Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions

Ziaur Rahman [1], Xun Yi [1], Sk. Tanzir Mehedi[2], Rafiqul Islam[3] and Andrei Kelarev [1]

[1] School Science, RMIT University, Melbourne 3001, Australia; (rahman.ziaur, xun.yi, andrei.kelarev)@rmit.edu.au
[2] Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Tangail 1902, Bangladesh; tanzirmehedi@ieee.org
[3] School of Computing, Mathematics and Engineering, Wagga Wagga NSW 2678 Australia; mislam@csu.edu.au
* Correspondence: s3677291@student.rmit.edu.au; Tel.: +61-0426-117-006 (AU)

Abstract: Blockchain has recently been able to draw wider attention throughout the research community. Since its emergence, the world has seen the mind-blowing expansion of this new technology, which was initially developed as a pawn of digital currency more than a decade back. A self-administering ledger that ensures extensive data immutability over the peer-to-peer network has made it attractive for cybersecurity applications such as a sensor-enabled system called the Internet of things (IoT). Brand new challenges and questions now demand solutions as huge IoT devices are now online in a distributed fashion to ease our everyday lives. After being motivated by those challenges, the work here has figured out the issues and perspectives an IoT infrastructure can suffer because of the wrong choice of blockchain technology. Though it may look like a typical review, however, unlike that, this paper targets sorting out the specific security challenges of the blockchain-IoT eco-system through critical findings and applicable use-cases. Therefore, the contribution includes directing Blockchain architects, designers, and researchers in the broad domain to select the unblemished combinations of Blockchain-powered IoT applications. In addition, the paper promises to bring a deep insight into the state-of-the-art Blockchain platforms, namely Ethereum, Hyperledger, and IOTA, to exhibit the respective challenges, constraints, and prospects in terms of performance and scalability.

Keywords: Blockchain; Hyperledger; Ethreum; Distributed Ledger; Internet of Things; Public Consensus; Scalability

Citation: Rahman, Z.; Yi, X.; Mehedi, SK. T; Islam, R.; Kelarev, A. Title. *Journal Not Specified* **2022**, *1*, 0. https://doi.org/

Received:
Accepted:
Published:

Publisher's Note:

1. Introduction

The integration of blockchain (BC) with IoT has been able to show immense effectiveness and potential for future improvements of scalability and productivity. Therefore, how these emerging technologies could be deployed together to secure end-to-end and sensor-embedded automated solutions while ensuring their scalability and productivity has become a key-priority. The world has already been amazed at the adaptations of different heterogeneous IoT solutions, ranging from healthcare to transportation systems [1]. The existing centralized Edge and Fog-based IoT infrastructure/applications may not be secure, scalable, and efficient enough to address larger enterprise challenges. Furthermore, the majority of existing IoT solutions are concerned with the network of sensor-enabled smart appliances, which permits physical device services on the cloud [1]. Moreover, an immutable timestamp ledger is used for distributed data including either payment, contract, personal data storing, data sharing, and healthcare systems due to its salient features such as immutability, distributed structure, consensus-driven behavior, and transparency [2].

There are various reasons why the BC technology may be highly promising for assuring the efficiency, scalability, and security of the heterogeneous IoT setup. The commonly aroused issues in the emerging IoT networks and several BC roles can be enlisted with proper responses as follows. Firstly, approximately fifty billion devices will be connected by 2022 [3]. Several efforts have been found have been working to reveal the challenges [4]. In response to the adaptability of trillions of devices in the near future, it should not be a big deal to handle by using decentralized BC technology. As BC requires no centralized database and addresses are directly addressable, one device can directly send information to another [5]. That means this technology has limitless and scalable registration capability. The second issue is how to control a large number of devices on a distributed and decentralized platform. In response, BC technology provides open peer-to-peer connectivity for intra-device communication, either physical or virtual appliances [3]. The third one is how it provides compliance and legitimate governess for all autonomous systems involved. In response, BC technology has a smart contract-based immutable open ledger system. So, transparency is one of the most eye-catching characteristics of this technology that ensures more comprehensive autonomy and trustworthy governance [6]. The last concern is how BC technology would address the security complexities of the new heterogeneous IoT ecosystem that is emerging and evolving so rapidly. In essence, the world has already experienced bitcoin excellence since 2008, and it has been evolving and maintaining on-growing internet challenges so far [2]. Apart from financial transactions, it has shown immense potential in the field of IoT, incorporating features like elliptic curve digital signature algorithm (ECDSA) [7], zero-knowledge proof (ZKP) [8], message signing, differential privacy [5], cryptographic message verification, and so many more.

The goal of this research is to identify the trade-offs that the heterogeneous IoT ecosystem typically faces due to the wrong choice of BC technology. Unlike a survey or review, the essential findings of this research are aimed at solving particular performance and scalability issues in the BC-enabled IoT architecture. The contribution covers how to direct developers and academics in this field to select the best BC-enabled IoT applications. The claimed contributions are justified through the respective sections of the paper. We have discussed BC suitability to eliminate the problems that emerge because of BC and IoT integration [9]. We also explained how the existing solutions, namely Microsoft (MS)-Azure IoT workbench and IBM IoT architecture, adopt different BC platforms such as Bitcoin (BTC), Ethereum (ETH), Hyperledger (HLF), Kovan, etc. The following section illustrates BC's potential for specific IoT issues. The challenges come to light while a sensor-enabled system finds appropriate devices, manages access control, and supports the compliance of smart contracts through respective use-case analysis. In addition, the research supports the use of smart contracts in IoT systems and points out possible flaws in data integrity, scalability, and confidentiality.

The research paper is organized as follows: First of all, Section 2 discusses the related work done with in this field. Section 3 discusses the internal design of the BC technology and the specialized categories within which it can be applied. The suitability of BC technology for IoT applications with comparative analysis and contemporary technologies including HLF, IOTA, and MS-Azure IoT architecture is discussed in Section 4. Then the following Section 5 summarizes with a brief table and graphs showing the challenges and proposed solutions at a glance as well as their applicability concerning throughput, latency, and execution time. Section 6 discusses a set of use-cases where BC technology is an inevitable peer of the IoT mentioned before the conclusion. Finally, Section 7 and 8 includes the overall discussion and summary and feasible future directions with theoretical and practical implications respectively.

2. Related Work

Apart from the financial domain, BC technology has been showing its far-reaching prospects in different application areas since its first emergence in 2008 [10]. Once written cannot be modified, BC ledger's nature besides its pseudo-anonymous, traceable peers over the transparent distributed network have made BC an unbeatable tool on the IoT [11]. The field includes smart areas, grids, vehicles, and Industry, Supply chain, Food or Drug Safety, and E-commerce of Agricultural product, Medical Technology, Industrial predictive maintenance [12]. On top of these fields, significant research activities found in the domain of Copyright protection of Digital data, ID verification, Real State land ownership transfer, smart-taxation immigration, electronic voting, privacy-principle compliance [13]. Even in the IT-sector such as Blockstack [14], BigchainDB [15] utilizes the BC smart-contract and consensus mechanism.

Namecoin incorporate Distributed Hash Table (DHT) that communicates with the virtual-chain after separating the BC dApps, operations, and an off-chain storage entity [16]. It hashes the name data tuples, state-transitions, records in the on-chain BC ledger, whereas the DHT stores the payload, digital data, and associated signatures. However, the authors seemed to be practicing the immense benefits of IPFS for storing access control and compliance data [17]. They proposed customizing the attribute-based encryption after replacing the centralized cloud-dependency by leveraging the public chain, namely Ethreum. In line with that, BigchainDB employs a Tendermint distributed database based on the idea of weak-synchronization of the BC engine deployed on the Byzantine Consensus (BFT) [18]. The promising data and execution embarkation brings a way for large-scale and real-time data protection and management such as Industrial IoT security and privacy.

The rapid growth of employing IoT sensors encounters several challenges, such as data protection, analytical management, and storing voluminous real-time data, etc [19], [20]. NoSQL or Hadoop repository initially attracted researchers in the IoT domain but was unable to convince because of its centralized structure, Single Point of Failure (SPOF) nature, and security issues [21]. Based on the legacy, the authors proposed an approach after attaching multiple cloud-centric database models that were promising and worth mentioning [20]. However, various dependencies should lead to SPOF, trust, and security intricacies. Several comprehensive works suggested Edge solution purposing to address such challenges, which enormously motivated, forming the idea we introduced on BC technology. However, besides the high-energy conducive miners' incentive disputes, the Blockchain network encounters the scalability issues that some existing-works [22], [23] concentrated on and aimed at solving through plausible remedies [24]. Some of the demonstrations, including channel-driven communication between the data owner and requester using shared secret keys [25], and BC for trusted computing, utilized the underlying public Blockchain (i.e., BTC, ETH) to provide the miner's network emulating a trusted server. However, apart from the potential threat of leaking secure, shared secrets, establishing a secure channel without consortium BC (i.e., HLF, Corda) seems not trustworthy.

In August 2018, focusing on security and privacy, a group of authors proposed applying multi-signature and BC for decentralized energy trading [26], [24]. Following the same motivation of multi-signature and consortium BC, the authors improved their P2P vehicle trading mechanism to the IIoT energy trading system in September 2018.

