On the Convergence of Blockchain and Internet of Things (IoT) Technologies

Mohammad Maroufi
University of Tabriz

Reza Abdolee
California State University, Bakersfield (CSUB)

Behzad Mozaffari Tazekand
University of Tabriz

The Internet of Things (IoT) technology will soon become an integral part of our daily lives to facilitate the control and monitoring of processes and objects and revolutionize the ways that human interact with the physical world. For all features of IoT to become fully functional in practice, there are several obstacles on the way to be surmounted and critical challenges to be addressed. These include, but are not limited to cybersecurity, data privacy, energy consumption and scalability. The Blockchain decentralized nature and its multi-faceted procedures offers a useful mechanism to tackle several of these IoT challenges. However, applying the Blockchain protocols to IoT without considering their tremendous computational loads, delays, and bandwidth overhead can let to a new set of problems. This review evaluates some of the main challenges we face in the integration of Blockchain and IoT technologies and provides insights and high level solutions that can potentially handle the shortcomings and constraints of both IoT and Blockchain technologies.

INTRODUCTION

Internet of Things (IoT) enables a network of physical objects (things), empowered by sensing, processing and communication units, to sense physical events, exchange data and interact with the environment to accordingly make decisions or monitor some processes and events without human interventions. One of the prominent motivation behind the advent of IoT systems was to facilitate the real-time data collection and to provide automatic and remote control mechanisms replacing the today's conventional monitoring and control systems across different industries, such manufacturing, environmental monitoring, digital agriculture, smart cities and home, business management and asset tracking (Rayes and Salam, 2017). It is predicted that by 2020, the number of connected devices surpasses 20 billion (Hung, 2017). This growing demands and the tremendous expansion of IoT across emerging industries requires swift advancement in the current IoT protocols, technologies, and architectures and substantial progress in identifying the supporting IoT standards.

IoT systems generate massive volumes of data that require network connectivity and power, processing and storage resources to transform these data into meaningful information or services. Beside reliable connectivity and network scalability, cybersecurity and data privacy of are crucial importance in using IoT networks. Currently, centralized architecture models widely used to authenticate, authorize and connect different nodes in an IoT network. With the growing number of devices to hundreds of billions, centralized systems will break down and fail when the centralized server becomes unavailable. Decentralized IoT architecture was proposed to solve this issue, in which it moves away some of the network processing tasks to the edge (Ai et al., 2018). For instance, in fog computing models, some of the critical operations that used to be processed by cloud servers are now assigned to be performed by IoT hubs or fog (Alrawais et al., 2017). Peer-to-peer (P2P) architecture provides another solution, where neighboring devices directly interact with each other in meshes to identify, authenticate and exchange information without using any centralized node or agent between them (Buyya and Dastjerdi, 2016).

IoT devices include both resource-constrained and resource-rich devices. Although some IoT devices such as smartphones and Raspberry Pi utilize sufficient resources, most of them feature limited power, processing, and memory resources due to their small sizes and low inherent design cost. Therefore, IoT devices and their protocols have to be designed to be resource efficient and meanwhile perform real-time processing, keep connectivity and protect the security and privacy of the transmit data (Haroon et al., 2016; Musaddiq et al., 2018).

The battery capacity and computing power limitation created an obstacle to executing heavy and advanced cryptography algorithms to protect information. Critical security and privacy issues may arise in IoT devices because of sensitive personal data which connected things/objects reveal about their owners behavior and activities. Collecting such crucial data in centralized untrusted entities may create a significant privacy risk. This is probable in practice. For instance, Edward Snowden revealed that the PRISM program which operates under the United States National Security Agency (NSA), collects the data generated from Internet communications from various U.S. internet providers (Conoscenti et al., 2016; Yang et al., 2017).

Due to the critical role of IoT devices in sensing the surrounding world and activating appropriately, collecting reliable data has a vital bearing on the precise functionality of these devices. IoT data reliability can be achieved by using distributed signal processing methods which execute a verification process among all its participants to ensure that data remain immutable and not tampered. Considering this and understanding the basic features of Blockchain technology, which used as a cornerstone of Bitcoin (Nakamoto, 2009), we can intuitively find out the potential that Blockchain can offer to address the data reliability challenge in IoT. Bitcoin is supported by the Blockchain protocol to ensure that the information remains immutable. This protocol was proposed by a group of researchers in 1991 to timestamp digital documents and makes it impossible to backdate or tamper with them (Bashir, 2018).

The Blockchain suggests a way to record transactions or any digital interaction that is designed to be secure, transparent, highly resistant to outages, auditable, and efficient which encourage IoT companies to enhance their IoT network-based to Blockchain-based technology. It is a distributed ledger which managed by a peer-to-peer network to provides inter-node communication and verifying new blocks. Security may be considered as one of the most valuable features of the Blockchain. Once data recorded in the Blockchain, it cannot be modified without modification of all subsequent blocks and that needs a consensus of the network majority. The consensus algorithms used in Blockchain slow down the creation of new blocks and make it hard to tamper with previous blocks (Mougayar and Buterin, 2016).

An intelligence convergence of IoT and Blockchain technologies can lead to a verifiable, secure and robust mechanism of storing and managing data generated or processed by smart connected devices. This network of interconnected devices will be able to interact with their environment and make decisions without any human intervention (Wood, 2018).Although, integrating Blockchain technology in IoT will enhance security, data privacy, and reliability of IoT devices, it create a new set of challenges. In recent years, researchers have widely studied the integration approaches, benefits, and challenges in IoT devices and networks (Conoscenti et al., 2016; Reyna et al., 2018b; Atlam et al., 2018).A detailed literature review on the Blockchain applications in IoT was reported by (Conoscenti et al., 2016), in which the authors categorize previous research based on the Blockchain use cases in IoT and discuss their advantage and disadvantages. In (Reyna et al., 2018b; Atlam et al., 2018) researchers have introduced the key features of Blockchain, their application in IoT devices, challenges, and solutions to overcome challenges in IoT technology. Some investigations focused on the Blockchain distinct features and their impacts in integration with IoT. (He et al., 2018) reviewed the main consensus mechanisms and pointed out their strengths and weaknesses in IoT applications. They provided a comprehensive guide for developers to choose and design consensus mechanisms for Blockchain based consensus algorithms for IoT applications by considering their limited resources. In (Dorri et al., 2017; Roman et al., 2013) investigators have analyzed the cybersecurity and data privacy issues of IoT networks and explored Blockchain protocols as one of the potential solutions. Smart contracts and their roles in efficient controlling of IoT devices and related cybersecurity issues were discussed in (Christidis and Devetsikiotis, 2016).

The aim of this paper is to present a comprehensive study on the integration of Blockchain and IoT and analyze different aspects of these embedded technologies. We attempt to provide strategic and technical insights into IoT restrictions and challenges, Blockchain specification and weaknesses, Blockchain-IoT integration approaches and solutions to overcome implementation challenges. The paper also provides condensed high-level knowledge about IoT and Blockchain technologies to identify use cases of Blockchain in IoT systems and networks.

The remainder of the paper is organized as follows: In Section 2, we briefly explain the Blockchain functionality and describe its advantages and disadvantages. Section 3, presents the integration of Blockchain and IoT systems. In Section 4, we discuss solutions and challenges in this integration. Finally, in Section 5, we provide conclusions and future works.

