


Towards building a blockchain framework for IoT

Deepa Pavithran¹  · Khaled Shaalan² · Jamal N. Al-Karaki^{1,3} · Amjad Gawanmeh⁴

Received: 4 September 2019 / Revised: 7 December 2019 / Accepted: 27 January 2020 / Published online: 5 February 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Blockchain is a very promising technology that spans many use cases other than cryptocurrencies. For example, its implementation in the Internet of Things (IoT) based networks is still unclear and demands further research. This is mainly due to the limited constraints of IoT devices and the ledger-based design of blockchain protocol. IoT may offer many benefits if blockchain features can be balanced to fit it. As such, many current problems in IoT can be resolved. However, implementing blockchain for IoT may still impose a variety of challenges. In this paper, we provide a recent literature review analysis on blockchain in IoT. In particular, we identify five key components along with their design considerations and challenges that should be considered while creating blockchain architecture for IoT. We also define gaps that hinder creating a secure blockchain framework for IoT. We simulated two different types of blockchain implementation and identified that device to device architecture has comparatively better throughput than gateway based implementations.

Keywords Blockchain · Blockchain technology · Internet of Things · Sensors

1 Introduction

Information and communication technology is growing at a rapid pace. Advancement in semiconductor devices and communication technologies allows a multitude of devices to communicate through the internet. These devices enable machine to machine and machine to human communication. Such a trend can be referred to by many terms,

including Internet-of-Things (IoT), Internet-of-Everything (IoE), Internet-of Vehicles (IoV), Internet-of-Medical-Things (IoMT), Internet-of-Battlefield-Things (IoBT), and so on [4]. These devices usually have sensors that can detect data from the physical environment. The detected data is then stored into centralized cloud storage for analysis and processing by various applications. The data residing in the centralized cloud is vulnerable to various forms of attack.

Blockchain is essentially a decentralized platform where a copy of each transaction is kept by all parties [44]. The transactions are transparent and any modifications in them can be easily detected. Consider the example of a smart city where parking spaces are shown to users in real-time. Once sensors detect a free parking space, they update the centralized database. It is possible for a system administrator who manages this database to reserve a parking space for himself without showing this slot to others. In this case, the integrity of the data from the sensor is compromised. The purpose of a blockchain network of interconnected devices is to eliminate the use of a third party and, hence, ensure that the real-time data provided by the sensor can reach every node in the network without any modification. In addition, blockchain allows IoT devices to communicate among themselves and make decisions automatically.

✉ Deepa Pavithran
deepa.pavithran@adpoly.ac.ae
Khaled Shaalan
khaled.shaalan@buid.ac.ae
Jamal N. Al-Karaki
jamal.alkaraki@adpoly.ac.ae
Amjad Gawanmeh
amjad.gawanmeh@ud.ac.ae

¹ Abu Dhabi Polytechnic, P.O. Box 111499, Abu Dhabi, United Arab Emirates
² The British University in Dubai, PO BOX 345015, Dubai, United Arab Emirates
³ Computer Eng. Department, The Hashemite University, Zarqa, Jordan
⁴ College of Engineering and IT, University of Dubai, Dubai, United Arab Emirates

Decentralizing the IoT network has various advantages, including reduced costs associated with maintaining a central database for IoT transactions, as well as improved security and privacy, which eliminates the need for a third party. However, it remains unclear as to how these features can be implemented in IoT. This is mainly due to the limitations of IoT devices in terms of computational capacity, power and storage. For this reason, the blockchain protocol designed for cryptocurrencies cannot be used for IoT applications. Various IoT applications that can benefit from blockchain are shown in Fig. 1. This includes supply chain management, health care, smart city, home equipment automation, energy management and asset tracking.

In traditional supply-chain management, there is no traceability and accountability. The price of goods can be artificially crafted. Blockchain can help the supply-chain industry to keep tamperproof ledgers and can keep track of products without an intermediary [1, 7]. This ensures greater transparency and reduces corruption in the supply chain industry. In healthcare, the combination of IoT and blockchain help to easily collect patient data, monitor in real-time, and store data securely [54]. Home equipment and IoT in smart cities can be automated using blockchain, enabling device to device communication between equipment. Energy sectors are moving to implement blockchain because of its ability to lower cost and reduce harmful environmental impacts [16]. Blockchain can help asset tracking by providing transparent, secure and accountable data collected from IoT devices attached to assets.

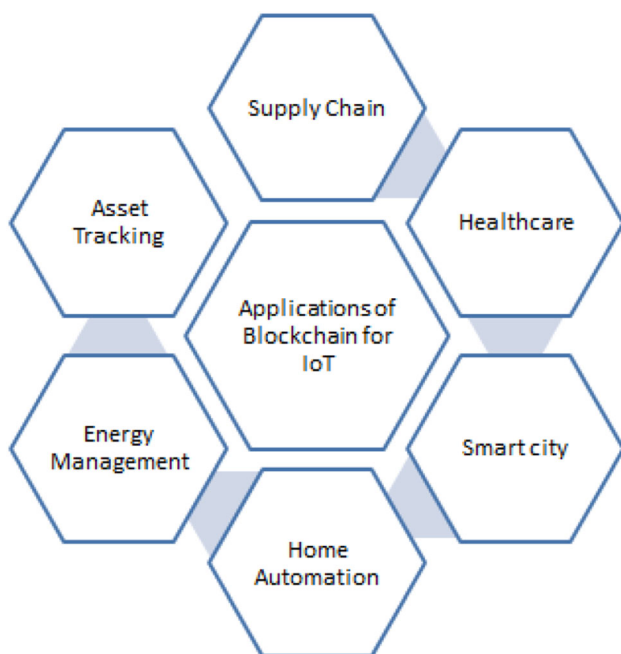


Fig. 1 Applications of blockchain for IoT

Therefore energy efficiency is one of the relevant issues that should be addressed when blockchain and IoT are integrated.

Current approaches in IoT implementations are largely centralized, which raises several security concerns like single point of failure, trust and privacy. In addition, it limits their scalability and subsequently alarmed the need for a decentralized trust mechanism in IoT. Blockchain can provide trust through cryptographic techniques without the need for a central authority. Recently several blockchain based applications for IoT have gained attention due to its potential for improving security and privacy. A recent study by Juniper research [32] predicts that a combination of IoT and blockchain on food industry can save billion dollars by reducing the retailers' cost, simplifying regulatory compliance and tackling fraud. Giants in the food industry like Carrefour, Nestle and Cermag have already started using Hyperledger Fabric, a blockchain application developed by IBM [9, 11, 45].

The contributions of this paper are multifold as follows:

- A recent literature review analysis for state of the art on blockchain technology applications in IoT was conducted.
- The most important components that should be considered while creating a blockchain of IoT devices were identified and explained. This includes identifying the type of IoT devices, the usecases and applications that will be implemented, the design of storage and how data should be utilized, the security considerations and the required parameters for blockchain.
- The integration requirements of blockchain and IoT were identified and utilized.
- Recommendations on how to enable IoT devices for better integration with blockchain technology are introduced.
- An evaluation of the generic blockchain framework for applications in IoT is provided.

The rest of this paper is organized as follows: In Sect. 2, we review the current context of IoT and how blockchain can be related to IoT. In Sect. 3, we provide the related work. In Sect. 4, we briefly describe the key components to be considered while creating architecture for IoT. In Sect. 5, we compare existing architectures, Sect. 6 provides implementation and performance evaluation and conclusion is provided in Sect. 7.