The certificate-less cryptography was initially introduced to abolish the IBE key-escrow issues in the early years of this century; however, several works coauthored in the following years toward its efficient improvement [27], [28]. From the IoT perspective, multi-signature based certificate-less authentication saves computational costs, signing latency, especially for the network involved light-weight sensors [29]. Considering the key dissipation hardship, costs, and latency, one of the latest works portrays convincing resolution upon aggregating the Edge and DHT. The works claimed to be suitable for Industrial IoT but lack details on how it overcomes the public BC network deployment and delay in the transaction (TX) generation, verification and broadcasting [30]. Moreover, the adaption and construction of the Key Distribution Center (KDC) look to extenuate the system performance toward centralized architecture [31], [32]. Table 1 concludes the overview of the selected recent literature reviews on BC and BC-based IoT applications.

Table 1. Overview of the selected recent literature reviews on BC and BC-based IoT applications

Ref.	Year	Research Area	Summary Contributions and Features
[11]	2017	BC for CPS	Resilience of Interacting distributed energy at speed, scale and security with blockchain
[33]	2017	BC Improvement	Scaling PBFT agreements for further improvment of Bitcoin
[34]	2017	IoT Security	SecKit: a model-based security toolkit for the internet of things
[35]	2018	BC-based IoT security	A Review, blockchain solutions, and open challenges
[28]	2018	BC for Cloud Security	How to adapt BC for securing Cloud
[36]	2018	Public BC for Security	A Special Model called RapidChain for fast Protocol using full Sharding methods
[20]	2018	BC for Iot Security	How BC could be applied for a large scale IoT System focusing data storage and protection.
[37]	2019	BC Consensus on PBFT	How Practical Byzantine is more efficient that PoW or PoS
[38]	2019	Permissioned BC	Showing the immense prospects of Hyperledger Fabric for distributed system
[39]	2020	BC Access Control for IoT	BC has verified features for scalable access management of IoT
[18]	2020	BC for Data Management	BC based data maintenance with identity management
[40]	2021	BC for Access Control	An extended model for Access control using Permissioned Blockchain
[41]	2021	BC for Access Control	Data Accountability and Provenance Tracking using BC
[26]	2021	BC-based Security Framework for CPS	Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System
[12]	2022	BC-based AI-enabled CPS	Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat

3. Preliminaries of BC Technology

The BC's main task is to replace traditional and trust-created intermediaries with distributed systems to solve common trust issues [5]. It also helps in forming a permanent and transparent record of the exchange of processing and avoids the need for an intermediary. Instant value exchange, decentralized value exchange, and pseudonymous value transfer are all terms used to describe BC technology's [42]. It also makes sure that the ledger building preserves a set of transactions shared among all participating nodes, which needs to be necessarily verified and validated by others [5,43]. Joining brand-new transactions is commonly referred to as "mining" and it requires the solution of a sophisticated and large computational problem, which in nature is a complex answer, but the easiest to authenticate using a selected consensus algorithm in a network of untrusted and anonymous nodes. The consensus algorithm requires a significant amount of resources in order to ensure that only authorized blocks may join the network. In addition, the communication between nodes is encrypted using changeable public keys (PK) to avoid monitoring, which has attracted attention in non-monetary applications [6]. Moreover, the hash of the previous block, the timestamp, the transaction root, and the nonce generated by the miner are also seen in a sample chain of blocks, which makes the BC more secured [44]. Figure 1 shows an overview of different blocks with timestamp, hashes, nones, and transaction data. So, using BC-enabled applications has become much more transparent because of this development.

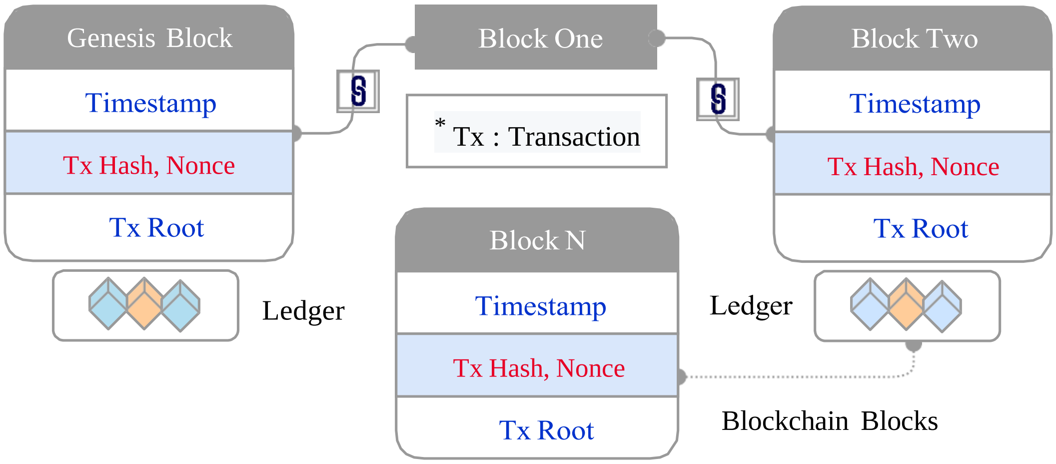


Figure 1. Overview of different blocks with timestamp, hashes, nones, and transaction data.

Using high-security smart devices and smart technologies for authentication to ensure seamless communication, decentralized data processing, or even autonomous systems for data purchase and others, it may demonstrate its promise in this field [45]. Consequently, the IoT devices might be equipped with the Internet to make every part of human life more convenient and less tedious [46][47] .

3.1. *Category of BC Technology*

In this section, we have covered three different approaches to BC technology: public ledger-based, private ledger-based, and protected ledger-based. Comparative categorization of BC ledgers is shown in figure 2 based on the accessibility of the considered ledger.

3.1.1. Public Ledger-based BC

In public ledger-based BC technology, anyone can transmit, verify, and read transactions on the network, as well as get and run the scripts necessary to participate in the BC's mining process using several consensus methods, making it known as a "permission-less" BC technology [42]. Even though any anonymous user may transmit, view, and authenticate an incognito transaction, it offers the highest level of anonymity and transparency [48]. ETH [49] and BTC are two of the most common examples of public BC technology.

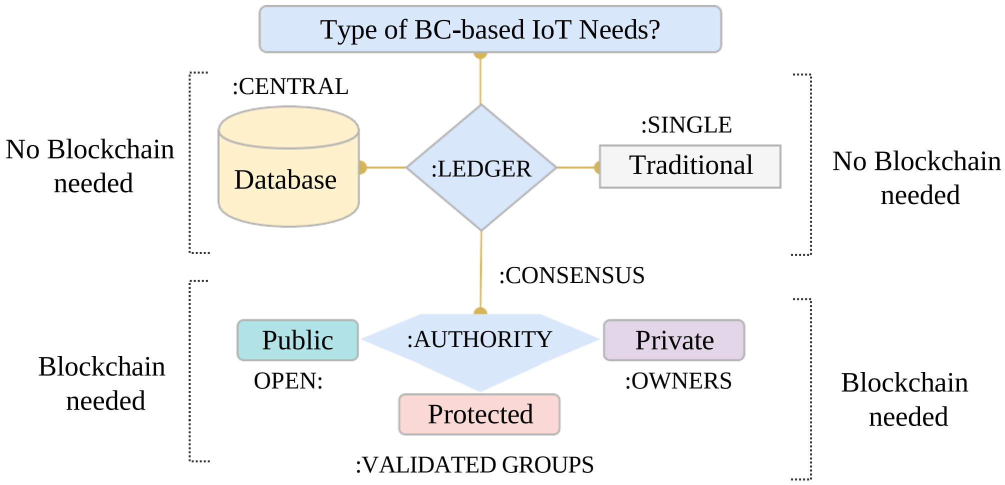


Figure 2. The classification of BCs according to the requirements analysis.

3.1.2. Private Ledger-based BC

Private ledger-based BC does not require a consensus mechanism or mining to provide anonymity because it restricts read and modification rights to a certain organization. The read authority is sometimes restricted to an arbitrary level, but most of the time, transaction editing is rigorously permissioned [50]. Private-typed BC approaches might be stated to be used in the ledger-building process for coins controlled by Eris and Monax or the Multichain [43]. To cite an example, a permissioned-based BC technology like Quorum is now available on ETH, though ETH itself is a public ledger-based BC technology.

3.1.3. Protected Ledger-based BC

The protected ledger-based BC is also known as consortium/federated, hybrid, or public permissioned BC, which is run by a group of owners or users and is kept up by them [48]. Protected ledger-based BC include HLF by Linux Foundation [1] and IBM, R3 with Corda or Energy Web Foundation [50]. Moreover, if the authority is restricted within a validated group, then protected ledger-based BC seems to suit more than public or private ledger-based BC system [51].

Moreover, figure 2 shows that if the system has a centralized or single ledger system, no category of the BC is needed there. Additionally, we discussed the performance comparison between IOTA and the other BC technologies. According to the IOTA team, its ledger is a public permission-less backbone for the IoTs [47]. That means it will enable transactions between connected devices, and anyone on the network can access its ledger.

4. Suitability of BC Technology for IoTs

Although BC technology is capable of solving all IoT-related issues, there are a few situations when a centralized database is preferable. BC-based use-cases need to be explored before being implemented in this area.