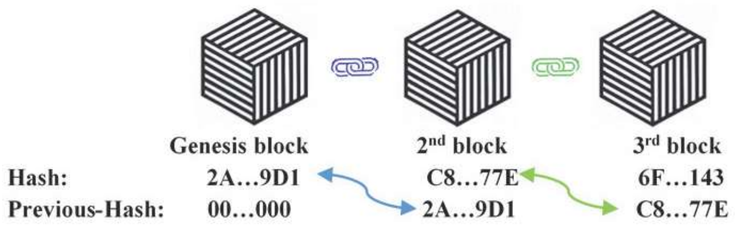
BLOCKCHAIN

The Blockchain as derived from its name consists of a chain of blocks. A block is a data structure which allows Blockchain to record the generated and exchanged transactions and each block is linked to the chain by cryptography (Wüst and Gervais, 2017). The Blockchain is a distributed ledger which has three fundamental attributes: recorded, transparent, and decentralized. Blockchain forms participants in a P2P distributed ledger to records transactions safely and interact with each other via a trustless method, meaning that there is no need to trust other devices and third parties. All participants keep and update a copy of distributed ledger to check and validate transactions which makes Blockchain transparent and impossible to hack or lost any data (Laurence, 2018). Each transaction includes three main components, i.e., the data, the hash, and the hash of the previous block (Decuyper, 2018). The data and hash can be defined as follow:

- ***Data:*** The data which is collected inside a block. There can be different data types, depending on the Blockchain applications, for instance, Bitcoin Blockchain stores the transaction information such as the sender, receiver and the number of coins.
- ***Hash:*** The hash is a function that converts a block and all of its contents to a unique fixed-length output which can be interpreted as a fingerprint of the block. Blockchain determines hash once a block created. Modifying the contents of a block will change the hash. Hashes are very useful to detect block tampers. Once the block fingerprint changes, it will be no longer considered as the same block. Hash algorithms take the variable length input string and give out a fixed length output. For instance, Bitcoin uses SHA256 as a hashing algorithm.

Each block in the network records the hash of the previous block. This leads to a chain of blocks with enhanced security. For example, in Figure 1, there is a chain of three blocks. Block 3 points to block 2 and block 2 points to block 1 using the hashes of previous blocks.[1] If hackers tamper the second block data, the related block hashes changes. This makes the third block and all subsequent blocks invalid because they have not stored a valid hash of the previous block (Decuyper, 2018). Moreover, any user has two keys: a public key which is known to other users to encrypt their transactions and a private key to read encrypted transactions by the user. Therefore, asymmetric cryptography is used to decrypt the message encrypted by the corresponding public key (Ferrag et al., 2018).

FIGURE 1
BLOCKCHAIN HASHING MECHANISM



In a P2P network, control and responsibility spread out among lots of different peers, which improve network security. Blockchain utilizes a P2P distributed ledger to eliminate the centralized database risks by storing data across its network and lets everyone to join it. When a node connects to this network, it obtains a full copy of the Blockchain that can later be used to verify if everything is still in order (Norman, 2017). A node can be any electronic device, including a computer, phone, a printer or even a fridge, as long as connects to the internet. All nodes have equal importance on a Blockchain. However, each node has different tasks in making a Blockchain. Nodes and their roles can be categorized as follows (Norman, 2017):

- ***Light node:*** Store some of the information recorded on a Blockchain.
- ***Full node:*** Store a copy of all of the information recorded on a Blockchain.
- ***Mining or forging node:*** Process transactions, put them into blocks, add blocks to a Blockchain, approve and broadcast joined block to the network.

These nodes work together to manage, secure and, expand the blockchain. Users in the Blockchain network utilize mining nodes to creating new blocks, verifying their information and adding them to a distributed ledger by executing the consensus algorithm as below (Ferrag et al., 2018):

- User utilizes its private key to sign a transaction and advertises it to its peers.
- User peers validate the received transaction and advertise it over the network.
- All the involved participates commonly verify the transaction to meet a consensus agreement.
- Miners add the valid transaction into a time-stamped block and broadcast it again into the network.
- After verifying the advertised block and matching its hash with the previous block, this block joins the Blockchain.

Consensus protocols are one of the most important and revolutionary aspects of Blockchain technology. Consensus protocol contains rules and verification procedures to validate data which lets the devices around the world, to agree about adding data to the Blockchain (Bashir, 2018). Based on Blockchain requirements, a large variety of consensus protocols exist. The four main consensus protocols are (Bach et al., 2018):

- ***Proof of Work (PoW):*** Consists of solving a complex mathematical problem to add a new block to the chain. The process is costly and time-consuming but once solved the solution can be easily verified by other participants. Miners solve a problem, publish the solution and add the new block to the chain that will be spread over the network to be verified by all participants. This process can simultaneously happen in different parts of the network. When peers plan to add a new block, they have to check the branch size and choose the most accumulated work (the longest chain) which is assumed to be the valid one (Gupta et al., 2018). The proof-of-work defines one CPU one vote approach as a solution for representation problem in majority decision-making. If the majority of CPU powers belong to honest nodes, they control the decision with the fastest growing chain. To modify a past blocks, an attacker would have to redo the proof-of-work of the block and all blocks after it and provides higher CPU power than the honest nodes (Nakamoto, 2009).

- ***Proof of Stake (PoS):*** Similar to PoW, it attempts to provide consensus. In the PoS the originator of next block is chosen based on the various randomized combination of minors cryptocurrencies resources and the duration that they hold their resources. Contrary to PoW miners that may not have cryptocurrency and only attempt to maximize profits by increasing computational power, PoS miners defend Blockchain network to protect their wealth and profits. As long as the stake is higher than the transaction fees, participants can trust them to do their job correctly (Vashchuk and Shuwar, 2018).
- ***Practical Byzantine Fault Tolerance****:* Practical Byzantine Fault Tolerance (PBFT) idea derives from a story about a group of generals, independently commanding a section of the Byzantine army, surrounding a city which they intended to capture. The most important thing is that all generals reach a mutual decision to attack or retreat. The Byzantine problem becomes even more complicated when disloyal generals, votes for an irrelevant strategy (Prashanth Joshi et al., 2018). The Byzantine consensus algorithm determines new blocks in rounds and selects the sponsor to advertise an uncorroborated block. The transaction validation includes three steps and in all the phases, the node enters the next stage only after obtaining 2/3 of all network nodes vote (Prashanth Joshi, et al. 2018; Castro and Liskov, 2002):
    1) Pre-vote step: validators indicate the need to broadcast a block for pre-voting. It is possible to skip this step if the validators believe it is unnecessary for a particular transaction and they can directly approve the pre-voting of a block or transaction by gaining 2/3 votes from the network.
    2) Pre-commit step: If PBFT neglected the pre-vote step; the pre-commit phase goes through the tedious voting phase for broadcast and validation. Once the block receives 2/3 votes for the pre-commit step, it enters the commit phase.
    3) Commit step: a node validates a block or transaction and broadcasts a commit for it. This phase accepts the block or transaction validation with 2/3 votes.
- ***Delegated Proof of Stake (DPoS):*** Delegated Proof of Stake is one of the fastest, efficient, decentralized, and most flexible consensus models available. DPOS leverages the power of stakeholder approval voting to resolve consensus issues in a fair and democratic way. All network parameters, from fee schedules to block intervals and transaction sizes, can be tuned via elected delegates. The people who hold the particular cryptocurrency will be able to make votes by their token to choose who runs the network. Deterministic selection of block producers allows delegates to confirm transactions in an average of just a second. Perhaps most importantly, the consensus protocol is designed to protect all participants against unwanted regulatory interference (Larimor, 2016).