2 Background on Blockchain and Internet of Things

2.1 Background on Internet of Things

In the recent years, we have seen a steady advancement in the wireless sensor networks, communication and information technology. The devices are reducing in size, consumes less energy and reduced hardware cost. This enabled them to be integrated into everyday objects [41]. As cited in [61] the term ‘Internet of Things’ came into attention in September 2003 when Auto-ID Centre launched its vision of a supply chain management that can be automatically tracked. This trend has created a vast number of tiny devices that are connected to the internet to serve specific functionalities. Such types of devices are collectively called the Internet of Things. It is considered as a global network infrastructure where numerous devices are connected to each other through the internet [17]. They are rapidly growing and have a high impact on everyday life. These devices can be referred to as smart objects that have the ability to interact and communicate with each other, within themselves, with an end-user, or with an interconnected object [2]. These objects have minimal communication and computational facilities. They consist of sensors, actuators, mobile devices, and RFID tags. When the number of devices connected to the internet increased, the problem of addressing these devices with a unique address was a challenge. Identifying these devices with a unique address was made possible by the IPV6 remarkable decision to increase the address space. This helped in creating a fully functional IoT. The huge address space provided by the IPV6 can provide unique addresses to billions of devices [23].

2.2 Key applications of Internet of Things

According to a survey by GSMA [25], the top trending IoT applications of users’ choice are smart appliances, smart energy meters, wearable devices, connected cars and smart health devices. These devices are mainly used in environmental monitoring, surveillance, smart cities, smart homes and industrial equipment [42]. Some of these applications are briefly described below.

- *Smart Homes* A smart home consists of various devices at home connected to a network that can be controlled by the owner. This provides improved security and manages home appliances and energy efficiently. A few examples of such energy-saving products for the smart home could be smart bulbs, air conditioners, refrigerators, washing machines and air pollution sensors [26].

- *Wearables* Wearable IoT devices are mainly used for health monitoring, fitness and entertainment. These devices are small in size and include features that serve purposes such as activity tracking, monitoring sleeping pattern and heart rate tracking.
- *Smart Cities* A smart city is equipped with devices that can send and receive data or signals through the internet. For example, each street light can gather and send information. Parking slots can be shown to the user in real-time and can find charging stations for electric vehicles. The waste bin will be triggered when it is full. Watering system monitoring will be automatic. Sensors will detect leaks and are triggered when necessary. It can plan its preventive maintenance activities and can monitor security activities [27].
- *Industrial equipment* IoT devices play a major role in many industries today. This includes automatic managing of workers through surveillance and an alarming system to temperature sensors in the office buildings. Some of the industries that have adopted IoT include agriculture, food processing, environmental monitoring and health care [17].

2.3 Architecture of Internet of Things

The architecture of IoT varies within devices due to the heterogeneity of the devices. These devices are manufactured by various companies with different specifications. The basic architecture of IoT is shown in Fig. 2. This architecture consists of sensing/perception layer, networking layer, middleware layer, application layer and business layer [33]. The perception layer consists of the physical object or the sensor devices. These objects sense data from the physical layer and communicate to the middleware layer through the network layer. These objects can be 2D-Barcode, RFID, or infrared sensors. The information coming from barcode scan events, RFID-based locations,

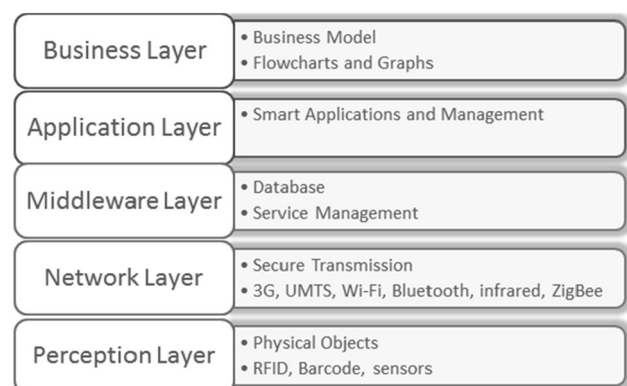


Fig. 2 Architecture of IoT

or data received from the sensors are passed through the network layer. The network layer uses ZigBee, Bluetooth, 3G, and WIFI as the transmission medium to pass these data to the middleware layer.

The middleware layer use database to store the data collected by the sensor. These data will be passed to a centralized database for further processing. The application layer collects the data from the middleware layer and integrates it with smart apps. The business layer is responsible for the overall management of the IoT system and services. It builds business models, flowcharts and graphs based on the data received from the application layer.

2.4 Challenges in Internet of Things

The recent growth in IoT devices has imposed many challenges in the world of electronics and communications. Some of the key challenges in IoT are security and privacy, interoperability of IoT and identity management. Due to the limited computational power of IoT, it is inefficient to use some of the conventional public-key cryptosystems. Hence, IoT requires lightweight cryptography [3]. The data from the sensor devices are transmitted through the network layer, which is vulnerable to many types of attacks.

Manufacturers create devices using their own technologies and standards. Hence, standardizing these devices to work and collaborate with other devices is a key challenge.

As far as naming and identity management are concerned, every IoT device requires a unique identity. As organizations rush to launch new IoT initiatives, they are less concerned about what level of access do these devices have on sensitive and non-sensitive data. Hence dynamically assigning identities for the IoT device is a challenge [33].

2.5 Background on blockchain

Blockchain is essentially a distributed database where assets can be stored and exchanged through a decentralized network of computers while still providing security and anonymity. Even though the asset is distributed, only the owner who has the private key can make transactions on this asset. The other computers in the network act as validators for the transaction. It securely records transactions into a public ledger among nodes without the need for a trusted third party. In the centralized cloud approach when an asset is owned, it is either stored in the custody of the owner or with a trusted intermediary or a centralized authority like a bank.

Some of the popular applications that use blockchain are smart contracts, distributed cloud and digital assets [49].

Some of the industries that can benefit from blockchain are finance, cross-border transactions, Insurance, Government, Supply chain management, Healthcare and Internet of Things.

Bitcoin [44] launched in 2008 was the first decentralized digital currency that is built on the blockchain technology. The value of the currency is created and stored in transactions. What differentiates Bitcoin from traditional currencies and payment card systems is that Bitcoin is a data structure that is replicated in many different nodes that are part of the network. There is no central authority or central server that stores the user's asset value making it difficult for cyber attackers to target a single machine. Bitcoin allows only values to be exchanged. Transactions are hashed and added to the block. Identity of the customer is verified through a public–private key pair where a customer can have more than one public–private key pairs. Each user maintains public–private key pair where the public key is shared with other agents whereas the private key is maintained as private in the wallet. To make a transaction, the sender uses the public key of the receiver and digitally signs the transaction using senders private key to provide authentication.

2.6 How blockchain works?

Blockchain records the transactions in units of block. Each block contains the hash of the previous block, hash of the current block, timestamp, other information and transactions for that block. When a sender node creates a transaction, it distributes it to all other nodes in the network. The receiving nodes validate this transaction and perform proof of work. The node that succeeds the proof of work will broadcast it to all other nodes and add the block to the chain [44]. The transaction includes the public key of the receiver and is signed by the sender. Hence every other node can validate the authenticity of the transaction. Each block contains a hash of the previous block which means every block is linked to each other as shown in Fig. 3 [44]

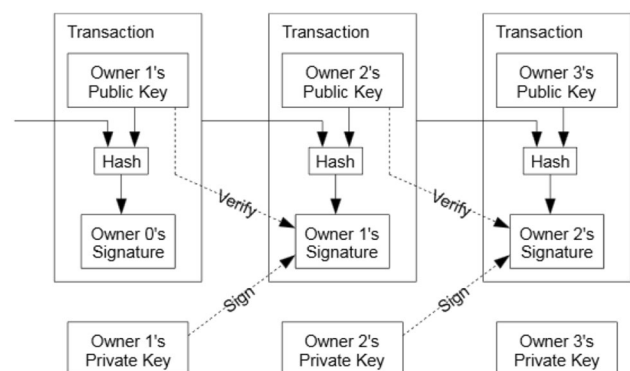


Fig. 3 Bitcoin transactions

making it difficult for an attacker to modify the transactions or blocks.

2.7 How blockchain can address IoT challenges?

IoT devices in the cloud architecture are connected through a cloud server. It processes and store the data sent and received by the devices. However, devices connected to the cloud are vulnerable to various attacks. Each block of IoT architecture could act as a bottleneck or single point of failure [57]. The cloud model is susceptible to manipulation. For Example: In the city of Flint, Michigan, smart water meters were used to measure the quality of water. The authorities were insisting on the fact that water in the city is safe to drink whereas CNN article asserted that officials might have altered sample data to lower the lead level in water [37]. It reported that two of the collected samples were discarded by the officials. Such types of malpractice can be avoided by implementing blockchain for IoT. This is because the data generated by the sensors could not be modified.