4.1. Comparison of Several Consensus Protocols

Table 2 describes the comparison among different popularly used consensus mechanisms for BC technology. It shows that Proof-of-Work (PoW) and Proof-of-Stake (PoS) need more computational resources in contrast to Byzantine Fault Tolerance (BFT) and Proof-of-Authority (PoA), which have better performance in comparison to their peers. But BFT and PoA are both hard to adjust [52]. Even though they have dependencies, they seem to work for IoT nodes. For scalability and overhead, blocks needed to be verified by all nodes available in the network, with a quadratic increase in traffic and a disobedient overhead of data processing power, which needs a lot of expandable, but IoT devices (e.g., LORA) have limited bandwidth [45]. IoT devices tend to fail with higher delays, but BTC takes nearly 30 minutes to finalize a transaction. It also has security overheads, making it inapplicable for IoT [53]. Because of the huge interaction between IoT nodes, the throughput of BTC (7/transaction) will push it over the limit. As a result, many people have switched from BTC to BFT-based HLF or non-consensus-driven systems like IOTA [1,42]. The applicability of different BC-based systems depends on whether consensus and non-consensus approaches are discussed.

4.2. Comparative Analysis of ETH, HLF, and IOTA Technology

First of all, the ETH technology, launched with the intention of competing with BTC, is a flexible BC platform with a required smart-contract and PoW consensus mechanism named *Ethash*, which generates the probabilistic hash using Directed Acyclic Graphs (DAG) [6]. It greatly helps with extensive IoT applications and some of its efficiency trade-offs. ETH needs almost 20 seconds to open a new block after mining, as *Ethash* works based on the PoW mechanism [42].

Secondly, HLF is an authenticated and encrypted type of BC technology. It applies authentication widely, as well as chain-code-based smart contracts and consensus with existing Practical-Byzantine-Fault-Tolerance (PBFT) [7]. Anchors of trust are added to the

Table 2. A comparison of several widely used consensus techniques for BC technology.

Attributes	PoW	PoS	BFT	PoA
Category	Public	Pub/Protected	Private	Protected
Throughput	Little	Big	Big	Big
Random	No	Yes	No	No
P-Cost	Has	Has	Not	Not
Token	Has	Has	Not	Native
Trust	Trust-less	Trust-less	Semi	Trusted
Scalability	Big	Big	Little	Medium
Reward	Yes	No	No	No
Example	BTC	ETH	HLF	Kovan

asymmetric cryptographic technique and digital signature qualities with SHA3 or ECDSA as an additional feature of the system [42]. A self-execution capacity such as asset or resource transfer across network peers is required for its implementation of smart contracts. It has low latency with respect to other comparative distributed ledger implementations. Furthermore, according to IBM's Bluemix-Watson IoT design, which is shown in the next section, Fabric was selected as the BC medium.

Finally, IOTA is an unique distributed ledger that does not use an explicit BC at all; rather implements a DAG of transactions - in place of multi-block transactions, individual transaction approves and implies back to two other transactions [42]. IOTA tangles have the potential to be effectively integrated with IoT in order to provide security and privacy. Figure 3 shows the comparative analysis among ETH, HLF, and IoTA technology in terms of performance and scalability.

BC Type	Consensus	Delay & SC		Distinct Characteristics
HLF	PBFT	10-100 ms	Yes	High computation-intensive
ETH	Ethash	10k ms	Yes	Light computation-intensive, High network use
IOTA	No [DAG]	10 ms	No	Light computation-intensive, Low network use

Figure 3. The comparative analysis among ETH, HLF, and IOTA technology.

4.3. MS-Azure IoT Workbench

Figure 4 shows the Azure IoT framework, which, depending on the smart-contract, streamlines client-side based applications for both web and mobile. It is used to validate, retrieve, and test programs or to consider novel use cases. A user interface is introduced for the end users to interact with in different ways. Authenticated users can interact with the admin console, allowing them to use many functionalities such as uploading and deploying smart-contacts depending on appropriate roles.

Figure 4 illustrates the REST API-based gateway service API used to replicate and send messages to an event broker as data is attempted to be expanded into the BC technology. When data is requested, quarries are submitted to an off-chain database. Replicas of all chained meta-data and bulk-data that issue relevant configurations for smart-contract support are contained in the SQL database. Thus, developers can directly access the gateway servicing API to develop BC technology. Direct data submission to the service bus is an option for users who want their messages to be sent widely throughout the Azure infrastructure. As an example, this API may be used to build sensor-based tools or federated systems. In addition, there are several events hosted over the life of the application [42]. The gateway API or even the ledger's alerting trigger downstream-code

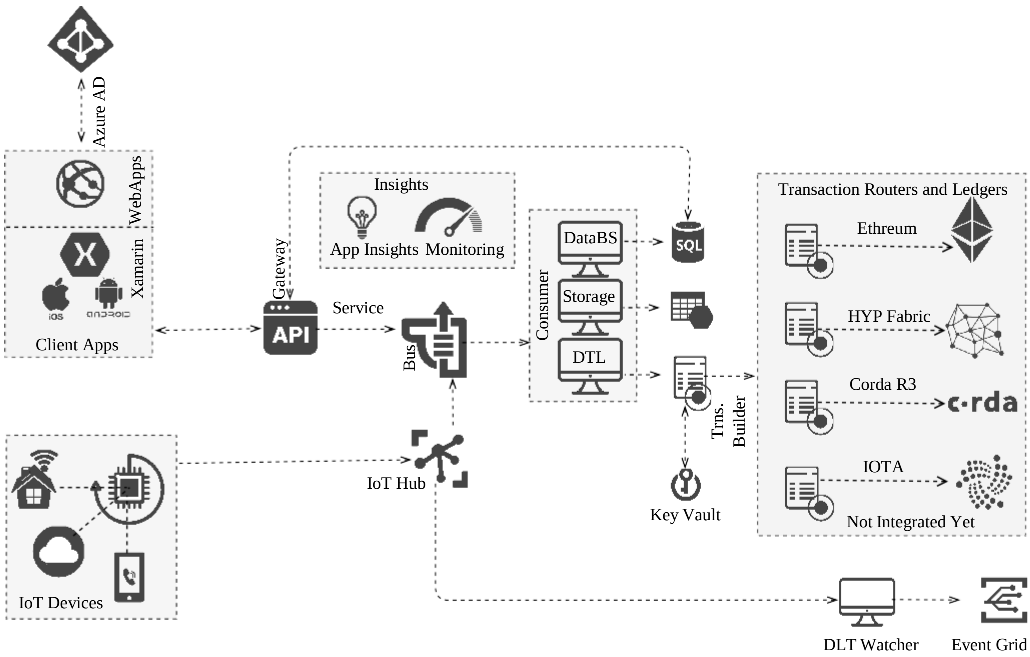


Figure 4. Azure IoT reference architecture that has been integrated with BC for securing IoT devices.

can accomplish this depending on previous events that have happened. There are two types of event consumers that the MS-Azure consortium may locate [1]. The first one, which is enabled by the events, remains on the BC to access the off-chain SQL database. As a final response, it collects meta-data from API events related to document upload and storage. Figure 4 elaborates how the MS Azure IoT workbench gets familiar with different BC frameworks. The MS Azure architecture may also be used to support HLF Fabric, Corda R3, and IOTA. The IoT Hub is connected to the IoT sensors through a bus, and the Transaction Builder is connected to this bus. Finally, in order to create a scalable and secure IoT device, an existing IoT workbench may be integrated with MS Azure.

4.4. IBM BC Integrated IoT Architecture

The IBM BC architecture for IoT solutions has three principal tiers; each has different roles [1]. Figure 5 shows a high-level IoT architecture that includes HLF Fabric as a BC service, Watson as an IoT Platform, and Bluemix as a cloud environment [8]. It can be divided into several components, as shown in figure 5. It has been addressed with its three layers, service execution method, and the challenges it confronts. It also shows how IBM Blumix works. When executed, data gathered by smart devices and intelligent sensors is introduced to Watson using the ISO standard Message-Queuing-Telemetry-Transport (MQTT) protocol. Depending on the settlement, certain BC proxies are used to send data from Watson to the chain-code of the HLF Fabric and executed in the cloud.