The smart-contracts are another relevant feature of Blockchain which includes self-executing programs with the terms of the transaction between users. They promise low transaction fees compared to traditional systems that require a trusted third party to enforce and execute the terms of an agreement. They contain a set of code and data that store in a particular Blockchain address and devices can call public functions via this address. Smart contracts give autonomy, trust, backup, safety, saving money, and accuracy to the Blockchain. Even Bitcoin allows some limited set of smart contracts to execute. Ethereum (Gavin, 2014) was the first Blockchain platform which supports arbitrary code execution on the Blockchain (Alharby and Moorsal, 2017).

Blockchain can be classified either as private or public which provide a certain level of immunity against faulty or unwanted users for the ledger. The main differences between private and public Blockchains lie in the execution of the consensus protocol, the maintenance of the ledger, and the authorization to join the P2P network. In a private Blockchain, the centralized trusted authority that manages the authentication and authorization process selects the miners. In a public Blockchain, there is no intervention of any third party for the miner selection and joining of a new user to the Blockchain network (Fernandez-Carames and Fraga-Lamas, 2018). Private Blockchains possess some advantages in comparison with public ones such as (Buterin, 2015):

1- Companies can change the rules of a Blockchain, return transactions, and adjust balances.
2- The known validators protect Blockchain from a majority attack risk.
3- The cheaper transactions due to less processing power consumption of fewer validator nodes.
4- Provide a higher level of privacy for reading restricted permissions.

Blockchain Benefits

Considering the information provided in the previous section, the most important benefits of Blockchain technology are (Dorri et al., 2017; Laurence, 2018; Wüst and Gervais, 2017):

Security

Big companies may put millions of their customers at serious risk if they couldn't provide a secure centralized database. Blockchain uses a distributed ledger to secure its information and protects them against the failure of a centralized decision maker. Furthermore, decentralization guarantees that data remains secure even if one of these devices/nodes fails. Blockchain suggests a high level of security to each individual user as it eliminates using the passwords and online identities by employing powerful cryptography. It provides an address and associated crypto-assets through a combination of public and private keys, making the users identities to not have a direct association with their addresses. (Prashanth Joshi et al., 2018).

Transaction Verifiability

Blockchain allows any participant to confirm the integrity of transactions. In a centralized network, the central entity provides the correct state of observers instead of verifying that all state transitions were executed correctly or not. In a distributed ledger, the restricted set of participants serve as verifiers or miners which confirm any changes, while other participants can check the changes as an observer. The ability to validate the transaction by themselves enhances the Blockchain security and reliability (Wüst and Gervais, 2017).

Transparency

Blockchain as a distributed ledger provides data transparency by sharing the same documentations to all participants. These documentations are the immutable data accessible by all Blockchain members which can be only updated by a consensus mechanism. Thus, data transparency on a Blockchain creates a more accurate, consistent database to protect essential data. The participants' level of access to information can change from one to another based on their permission (Reyna et al., 2018).

Privacy

There is an inherent trade-off between privacy and transparency. Achieving data privacy in the centralized architecture is easier than the transparent distributed system. However, Blockchain does not need any integrity for the network layer to guarantee the protection of information from unauthorized changes. Cryptography concealed the user identity which makes it arguably impossible to determine the identity accounts owner (Wüst and Gervais, 2017).

Trustless

In Blockchain, participants run consensus protocols to agree on what should be unanimously and securely added to the distributed ledger. Blockchain can verify ownership of anything entirely without the need for a central authority. Smart contracts execute automatically once their terms met. This Blockchain feature eliminates the disputing contracts and contributes to its trustless nature. It is not a case of whether a third party is trusted to carry out tasks, as it is an automated and immutable system in which there is no trust required (Atlam et al., 2018).

Blockchain Challenges

Although the fundamental concept of Blockchain is simple, its implementation faces numerous difficulties. This section presents the main challenges in the implementation of Blockchain.

Storage Capacity and Scalability

With the continuous growth of transaction amount, the Blockchain size increases and any nodes in the network needs significant storage resources to store data. Although the full copy of Blockchain just saves in the full-nodes, an oversized Blockchain has a negative impact on network functionality. For instance, it will slow down the propagation speed and increases the users' synchronization time, leading to Blockchain unwanted forks. Due to the Blockchain size growth, the validation time increases and that needs more computational power to verify the activities over the network. Transaction validation is a fundamental component of consensus protocol which has a direct impact on the Blockchain network scalability (Zheng et al., 2017).

Security

Blockchain technology uses numerous techniques to achieve the highest level of security for transactions. Blockchain employs a combination of public and private key to securely encrypt and decrypt data. Blockchain eliminates the 51% majority attack and fork problems by determining the longest chain as an authentic block (Prashanth Joshi et al., 2018). If a Blockchain participant able to manage more than 51% of the mining power, majority attack happens and in this situation this particular participant is able to control the consensus in the network. The accelerated evolution of mining pools increases the probability of majority attack which could compromise the integrity of Blockchain (Eyal and Sirer, 2018). The double-spend attack tries to spend the same money more than once. Upon a successful attack, the victim is left with an invalidated payment while having already delivered the service. Bitcoin users protect themselves from double spending fraud by waiting for confirmations when receiving payments on the Blockchain. Multiple variants of the double-spend attack exist. The race attack does only work for fast payment scenarios, e.g., ATMs, cafes or fast food chains. The user sends an unconfirmed transaction directly to the merchant, who accepts it and do not wait for Blockchain confirmation. Meanwhile, they broadcast a conflicting transaction to the network. As the merchant saw their own transaction first, they are under the illusion of getting paid, while the rest of the network predominantly saw the double-spend first and thus it's likely the merchant will in fact not get paid. The second transaction is more likely to be confirmed, and the merchant is cheated. Furthermore, the Finney attack, Denial of Service (DoS), Man in the Middle (MitM) or Sybil can obstruct the network operation (Karame et al., 2012).

Anonymity and Data Privacy

Privacy in Blockchain enables the user to perform transactions without leaking its identification information in the network. The Blockchain transparency compromises data privacy even though there is no direct relationship between transactions and individuals. They can reveal the user identity by checking, auditing and tracing each transaction from the system's very first transaction. Therefore, many applications based on public Blockchain technology require a higher level of privacy, specifically in sensitive data use cases. The Blockchain platform accumulates transactions as encrypted data to enhance data privacy. Consequently, the Blockchain compiler is responsible for translating the generic code into cryptographic primitives that supply information anonymity in transactions (Reyna et al., 2018). Another approach to tackle data privacy is to store sensitive data outside the chain, referred to as the off-chain solution. This kind of solution supports systems that manage large amounts of data since it would be impractical to store them inside the Blockchain. They are particularly suitable for highly sensitive data systems which need tighter access control, such as healthcare applications. Users can utilize the public Blockchain to store anchor data and verify data without relying on authorities, when protected data safely stored off-chain. These off-chain sources must be fault tolerant and should not introduce bottlenecks or single points of failure (Lazarovich, 2015).