In blockchain, devices rely on smart contract to exchange messages. Authentication is done by digitally signing the message with the private key of the owner which ensures that the message originated from the owner itself. This eliminates the possibility of man-in-the-middle, replay and other types of attacks [57]. Some of the advantages of using blockchain for IoT are:

- *Reduced cost* According to Gartner [24] 8.4 billion IoT devices was used in 2017 which is 31% increase when compared with 2016. This radically increased the storage and network capacity required by these devices. Using blockchain, devices can communicate with each other and can execute actions automatically. Hence cloud storage and administrative staff for maintaining cloud storage will not be required [56].
- *Single Point of failure* Each entity in the IoT architecture is independent in its functions. Hence malfunctioning of any device can create a single point of failure. In a blockchain, all the devices are connected to each other and all transactions are copied to every node in the blockchain; hence, malfunctioning of a single device does not affect the operations of other devices.
- *Resistant to Malicious Attack* IoT devices are vulnerable to many types of attacks due to its centralized architecture. Some examples of attacks are distributed denial of service, deception attack, and data theft. These can be avoided with the blockchain architecture for IoT whereas blockchain is vulnerable to some other types of attacks as described in Section 2.8.
- *Trust* A trusted third party is used in centralized architecture of IoT, whereas in blockchain, trust is provided automatically using cryptographic protocols.
- *Security and Privacy* Due to centralized architecture of IoT, information is likely to be manipulated whereas in blockchain, devices are interlinked and hashed. Hence, manipulation of data on one device cannot be propagated to other devices in the blockchain.

2.8 Attacks on blockchain

Although several attacks are documented for blockchain most of them are not relevant in practice [8]. Some of the attacks available in the literature are:

- *Malwares* The distributed nature of blockchain architecture introduces the spreading of malwares. With the development of newer protocols and the ability to store and compute data, it would be possible to store malicious data within the blockchain [12]. Malware effects on the devices in blockchain will result in its propagation to other nodes in the blockchain. This can result in crashing of the nodes.
- *Distributed Denial of Service Attacks (DDOS)* The study conducted by Vasek et al. [62] found that 7.4% bitcoin-related services have experienced DDOS. In these, eWallets, financial services, mining pools are more likely to be attacked. Just like, in the case of a traditional wallet, the bitcoin wallet also needs to be protected. It is recommended to use two-factor authentication to protect the bitcoin wallet. For additional layer of security, the wallet should be encrypted and backup to be taken.
- *Phishing attacks on bitcoin wallets* Several phishing attacks on bitcoin wallets and blockchain.info site were reported in 2018 [13]. Hackers created a site similar to blockchain.info and tried to steal the wallet information. In another case, hackers impersonated legitimate recipients and persuaded the investors to send bitcoins to their address. Once the bitcoin was sent, it could not be recovered.
- *Majority Attacks* This type of attack is also known as the 51% attack. Group of miners can decide which transactions should be approved or not if they can control the majority of the network mining power. This would allow them to reject other transactions or double-spend their own transactions. If the blockchain network is free and open, this could be made possible especially with the rise of mining pools. However, the attack doesn't give full control over the bitcoin network. Similarly, in a private or permissioned blockchain,

proof-of-work will be implemented under the regulator's direction; therefore regulator will have authority to control the network [12].

- *Sybil Attack* Sybil attack [21] is controlling a peer to peer network using multiple identities. A single entity creates multiple fake identities to control the network. If an attacker is possible to control the majority of mining nodes in the blockchain, then he can create a fake transaction and add it to the blockchain.
- *Eclipse attack* [28] It is a targeted attack on the distributed system, where a malicious attacker isolates a specific node and cut off all its inbound/outbound connections with its peers. So attackers try to gain 51% of the mining power by trying to isolate some of the mining nodes.

3 Related work

The majority of the work on IoT blockchain is that proposes architecture, consensus and security. We compared some of the existing architecture under Sect. 5. Performance and scalability are the main problems in IoT blockchain [38]. This is due to the large volume of data generated by the devices. Several papers identified potential challenges and technologies in IoT blockchain [18, 66]. Authors in [18] identified key challenges and potential applications for IoT blockchain. They provided a detailed description of various challenges, types of blockchain and consensus used in blockchain. A detailed description of variety of Byzantines Fault Tolerance (BFT) techniques with its negative and positive aspects is summarized in the paper. A variety of literature use variant of Byzantines fault Tolerance consensus for IoT blockchain [55]. Proof of Work based consensus is not widely used in IoT blockchain due to the resource-constrained nature of IoT devices. Various use-cases of blockchain beyond cryptocurrencies are provided in [14]. They also provide a detailed list of the type of data that are stored in blockchain and the implementation differences in IoT blockchain and cryptocurrencies. A detailed description of various blockchain based consensus methods, platforms and implementations for IoT are surveyed in [51]. In [47] authors provide a decision framework to choose when to use blockchain and what platform to choose while creating blockchain for IoT.

4 Key components in creating blockchain for IoT

In this section, we provide the key components that should be considered while creating blockchain for IoT.

4.1 Identify the type of IoT device

The first step is to identify the type of IoT devices. This is provided in Fig. 4. Some devices have only the sensor functionalities, with computations only to share the sensor data to a database. Whereas other devices will have sensor functionalities along with computation capabilities to encrypt or process data. In the first case, a blockchain of edge nodes or gateways based architecture would be ideal, whereas, in the latter case, a device-only architecture could also be used. A full node can carry the full copy of the blockchain and can perform the computation required in blockchain, whereas a light node does not hold the blockchain data instead, refer to a full node.

As IoT devices are different in their design and architecture, interoperability within these devices under a common blockchain will be a challenging issue. Bringing different types of devices under the same blockchain can be a trivial task. This issue can be addressed by standardizing the IoT manufacturing and blockchain implementation. Devices owned by different entities or owners will need standardized policies on the data that could be accessed and stored. The blockchain should be linked with the regulatory authorities to adopt consistent regulations. To provide efficiency, certain security and privacy controls should be in place like such as the risk management process. In addition, there should be rules to govern the interactions between participants.

4.2 Identify the type of application

While building applications based on blockchain, we need to systematically consider the features and configurations that are required and assess the impact and quality of these

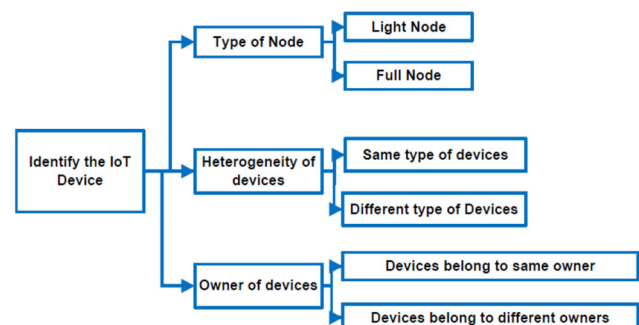


Fig. 4 Identify the IoT device type

with IoT. Requirements to identify the application types are provided in Fig. 5

Based on the type of implementation, blockchain can be classified into permissioned, permissionless or Hybrid blockchain [63]. In the case of permissionless blockchain, anyone can join the network and can participate in consensus procedure. It has open read/write access to the database. Bitcoin is an example of a permissionless blockchain. Whereas in the case of permissioned blockchain, only selected participants can be part of consensus procedure. IBM's Hyperledger blockchain is an example of a permissioned blockchain. Hybrid blockchain is a combination of permissioned and permissionless blockchain. A hybrid blockchain will have a public facing network for the customers and an internal private blockchain network. In a permissionless network, all the full nodes will be running all the applications. In the case of IoT this will affect the performance of the IoT device due to the resource-constrained nature of these devices. In permissioned blockchain, every node will only need to perform the computations required for a given application. A comparison of permissioned and permissionless blockchain is provided in Table 1.