Furthermore, the HLF fabric uses chain-code, written in Go, instead of smart contracts. The desired business logic is elaborated by it and given shape to the core distributed ledger solutions. Each transaction is preserved and prevailed, which is needed for BC transactions. Fabric contracts being chain-coded need certain APIs to run. As such, the chain-code is in need of registration with services using any predefined APIs. Software Development Kits (SDK) help developers to make Node.js applications that can maintain communication with BC networks. APIs are used to register and submit applications. IBM BC integrated IoT architecture on Bluemix provides many benefits to the distributed network, such as trust, autonomy, scalability, and security. There are many issues to be resolved. One of the important issues is hardware resources [6]. That is because IoT devices are mostly low-powered devices and have less computation power. So, the encryption and transaction

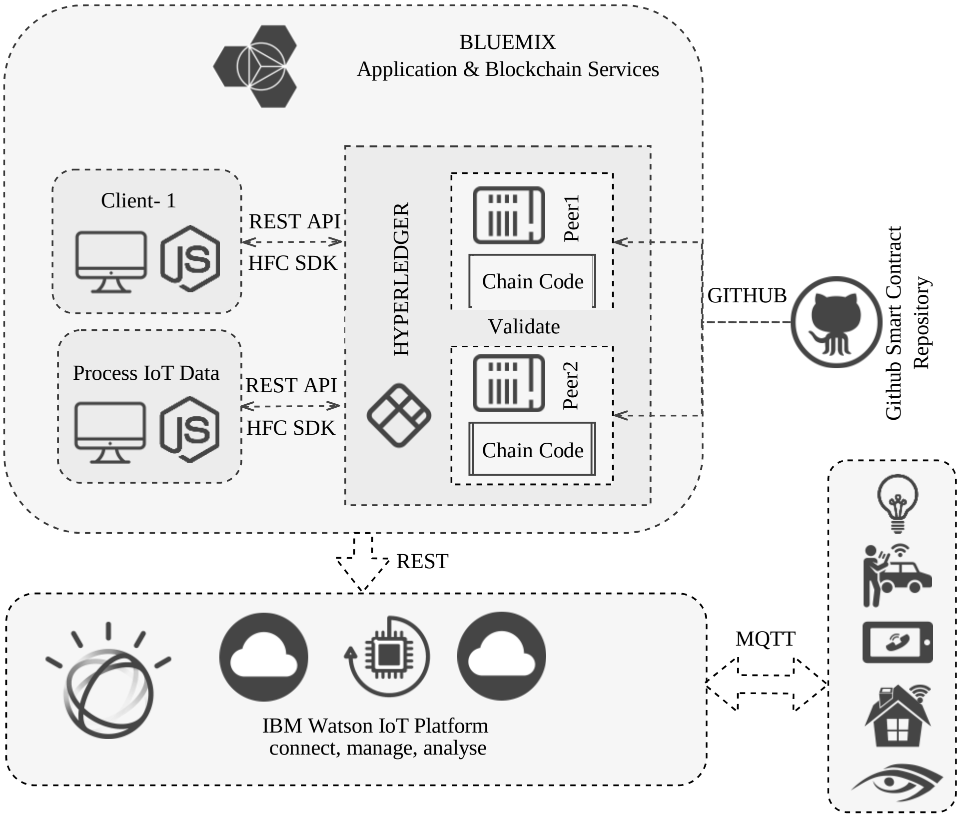


Figure 5. IBM Watson and Bluemix have been integrated with the IoT-BC service. Using Bluemix's BC network, Watson can communicate with IoT devices via Github's smart contact repository.

verification may use a lot of electricity. As a result, it will increase both energy consumption and costs.

5. Challenges and Solutions for BC-based IoTs

Despite the many appealing features of BC for IoT applications, there are several challenges that must be addressed before successful adoption. The storage capacity, throughput, latency, execution time, privacy and security, and scalability of the BC-based IoT applications are addressed in this section. Following that, we have also thoroughly explained some inevitable challenges and their possible solutions. Figure 6 shows the challenges in BC-based IoT applications.

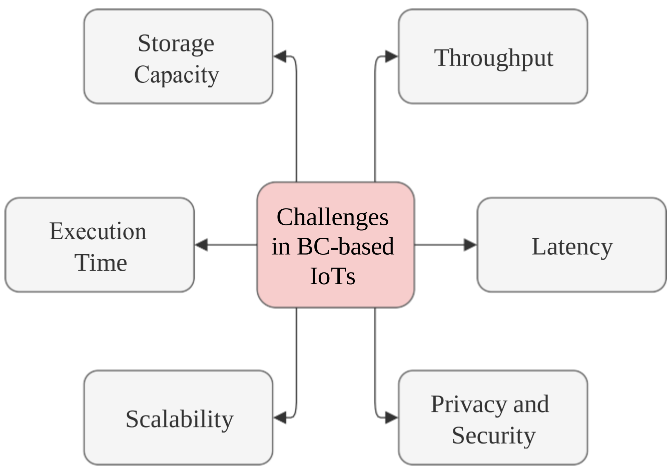


Figure 6. Challenges in BC-based IoT applications.

5.1. Challenges in Storage Capacity

As previously discussed, ETH and BTC have storage issues. Figure 7 shows how the storage capacity has been increasing day by day from 2015 to the first quarter of August 2021. The storage-intensive BC infrastructure is less suitable for heterogeneous IoT systems[54]. The massive amount of data generated by IoT devices raises the likelihood of a system crash due to the additional storage overhead [55]. In real-time heterogeneous IoT systems, ETH appears to be more suited for storage capacity than BTC, as shown in figure 7. However, the storage capacity of a BC is not the only aspect that determines whether it is suited for heterogeneous IoT systems.

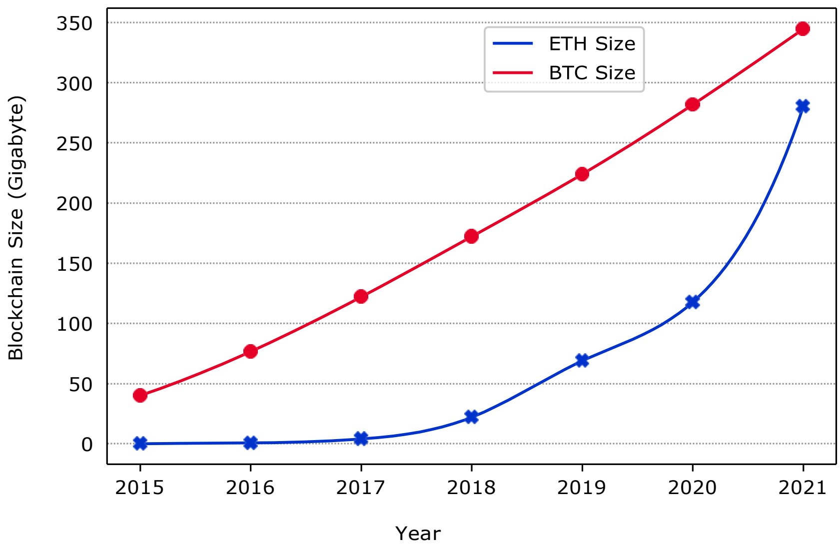


Figure 7. Storage capacity comparison between BTC and ETH technology using data from the Blockchain, Etherscan and Statista websites.

5.2. Challenges in Throughput

Furthermore, we have considered the throughput of several BC technology. Figure 8 compares the throughput of ETH, ETH Parity, and HLF fabric in terms of the number of transactions per second, where HLF has the highest throughput for Yahoo-Cloud-Serving-Benchmark (YCSB) and Smallbank database. The dataset were found from [42], where they used Blockbench framework to collect data. ETH Parity, on the other hand, has the lowest throughput compared to the others, implying that it is less appropriate for real-time heterogeneous BC-based IoT infrastructures.

5.3. Challenges in Latency and Execution Time

We have also considered the latency and execution time of several BC technology. Figure 9 compares the latency and execution time of ETH, ETH Parity, and HLF fabric, where HLF has the lowest latency and execution time for both database. One of the ETH implementations, ETH Parity, is an alternative BC solution for the IoT applications. Therefore, we considered both the ETH and ETH Parity to calculate latency and execution time. In addition, the Linux Foundation hosts the HLF, an open-source collaborative program aimed at improving cross-industry BC technology [47].

5.4. Challenges in Privacy and Security

BC technology works like a public ledger that secures and authenticates transactions and data through cryptography, which is more complex. With the rise and widespread adoption of BC technology, data breaches have become frequent. User information and data are often stored, mishandled, and misused, posing a threat to personal security and

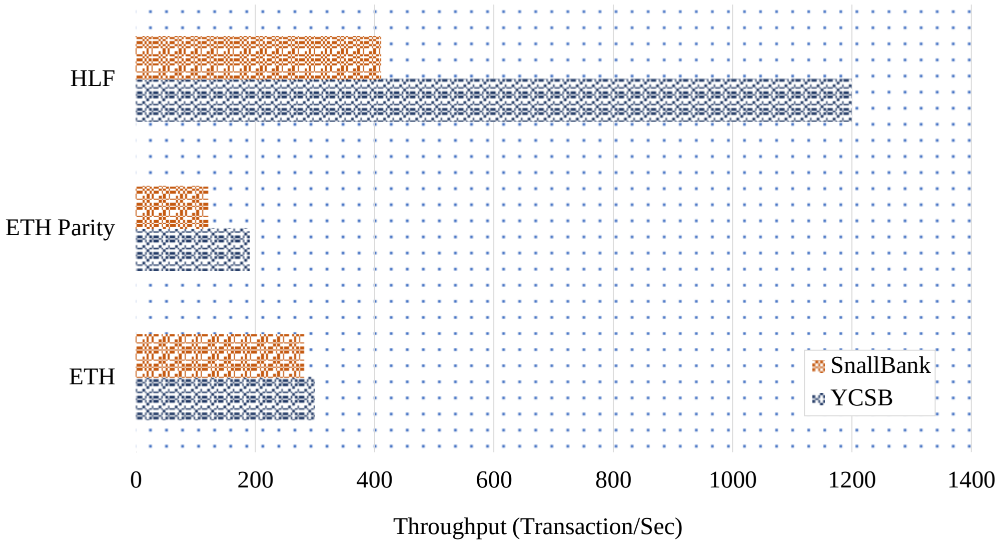
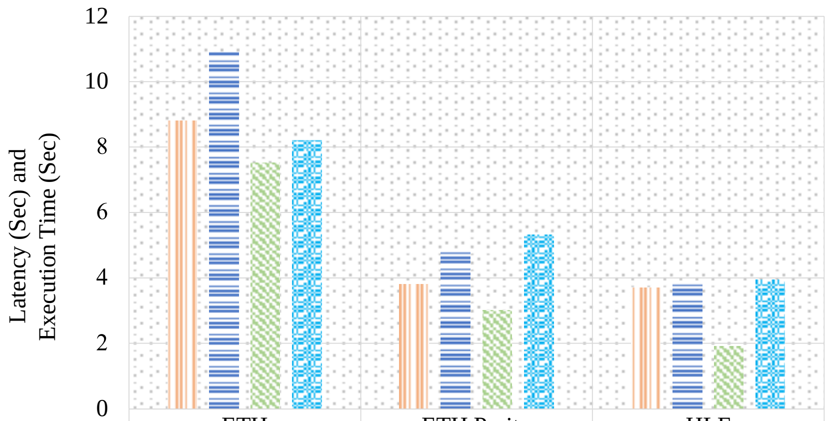


Figure 8. Throughput comparison between ETH, ETH Parity, and HLF fabric.