Smart Contracts

In 1994, Nick Szabo proposed the smart-contract concept. It is a self-executable code that runs on the Blockchain to facilitate, perform and enforce the terms of an agreement. Thus, smart contracts guarantee low transaction fees, high-speed, precision, efficiency, and transparency, compared to traditional systems that require a trusted third party to enforce and execute the terms of an agreement. The Blockchain stores smart contracts and allocate a unique address to identify each contract which let any user operate with them only by sending a transaction to this address (Szabo, 1997). The benefits of smart-contracts are not obtained at no cost, as they are vulnerable to a series of attacks that creates several new challenges such as hacking, bugs, viruses or communication failures. Bugs in contract coding are highly critical because of the irreversibly and immutable nature of the system. Mechanisms to verify and guarantee the correct operation of smart contracts are necessary to be widely and safety adopted by clients and providers (Delmolino et al., 2016).

Legal Issue

Like any new technology, Blockchain gives rise to some delicate legal challenges. Most of the related laws are becoming obsolete and need to be revised, especially since the emergence of new disruptive technologies such as Blockchain. The development of new laws and standards can ease the certification of security features of devices, and that may help building the most secure and trusted network. Any Blockchain system that holds personal data, for instance, IoT domain applications, will need to comply with applicable data protection laws. The distributed nature of Blockchain is of concern because of cross-border transactions and the ways to execute regulations among different countries with distinct rules. More importantly, creating large data repositories on a Blockchain gives rise to security breaches. Blockchain operators will need to take cybersecurity seriously to avoid potential regulatory action and reputational damage. The need to add more control components over the network has introduced private and consortium Blockchains. These regulations will have an impact on the Blockchain and IoT future and could disrupt the decentralized and free nature of Blockchain by introducing a controlling, centralized participant such as a country (McKenzie, 2017; Reyna et al., 2018).

Consensus

Consensus consist of two functions: First, it allows Blockchain to be updated while ensuring that every block in the chain is valid as well as keeping participants incentivized and second, it prevents any single entity from controlling or crashing the whole Blockchain system. The consensus aim is to create a distributed network without central authorities with participants who do not necessarily need to trust each other (Laurence, 2018). An essential disadvantage of primitive consensus protocol is that PoW makes Bitcoin depend on energy consumption. Moreover, miners solve the PoW algorithm to receive the transaction fee and this has led to the situation where people are building larger mining farms. PoW provides more rewards to people with better and more equipment. Even further miners can come together in mining pools to combine their hashing power and distribute the awards across everyone in the pool which makes the Blockchain more centralized as opposed to its decentralized nature and encourage using massive amounts of electricity (Gupta et al., 2018).

PoS is the most popular alternative of PoW consensus approach in Blockchain. It is established on the fact that those users who own more coins, are more interested in the survival and the correct functioning of the system, and, therefore, are the most suitable to carry the responsibility of protecting the system (Vashchuk and Shuwar, 2018). Validators are not chosen completely randomly to verify transactions. A node has to deposit a certain amount of coins into the network as stake that can be considered as security. There is a direct relationship between the validator stake size and its chances to be chosen as forging validator of the next block. PoS consensus protocol might not seem fair because it supports the rich but in reality, it is fairer compared to PoW. In essence, the difference between PoW and PoS are quite significant. PoS does not let everyone mine new blocks and therefore it uses considerably less energy. It is also more decentralized in comparison with PoW that has mining pools (Mougayar and Buterin, 2016).

BLOCKCHAIN & IOT CONVERGENCE

The Internet of Things (IoT) promises to make our lives more convenient by turning each physical object in our surrounding environment into a smart object. IoT exponential extension in recent years creates fundamental challenges in several aspects such as security, privacy, scalability, and maintainability. IoT devices need to operate on effective architecture even in performing simple tasks such as sensing, processing, data collections and communicating. The Blockchain provides many attractive features, such as decentralization, persistency, anonymity, and auditability. These features make Blockchain a promising solution to address some of the paramount challenges in IoT. IoT applications can commonly use Blockchain to access things and store data. Users must be able to access data remotely from any location by using a secure mean and ensure about the privacy of data stored in the network (Rayes and Salam, 2017; Yang et al., 2017; He et al., 2018; Lin et al., 2017). According to Gartner investigation (Walker et al., 2016) in 2025 IoT industries faced five main issues that will be solved by Blockchain technology as below:

- ***How will industries connect 50 billion devices by 2020?*** Blockchain can store 2^{160} addresses which provide IoT devices addressability. More importantly, the Blockchain P2P ledger creates a direct connection between each device to send their information instead of look through a database of billions of records to find that device.
- ***How will industries create controls for vast number of decentralized devices?*** Blockchain sends a cryptographically signed message between devices that no hacker can do a man in the middle (MitM) attack or penetrate in it. A user can send control signals from a central location to other decentralized devices.
- ***How will industries enable P2P communication between globally distributed devices?*** Blockchain provides open P2P connectivity for intra-device communication in a natural fashion. Therefore, it becomes very simple to directly send or receive data over the network.
- ***How will industries provide compliance and governance for autonomous systems?*** The Blockchain is an immutable ledger, in other words, the stored data cannot be deleted or edited using which the governance and compliance of autonomous systems become feasible.
- ***How will industries address the security complexities of IoT landscape?*** Bitcoin has proven over ten years that Blockchain powerful protection method could present the strongest communication security in the world for all of IoT devices.

Then Blockchain technology presents sufficient advantages for IoT infrastructure that encourages companies to enhance network-based IoT to Blockchain-based one. The Blockchain technology is identified as the main solution for scalability, privacy, and reliability issues in the IoT paradigm. The integration of Blockchain features and protocols in IoT can provide substantial improvements to many IoT applications, for instance (Zheng et al., 2017; Dorri and Jurdak, 2018; Kshetri, 2017):

- ***Decentralization:*** Blockchain offers an effective mechanism to change IoT centralized architecture to a P2P distributed ledger which ensures scalability and robustness using all participants resources and eliminating many-to-one traffic flows. It will decrease latency and solve a single point of failure problem that exist in centralized models (Song et al., 2018). Blockchain prevents the individual authority by using the majority decisions to validate transactions and add them to the distributed ledger (Yang et al., 2018).
- ***Immutability:*** Blockchain distributed ledger is immutable, meaning that any data modification must be verified by the majority of the network nodes. Therefore, Blockchain efficiently protects transactions from adjusting or removing. Immutable ledger employment will enhance security and privacy of IoT systems (Boudguiga et al., 2017).
- ***Identity &Access Management:*** Blockchain-based identity and access management systems can be leveraged to strengthen IoT security. Public Blockchains let participants identify every single device and their immutable data. They can implement trusted distributed authentication and authorization of devices in IoT applications. Moreover, IoT devices use private