Depending on the type of application, IoT devices can be classified into consumer, enterprise or industrial IoT. Consumer IoT is solutions made for individual non-commercial usage. IoT devices in a smart home are a consumer-based IoT. Solutions created for large commercial buildings or in an enterprise are classified under enterprise IoT. Examples are IoT used in supplychain industry, IoT in street light, etc. Industrial IoT is devices used in the factory or farm. An example is devices to monitor fuel levels, and trigger when fuel is empty. A selection of the blockchain use-cases for IoT available in the literature is provided in Table 2.

4.3 Identify data and storage requirements

Identifying what data should be stored in the blockchain is a significant component while designing blockchain. Figure 6 provides an overview of this requirement. These can

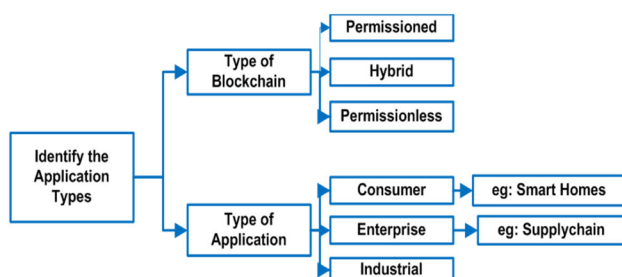


Fig. 5 Identify the type of applications

be IoT sensor data, device identity, public key, or reference to data stored in cloud.

Each node in the blockchain maintains a distributed ledger, which is a database that requires storage space. To add a new device into the block, the device should download all the transactions from the first block. Hence in such architectures, IoT devices should have enough storage capacity to maintain a copy of the transactions. IoT sensors generate a vast amount of data. Replicating this data to many different nodes require high storage capacity for the nodes and high-speed data transfer facilities. One of the major challenges would be on how to avoid the large amount of unwanted data generated by sensors without being replicated to other nodes. AI techniques should be used to parse the raw data and remove unwanted data. Blockchain, on the other hand, usually processes a limited number of transactions per second; therefore, this may create a gap between the data being generated and the capability of processing the data.

Every transaction in the blockchain is signed using the private key, which should be kept securely. One of the main challenges in designing blockchain for IoT would be finding a solution on how to store the private keys securely within IoT. Most of the IoT devices reside in public places and hence it could be compromised easily. In bitcoin private keys are stored securely in the owner's bitcoin wallet. If the owner loses his bitcoin wallet, he/she will lose all the bitcoins associated with that wallet. Majority of the attack on bitcoin is due to stolen wallet. Hence private keys within the IoT devices should be stored securely. Hardware embedded secure keys should be used in such a case.

4.4 Identify security requirements

Blockchain is capable of solving the security challenges in IoT. The traditional bitcoin protocol provides integrity, authentication and pseudo-anonymity. However, in the case of IoT, the confidentiality of the data generated by sensors should be protected depending on the sensitivity of data. Highly sensitive data generated by IoT devices need to be protected from unauthorized people. The distributed nature of blockchain stores all transactions in all the participating nodes. Controlling access to the data within devices should also be considered.

Figure 7 identifies the security requirement while creating IoT blockchain. Even though blockchain technology reduces the potential risks in traditional centralized architecture, still security breaches are unavoidable. If a user's private key is compromised, the attacker can perform transactions on the user's behalf. Security is provided in blockchain through asymmetric cryptography which requires substantial computational efforts to break the cipher. This is because classical computers encode

Table 1 Permissioned and permissionless blockchain

Permissionless	Permissioned
No restriction on who can perform transactions	Restriction on who can perform transactions
No restrictions on adding as a node	Restrictions on adding as a node
No restriction to participate in consensus mechanism	Restriction to participate in consensus mechanism
Low performance when compared with permissioned	High scalability and faster
Less cost effective	Cost effective
More chance of spreading malwares	Security depends on the access control system implemented
Fully decentralized	Not fully decentralized

Table 2 Usecases of Blockchain for IoT

Usecases example	References
Home automation	[19, 20]
Blockchain based sharing services towards smart cities	[56]
Blockchain ready: manufacturing supply chain using distributed ledger	[1]
Pharma supply chain	[6]
Supply chain traceability system for food safety	[58, 59]
Access control framework	[46]
Logistics and supply chain	[1, 35]
Energy management	[30]
Data storage management	[68]
Trade of items and data	[65, 67]
E-business model for smart property management	[67]
Power generation and distribution	[39]
Modum framework for supply chain	[43]

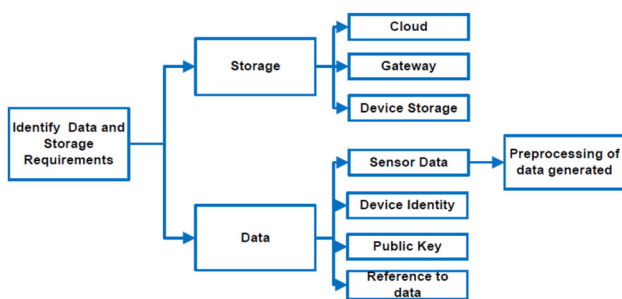


Fig. 6 Identify data and storage requirements

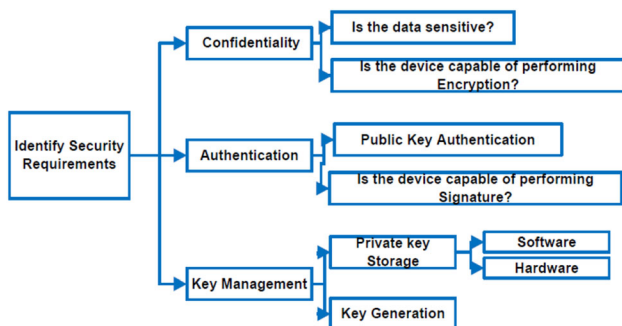


Fig. 7 Identify security requirement

information as bits. Quantum computing takes a new approach in processing information which will be much faster than the classical approach. If the information can be processed much faster, then the computation efforts to break the asymmetric cryptography will be easy. Hence quantum resistant cryptography for blockchain [34] will be required in future.

Another issue related to security is the reliability of the IoT data. Since blockchain can only ensure the reliability of data stored within the chain, however, if this data is already malicious from IoT source, then it will remain as is within the blockchain. Finally, several IoT devices rely on existing complex and centralized security protocols that are based on PKI, such as TLS and DTLS, therefore, integrating these devices with decentralized blockchain enabled systems may raise several concerns about interoperability.

4.5 Identify blockchain parameters

It is trivial to identify the participating IoT and trusted nodes that verify the transaction.

A central authority or a group of stakeholders can decide on the nodes that will be added to the network. Such type of design will be like a hybrid blockchain that uses the basic features of blockchain and mining will be done by one or more trusted parties. A variety of blockchain parameters are provided in Fig. 8. Identifying the optimal consensus and optimal platform for implementation is an important task.

4.5.1 Consensus

Consensus in the literal terms means agreement. Seibold and Samman [53] define a consensus mechanism as a method of authenticating or validating a value or transaction on a Blockchain or a distributed ledger without the need to trust or rely on a central authority. In a distributed or decentralized network, for nodes to reach a common agreement, consensus algorithms are used. Bitcoin uses proof of work based consensus, which consumes high energy. Such kind of consensus cannot be used for IoT. Blockchain platforms use a range of consensus model which are built on Byzantines Fault tolerance.

In a decentralized environment where there is no central authority to keep the ledger, this process is done through consensus mechanisms that allow secure updating of a distributed shared state. Cryptocurrencies powered by blockchain uses a decentralized environment, where each ledger is distributed among all nodes in the network. The process of validating the transactions and adding them to the ledger is done by nodes in the network. But how do we trust these nodes? What if some validating nodes are malicious? They may be trying to perform double spending or trying to discard some transactions. Such types of problems can be considered as Byzantine Generals Problem. A byzantine node can mislead other nodes involved in the consensus mechanism. Hence the consensus mechanism should be able to operate correctly and reach consensus even in the presence of byzantine nodes. A solution

to Byzantine Generals Problem is PBFT (Practical Byzantine Fault tolerance) [10]. Permissioned blockchain platforms mainly use PBFT. In PBFT, Each party maintains an internal state. When a transaction is received, each party uses its internal state and run computations to validate a transaction. This computation will lead to the party's decision about the transaction. This will be shared with all other nodes in the blockchain. The final decision is based on the total decision of all parties. When enough responses are reached, a transaction is verified to be a valid transaction.