	ETH	ETH Parity	HLF
YCSB (Latency)	8.8	3.8	3.7
SmallBnak(Latency)	10.9	4.8	3.9
YCSB (Execution Time)	7.52	3.01	1.9
SmallBank (Execution Time)	8.2	5.32	3.94

Figure 9. Latency and execution time comparison between ETH, ETH Parity, and HLF fabric.

privacy. In terms of security, the data needs to be tamper-proof, where some of the nodes may act maliciously or be compromised. As a result, proper security must be ensured before integrating with the IoT infrastructure. Moreover, in terms of privacy, the data or transactions belong to various nodes in BC technology. So, privacy needs to be ensured before integrating with the IoT infrastructure.

5.5. Challenges in Scalability

Finally, we have considered the scalability of several BC technologies. The scalability of BC technology is composed of node-scalability and performance scalability. Node-scalability in BC networks refers to the extent to which the network can add more participants without a loss in performance. Performance-scalability refers to the number of transactions processed per second, impacted by the latency between transactions and each block size. A BC technology is considered scalable if it can add thousands of globally distributed nodes while still processing thousands of transactions per second. Currently, none of the existing BCs are really scalable. Figure 10 shows a comparison of scalability, some of which are currently in use and some of which are in development.

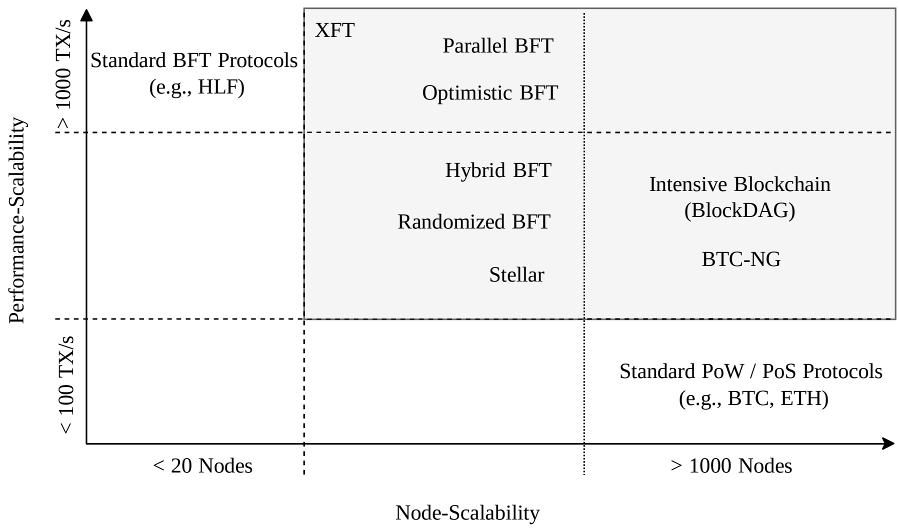


Figure 10. Scalability comparison between ETH, BTC, HLF, and some of which are in development.

Public BCs such as BTC and ETH have high node-scalability and low performance scalability by using PoW consensus mechanisms. On the contrary, a HLF Fabric has low node-scalability but high performance-scalability. For heterogeneous IoT infrastructures of less than 20 nodes, this technology might be a viable solution. However, if we need more nodes, the amount of messaging that takes place between the nodes in PBFT can lower transaction throughput significantly. Therefore, the large-scale IoT system will be unable to successfully integrate with BC technology unless all the challenges are appropriately solved.

5.6. Prominent Challenges and Solutions

There is a wide variety of IoT systems, from simple to complex cyber-physical systems, making it impossible to put all of the challenges and possible solutions on one table. Table 3 summarizes some challenges, important characteristics and their possible solutions, respectively [8]. We have identified seven potential challenges and their respective BC solutions with key attributes that may be addressed before being deployed to IoT infrastructure [56].

6. Use-case Analysis

The emerging application of distributed ledgers for BC technology can be divided into three categories: areas with common IoT controls, areas where IoT is suitable, and areas with efficient IoT solutions, according to the research on BC and distributed ledgers conducted by GSMA in collaboration with several mobile operators [57]. Figure 11 shows a comparison of different application areas, where six application areas (e.g., Support Compliance, Device Identity, Data Sharing, Access Control, Micro-payments, and Supply Chain) are considered for BC-based IoT use-cases following to the suggestions by ten operators with their applicability and priority. The priority of interest of the operators are divided into three categories- minimum, medium, and maximum. For data-sharing applications, three different operators suggests that it should be minimum and medium priority, while five operators suggests that it should be the most important priority for them as shown in figure 11. On the other hand, all the operators leave the access control application with the minimum priority. Furthermore, not all operators recommend micro-payment applications with medium priority. Rather, five operators suggest either the maximum or the minimum priority. For support compliance and device identity applications, five operators suggests that it is medium priority for them. However, according to GSMA, the

Table 3. BC-IoT Implementation Challenges, Important Characteristics, and Possible Solutions.

Challenges	Important Characteristics	Possible Solutions
Transaction Throughput	The real-time IoT data may be lost if the transaction confirmation time of pub- lic ledgers spans from 100 to 2000 TPS (Transactions Per Second).	Ripple claims to consume less time each transaction compared to BTC, ETH, Corda, and Quorum.
Consumption of Energy	In order to run cryptographic algorithms, IoT systems must be light-weight and have enough power.	Adaptation may be possible if manufacturing processes are planned to utilize energy.
Confidential Private-Key Features	To protect against eavesdropping, DTL frequently employs an asymmetric encryption strategy that takes advantage of the IoT's public key infrastructure.	Distributed IoT ledgers may be structured so that the entire ledger does not need to be replicated either.
Availability of the Data Transmission Space	A block size of 1 MB takes 10 minutes, which means that the data rate might be close to 150 MB per day. A lot of bandwidth would be required for this, and tiny IoT WANs like Sigfox or LoRA don't have that.	Distributed IoT ledgers may be structured so that the entire ledger does not need to be replicated either.
Congestion of the Transactions	A transaction may occur if the transaction exceeds the ledger's maximum throughput limit, which may result in increased user costs. Even with the limit provided by ripple or ETH, the real-time requirement is still not met.	Non-mining tangle-based IOTA's zero-fee transactions technique might be used.
The Cost of Mining and the Volatility of the Price	IoT devices that are sensitive to power consumption may not be able to use public BCs because they require high-priced hardware that relies on high-power computing.	Low-power consensus, private BCs, and non-mining DTL are all viable solutions.
Storage and Scalability of the Data Chain	In January 2019, BTC, ETH, and IOTA had each surpassed 200 GB, 125 GB, and 25 GB in size, indicating that the volume of data that would need to be stored to support 75 billion intelligent devices will become increasingly difficult to handle.	Distributed ledgers and big-data handling solutions might help alleviate the problem.

dataset was generated with sincerely exploring all the operators, but more investigation is needed before it can be used for technical and industrial purposes. Apart from the these applications, Blockchain are also used for Software-defined IoT Infrastructures [58]. Similar works found in [59]. The next sections address most important four use-cases that are closely related to performance, security, and scalability.

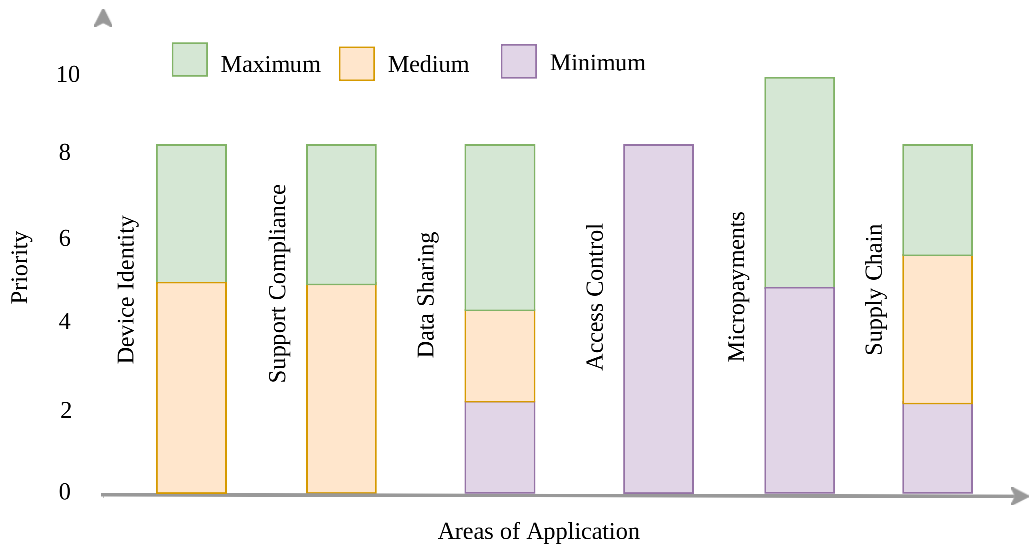


Figure 11. Application areas of six considered BC-based IoT use-cases following to the suggestions by ten operators with their applicability and priority.