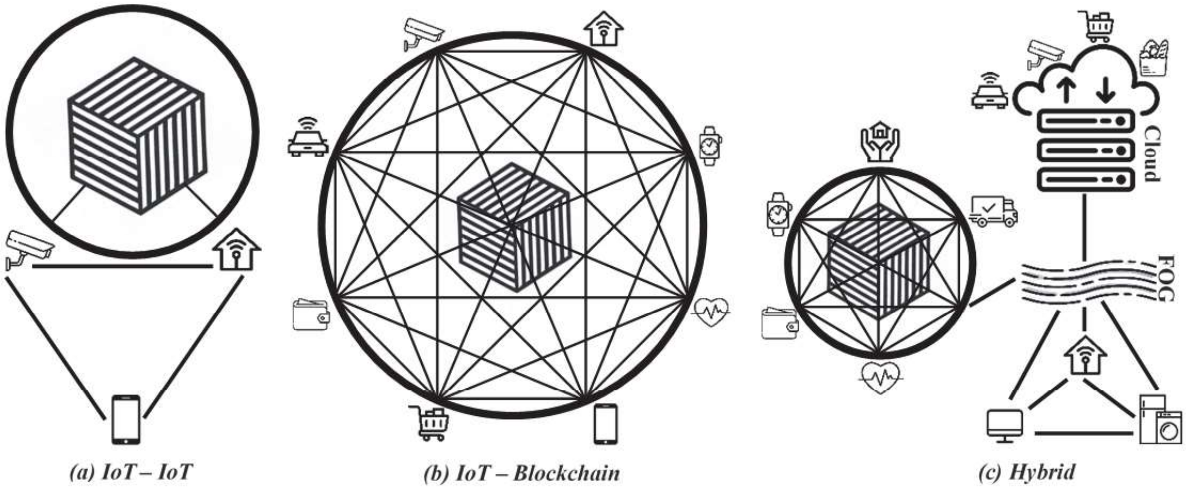
Blockchains to store cryptographic hashes of singular device firmware which creates a permanent record of device state and configuration. This record can be used to verify the genuinity of a given device and whether its software and settings have been tampered. Blockchain-based identity and access management systems can provide stronger defense against attacks involving IP spoofing or IP address forgery. The Blockchain resistances against data alteration in the previous blocks make it impossible for devices to connect to network by covering themselves via injecting fake signatures (Novo, 2018; Huh et al., 2017).

- ***Resiliency:*** Each node stores a copy of the distributed ledger on its memory that contains all transactions have ever made in the Blockchain to combat attacks more efficiently. Keeping such a massive volume of Blockchain data at each IoT node will increase system demand to share information which adds some additional processing, storage, and power consumption to reach more resiliencies in IoT devices (De Castro, 2017).
- ***Reliability:*** IoT devices can keep their information immutable and distributed over time via Blockchain technology. Blockchain facilitates sensor data traceability and accountability for tracking billions of connected devices, transactions process, and intra-device coordination. This broad functionality in one technology allows IoT manufacturers to save their resources and budgets. Blockchain full redundancy provides a hundred percent uptime and guaranteeing message delivery (Liu et al., 2017).
- ***Security:*** IoT devices security flaws typically revolve around three areas: authentication, connection, and transaction. Devices that verify, connect or spend improperly with other devices are all major concerns. IoT system with numerous and heterogeneous devices need Blockchain ability to provide a secure network over untrusted parties. By using Blockchain to manage access to data from IoT devices any attacker would have to bypass an additional layer of security that is underpinned by some of the most robust encryption standards available (Halpin and Piekarska, 2017, Wood 2018). In addition, because there is no centralized authority, single-point failure concerns can no longer be a problem. Therefore, the Blockchain will provide a secure platform for IoT devices by providing a massive amount of trust since the majority of the participants in the network has to reach an agreement to validate transactions. Blockchain can exchange IoT device messages as transactions and validate them by smart contracts. Hack-proof cryptography eliminates attack vectors such as man-in-the-middle (MitM) attacks and all of the other attacks that have been popularized in the last few years when dealing with IoT or industrial internet devices (Dorri et al., 2017).
- ***Autonomy:*** Blockchain ability to support IoT devices intra-connection without using any server interposition allow them to communicate autonomously on a worldwide scale. These devices can listen, record or trigger events. The device can transmit a message to other devices based on events that happen autonomously via smart contracts or assets (Dorri and Jurdak, 2018).
- ***Anonymity:*** In Blockchain, both customer and dealer use unknown and unique addresses which privately hold their identities to process the transaction. This feature has been criticized by the government as it increases the use of cryptocurrencies in illegal online markets. However, it could be seen as an advantage if used for other purposes, for example, electoral voting systems (Samaniego and Deters, 2016).
- ***Cost saving:*** Available IoT solutions are expensive because of the high infrastructure and maintenance cost associated with centralized architecture, large server farms, and networking equipment. The total amount of communications that will have to be handled when there are tens of billions of IoT devices will increase those costs substantially (Atlam et al., 2018).

Despite increasing agreement on the potential of Blockchain and IoT integration, the main issue about the place where Blockchain would be hosted remains as a disputable topic. Hosting the Blockchain directly on resource-constrained IoT devices are inadvisable due to lack of computational resources, limited bandwidth and their need to preserve power. The cloud and fog are two adapted hosting service platforms for a Blockchain regarding computational resources and latency. While the fog has limited resources and exhibits low latency, cloud-hosted applications can scale out and thus overcome resource constraints at the price of significant latency issues (Alenezi et al., 2017). Based on IoT devices constraint, characteristic, and challenges, the large variety of models proposed for Blockchain and IoT combination in previous researches. These can be classified into three main approaches (Reyna et al., 2018b):

- ***IoT–IoT:*** IoT devices usually communicate with each other via discovery and routing mechanisms. Only part of IoT data will be stored in Blockchain whereas the IoT interactions take place without using the Blockchain. This approach is useful in scenarios with reliable IoTinteractions with low latency (Figure 2(a)).
- ***IoT–Blockchain:*** All the interactions and their associated data go through Blockchain, to collect an immutable and traceable record of interactions. This approach is useful in trade and rent scenarios to obtain reliability and security but recording all the interactions increase bandwidth and data resource consumption (Figure 2(b)).
- ***Hybrid approach:*** In this approach only part of the interactions take place in the Blockchain and the rest are directly shared between the IoT devices. One of the challenges in this approach is choosing which interactions should go through the Blockchain and providing the way to decide this in run-time. This approach is a perfect way to leverages the benefits of both Blockchain and real-time IoT interactions (Figure 2(c)).

FIGURE 2
IOT- BLOCKCHAIN CONVERGENCE APPROACH.



Researchers (Wüst and Gervais, 2017) suggest an algorithm which determines whether Blockchain technology is beneficial or not for any system based on storage demand, writers amount, and trusted third-party requirements. In the cases that companies decided to use blockchain, select a capable integration method depends on requirement appears as another critical point. Table 1 presents IoT application requirements such as throughput, data media, latency, security, and resources consumption in different approaches which provides an overall view of their advantage and disadvantages.

TABLE 1
INTEGRATION APPROACH STATE

	IoT – IoT	*Hybrid*	*IoT-Blockchain*	*Central Database*
Throughput	Low	Medium	High	Very High
Latency	Fast	Medium	Slow	Fast
Num. of writers	High	High	High	High
Num. of untrusted writers	High	Low	Low	0
Data media	BC/IoT devices	BC/IoT devices/Fog	Blockchain	Cloud
Interaction media	IoT devices	BC/IoT devices/Fog	Blockchain	Cloud
Consensus Mechanism	PoW, PoS	PoW, PoS and BFT	BFT protocols	None
Security	Medium	High	Very High	Low
Consumption Resources	Low	Medium	High	High

The full and mining nodes functionality would be useless in IoT devices due to the restricted power and computation resources. Considering the importance of security in IoT applications, the consensus protocol can be simplified to support more IoT devices. Also, the transaction authentication process can be verified and maintained by lightweight IoT nodes without having to download the entire Blockchain. In any case, Blockchain could be used as an external service to provide secure and reliable storage (Reyna et al., 2018, Prashanth Joshi et al., 2018).