4.5.2 Blockchain platforms for IoT

- IOTA [31] is a permissionless distributed ledger that uses the 'Tangle' consensus. It is based on Directed Acyclic Graph (DAG), where the vertices in the DAG represent transactions, and edges represent approvals. Tangle uses lightweight consensus specifically designed for IoT. It does not use block to store data; instead each transaction is a unique block. To create a transaction, nodes initially sign the transaction and randomly choose two previous transactions to approve. When a node issues a new transaction, it must approve two previous nodes. The newly created node is then called 'tip'. This node will remain as 'tip' until a newly created node approves it. As most of the other protocols use cryptographic algorithms that will be obsolete with quantum computing, IOTA uses quantum-resistant cryptography, 'curl-p' for hashing and Winternitz signature for authentication. It is fast and scalable. However, the main drawback is that there is no rule in Tangle on how to choose the two nodes for approval. All the tokens are generated in the genesis transaction and hence there is no mining for generating tokens. All the nodes contribute to providing network security by approving two other transactions. For a node to issue a valid transaction, the node must solve a cryptographic puzzle similar to bitcoin. This is achieved by finding a nonce such that the hash of that nonce concatenated with some data from the approved transaction has a particular form [48].
- Hyperledger Fabric [29] is an open-source blockchain platform developed by IBM. This is the most widely used blockchain platform which is used across different industries and use-cases. It is used in several prototypes, proof of concepts, and in production distributed ledger system. Hyperledger Fabric is a permissioned blockchain with pluggable consensus. It is one of the projects of Hyperledger which is under the Linux Foundation. It is the first blockchain system that allows the execution of distributed applications written in standard

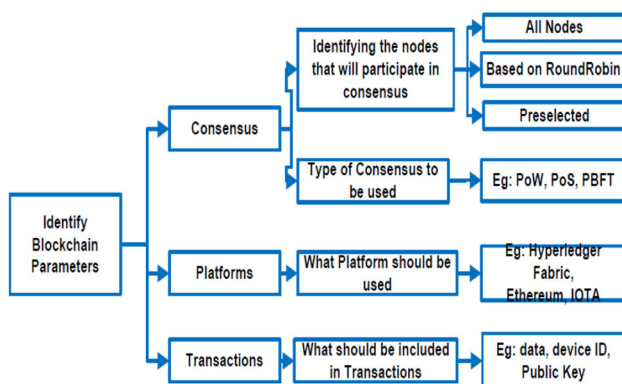


Fig. 8 Identify blockchain parameters

programming. While the traditional blockchain uses order-execute-validate architecture, Hyperledger Fabric uses execute- order-validate architecture. It uses an endorsement policy that is evaluated in the validation phase. Endorsement policy is managed by designated administrators and act as a static library for transaction validation. Examples of endorsement policies are “Three out of five” or “(AVB) \wedge C.” Custom endorsement policies can also be written. One of the disadvantages is that a central authority is managing the endorsement policy and will be implementing it in the network forcing all others to accept it. This is due to the fact that the BFT used in Hyperledger Fabric assumes certain parties of the network to be trustworthy. Within an organization, it assumes that all peers to be trustworthy. This reduces transaction processing, as not all nodes need to execute the transaction. Hyperledger Fabric allows writing smart contracts in a general-purpose language. The framework cannot be used for large scale applications similar to public blockchain due to the network overhead caused when the number of nodes is increased [51].

- Ethereum [22] is a project that can create a generalized technology on which all transaction-based state machine concepts can be built. Ethereum enables developers to build and deploy centralized applications. Thousands of different applications can be created using the Ethereum platform. Its core innovation, the Ethereum Virtual Machine (EVM), helps in creating blockchain applications easier. Developers do not have to start coding from scratch, instead, they can use the Ethereum platform and can create their transaction formats, rules and state transition functions [64]. A comparison of these platforms is provided in Table 3.

5 Comparison of existing architecture for IoT blockchain

In this section, we compare various architectures available in the literature. Figure 9 shows a generic blockchain for IoT architecture with support for several types of IoT devices as well as different infrastructures. The integration of IoT devices involve cloud systems, edge computing, gateways, and different types of IoT devices that range from simple sensors that can only communicate through nearby gateways to devices with computational and processing capabilities.

Table 4 shows a comparison of various architectures available in literature based on the type of storage used, consensus and security. IOTchain [5] is a three-tier blockchain-based IoT security architecture. The three layers are authentication layer (Certification layer), blockchain layer and application layer. It is designed to achieve identity, authentication, access control, privacy protection, lightweight, fault tolerance, DOS attack resilience and storage integrity. Hardware security model (HSM) is used to generate, store and handle key pairs and hashes are stored as Merkle tree. Any lightweight consensus can be used with IoTchain, it can be Practical Byzantine Fault-Tolerance Algorithm (PBFT) or Proof of stake (PoS). Initially, nodes register through the certification layer, which provides the key pair after a valid authentication step. The keys are then added to the HSM to prevent tampering the key.

Hybrid IoT uses both Proof of work and BFT. Proof of work based sub blockchain is created, which are then interconnected using BFT [50]. They use separate centralized storage for each sub blockchain.

Blockchain based framework for edge and fog computing is proposed in [60]. Fog computing brings the

Table 3 Comparison of Ethereum, Hyperledger fabric and IOTA

Characteristics	Ethereum	Hyperledger fabric	IOTA
Description of platform	Permissioned/permissionless	Permissioned	Permissionless
Type	Open source	Open source	Not fully open source
Governance	Ethereum developers	IBM	IOTA foundation
Consensus	Customizable	Pluggable consensus	Tangle
Smart contract	Yes	Yes	No
Data confidentiality	No	Yes	No
Advantages	Allow public and private blockchains	Allow writing smart contract in a general purpose language	Use quantum resistant cryptography
Drawbacks	Does not allow confidential transaction	Framework cannot be used for large scale applications	There is no rule in Tangle on how to choose the two nodes for approval

