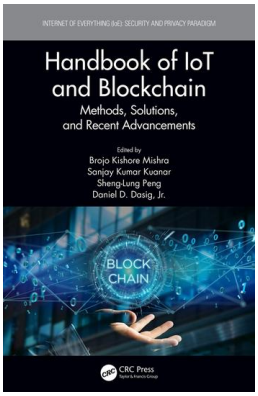

Handbook of IoT and Blockchain
Methods, Solutions, and Recent Advancements

Brojo Kishore Mishra, Sanjay Kumar Kuanar, Sheng-Lung Peng, Daniel D. Dasig

Blockchain-Enabled Security and Privacy Schemes in IoT Technologies

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780367854744-1
Siddhant Banyal, Mayank Saxena, Deepak Kumar Sharma
Published online on: 26 Nov 2020

1 Blockchain-Enabled Security and Privacy Schemes in IoT Technologies

Siddhant Banyal[1], Mayank Saxena[2], and Deepak Kumar Sharma[3]

[1]Department of Instrumentation and Control, Netaji Subhas University of Technology

(Formerly known as Netaji Subhas Institute of Technology), New Delhi, India

[2]Department of Electronics and Communications Engineering, Netaji Subhas University of Technology

(Formerly known as Netaji Subhas Institute of Technology), New Delhi, India

[3]Department of Information Technology, Netaji Subhas University of Technology

(Formerly known as Netaji Subhas Institute of Technology), New Delhi, India

CONTENTS

1.1 INTRODUCTION AND MOTIVATION

1.1.1 Internet of Things

The last two decades have been catalyzed by developments on a myriad of technological fronts and these developments have severely affected the way in which society functions. Technology has been increasingly integrated with our way of living and daily life, ranging from the moment we wake up at home and use smart home appliances to the usage of integrated technology in the workplace to health monitoring and analytics of our sleep. This development has asymmetrically changed the way industries perceive and use technology and with the incumbent developments they have been trying more and more to integrate them into their operations for efficiency. The reports suggest that the estimated count of connected IoT devices is set to rise to 50 billion by the end of this decade [1]. The ecosystem involves a myriad of elements such as: IoT devices, sensors, actuators, network elements (servers, routers etc.) and associated industrial machinery. In this pursuit of connecting conventional devices across networks and over the internet, the Internet of Things and Web of Things (WoT) have been pivotal in catalyzing and catering to this need. IoT as an emerging technology offers novel solutions and optimizing paradigms to both conventional and unconventional industrial operations. One such example of this innovative behavior is the case of innovative transportation in the field of Intelligent Transportation Systems (ITS) where IoT and associated technology have provided the ability for smart traffic management and traffic prediction through monitoring and predicting traffic location.

As discussed above, the Internet of Things or IoT encompasses a global network of nodes and devices that are addressable uniquely via standard communication protocols. The Internet of Things, which has witnessed a dramatic surge in the recent past, has had an immense impact on every aspect of human lives, ranging from wearable gear to sensors monitoring ecological changes in remote locations to regulating physical metrics in manufacturing processes. The set of devices or the "Things" which share a common resemblance in order to directly or indirectly connect to the Internet, operate within the confines of their functionality and exchange, analyze, process and deliver data in the common language; these sets of devices working in tandem are defined as "Internet of Things". Although large swathes in advancement in technology have unequivocally reduced human intervention and have significantly integrated devices with the real world, the big question of privacy and protection in IoT devices has been left largely unaddressed and now presents a potential threat to the cyber landscape. The lack of a standard IoT framework safeguarding privacy across all platforms has been attributed to varied communication protocols, a multitude of programming languages and differing levels of distributed computing in devices, networking and perceiving data in real-time systems [2].