BLOCKCHAIN & IOT INTEGRATION CHALLENGES AND SOLUTIONS

In spite of IoT and Blockchain convergence benefits, this combination is not straightforward. This section studies the main challenges and their related solutions of employing the Blockchain technology which designs for devices with permanent storage and computing resource on the restricted resources IoT devices. The main integration challenges can be summarized as below (Reyna et al., 2018; Atlam et al., 2018):

Blockchain & IoT Integration Challenges

Scalability

The Blockchain size grows with an increasing number of connected devices because of its need to store all transactions to validate them. This is major integration drawback as IoT networks are expected to contain a large number of nodes which can generate massive amount of data in real-time. Additionally, some current Blockchain implementations can only process a few transactions per second. This could be a potential bottleneck for the IoT (Zheng et al., 2017). To address the Blockchain scalability issue, researchers proposed the Blockchain storage optimization to solve the Blockchain resource challenge via removing old transaction records (Bruce, 2014). Moreover, they worked on redesign Blockchain based on IoT limits. For instance, Bitcoin-NG (Gencer et al., 2016) decouple the common block into the key block for leader election and micro-block to store transactions. Miners are competing to become a leader which responsible for the micro-block generation.

Security

The increasing number of attacks on IoT networks and their severe impacts make it necessary to secure IoT devices with Blockchain. This feature maybe creates a severe problem when IoT tools do not operate properly, and corrupted data arrives and remain in the Blockchain. IoT devices should be tested before their integration with Blockchain because of undetectable nature of this problem (Roman et al., 2013). They are likely to be hacked since their constraints limit the firmware updates, preventing them from actuating over possible bugs or security breaches. Moreover, it is difficult to update devices one by one, as required in global IoT deployments. Therefore, run-time upgrading and reconfiguration mechanisms should be placed in the IoT to keep it running over time (Reyna et al., 2018).

Anonymity and Data Privacy

Privacy is a critical concern in IoT. Large amounts of privacy-sensitive data can be generated, processed, and transferred between devices. The Blockchain presents an ideal solution to address identity management in IoT with the ability to hide the identity of the person when sending personal data that protect user data privacy. The problem of data privacy in transparent and public Blockchains has already been discussed, together with some of the existing solutions. The Blockchain transactions use distinct and even dynamic addresses instead of identities. The user anonymity can be revealed by analyzing transactions address which advertised to every participant (He et al., 2018). The IoT devices secured data storage and authorized access, is a challenge since it requires the integration of security cryptographic software to the device taking into account limit resources.

Consensus and Resource Utilization

Trusted authority in centralized architectures, guarantee the consensus integrity while in the decentralized environment, nodes of the network need to reach consensus by voting, which is a resource-intensive process. IoT devices characterized by relatively low computing capabilities and low power consumption, as well as low-bandwidth wireless connectivity. For instance, Blockchains which utilize PoW as a consensus requires a lot of computing power and consumes a large amount of energy for the mining process. Computationally complex consensus mechanisms are not suitable for IoT scenarios, and the restricted resource should be allocated to reach an agreement. PoS is more likely to be used in IoT, but none of these have yet been deployed in IoT as a standard adoption (Atlam et al., 2018; Danzi et al., 2017). A decentralized architecture can reduce the overall cost of the IoT system in comparison to centralized architectures. However, Blockchain as a decentralized architecture suffers from a new type of resource wasting, which poses challenges for its integration with IoT. Resource requirements depend on the particular type of consensus protocol in the Blockchain network. Typically, solutions tend to delegate these tasks to gateways, or any other unconstrained device, capable of providing this functionality. Optionally off-chain solutions, which move information outside the Blockchain to reduce the high latency in the Blockchain, could provide the functionality (Reyna et al., 2018).

Smart Contracts

Devices can call smart contract functions with addresses or prompt them as application reaction to listening events. They provide a secure and reliable feature for the IoT which record and manage their interactions. Working with smart contracts requires the use of oracles which consist of specific entities that provide real-world data in a trusted manner. Smart contracts executed in individual node whereas simultaneously the code performed by multiple nodes. In other words, instead of using this distribution to execute all tasks, just validation process distributed. Smart contracts should take into account the heterogeneity and limitations which presented in the IoT. Filtering and group mechanisms should be complemented by smart contracts to enable applications to address the IoT problems depending on the context and requirements. Lastly, actuation mechanisms directly from smart contracts would enable faster reactions with the IoT (Reyna et al., 2018).

Predictability

Devices in IoT need real-time communication with their environment which means the time used by interactions between things should be predictable and the latency of communication between devices should be bounded. Predictability is even more critical when it comes to healthcare applications based on IoT (Bui and Zorzi, 2011). For example, the transaction finality in Blockchain under many consensus mechanisms, such as PoW and PoS, is probabilistic and the confirmation confidence of the transaction in confusion is also probabilistic. It remains a fundamental challenge to incorporate predictability concerns in the Blockchain architecture (He et al., 2018).

Legal Issues

The Blockchain connects different people from various countries without having any legal or compliance code to follow which make a serious concern for both manufacturers and service providers. As stated, the lack of regulations for private-key retrieval or reset, or transaction reversion mechanisms creates problems. Some IoT applications envision a global, unique Blockchain for devices but it is unclear if this type of network is intended to be managed by manufacturers or open to users. In any case, Blockchain will require legal regulation. These regulations will have an influence on the future of Blockchain and IoT and maybe disrupt the decentralized and free nature of Blockchain by introducing a controlling, centralized participant such as a country (McKenzie, 2017).

Blockchain and IoT Integration Solutions:

The diversity of solutions for Blockchain integration with IoT, and different type of IoT devices and their applications, IoT designers should select an appropriate solution based on their restrictions and requirements. In spite of considerable research on solutions, there has been no comprehensive analysis and resolutions for IoT manufacturers to adopt a suitable Blockchain platform for their integrations. IoT devices need Blockchain to store their state, manage multiple writers, and prevent to hire trusted third party. Figure 3 presents a simplified flowchart to determine which kind of Blockchain is suitable for IoT applications (Wüst and Gervais, 2017; Gencer et al., 2016; Kshetri, 2017; Song et al., 2018).