6.1. *Use-Case : Finding Appreciate IoT Devices*

Device credential retrieval and tracking has been an important aspect in IoT enabling. Examples of intelligent IoT devices may be found in the following cases.

- ***Case 1***: For authentication reasons, the original data and the current state of the device are stored. For example, it is important to verify the serial numbers supplied to ensure that the manufacturing firm or party is accredited by a third-party quality assurance body.

- ***Case 2***: Use the ledger's metadata to verify the authenticity of software upgrades from trusted sources.

- ***Case 3***: Personal data such as hardware configurations, software versions, and boot code installations should be preserved to maintain privacy.

Table 4. Key advantages and BC applicability for the IoT finding use-case.

Use-Case	Finding Appreciate IoT Devices
Key Advantages	Ensuring consistent device identification information is a part and parcel of preventing vulnerabilities to unexpected third-party surveillance attacks. It can also help to keep track while adding new devices to the ledger. Any company or entity with an interest and legitimate rights can get the necessary information before making any deal.
BC Applicability	Both public and protected type BC could be resilient as an applica- tion in response to cases mentioned. Sovrin with zero knowledge proof allows users asserting their own identity information with- out disclosing data directly through the ledger can be a good solution here.

6.2. Use-Case : Manage IoT Access Control

In order to retain access control data for physical and virtual resources, an IoT network monitoring and recording system is unavoidable. The following are some examples of possible applications.

- ***Case 1***: The ledger is used by the virtual file sharing server to protect the identity of persons and apps by encrypting access privileges for printing, saving, and editing. For example, you purchase anything online while you are away from home, you may not receive it. For clients, adopting a distributed ledger rather than a key, address, or other potentially abused code can be an advantage.

- ***Case 2***: Use the ledger's metadata to verify the authenticity of software upgrades from trusted sources.

Table 5. Key advantages and BC applicability for the IoT access control use-case.

Use-Case	Manage IoT Access Control
Key Advantages	Limiting resource access for a specific time using a generalized API solution using smart contract rules. Access could be moni- tored and stored or temporarily locked by using immutable trace- ability to ward off illegitimate requests as well as keep informa-tion for later use. Better availability and attack resilience could be achieved by copying the permission among participating nodes.
BC Applicability	Public BCs supporting smart contracts such as Ethereum and crypto projects such as Sovrin are able to build access manage- ment and privacy. HLF Fabric supports smart contracts like chain- code approaches that can easily solve access control scenarios as discussed.

6.3. Use-Case : Supporting the Compliance of Smart Contracts

There are several situations involving various organizations in which it is crucial to determine whether or not all of them are being effectively complied with. Thus, BC smart contracts may be used to quickly and effectively enforce compliance. The following are some cases of possible applications.

Case 1: Distributed ledgers can be used by some individuals who share personal data with their healthcare provider to ensure that only authorized medical personnel have access to the information. Ideally, the pharmacy and the general practitioner in a multi-party system should only communicate the patient's blood pressure readings in order to facilitate the easy dispensing of recommended medication.

Case 2: If a flight is delayed by 30 minutes, an individual may have to pay an additional $2 for airport cab service. Upon arrival, the smart contract may detect whether the additional premium has been paid in full or not in the event of micro-insurance premiums like this reduced cost feature of service delivery in the smart contract For all of the problems raised in the use cases, BC technology may be an effective solution.

Case 3: There must be verification of one's driving credentials, such as a valid driver's licence and a clean criminal history record before one may drive a linked automobile. Even the automobile itself may submit trip data, service history, and even self-reported defects. One of the most efficient ways to gather data in a situation where hundreds of thousands of people are involved is to use a smart contract and BC technology.

Table 6. Key advantages and BC applicability for the supporting smart contract compliance use-case.

Use-Case	Supporting the Compliance of Smart Contracts
Key Advantages	Smart contract data is immutable, therefore tricky mileage changes could easily be prevented with necessary transparency. For example, the journey transaction will only be added to the ledger if the odometer reading at the end is greater than the initial record.
BC Applicability	Public BCs like Ethereum or open source projects like HLF could be applied. Given that the ledger is not competing with the resource, permissioning administration, and transaction fee exemption, IBM HLF Fabric is better suited for this type of scenario.Ripple seems to be scaling in the visa payment system. However, applying IOTA could be more meaningful in a micro-payment case like Case 1, as it is designed to suit the necessarily required IoT scalability.

6.4. Use-Case : Maintain Data-Integrity and Confidentiality

In a distributed ledger paradigm, it is frequently hoped that data exchange while maintaining sufficient confidentiality will be very conceivable [60]. The ability to retain the sequence of digital-signatures and data-hashes provided by BC may be used to assert data integrity and IoT-related data effectively. A use-case for this can as following. The following are some examples of possible applications.

- ***Case 1***: The manufacturing company's servers are expected to receive data from IoT devices. For instance, an intelligent thermostat linked to cloud services can provide data to the firm concerning component wear when it chooses when to turn on and off based on the current weather situation. This problem can be addressed using existing solutions like Public-Key-Infrastructure (PKI) driven approaches, but BC appears to be more efficient in preventing the need to reinvent procedures with regard to integrity and privacy.

- ***Case 2***: An alarm system for a home or workplace may be managed by a variety of people with varying levels of access credentials. If intruders get access to it, law enforcement officials may need to use remote access to investigate. Distributed Ledger might be particularly beneficial in this situation, which involves millions of devices being interconnected [47].

- ***Case 3***: An individual's health care dart wants may be shared with the researcher or medical staff by use of a personal fitness tracker. As a result, an individual may be ready to pay a micro premium for services provided by a manufacturer. When smart houses feature weather station/air monitoring IoT products that are shared by many parties, the same situation might occur. Distributed ledger may be the only option for a network of machine manufacturers, practitioners, and researchers that appears to be unreasonably vast.

- ***Case 4***: As a micro-generator such as a wind turbines, BC may be integrated into smart power grids to record the entire quantity of energy generated and then be used to calculate net supplier payments. Using a distributed ledger and a smart contract, it is possible to ensure that payments are made on time and in accordance with the agreed-upon rate.

Table 7. Key advantages and BC applicability for the data integrity and confidentiality use-case.

Use-Case	Maintain Data Integrity and Confidentiality
Key Advantages	In contrast with mobile or web applications based on relational databases, which demand operation and development efforts, distributed ledgers can easily maintain ledgers with multiple parties. There is no need for them to develop their own bespoke API either. The common API and functions of the distributed ledger save time and effort involved in besides, no extra scalability is required to ensure data integrity, security, and privacy.
BC Applicability	Though public BCs such as BTC and ETH show inefficiency, di- rected acyclic graph-based IOTA is able to meet the challenges considering scalability issues required by the micro-payment system and data sharing with integrity. Linux's open source project, namely HLF Fabric, is also able to ensure data sharing and integrity.

7. Discussion

Disruptive innovations always elicit a tremendous deal of discussion and debate. Despite the fact that there are many opponents of virtual currencies, it appears unassailable that the technology that underpins them represents a big step forward in technical development. BC is a technology that is here to stay. But there are hazards that one can easily fall into, such as updating the technology without fully insuring its operation or applying it to scenarios where the cost of the improvement does not outweigh the cost of the modification. As a result, the advantages of using BC technology to the IoTs should be thoroughly considered and approached with prudence. For the purpose of achieving successful collaboration between BC technology and IoT applications, this study gives an overview of the major hurdles that both technologies must overcome. We have identified the critical areas in which BC technology may assist in the improvement of IoT applications. In addition, an evaluation has been presented to demonstrate the viability of using BC nodes on IoT devices. For the purpose of completing the study, existing platforms and applications were also analyzed, providing a comprehensive picture of the interplay between BC technology and the IoT paradigm. It is expected that BC technology will revolutionize the IoT devices. The integration of these two technologies should be addressed, taking into account the challenges identified in this paper. The adoption of regulations is key to the inclusion of BC technology and the IoT devices. This adoption would speed up the future fourth industrial revaluation. Consensus will also play a key role in the inclusion of the IoT as part of the mining processes and distributing even more BC technology. Nevertheless, a dualism between data confidence and facilitating the inclusion of embedded devices could arise. Lastly, beyond the throughput, scalability, latency, and storage capacity which affect both technologies, research efforts should also be made to ensure the security and privacy of critical technologies that the IoT and BC technology can become.