The developers and research community have been meticulously working to develop tailor-made frameworks and structures for specific platforms. In its pursuit of this, the community has encountered several challenges pertaining to hardware which involve energy efficiency, ranging from the lightweight computation of devices and sensors to virtual threats including encryption attacks which occur on system vulnerabilities and tend to impede system integrity. Privacy is another concern that many nations across the globe have echoed. Policy measures such as the EU's General Data Protection Regulation (EU GDPR) have already been enforced with stringent rules for privacy yet there exist several challenges on the regulatory and technological front which this chapter touches upon in its first section. Industries such as healthcare, which incorporates one of the largest numbers of IoT devices, are especially under threat as revealed in the analysis by the Ponemon Institute and IBM. The most severe example of this is the case of Singapore, when an attack on SingHealth exposed the data of more than 1.5 million patients. The aforementioned cyber threats present us with a unique conundrum.

1.1.1.1 IoT Architecture

Every IoT system implemented globally is different; however, the data process flow and general architecture have some similarity. The first element is "Things"; this entails the nodes/devices that sense data from the environment via embedded sensors and actuators and are connected to the internet via appropriate gateways. The second layer includes the data acquisition systems and gateways that are responsible for gathering large amounts of raw and processed data (filtration, amplification and other associated electronic signal conditioning), and convert it into a digital form that is ready for further analysis. The third layer is where data visualization and intelligent control steps in, through which the processed data is transferred for long-term storage to data centers and cloud-based facilities which form the fourth layer.

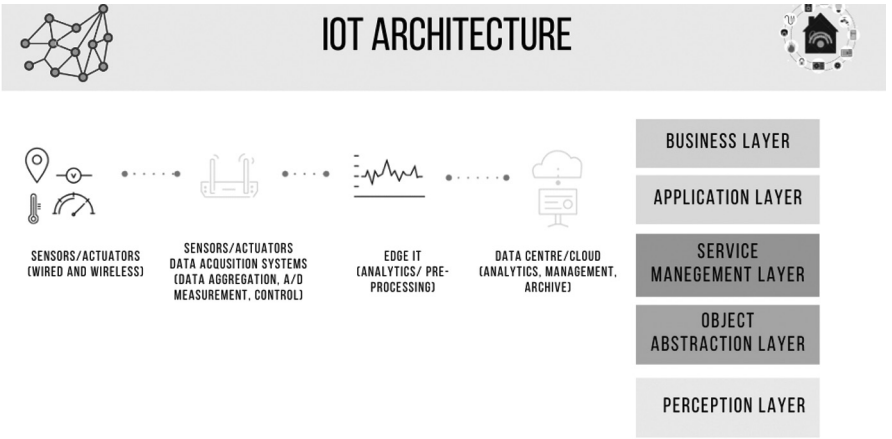

FIGURE 1.1 IoT general Architecture.

These four layers are illustrated in Figure 1.1 of this chapter. The figures entail a five-layer architecture that comprises of:

1. Business Layer
2. Application Layer
3. Service Management Layer
4. Object Abstraction Layer
5. Perception Layer

The business layer is responsible for the management of all activities, services and development of business models, graphs, and flowcharts based on the data it receives from the application layer. Further, this layer is responsible for supporting the decision-making aspect, based on big data analysis and determining the course of action. The application layer is responsible for service delivery and acts as an interface to the business layer. Furthermore, it is responsible for providing a control mechanism for accessing data and provides global management of the application based on objects' information processed in middleware. The service management layer is responsible for the pairing of services with their requester based on addresses and names, and for processing received data, making decisions and delivering the required services over network wire protocols. Furthermore, it is tasked to receive and process data from other layers. The object abstraction layer is responsible for the transfer of data produced by the objects to the service management layer. Also, it is responsible for transmitting data between devices and from devices to the receiver. Lastly, the object or perception layer is responsible for collecting sensor data in addition to digitizing and transferring data to the object abstraction layer. The details of the architecture and associated aspects are described in online literature [3–7].