FIGURE 3
FACILITATED FLOWCHART OF BLOCKCHAIN TYPE SELECTION

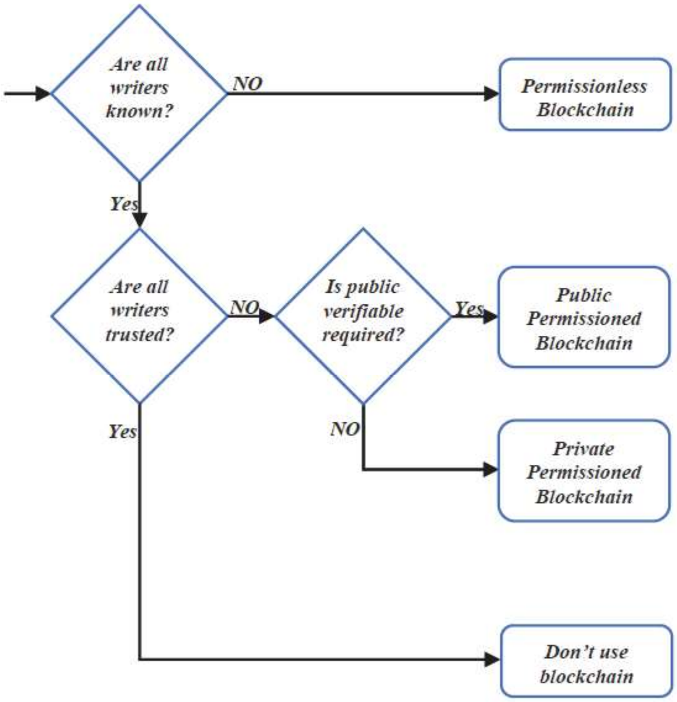

Are all writers known?
NO
Permissionless Blockchain
Yes
Are all writers trusted?
NO
Is public verifiable required?
Yes
Public Permissioned Blockchain
NO
Private Permissioned Blockchain
Yes
Don't use blockchain

Table 2 illustrates Blockchain platforms characteristic and evaluation parameters. This table summarizes important information and evaluation characteristic of well-known Blockchain platforms like Ethereum, Hyperledger fabric (Androulaki et al., 2018), Multichain (Greenspan. 2015), Lisk (Lisk team, 2016), Neo (Neo team, 2014), and EOS (Larimer, 2017).

TABLE 2
BLOCKCHAIN PLATFORMS CHARACTERISTIC AND EVALUATION PARAMETERS

NAME	***CONSENSUS MECHANISM***	***BLOCK TIME***	***TPS***	***SCALABILITY***	***SECURITY***	***ANONYMITY AND PRIVACY***	***SMART CONTRACT***	***PUBLIC/PRIVATE & PERMISSION STATE***
ETHEREUM	POW	~15 S	~15	MEDIUM	HIGH	MEDIUM	HIGH	PUBLIC PERMISSIONED/ PERMISSIONLESS
HYPERLEDGER FABRIC	PBTF	~1S	~3500	VERY HIGH	HIGH	HIGH	HIGH	PUBLIC PERMISSIONED
MULTICHAIN	PBTF	ADJUST	~500-1000	VERY HIGH	VERY HIGH	VERY HIGH	LOW	PRIVATE PERMISSIONED
LISK	DPOS	~10S	~2.5	HIGH	HIGH	HIGH	HIGH	PUBLIC PERMISSIONED/ PERMISSIONLESS
NEO	DBFT	~15S	~1000	HIGH	HIGH	HIGH	HIGH	PUBLIC PERMISSIONED/ PERMISSIONLESS
EOS	DPOS	~0.5S	~10000	HIGH	MEDIUM	VERY HIGH	HIGH	PRIVATE PERMISSIONED

In addition to consensus protocol, block time, and transactions per second (TPS) considered based on their importance for IoT devices to choose an appropriate platform. Any IoT application has perfect knowledge about its restrictions and requirements such as the time-sensitivity, volume of transactions and its resources. This awareness helps IoT devices to define the proper platform. Scalability, security, privacy, and smart contract capability are other metrics that need to be satisfied before platform implementation on IoT devices. Table 2 introduces these parameters in a qualitative manner to evaluate their performance.

Furthermore, building a powerful decentralized network requires some developer tools to work together for smart contracts, faster computation, security, and contract execution to provide a high level of reliability. These protocols are not centralized in data silos and can talk together which enables new use cases to emerge through sharing of data and functionality from multiple protocols in a single application.

CONCLUSION & POTENTIAL RESEARCH DIRECTION

With a rapid growth in the number of connected IoT device, many obstacles arise that may slow down the adoption of the IoT across different industries. First, the market for IoT devices and platforms is fragmented, with many standards and many vendors. Second, there are concerns about interoperability, as the solutions implemented often tend to create new data silos. IoT device data often stored in the clouds securely, but they are not protected against compromised integrity devices or tampering at the source. More importantly, the centralized architecture of most IoT solutions require the IoT device owners to trust to these organizations to keep their data safe, to give control over their data and compromise their data if hackers attack the central server.

In contrast, the Blockchain is an emerging technology that can help with IoT systems resiliency. It provides a distributed ledger to avoid centralized architecture challenges and stores data in a secure process via its characteristics. The Blockchain build trust between IoT devices and reducing the risk of tampering with Blockchain cryptography. Moreover, it reduces the cost by eliminating the middlemen and intermediaries overhead. It is intuitive that the Blockchain can provide a promising solution to address many IoT challenges but any convergence between two embedded technologies, create some new issues and obstacles.

IoT devices have limited power and storage resources which cannot handle the resource-intensive distributed ledgers full copy storage, consensus protocol execution and encryption in each node. Moreover, the characteristic of conventional Blockchain should be modified due to IoT requirements such as security, data privacy, the consensus protocol, and smart contracts. One of the main challenges is the heterogeneous solutions that suggest by various types of IoT applications to integrate blockchain with IoT technologies based on their demands and requirements. In other words, these solutions only focused on specific use cases and couldn't be used by a wide range of applications as a general solution. Therefore, we need to offer standards based on the basic requirements to concentrate on the better solution for them instead of application solutions.

ENDNOTES

1. The first bock is a bit special because it cannot point to previous blocks. The first block is called the genesis block.

REFERENCES

Ai, Y., Peng, M., & Zhang, K. (2018). Edge computing technologies for Internet of Things: a primer. *Digital Communications and Networks*, 4(2), 77-86.

Alenezi A., Alharthi, A., Walters, R., Atlam H.F., & Wills, G., (2017). Integration of cloud computing with internet of things: challenges and open issues. *In 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* 21-23 June 2017, Exeter, UK, pages 670–675.

Alharby, M., & Moorsel, A. (2017). Blockchain Based Smart Contracts: A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT),* 125–140.

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, 21(2), 34-42.

Androulaki, E., et. al. (2018). Hyperledger fabric. *In EuroSys '18 Proceedings of the Thirteenth EuroSys Conference*, 23-26 April 2018, Porto, Portugal.

Atlam, H., Alassafi, M., & Wills, G. (2018). Blockchain with Internet of Things: Benefits, Challenges, and Future Directions*, Int. Journal of Intelligent Systems and Applications*, 10(6), 40–48.

Bach, L., Mihaljevic, B., and Zagar, M. (2018). Comparative analysis of Blockchain consensus algorithms. *In International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),* 21-25 May 2018, Opatija, Croatia, pages 1545–1550.

Bashir, I. (2018). MASTERING BLOCKCHAIN. *In Distributed ledger technology, decentralization, and smart contracts explained*, Birmingham, UK. Packt Publishing.

Boudguiga, A., Bouzerna, N., Granboulan, L., Olivereau, A., & Quesnel, F. (2017). Towards Better Availability and Accountability for IoT Updates by means of a Blockchain, *In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* 26-28 April 2017, Paris, France, pages 50–58.

Bruce, J. (2014). The Mini-Blockchain Scheme. Retrieved from http://cryptonite.info/files/mbc-scheme-rev2.pdf

Bui, N., & Zorzi, M. (2011). Health care applications: a solution based on the internet of things. *In Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies,* 26-29 October 2011, Barcelona, Spain. ACM.

Buterin, V. (2015). On Public and Private Blockchains. Retrieved from https://blog.ethereum.org/2015/08/07/on-public-andprivate-Blockchains/

Buyya, R., & Dastjerdi, A. V. (2016). Internet of things. *In Principles and Paradigms*, Amsterdam. Elsevier/Morgan Kaufmann.

