A. A Systematic Literature Review of Lightweight Blockchain for IoT. *IEEE Access* **2022**, *10*, 123138–123159. [CrossRef]
36. Dotan, M.; Pignolet, Y.A.; Schmid, S.; Tochner, S.; Zohar, A. Survey on Blockchain Networking: Context, State-of-the-Art, Challenges. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 107. [CrossRef]
37. Sadawi, A.A.; Hassan, M.S.; Ndiaye, M. A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges. *IEEE Access* **2021**, *9*, 54478–54497. [CrossRef]
38. Ayub Khan, A.; Laghari, A.A.; Shaikh, Z.A.; Dacko-Pikiewicz, Z.; Kot, S. Internet of Things (IoT) Security with Blockchain Technology: A State-of-the-Art Review. *IEEE Access* **2022**, *10*, 122679–122695. [CrossRef]
39. Jabbar, R.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, K. Blockchain for the Internet of Vehicles: A Decentralized IoT Solution for Vehicles Communication Using Ethereum. *Sensors* **2020**, *20*, 3928. [CrossRef] [PubMed]
40. Hussein, D.H.; Anbarasu, R.; Matrawy, A.; Ibnkahla, M. Towards a Decentralized Access Control System for IoT Platforms based on Blockchain Technology. In Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 20–22 October 2020; pp. 1–6. [CrossRef]
41. Othman, A.A.H.; Muhammed, E.A.A.; Mujahid, H.K.M.; Muhammed, H.A.A.; Mosleh, M.A.A. Online Voting System Based on IoT and Ethereum Blockchain. In Proceedings of the 2021 International Conference of Technology, Science and Administration (ICTSA), Taiz, Yemen, 22–24 March 2021; pp. 1–6. [CrossRef]
42. Bawankar Chetan, D.; Kukkar Sayali, D.; Chaudhari Vaishnavi, J.; Rashinkar Suraj, R.; Solanke Sanket, U. Preventing Data Counterfeiting Among Internet of Things (IoT) Devices using Ethereum Blockchain. In Proceedings of the 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021; pp. 484–488. [CrossRef]
43. Patil, S.; Adsul, D.; Desale, S.; Gandole, K. Smart Vehicle Rental Application using Blockchain and IoT. In Proceedings of the 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 23–25 December 2022; pp. 1–6. [CrossRef]
44. Sureshkumar, T.; Sivaraj, R.; Vijayakumar, M. Design and implementation of a framework for blockchain based security using IoT. *J. Intell. Fuzzy Syst.* **2023**, *44*, 905–918. [CrossRef]
45. Gupta, S.; Chithaluru, P.; El Barachi, M.; Kumar, M. Secure data access using blockchain technology through IoT cloud and fabric environment. *Secur. Priv.* **2024**, *7*, e356. [CrossRef]
46. Raj, A.; Maji, K.; Shetty, S.D. Ethereum for Internet of Things security. *Multimed. Tools Appl.* **2021**, *80*, 18901–18915. [CrossRef]
47. Jeyakkannan, N.; Subathra, G.; Karthika, R.; Lavanya, A.; Kirupanithi, N. Simulation of distributed denial of service attack against ethereum smart contract on the blockchain. In Proceedings of the International Conference on Computer Vision and Internet of Things 2023 (ICCVIoT'23), Coimbatore, India, 7–8 December 2023. [CrossRef]
48. Al-Joboury, I.M.; Al-Hemiary, E.H. Automated Decentralized IoT Based Blockchain Using Ethereum Smart Contract for Healthcare. In *Enhanced Telemedicine and e-Health: Advanced IoT Enabled Soft Computing Framework*; Springer: Berlin/Heidelberg, Germany, 2021 ; pp. 179–198. [CrossRef]
49. Narayanan, N.C.; Withana, C.; Elchouemi, A.; Li, G. Leveraging Blockchain Technology for a secure IoT data sharing. In Proceedings of the 2023 International Conference on Intelligent Education and Intelligent Research, IEIR 2023, Wuhan, China, 5–7 November 2023. [CrossRef]
50. Pajooh, H.H.; Rashid, M.; Alam, F.; Demidenko, S. Hyperledger fabric blockchain for securing the edge internet of things. *Sensors* **2021**, *21*, 359. [CrossRef]
51. Lu, Y.; Liu, Z.; Wang, S.; Li, Z.; Liu, W.; Chen, X. Temporal Index Scheme of Hyperledger Fabric System in IoT. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9945530. [CrossRef]
52. Alshehri, S.; Bamasag, O. AAC-IoT: Attribute Access Control Scheme for IoT Using Lightweight Cryptography and Hyperledger Fabric Blockchain. *Appl. Sci.* **2022**, *12*, 8111. [CrossRef]
53. Bettayeb, M.; Nasir, Q.; Talib, M.A. Hyperledger-Based secure Firmware update delivery for IoT devices. In Proceedings of the ArabWIC 2021: The 7th Annual International Conference on Arab Women in Computing in Conjunction with the 2nd Forum of Women in Research, Sharjah, United Arab Emirates, 25–26 August 2021. [CrossRef]
54. Lee, S.; Kim, M.; Lee, J.; Hsu, R.H.; Kim, M.S.; Quek, T.Q.S. Facing to Latency of Hyperledger Fabric for Blockchain-enabled IoT: Modeling and Analysis. *arXiv* **2021**, arXiv:2102.09166.