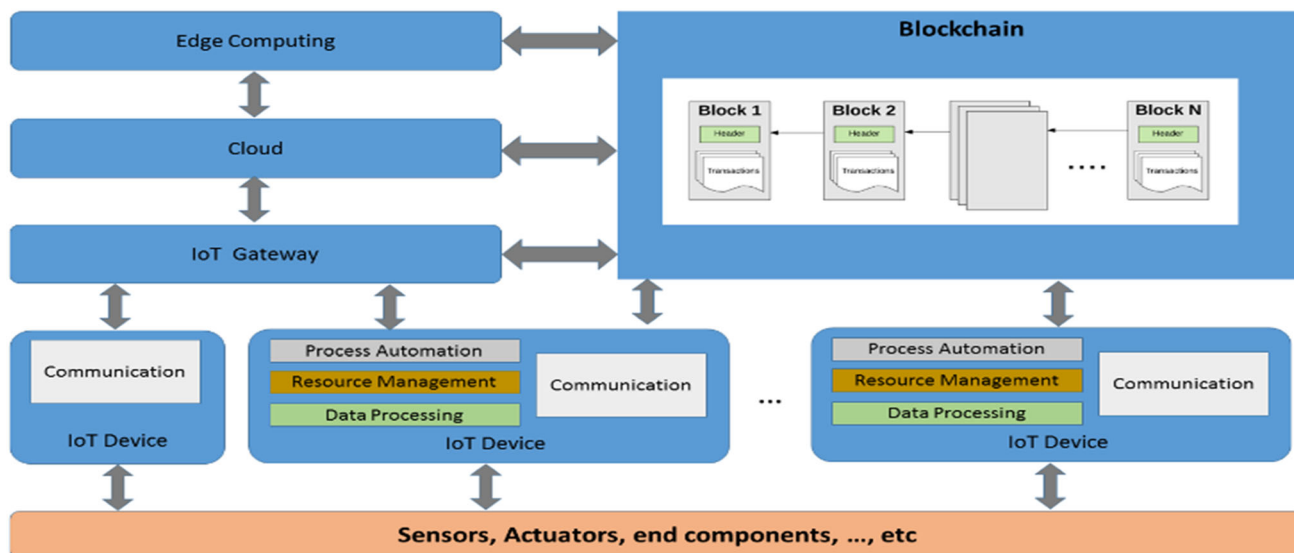


Fig. 9 A Generic blockchain for IoT architecture

Table 4 Comparison of architectures for IoT Blockchain

Name	Architecture type	Consensus used	Storage used	Encryption layer	References
IoT chain	Three layer architecture	Any lightweight consensus	Distributed storage	No	[5]
Hybrid IoT	Proof of work based sub blockchain interconnected with BFT	Proof of work and BFT	A transaction pool for each sub blockchain	No	[50]
Fogbus	Platform independent interface Scalable cost efficient	Proof of work	Distributed repository nodes and later backup to cloud infrastructure	Yes	[60]
Proxy re-encryption scheme	Without the involvement of trusted third party, IoT data is encrypted and stored in cloud	Ethereum Smart contract	Data stored in cloud and Address of the data stored in blockchain	Yes	[40]
Multichain and arduino	Two layers: FOG and IoT	Round robin	Data processed in FOG	NO	[52]

network and cloud computing resources closer to the edge. Hence computations can be performed near to the IoT devices instead of sending it to the cloud datacenter [36]. FogBus can integrate different IoT systems into fog and cloud infrastructure. It functions as a platform-as-a-Service model where developers can build different types of IoT applications, customize the services and manage resources. A case study of health monitoring is provided in the paper. It also provides authentication and encryption techniques to protect the data.

A novel blockchain based scheme with a proxy re-encryption scheme to ensure confidentiality is proposed in [40]. The architecture includes IoT devices, miners, cloud server and data requester connected through the internet. The IoT sensors capture and transmit the data to cloud

storage. This data will be encrypted and stored in the cloud. The sensor owner activates the sensor and registers them on the blockchain. Blockchain executes smart contracts on the sensor transactions and provides the required key to the sensor to encrypt the data. According to the architecture, the data are not stored in the blockchain, whereas it is stored encrypted in a central cloud which is a centralized architecture and also a single point of failure. In [52] a blockchain system is implemented using multiple nodes, including an Arduino in-order to illustrate an IoT–blockchain application.

6 Implementation and performance evaluation

To compare the performance of IoT-device-only type of architecture and Gateway-based architecture, we conducted simulation using the Cooja simulator for the Contiki operating system [15]. We used Z1 motes generated at random locations. We simulated a network of 5, 10, 20 and 40 nodes. The nodes use IPV6 over low power wireless personal, regional networks (6LoWPAN) to connect. In this simulation, we have not considered the computation and storage procedures. We considered only the communication process. We are assuming 72 bytes for elliptic curve signature size and 32 bytes for SHA-256 hash functions and an average transaction size of 77 bytes. We fixed the transaction size and varied the number of nodes.

We compared the average time of communication between nodes in the blockchain on an IoT-device-only architecture and gateway architecture. Based on the result from throughout, a graph was plotted. The X-axis in the graph shows the number of nodes and Y-axis shows the number of transactions. We collected the number of transactions in a period of 5 s and 10 s. From the result, we identified that the throughput is low while using gateways, as shown in Fig. 10 and 11.

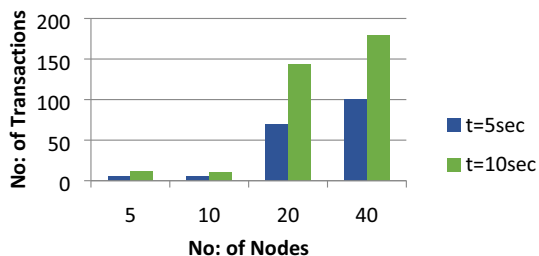


Fig. 10 Average throughput for IoT-device-only type of architecture

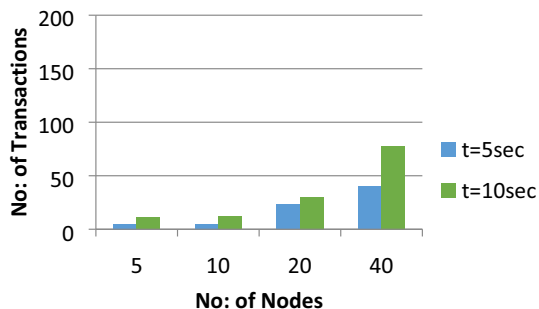


Fig. 11 Average throughput for device with Gateway type of architecture

7 Conclusions

IoT devices participating in blockchain technologies enable a lot of challenging applications, including supply chain management, health care, weather predictions, and food safety. This could be a clear replacement for the untrusted cloud technology providing security and privacy for the user's data. While creating an architecture for IoT, we identified that five components should be considered. They are IoT device types, types of applications, blockchain types and nodes, data and storage, and security.

Blockchain based IoT requires energy-efficient design along with security and the ability to scale. IoT devices should be equipped with scalable storage solutions and computational power required to hash the transactions and verify the digital signatures. Implementation should address the challenges of both IoT and blockchain. We compared the most widely used platforms for IoT blockchain, which are Ethereum, Hyperledger Fabric and IOTA. We identified that Hyperledger Fabric is the most preferred platform due to its pluggable consensus and provides confidentiality to the data, which is most important in the case of IoT due to the sensitive nature of the data. We identified that (PBFT) is the most widely used consensus for IoT blockchain due to the minimal requirement of computation than other consensus.

We compared the architectures and frameworks for IoT Blockchain. Designing the storage and confidentiality of data are the crucial components that should be done carefully in IoT blockchain. Most of the architectures we analyzed use centralized cloud storage, which contradicts with the original objective of blockchain and can be a single point of failure. However, some of them have used distributed storage, which does not have any protection on data. This is because providing confidentiality for distributed storage is not an easy task. Hence we identified that an efficient architecture for IoT blockchain is still not available. Considering the vast advantages that blockchain can provide for IoT, we believed that blockchain would overhaul cloud computing systems. Our research delivers insight into how changes in IoT due to blockchain technology, progress and in what directions firms have to think while changing their business model.

References

1. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. *Int. J. Res. Eng. Technol.* **5**(09), 1–10 (2016)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. *Comput. Netw.* **54**(15), 2787–2805 (2010)