8. Conclusion

The usage of BC technology is one of the most emerging areas of research for the development of efficient and scalable solutions for heterogeneous IoT applications. There's a lot of concern about how efficiently BC technology could integrate with usual IoT devices while maintaining maximum throughput and privacy. In this manuscript, we have introduced different existing BC platforms and key-challenges before integrating with IoTs. In addition, this paper also provides a comprehensive analysis of how different BC platforms (e.g., BTC, ETH, and IOTA) could be used in IoT applications. Finally, we have discussed some relevant use cases for the IoT's leading BC technology that could be helpful while working on it. It concludes that all of those have extensive potential to be used as a development platform with the purpose of enabling the efficient and real-time deployment of heterogeneous smart devices on a distributed network. In all, the IOTA technology is an open-source distributed ledger and cryptocurrency designed for IoT devices, which is more efficient in solving transaction-latency and mining reward issues by saving costs and increasing performance. Furthermore, as public, private, and protected BCs each have their own set of benefits and limitations in various situations, further study may be conducted to pinpoint the precise gaps in-between. If the challenges and issues that arise can be minimized, it could be a driving force in the future secured technology-driven world where real-time automation and secure data processing are the main challenges.

Theoretical Implications

It brings BC insights and applicability to IoT, so BC researchers and developers from the industry can decide before integrating it into their potential system. The research shows if a system really needs BC for a challenge. It concludes that for a centralized solution, BC would not add any value. In addition, it also discusses different consensus mechanisms to understand what sort of consensus seems applicable to a problem. The comparison appears to provide conclusive evidence that private and consortium-type BCs are better suited for IoT security applications. In addition, various types of applications, such as IBM's Watson and Microsoft Azure, are discussed so that researchers can gain practical knowledge in the domain. Furthermore, apart from BC, this research discussed IOTA, which is a BC-like solution but not BC in nature. This brings an alternative means of IoT security. IOTA seems to have higher performance because of its DAG ledger structure. Finally, it also brings up industry standard use-cases with specific problems to extract a deep insight into how BC integration affects several problems. It has a lot of advantages and can be used in a lot of different ways, which should help researchers and developers in the field.

Practical Implications

In terms of the practical implications of our findings, future researchers in this field can use the findings of this study to develop new BC-based IoT applications. Furthermore, researchers should be aware of the privacy and security issues that can result from the failed integration of these technologies or their misuse. In addition, companies can use our results to better understand users' appreciation of the security of BC-based IoT connected devices, improve their products, or make users thoroughly understand the risks of excessive use of such devices.

Limitations and Future Research

There are three major limitations to this study that could be addressed in future research. First, the study focused on only six performance parameters (e.g., storage capacity, throughput, latency, privacy and security, scalability, and execution time) of BC-enabled IoT applications. In the future, we will consider more performance metrics related to these heterogeneous applications. The second limitation of the present study is related to the BC technology. In this paper, we have considered only ETH, BTC, and HLF. In the future, we will also consider some of the latest BC technology, some of which are in the development phase. Finally, in this paper, we considered only two existing workbenchs for BC-enabled IoT applications (e.g., MS-Azure IoT workbench and IBM BC integrated IoT workbench). In the future, we will look into more workbench techniques for these heterogeneous applications.

Furthermore, in further research, it would be necessary to focus on improving the analysis processes used in this study as well as identify new issues related to the safety of BC-enabled IoT devices and user privacy in smart living environments.

Abbreviations

The following abbreviations are used in this manuscript:

BC	Blockchain
HLF	Hyperledger
ETH	Ethereum
BTC	Bitcoin
IoT	Internet of Things
MS	Microsoft
ECDSA	Elliptic Curve Digital Signature Algorithm
ZKP	Zero-knowledge Proof
DP	Differential Privacy
CMV	Cryptographic Message Verification
IBM	International Business Machines Corporation
PK	Public Key
TX	Transaction
PoW	Proof-of-Work
PoS	Proof-of-Stake
BFT	Byzantine Fault Tolerance
PoA	Proof-of-Authority
DAG	Directed Acyclic Graph
SHA3	Secure Hash Algorithm 3
PBFT	Practical Byzantine Fault Tolerance
REST	Representational State Transfer
API	Application Programming Interface
MQTT	Message Queuing Telemetry Transport
SDK	Software Development Kit
YCSB	Yahoo Cloud Serving Benchmark
PKI	Public Key Infrastructure
HFC	Hyperledger Fabric Client
SDK	Software Development Kit
DLT	Distributed Ledger Technology
HYPF	Hyperledger Fabric
XFT	Cross Fault Tolerance
DHT	Distributed Hash Table
SPOF	Single Point of Failure

Author Contributions: The following statements should be used "Conceptualization, Rahman, Z. and Yi, X.; methodology, Rahman, Z.; software, Tanzir, M.; validation, Rahman, Yi, X.; and Rahman. Z.; formal analysis, Rahman. Z.; investigation, Islam, R. ; resources, Rahman. Z.; data curation, Tanzir, M.; writing original draft preparation, Rahman. Z.; writing review and editing, Rahman. Z., kelarev, A.; visualization, Billah, R.; supervision, Yi, X., Kelarev, A.; project administration, Yi, X.; funding acquisition, Yi, X. All authors have read and agreed to the published version of the manuscript.",

Funding: "The work was supported by RMIT Research Stipend Scholarship (RRSS) Program. The work of Xun Yi was supported in part by the Project "Privacy-Preserving Online User Matching" under the grant ARC DP180103251. "The APC was funded by RMIT Research Stipend Scholarship (RRSS) Program".

References

1. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of medical systems* **2018**, *42*, 130.
2. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin Whitepaper* **2008**.
3. Mehedi, S.K.T.; Shamim, A.A.M.; Miah, M.B.A. Blockchain-based security management of IoT infrastructure with Ethereum transactions. *Iran J Comput Sci* **2019**, *2*, 189–195. doi:https://doi.org/10.1007/s42044-019-00044-z.

4. Rahman, Z.; Yi, X.; Khalil, I.; Kelarev, A. Blockchain for IoT: A Critical Analysis Concerning Performance and Scalability. International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer, 2021, pp. 57–74.
5. Salman, T.; Zolanvari, M.; Erbad, A.; Jain, R.; Samaka, M. Security services using blockchains: A state of the art survey. *IEEE Communications Surveys & Tutorials* **2018**.
6. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal* **2018**.
7. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing* **2018**, *15*, 840–852.
8. Eckhoff, D.; Wagner, I. Privacy in the Smart City—Applications, Technologies, Challenges, and Solutions. *IEEE Communications Surveys & Tutorials* **2017**, *20*, 489–516.
9. Butun, I.; Österberg, P. A Review of Distributed Access Control for Blockchain Systems Towards Securing the Internet of Things. *IEEE Access* **2021**, *9*, 5428–5441. doi:10.1109/ACCESS.2020.3047902.
10. Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys Tutorials* **2016**, *18*, 2084–2123. doi:10.1109/COMST.2016.2535718.
11. Mylrea, M.; Gourisetti, S.N.G. Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security. 2017 Resilience Week (RWS). IEEE, 2017, pp. 18–23.
12. Rahman, Z.; Yi, X.; Khalil, I. Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet of Things Journal* **2022**, pp. 1–1. doi:10.1109/JIOT.2022.3147186.
13. Chang, T.; Svetinovic, D. Improving Bitcoin Ownership Identification Using Transaction Patterns Analysis. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2020**, *50*, 9–20. doi:10.1109/TSMC.2018.2867497.
14. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Communications Surveys Tutorials* **2019**, *21*, 1508–1532. doi:10.1109/COMST.2019.2894727.
15. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. *IEEE Communications Surveys Tutorials* **2019**, *21*, 1508–1532. doi:10.1109/COMST.2019.2894727.
16. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys Tutorials* **2019**, *21*, 1676–1717. doi:10.1109/COMST.2018.2886932.
17. Wang, S.; Zhang, Y.; Zhang, Y. A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. *IEEE Access* **2018**, *6*, 38437–38450. doi:10.1109/ACCESS.2018.2851611.
18. Faber, B.; Michelet, G.C.; Weidmann, N.; Mukkamala, R.R.; Vatrapu, R. BPDIMS: A blockchain-based personal data and identity management system. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2020.
19. Saura, J.R.; Ribeiro-Soriano, D.; Palacios-Marqués, D. Setting Privacy "by Default" in Social IoT: Theorizing the Challenges and Directions in Big Data Research. *Big Data Research* **2021**, *25*, 100245. doi:https://doi.org/10.1016/j.bdr.2021.100245.
20. Li, R.; Song, T.; Mei, B.; Li, H.; Cheng, X.; Sun, L. Blockchain for large-scale internet of things data storage and protection. *IEEE Transactions on Services Computing* **2018**.
21. Arcadius Tokognon, C.; Gao, B.; Tian, G.Y.; Yan, Y. Structural Health Monitoring Framework Based on Internet of Things: A Survey. *IEEE Internet of Things Journal* **2017**, *4*, 619–635. doi:10.1109/JIOT.2017.2664072.
22. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. LSB: A Lightweight ScalableBlockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing* **2019**, *134*, 180 – 197. doi:10.1016/j.jpdc.2019.08.005.
23. Zamani, M.; Movahedi, M.; Raykova, M. RapidChain: Scaling Blockchain via Full Sharding. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, 2018, p. 931–948. doi:10.1145/3243734.3243853.
24. Kiffer, L.; Rajaraman, R.; shelat, a. A Better Method to Analyze Blockchain Consistency. Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain. Association for Computing Machinery, 2018, CCS 18, p. 729–744. doi:10.1145/3243734.3243814.
25. Bartolucci, S.; Bernat, P.; Joseph, D. SHARVOT: Secret SHARe-Based VOTing on the Blockchain. Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain. Association for Computing Machinery, 2018, WETSEB 18, p. 30–34. doi:10.1145/3194113.3194118.
26. Rahman, Z.; Khalil, I.; Yi, X.; Atiquzzaman, M. Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. *IEEE Communications Magazine* **2021**, *59*, 128–134. doi:10.1109/MCOM.001.2000679.
27. Zhang, L.; Wu, Q.; Domingo-Ferrer, J.; Qin, B.; Zeng, P. Signatures in hierarchical certificateless cryptography: Efficient constructions and provable security. *Information Sciences* **2014**, *272*, 223 – 237. doi:10.1016/j.ins.2014.02.085.
28. Guo, J.; Yang, W.; Lam, K.Y.; Yi, X. Using Blockchain to Control Access to Cloud Data. International Conference on Information Security and Cryptology. Springer, 2018, pp. 274–288.
29. Kamil, I.A.; Ogundoyin, S.O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks. *Journal of Information Security and Applications* **2019**, *44*, 184 – 200. doi:10.1016/j.jisa.2018.12.004.
30. Mehedi, S.T.; Anwar, A.; Rahman, Z.; Ahmed, K.; Rafiqul, I. Dependable Intrusion Detection System for IoT: A Deep Transfer Learning-based Approach. *IEEE Transactions on Industrial Informatics* **2022**, *1*, 1–1. doi:10.1109/TII.2022.3164770.