55. Guo, F.; Xiao, X.; Hecker, A.; Dustdar, S. Modeling Ledger Dynamics in IOTA Blockchain. In Proceedings of the 2022 IEEE Global Communications Conference, GLOBECOM 2022, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 2650–2655. [CrossRef]
56. Silvano, W.F.; Marcelino, R. Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. *Future Gener. Comput. Syst.* **2020**, *112*, 307–319. [CrossRef]
57. Alshaikhli, M.; Elfouly, T.; Elharrouss, O.; Mohamed, A.; Ottakath, N. Evolution of Internet of Things from Blockchain to IOTA: A Survey. *IEEE Access* **2022**, *10*, 844–866. [CrossRef]
58. Divya, M.; Nagaveni B. IOTA-Next Generation Block chain. *Int. J. Eng. Comput. Sci.* **2018**, *7*, 23823–23826. [CrossRef]

59. IoTeX Team. IoTeX: A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain . 2018. Available online: https://www.google.com.hk/url?sa=t&source=web&rct=j&opi=89978449&url=https://s3.amazonaws.com/web-iotex-static/home/IoTeX_Whitepaper_1.5_EN.pdf&ved=2ahUKEwi8qffM6uSHAxVpsFYBHRKnNN8QFnoECBMQAQ&usg=AOvVaw2wmyly1o8p8XY1HbMqHlN3 (accessed on 1 May 2024).
60. Partida, A.; Criado, R.; Romance, M. Visibility graph analysis of IOTA and IoTeX price series: An intentional risk-based strategy to use 5G for IoT. *Electronics* **2021**, *10*, 2282. [CrossRef]
61. Fan, X.; Zhong, Z.; Chai, Q.; Guo, D. Ucam: A User-Centric, Blockchain-Based and End-to-End Secure Home IP Camera System. In *International Conference on Security and Privacy in Communication Systems*; Springer: Cham, Switzerland, 2020.
62. Ravichandran, V. *Wear-IoTex: Wearable e-Textile Glove Kit for In-Home Parkinson's Motor Assessment*; University of Rhode Island: Kingston, RI, USA, 2021.