3. Babar, S., Stango, A., Prasad, N., Sen, J., Prasad, R.: Proposed embedded security framework for internet of things (iot). In: 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011, pp. 1–5. IEEE (2011)
4. Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for internet of things security: a position paper. *Digital Commun. Netw.* **4**(3), 149–160 (2018)
5. Bao, Z., Shi, W., He, D., Chood, K.K.R.: IoTChain: a three-tier blockchain-based IoT security architecture. [arXiv:1806.02008](https://arxiv.org/abs/1806.02008) (2018)
6. Bocek, T., Rodrigues, B.B., Strasser, T., Stiller, B.: Blockchains everywhere—a use-case of blockchains in the pharma supply-chain. In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 772–777. IEEE. (2017)
7. Borah, M.D., Naik, V.B., Patgiri, R., Bhargav, A., Phukan, B., Basani, S.G.M.: *Supply Chain Management in Agriculture Using Blockchain and IoT*. Springer, Singapore (2020)
8. Buccafurri, F., Lax, G., Nicolazzo, S., Nocera, A.: Overcoming limits of blockchain for IoT applications. In: Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1–6 (2017)
9. Carrefour Group. Carrefour launches Europe’s first food blockchain. <https://www.carrefour.com/current-news/carrefour-launches-europes-first-food-blockchain> (2018). Accessed 4 Dec 2019.
10. Castro, M., Liskov, B.: Practical Byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186 (1999)
11. Cermaq.com. Cermaq | Cermaq contributes to traceability with blockchain. <https://www.cermaq.com/wps/wcm/connect/cermaq/news/mynewsdesk-press-release-2945012/> (2019). Accessed 4 Dec 2019
12. Cermeño, J.S.: Blockchain in financial services: regulatory landscape and future challenges for its commercial application. BBVA Research Working Paper, vol. 16/20. https://www.bbvarsearch.com/wp-content/uploads/2016/12/WP_16-20.pdf (2016)
13. Comodo News and Internet Security Information. Bitcoin Phishing Attack | Hacking Methods Used for Cryptowallets. <https://blog.comodo.com/comodo-news/bitcoin-phishing-attack-on-cryptowallet-owner/> (2018). Accessed 6 Dec 2019
14. Conoscenti, M., Vetro, A., De Martin, J.C.: Blockchain for the Internet of Things: a systematic literature review. In: Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA (2017)
15. Contiki-os.org. Contiki: The open source operating system for the Internet of Things. <https://www.contiki-os.org/> (2019). Accessed 6 Dec 2019
16. Consensys.net. Blockchain in the energy sector: uses and applications. <https://consensys.net/enterprise-ethereum/use-cases/energy-and-sustainability/> (2019). Accessed 4 Dec 2019.
17. Da Xu, L., He, W., Li, S.: Internet of things in industries: a survey. *IEEE Trans. Ind. Inform.* **10**(4), 2233–2243 (2014)
18. Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R.C., Michelin, R. A., Zorzo, A.F., Kanhere, S.S.: *Blockchain Technologies for IoT*. Springer, Singapore (2019)
19. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173–178. ACM (2017)
20. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: March. 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), pp. 618–623. IEEE (2017)
21. Douceur, J.R.: The sybil attack. In: International Workshop on Peer-to-Peer Systems, pp. 251–260. Springer, Berlin (2002)
22. Ethereum.org. Home | Ethereum. <https://ethereum.org/> (2019). [Accessed 6 Dec. 2019].
23. Foote K.: A brief history of the internet of things—DATAVERSITY. DATAVERSITY. <https://www.dataversity.net/brief-history-internet-things/> (2016). Accessed 30 Aug 2019
24. Gartner.com. Gartner says 8.4 billion connected. <https://www.gartner.com/newsroom/id/3598917> (2018). Accessed 30 Aug 2019
25. Gsma.com. <https://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf> (2018). Accessed 30 Aug 2019
26. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **29**(7), 1645–1660 (2013)
27. Hall, R.E., Bowerman, B., Braverman, J., Taylor, J., Todosow, H., Von Wimmersperg, U.: The vision of a smart city (No. BNL-67902; 04042). Brookhaven National Lab., Upton, NY (2000)
28. Heilman, E., Kendler, A., Zohar, A., Goldberg, S.: Eclipse attacks on bitcoin’s peer-to-peer network. In: 24th {USENIX} Security Symposium ({USENIX} Security 15), pp. 129–144 (2015)
29. Hyperledger. Hyperledger Fabric—Hyperledger. <https://www.hyperledger.org/projects/fabric> (2015). Accessed 6 Dec 2019
30. Imbault, F., Swiatek, M., De Beaufort, R., Plana, R.: The green blockchain: Managing decentralized energy production and consumption. In: 2017 IEEE International Conference on Environment and Electrical Engineering and 2017 IEEE Industrial and Commercial Power Systems Europe (IEEEIC/IE&CPS Europe), pp. 1–5. IEEE (2017)
31. Iota.org. The Next Generation of Distributed Ledger Technology | IOTA. <https://www.iota.org/> (2019). Accessed 6 Dec 2019
32. Juniperresearch.com. Blockchain to Save the Food Industry \$31 Billion by 2024. <https://www.juniperresearch.com/press/press-releases/blockchain-to-save-the-food-industry-%2431-billion-b> (2019). Accessed 4 Dec 2019
33. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future internet: the internet of things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology (FIT), pp. 257–260. IEEE (2012)
34. Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N., Trushechkin, A. S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A.I., Fedorov, A. K.: Quantum-secured blockchain. *Quantum Sci. Technol.* **3**(3), 035004 (2018)
35. Korpela, K., Hallikas, J., Dahlberg, T.: Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences (2017)
36. Kotb, Y., Al Ridhawi, I., Aloqaily, M., Baker, T., Jararweh, Y., Tawfik, H.: Cloud-based multi-agent cooperation for IoT devices using workflow-nets. *J. Grid Comput.* **17**(4), 1–26 (2019)
37. Library, C.: Flint water crisis fast facts. CNN. <https://edition.cnn.com/2016/03/04/us/flint-water-crisis-fast-facts/index.html> (2018). Accessed 30 Aug 2019
38. Lo, S.K., Liu, Y., Chia, S.Y., Xu, X., Lu, Q., Zhu, L., Ning, H.: Analysis of blockchain solutions for IoT: a systematic literature review. *IEEE Access.* **7**, 58822–58835 (2019)
39. LO3ENERGY. <https://lo3energy.com/> (2017). Accessed 30 Aug 2019
40. Manzoor, A., Liyanage, M., Braeken, A., Kanhere, S.S., Ylianttila, M.: Blockchain based proxy re-encryption scheme for secure IoT data sharing. In: 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 99–103. IEEE (2019)
41. Mattern, F., Floerkemeier, C.: From the internet of computers to the Internet of Things. In: From Active Data Management to Event-Based Systems and More, pp. 242–259. Springer, Berlin (2010)

42. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of things: vision, applications and research challenges. *Ad hoc Netw.* **10**(7), 1497–1516 (2012)
43. Modu. <https://modum.io/> (2018). Accessed 30 Aug 2019
44. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf> (2008). Accessed 30 Aug 2019
45. Nestlé Global. Nestlé breaks new ground with open blockchain pilot. <https://www.nestle.com/media/pressreleases/allpressreleases/nestle-open-blockchain-pilot> (2019). Accessed 4 Dec 2019
46. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: FairAccess: a new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Netw.* **9**(18), 5943–5964 (2016)
47. Pahl, C., El Ioini, N., Helmer, S.: A decision framework for blockchain platforms for IoT and edge computing. In: *IoTBDSS 2018—Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security*, pp. 105–113 (2018)
48. Popov S.: IOTA whitepaper v1.4.3, pp. 1–28 (2018)
49. Pilkington, M.: 11 Blockchain technology: principles and applications. *Research handbook on digital transformations*, p. 225 (2016)
50. Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J.D., Ragnoli, E.: Hybrid-iot: hybrid blockchain architecture for internet of things-pow sub-blockchains. In: *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1007–1016. IEEE (2018)
51. Salimitari, M., Chatterjee, M.: An overview of blockchain and consensus protocols for IoT networks. [arXiv:1809.05613](https://arxiv.org/abs/1809.05613) (2018)
52. Samaniego, M., Deters, R.: Internet of smart things-IoST: using blockchain and CLIPS to make things autonomous. In: *2017 IEEE International Conference on Cognitive Computing (ICCC)*, pp. 9–16. IEEE (2017)
53. Seibold, S., Samman, G., Consensus.: Immutable agreement for the Internet of value. KPMG. <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism.pdf> (2016). Accessed 30 Aug 2019
54. Simic, M., Sladic, G., Milosavljević, B.: A Case Study IoT and Blockchain powered Healthcare. In: *The 8th PSU-UNS International Conference on Engineering and Technology (ICET-2017)* (2017)
55. Sousa, J., Bessani, A., Vukolic, M.: A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In: *Proceedings—48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018, (Section 4)*, pp. 51–58 (2018)
56. Sun, J., Yan, J., Zhang, K.Z.: Blockchain-based sharing services: What blockchain technology can contribute to smart cities. *Financ. Innov.* **2**(1), 26 (2016)
57. Swan, M.: *Blockchain: Blueprint for a New Economy*. O'Reilly Media Inc, Newton (2015)
58. Tian, F.: An agri-food supply chain traceability system for China based on RFID & blockchain technology. In: *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6. IEEE (2016)
59. Tian, F.: A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In: *2017 International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6. IEEE (2017)
60. Tuli, S., Mahmud, R., Tuli, S., Buyya, R.: Fogbus: a blockchain-based lightweight framework for edge and fog computing. *J Syst Softw.* (2019)
61. Uckelmann, D., Harrison, M., Michahelles, F.: An architectural approach towards the future internet of things. In: *Architecting the internet of things*, pp. 1–24. Springer, Berlin (2011)
62. Vasek, M., Thornton, M., Moore, T.: Empirical analysis of denial-of-service attacks in the bitcoin ecosystem. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8438, pp. 57–71 (2014)
63. Vukolić, M.: Rethinking permissioned blockchains. In: *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, pp. 3–7. ACM (2017)
64. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper* **151**, 1–32 (2014)
65. Wörner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with Bitcoin. In: *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, pp. 295–298. ACM (2014)
66. Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H.: A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things J.* **4**(5), 1250–1258 (2017)
67. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. In: *2015 18th International Conference on Intelligence in Next Generation Networks (ICIN)*, pp. 184–191. IEEE (2015)
68. Zyskind, G., Nathan, O., Pentl, A.: Enigma: decentralized computation platform with guaranteed privacy. [arXiv:1506.03471](https://arxiv.org/abs/1506.03471). <https://enigma.media.mit.edu/enigmafull.pdf> (2015). Accessed 30 Aug 2019