31. Yang, G.; Tan, C.H. Certificateless cryptography with KGC trust level 3. *Theoretical Computer Science* **2011**, *412*, 5446 – 5457. doi:10.1016/j.tcs.2011.06.015.
32. Saura, J.R.; Palacios-Marqués, D.; Ribeiro-Soriano, D. Using data mining techniques to explore security issues in smart living environments in Twitter. *Computer Communications* **2021**, *179*, 285–295. doi:https://doi.org/10.1016/j.comcom.2021.08.021.
33. Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand: Scaling byzantine agreements for cryptocurrencies. Proceedings of the 26th Symposium on Operating Systems Principles. ACM, 2017, pp. 51–68.
34. Neisse, R.; Steri, G.; Fovino, I.N.; Baldini, G. SecKit: a model-based security toolkit for the internet of things. *computers & security* **2017**, *54*, 60–76.
35. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems* **2018**, *82*, 395–411. doi:https://doi.org/10.1016/j.future.2017.11.022.
36. Zamani, M.; Movahedi, M.; Raykova, M. RapidChain: A Fast Blockchain Protocol via Full Sharding. *IACR Cryptology ePrint Archive* **2018**, *2018*, 460.
37. Gramoli, V. From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems* **2019**.
38. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference. ACM, 2019, p. 30.
39. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal* **2020**, *5*, 1184–1195.
40. Khan, M.Y.; Zuhairi, M.F.; Ali, T.; Alghamdi, T.; Marmolejo-Saucedo, J.A. An extended access control model for permissioned blockchain frameworks. *Wireless Networks* **2021**, pp. 1–12.
41. Neisse, R.; Steri, G.; Nai-Fovino, I. A blockchain-based approach for data accountability and provenance tracking. Proceedings of the 12th International Conference on Availability, Reliability and Security. ACM, 2021, p. 14.
42. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering* **2018**, *30*, 1366–1385.
43. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**.
44. Minoli, D.; Occhiogrosso, B. Blockchain mechanisms for IoT security. *Internet of Things* **2018**, *1*, 1–13.
45. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security* **2018**, *78*, 126–142.
46. Rahman, Z.; Yi, X.; Khalil, I. Blockchain based AI-enabled Industry 4.0 CPS Protection against Advanced Persistent Threat. *IEEE Internet of Things Journal* **2022**, pp. 1–1. doi:10.1109/JIOT.2022.3147186.
47. Rahman, Z.; Khalil, I.; Yi, X.; Atiquzzaman, M. Blockchain-Based Security Framework for a Critical Industry 4.0 Cyber-Physical System. *IEEE Communications Magazine* **2021**, *59*, 128–134. doi:10.1109/MCOM.001.2000679.
48. Saraf, C.; Sabadra, S. Blockchain platforms: A compendium. Innovative Research and Development (ICIRD), 2018 IEEE International Conference on. IEEE, 2018, pp. 1–6.
49. Buterin, V.; et al. A next-generation smart contract and decentralized application platform. *Ethreum White Paper* **2014**.
50. Abdella, J.; Shuaib, K. Peer to Peer Distributed Energy Trading in Smart Grids: A Survey. *Energies* **2018**, *11*, 1560.
51. Kshetri, N. Can blockchain strengthen the internet of things? *IT professional* **2017**, *19*, 68–72.
52. Dorri, A.; Kanhere, S.S.; Jurdak, R. Towards an optimized blockchain for IoT. 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). IEEE, 2017, pp. 173–178.
53. Popov, S.; Saa, O.; Finardi, P. Equilibria in the Tangle. *arXiv preprint arXiv:1712.05385* **2017**.
54. Rahman, A.; Hossain, M.S.; Rahman, Z.; Shezan, S.A. Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain. *International Journal of Advanced Technology and Engineering Exploration* **2019**, *6*, 257–266.
55. Yang, R.; Wakefield, R.; Lyu, S.; Jayasuriya, S.; Han, F.; Yi, X.; Yang, X.; Amarasinghe, G.; Chen, S. Public and private blockchain in construction business process and information integration. *Automation in Construction* **2020**, *118*, 103276. doi:https://doi.org/10.1016/j.autcon.2020.103276.
56. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet of Things Journal* **2019**, *6*, 2188–2204. doi:10.1109/JIOT.2018.2882794.
57. Global System for Mobile Communications Association, O.G.S.M. Opportunities and Use Cases for Distributed Ledger Technologies in IoT, https://www.gsma.com/iot/opportunities-distributed-ledger-in-iot/, accessed on January 2019 [Survey made by Gartner].
58. Rahman, A.; Islam, M.J.; Rahman, Z.; Reza, M.M.; Anwar, A.; Mahmud, M.A.P.; Nasir, M.K.; Noor, R.M. DistB-Condo: Distributed Blockchain-Based IoT-SDN Model for Smart Condominium. *IEEE Access* **2020**, *8*, 209594–209609. doi:10.1109/ACCESS.2020.3039113.
59. Rahman, A.; Nasir, M.K.; Rahman, Z.; Mosavi, A.; S., S.; Minaei-Bidgoli, B. DistBlockBuilding: A Distributed Blockchain-Based SDN-IoT Network for Smart Building Management. *IEEE Access* **2020**, *8*, 140008–140018. doi:10.1109/ACCESS.2020.3012435.
60. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.

Short Biography of Authors 673

Ziaur Rahman is PhD candidate in Cyber security of RMIT University. He served Mawlana Bhashani Science & Technology University, Bangladesh as an Associate Professor in ICT. He casually served RMIT, Monash, Deakin and Charles Sturt University, Australia. Three (03) articles he coauthored were nominated and received the best paper awards. He is affiliated with the IEEE, ACM, Australian Computer Society. His research interests include blockchain technology, security of the internet of things (IoT), machine learning. 674

Xun Yi is currently a full Professor of Cybersecurity with the School of Computing Technologies with the School of Science, RMIT University, Melbourne, VIC, Australia. He has published more than 200 research papers in international journals and conference pro-ceedings. His research interests include applied cryptography, computer and network security, mobile and wireless communication security, and data privacy protection. Prof. Yi has ever undertaken program committee members for more than 30 international conferences. Recently, he has led some Australia Research Council Discovery Projects in Data Privacy Protection. From 2014 to 2018, he was an Associate Editor for IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. 675

Sk. Tanzir Mehedi graduated with a BSc. Engineering degree in Information and Communication Technology from Mawlana Bhashani Science and Technology University, Bangladesh. He worked as a Data Analyst Engineer (Trainee) at Fujitsu Research Institute, Tokyo, Japan major of R and Python programming. He is also a Java and PHP developer and open web contributor. Currently, he has been serving as a Lecturer at Department Of Information Technology (IT), University Of Information Technology And Sciences (UITS), Baridhara, Dhaka-1212, Bangladesh. His research interests include Data Science, Blockchain Technology, Machine Learning and Data Privacy Protection. 676

Rafiqul Islam has been working as an Associate Professor at the School of Computing, Mathematics and Engineering, Charles Sturt University, Australia. Dr Islam's main research background in cybersecurity focuses on malware analysis and classification, security in the cloud, privacy in social media, and the dark web. Dr. Islam has a strong research background in Cybersecurity with a specific focus on malware analysis and classification, Authentication, security in the cloud, privacy in social media and Internet of Things (IoT). He is leading the Cybersecurity research team and has developed a strong background in leadership, sustainability, collaborative research in the area. He has a strong publication record and has published more than 160 peer-reviewed research papers. His contribution is recognized both nationally and internationally through achieving various rewards such as professional excellence reward, research excellence award, leadership award. 677

Andrei Kelarev was an Associate Professor with the University of Wisconsin and the University of Nebraska, USA, and a Senior Lecturer with the University of Tasmania, Australia. He is currently a Research Fellow with the School of Science, RMIT University, Australia. He is an author of two books and 198 journal articles. He is involved in the cyber security applications of machine learning and data mining. He was a Chief Investigator of a large Discovery Grant from the Australian Research Council. His research interests include Cybersecurity. 678