63. Xu, X.; Wang, X.; Li, Z.; Yu, H.; Sun, G.; Maharjan, S.; Zhang, Y. Mitigating Conflicting Transactions in Hyperledger Fabric-Permissioned Blockchain for Delay-Sensitive IoT Applications. *IEEE Internet Things J.* **2021**, *8*, 10596–10607. [CrossRef]
64. Na, D.; Park, S. IoT-Chain and Monitoring-Chain Using Multilevel Blockchain for IoT Security. *Sensors* **2022**, *22*, 8271. [CrossRef] [PubMed]
65. Wadhwa, D.; Gupta, D.; Saini, S.; Bathla, R. Blockchain for IoT Security and Privacy. In Proceedings of the 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 3–4 September 2021 ; pp. 1–5. [CrossRef]
66. Montanaro, T.; Sergi, I.; Corvaglia, S.; Mainetti, L.; Vilei, A.; Rossi, B.; Palmieri, A.; Patrono, L. Blockchain technology based on algorand applied to low-power and low-cost IoT devices. In Proceedings of the 2021 6th International Conference on Smart and Sustainable Technologies, SpliTech 2021, Bol and Split, Croatia, 8–11 September 2021. [CrossRef]
67. Varavallo, G.; Caragnano, G.; Bertone, F.; Vernetti-Prot, L.; Terzo, O. Traceability Platform Based on Green Blockchain: An Application Case Study in Dairy Supply Chain. *Sustainability* **2022**, *14*, 3321. [CrossRef]
68. Cardamone, N.; Dalena, V.; Mauro, A.; Settembre, M.; Vecchia, G.; Vitaliti, A.; Dondossola, G.; Bartalesi, D.; Garrone, F.; Terruggia, R. Blockchain-Based Public Key Authentication of IoT Devices for Electrical Energy Systems. In Proceedings of the 2022 AEIT International Annual Conference (AEIT), Rome, Italy, 3–5 October 2022; pp. 1–6. [CrossRef]
69. Ismail, S.; Reza, H.; Zadeh, H.K.; Vasefi, F. A Blockchain-based IoT Security Solution Using Multichain. In Proceedings of the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023, Virtual Conference, 8–11 March 2023; pp. 1105–1111. [CrossRef]
70. Sawant, A.; Prabhu, N.; Nagpure, S. Securing IoT Using MultiChain. In Proceedings of the 2nd International Conference on Advances in Science & Technology (ICAST), Mumbai, India, 8–9 April 2019.
71. Umran, S.M.; Lu, S.; Abduljabbar, Z.A.; Nyangaresi, V.O. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. *Internet Things* **2023**, *24*, 100969. [CrossRef]
72. Chang, J.; Ni, J.; Xiao, J.; Dai, X.; Jin, H. SynergyChain: A Multichain-Based Data-Sharing Framework with Hierarchical Access Control. *IEEE Internet Things J.* **2022**, *9*, 14767–14778. [CrossRef]
73. Shehzad, F.; Javaid, N.; Farooq, U.; Tariq, H.; Ahmad, I.; Jabeen, S. IoT Enabled E-Business via Blockchain Technology Using Ethereum Platform. In *Web, Artificial Intelligence and Network Applications*; Springer: Cham, Switzerland, 2020; pp. 671–683. [CrossRef]
74. Frikha, T.; Chaabane, F.; Aouinti, N.; Cheikhrouhou, O.; Ben Amor, N.; Kerrouche, A. Implementation of Blockchain Consensus Algorithm on Embedded Architecture. *Secur. Commun. Netw.* **2021**, *2021*, 9918697. [CrossRef]
75. Mohanta, B.K.; Sahoo, A.; Pate, S.; Panda, S.S.; Jena, D.; Gountia, D. DecAuth: Decentralized Authentication Scheme for IoT Device Using Ethereum Blockchain. In Proceedings of the IEEE Region 10 Conference (TENCON 2019), Kochi, India, 17–20 October 2019; pp. 558–563.
76. Urien, P. Demonstrating Trusted Blockchain IoT Device Based on TLS-PSK Secure Element. In Proceedings of the 5th Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2023, Paris, France, 11–13 October 2023. [CrossRef]
77. Zhao, L.; Vigneri, L.; Cullen, A.; Sanders, W.; Ferraro, P.; Shorten, R. Secure Access Control for DAG-Based Distributed Ledgers. *IEEE Internet Things J.* **2022**, *9*, 10792–10806. [CrossRef]
78. Lin, B.Y.; Dziubałtowska, D.; Macek, P.; Penzkofer, A.; Müller, S. TangleSim: An Agent-based, Modular Simulator for DAG-based Distributed Ledger Technologies. *arXiv* **2023**, arXiv:2305.01232.
79. Fan, X.; Zhong, Z.; Guo, D.; Chai, Q.; Romano, S. Connecting Smart Devices to Smart Contracts with W3bstream. In Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, 1–5 May 2023; pp. 1–2. [CrossRef]
80. Alkhodair, A.; Mohanty, S.; Kougianos, E.; Puthal, D. McPoRA: A multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems. In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, ISVLSI, Limassol, Cyprus, 6–8 July 2020; pp. 446–451. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.