Castro, M., & Liskov, B. (2002). Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems.* Association for Computing Machinery, 20(4), 398–461.

Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, 4:2292–2303.

Conoscenti, M., Vetro, A., & Martin, J. D. (2016). Blockchain for the Internet of Things: A systematic literature review. *In IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA),* 29 Nov-2 Dec 2016, Agadir, Morocco.

Danzi, P., Stefanovi, C., & Popovski, P. (2017). Analysis of the communication traffic for Blockchain synchronization of IoT devices. *arXiv preprint, arXiv:1711.00540.*

De Castro, A. (2017). Chain of things. Retrieved from https: //www.Blockchainofthings.com/

Decuyper, X. (2018). How does Blockchain work? Retrieved from https://savjee.be/videos/simply-explained/how-does-a-Blockchain-work/

Delmolino, K., Arnett, M., Kosba, A. E., & Shi, E. (2016). Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. *In International Conference on Financial Cryptography and Data Security*, Christ Church, pages 79–94, Barbados. Springer.

Dorri, A., & Jurdak, R. (2018). Blockchain in internet of things: challenges and solutions. *arXiv preprint. arXiv:1608.05187.*

Dorri, A., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),* 13-17 March 2017, Kona, HI, USA.

Eyal, I., & Sirer, E. (2018). Majority is not enough: bitcoin mining is vulnerable. *Communications of the ACM,* 61(7), 95–102.

Fernandez-Carames, T., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. *IEEE Access*, 6:32979–33001.

Ferrag, M. A., Makhlouf, D., Mithun, M., Abdelouahid, D., Leandros, A. M., & Helge, J. (2018). Blockchain Technologies for the Internet of Things. Research Issues and Challenges. *CoRR,* 1806(9099).

Gencer, A. E., Sirer, E. G., Renesse, R. V., & Eyal, I. (2016). Bitcoin-NG: a scalable Blockchain protocol. *In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI16)*, 13-17 March 2016, Santa Clara, CA, USA, 45–59.

Greenspan, G. (2015). Multichain Private Blockchain White Paper. Retrived from https://www.multichain.com/download/MultiChainWhite-Paper

NEO group (2014). Neo white paper. Retrived from http://docs.neo. org/en-us/whitepaper.html

Gupta, D., Saia, J., & Young, M. (2018). Proof of Work without All the Work. *In Proceedings of the 19th International Conference on Distributed Computing and Networking (ICDCN '18),* 04-07 Jan. 2018, Varanasi, India, 04–07.

Halpin, H., & Piekarska, M. (2017). Introduction to Security and Privacy on the Blockchain, *In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* 26-28 April 2017, Paris, France, 1–3.

Haroon, A., Ali, M., Asim, Y., Naeem, W., Kamran, M., & Javaid, Q. (2016). Constraints in the IoT: The World in 2020 and Beyond. *International Journal of Advanced Computer Science and Applications*, 7(11), 252–271.

He, Q., Guan, N., Lv, M., & Yi, W. (2018). On the Consensus Mechanisms of Blockchain/DLT for Internet of Things. *In 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES),* 6-8 Jun. 2018. Graz, Austria. IEEE.

Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using Blockchain platform. *In 2017 19th International Conference on Advanced Communication Technology (ICACT)*, 464–467.

Hung, M. (2017). Leading the IoT Gartner insights on how to lead in a connected world.

Joshi, A. P., Han, M., & Wang, Y. (2018). A survey on security and privacy issues of Blockchain technology. *Mathematical Foundations of Computing*, 1(2), 121–147.

Karame, G., Androulaki, E., and Capkun, S. (2012). Double-spending fast payments in bitcoin. *In Proceedings of the 2012 ACM conference on Computer and communications security CCS '12,* October 16-18, 2012, Raleigh, North Carolina, USA, 906–917.

Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? *IT Professional,* 19(4), 68–72.

Larimer, D. (2016). Delegated Proof-of-Stake Consensus (BitShares). Retrieved from https://bitshares.org/technology/delegated-proof-of-stake-consensus/

Larimer, D. (2017). EOS.IO technical documentation. Retrieved from https://github.com/EOSIO/Documentation/blob/master/ TechnicalWhitePaper.md

Laurence, T. (2018). BLOCKCHAIN FOR DUMMIES. USA. *John Wiley & Sons.*

Lazarovich, A. (2015). Invisible Ink: Blockchain for Data Privacy.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal,* 4(5), 1125– 1142.

Liu, B., Yu, X., Chen, S., Xu, X., and Zhu, L. (2017). Blockchain Based Data Integrity Service Framework for IoT Data. *In 2017 IEEE International Conference on Web Services (ICWS),* pages 468–475.

Mckenzie, I. (2017). An introduction to Blockchain: the key legal issues. Retrieved from http://www.osborneclarke.com/insights/anintroduction-to-Blockchain-the-key-legal-issues/

Mougayar, W. and Buterin, V. (2016). The Business Blockchain. In Promise, Practice, and Application of the Next Internet Technology., USA. Wiley.

Musaddiq, A., Zikria, Y.B., Hahm, O., Yu, H., Bashir, A.K., and Kim, S.W. (2018). A Survey on Resource Management in IoT Operating Systems. *IEEE Access*, 6, 8459–8482.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Norman, A. T. (2017). Blockchain Technology Explained. In The Ultimate Beginner's Guide about Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA, and Smart Contracts.

Novo, O. (2018). Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195.

Rayes, A. and Salam, S. (2017). Internet of things from hype to reality. Cham. *Springer International Publishing AG*.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems,* 88, 173–190.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things, *Computer Network,* 57(10), 2266–2279.

Samaniego, M., & Deters, R. (2016). Blockchain as a Service for IoT. *In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).*

Song, J., Prevost, J., & Rad, P. (2018). Blockchain Design for Trusted Decentralized IoT Networks. *In 2018 13th Annual Conference on System of Systems Engineering (SoSE)*, pages 169–174.

Szabo, N. (1997). Formalizing and securing relationships on public networks. Retrieved from http://ojphi.org/ojs/index.php/fm/article/view/ 548/469

Lisk Team (2016). Lisk documentation. Retrieved from *https://docs.lisk.io/docs/the-liskprotocol.*

Vashchuk, O., & Shuwar, R. (2018). Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. *Electronics and Information Technologies*, 9, 106–112.

Walker, M., Jones, N., & Wallin, L. (2016). How to Address the Top Five IoT Challenges with Enterprise Architecture.

Wood, G. (2014). Ethereum: A secure decentralisedgeneralised transaction ledger. *Ethereum Project Yellow Paper*, 151, 1–32.

Wood, J. (2018). Blockchain of Things,cool things happen when IoT & Distributed Ledger Tech collide, Retrieved from https://medium.com/trivial-co/Blockchain-of-things-cool-things-happen-when-iot-distributed-ledger-tech-collide-3784dc62cc7b

Wüst, K., & Gervais, A. (2017). Do you need a Blockchain? *IACR Cryptology*, pages 1–7.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5), 1250–1258.

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. (2018). Blockchain-based Decentralized Trust Management in Vehicular Networks*. IEEE Internet of Things Journal*, 1–10.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *In 2017 IEEE International Congress on Big Data (Big Data Congress)*, 25-30 June 2017, Honolulu, HI, USA, pages 557–564.