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



ment at Abu Dhabi Polytechnic.

Deepa Pavithran has more than seven years' experience in the field of Information Security and Computer Science, which includes both Academic and Industrial. She holds Masters in Cyber Security and Bachelors in Computer science and Engineering with Professional Certifications, including CISSP and OSCP. Her area of interest includes Cryptography and Blockchain. She is currently working in the Information Security Engineering Department



Khaled Shaalan is a full professor of Computer Science at the British University in Dubai (BUiD), UAE. He is an Honorary Fellow at the School of Informatics, University of Edinburgh (UoE), UK. Prof Khaled is an Associate Editor on *ACM Transactions of Asian and Low Resource Language Information Processing (TALLIP)* editorial board, Association for Computing Machinery (ACM). Prof Khaled has a long experience in teaching in the field of Computer Science for both core and advanced undergraduate and postgraduate levels. He has taught more than 30 different courses

at the undergraduate and postgraduate levels. Over the last two decades, Prof Khaled has been contributing to a wide range of research topics in Arabic Natural Language Processing, including machine translation, parsing, spelling and grammatical checking, named entity recognition, and diacritization. Moreover, he has also worked on topics in knowledge management, knowledge-based systems, knowledge engineering methodology, including expert systems building tools, expert systems development, and knowledge verification. Nevertheless, Khaled worked on health informatics topics, including context-aware knowledge modelling for decision support in E-Health and game-based learning. Furthermore, Prof Khaled worked in educational topics, including intelligent tutoring, item banking, distance learning, and mobile learning. He has been the principal investigator or co-investigator on research grants from USA, UK, and UAE funding bodies. Prof Khaled has published over 190+ refereed publications and the impact of his research using Google Scholar's H-index metric is 30+. He has several research publications in his name in highly reputed journals such as Computational Linguistics, Journal of Natural Language Engineering, Journal of the American Society for Information Science and Technology, IEEE Transactions on Knowledge and Data Engineering, Expert Systems with Applications, Software-Practice & Experience, Journal of Information Science, Computer Assisted Language Learning, and European Journal of Scientific Research to name a few. Prof Khaled's research work is cited extensively worldwide (see his Google Scholar citation indices). He has guided several Doctoral and Master Students in the area of Arabic Natural Language Processing, healthcare, Intelligent Tutoring Systems, and Knowledge Management. Prof Khaled encourages and supports his students in publishing at highly ranked journals and conference proceedings. Prof Khaled has been actively and extensively supporting the local and international academic community. He is the founder and Co-Chair of The International Conference on Arabic Computational Linguistic (ACLing). He has participated in seminars and invited talks locally and internationally, invited to international group meetings, invited to review papers from leading conferences and premier journals in his field, and invited for reviewing promotion applications to the ranks of Associate and Full Professor for applicants from both British and Arab Universities. Prof Khaled is the Head of Programmes PhD in Computer Science, MSc in Informatics and MSc in IT Management, and BSc in Computer Science (Artificial Intelligence, Software Engineering).



Jamal N. Al-Karaki is an accomplished Information security and technology expert with 20+ years of versatile IT experience and expertise in corporate systems and network security architecture and management along with IT projects management, network and IT infrastructure design and implementation, curriculum design, training program design, and change management throughout the project life cycle in public and private sectors. In

addition, Dr. Al-Karaki has a rich University career in education, training and research including serving heavily in academic leadership capacity. He has many years of experience in curricula design, pedagogy in higher education and lead several teams at various universities in implementing curricula continuous improvement and attain national and international accreditation. He is a consultant in the fields of information technology and security for various governmental and commercial firms. Dr. Al-Karaki has served in several senior leadership positions as a Dean, Director, and Chairman. Dr. Al-

Karaki is the Co-Founder and Division Head of information Security Engineering Technology- Abu Dhabi Polytechnic (ADPoly), Abu Dhabi, UAE since Feb 2012. Before joining ADPoly, He served as the Dean of Information Technology College, at the Hashemite University, Zarka—Jordan. He also worked for faculty of computing, King Abdulaziz University, Jeddah, Saudi Arabia with knowledge comes a responsibility towards the society. Dr. Al-Karaki obtained his Ph.D. from Iowa State University where he was awarded the research excellence award on his pioneering work on wireless ad hoc networks. Dr. Al-Karaki has more than 60 published refereed technical articles in scholarly international journals and proceedings of international conferences. He also served on the Editorial Board of some international journals and as publicity chair and technical program committee member of several International conferences and workshops. He also attended training/gained reputable professional certificates that includes CISSP, OSCP, ECSA, GMOB, CHFI, RHCSA, and CCNA security. Dr. Al-Karaki constantly works collaboratively with industry, government, faculty, senior executive leadership, and with community stakeholders to encourage scholarly pursuits, engagement, and innovation as critical goals with sound budget planning. As active researcher, he developed plans to advance the research agenda, activity and productivity; outreach and community engagement. He also develops strategic plan for continuous improvement of undergraduate and graduate programs. He also developed notable experience with leadership in the development of new programs that meet international standards and success in building teamwork. In particular, he has excellent experience with ABET, CAA, NQA, and standards. His research work focuses on network security, cyber security, Penetration testing, Security audits, Cloud security, threat modelling, Blockchain, IoT, Big data, and e-learning. Dr. Al-Karaki is a senior member of the Institute of Electrical and Electronics Engineers (IEEE) and member of Association of computing and machinery (ACM) among other several professional organizations.



Amjad Gawanmeh is an Associate Professor at the College of Engineering and IT, University of Dubai, UAE, adjunct professor at Concordia University, Montreal, Canada, and a senior IEEE member. He received the M.S. and the Ph.D degrees from Concordia University, Montreal, Canada, 2003 and 2008. His research interests include, design and verification of medicals sensors, testing and verification of hardware systems, security systems, and healthcare

systems, modeling and analysis of complex systems such as CPS, performance analysis of complex systems, reliability of as medical system, and reliability of CPS. He has two edited books, three book chapters, more than 30 peer reviewed indexed journal papers, and more than 55 indexed conference papers. He was a visiting scientist at Syracuse University, Concordia University, and University of Quebec. He is an associate editor for IEEE Access Journal, and for Human-centric Computing and Information Sciences Journal, Springer. He acted as guest editor for several special issues. He is on the reviewer board for several journals in IEEE, Elsevier, Wiley, and many others. He is a member of the executive committee for IPCCC conference. He has co-chaired several conferences and chaired several workshops organized in key conferences including ICC, ICDCS, IPCCC, Healthcom, ISNCC, CHASE, WoWMoM, ITNG, and WiMob.