TABLE 1.1
Vulnerability in IoT device

Assailability in IoT Device	Type of Vulnerability
Hardware layer	a) Lack of tamper resistance b) Weak embedded crypto algorithms c) Weak hardware implementations
Software layer	a) Firmware Layer b) Operating system c) Application layer
Communication protocols	a) Link & network layer protocol threats b) Application layer protocol threat c) Network design flaws
Key Management	a) Absence of support for public key exchange b) Easily extractable communication keys c) Employing of common or no key

Attacks that focus on IoT devices that have resource constraints have increased significantly in the past few years. The vulnerabilities in the security sector of the IoT technologies used are incessantly being identified; these technologies are used in both industrial and home environments such as sensors, industrial actuators, home appliances, medical devices, etc. The current state of affairs is exacerbated by defects in application, hardware chips that are faulty, and tamperable devices along with misconfigurations.

This section aims to use a risk-like approach to examine cyber attacks with respect to IoT-enabled devices, so as to highlight its existing threat landscape and isolate hidden and covert attack paths taken against critical infrastructure.

In IoT-enabled cyber attacks, the device is the amplifier or the enabler of an attack; the perpetrator identifies and takes advantage of inherent vulnerabilities related to one or multiple layers of the device so as to achieve his/her goal. We classify IoT vulnerabilities in two primary classes: "Embedded Vulnerabilities" and "Network Vulnerabilities".

1.1.1.2 Distinguishing IoT from Conventional Networks

Since its inception, IoT has experienced significant development in parallel to conventional networks. In comparison to the internet the network connection is established via physical links between web pages. Conventional networks are relatively more mature and well established on the technological front and can communicate via natural languages with efficacy. This is the reason which substantiates the prevalence of traditional networks and ease of their operation. In the IoT domain the standardization efforts are in their infancy and currently require skilled programming experts to implement an application.

1.1.2 Blockchain: An Overview

Blockchain is defined as a "public, permanent, appended-only distributed ledger" [8]. The issue of trust in information systems is extremely complex and quite prevalent.

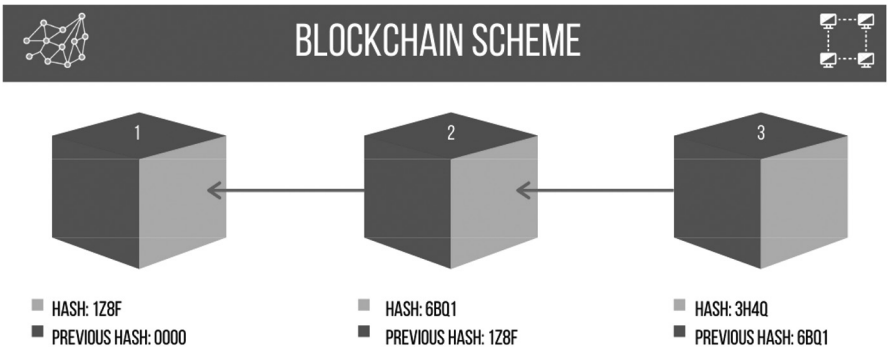

FIGURE 1.2 Blockchain Mechanism with use of reference Hash.

TABLE 1.2
Bitcoin node and functionality

	Wallet	Storage	Mining	Routing
Bitcoin Core	✓	✓	✓	✓
Full Node		✓		✓
Solo Miner		✓	✓	✓
Light Miner	✓			✓

This situation is exacerbated in the absence of audit and verification mechanisms, particularly in the case of systems handling sensitive information such as but not limited to financial and economic transactions. The problem of double spending is solved by enabling blockchain technology in a peer-to-peer network where there is an absence of a trust-based system. Blockchain enables verification of transactions by a group of unreliable actors. This aims to provide an immutable, distributed, secure, transparent and auditable ledger. The chain may be accessed openly allowing access to all transactions since the genesis transaction of the system. The protocol structures a chain of blocks that are linked to its previous block by a reference, thus forming a chain. Figure 1.2 describes the blockchain mechanism along with the use of a reference hash.

In order to support and operate the blockchain, network peers provide functionality which can include functions such as storage, wallet, and service and mining. Based on their functionality they can be part of different networks. Table 1.2 compares common types of nodes in bitcoin networks. Further, it does so establishing a consensus-based mechanism in which the nodes vote via their CPU power on the computation of a proof of work in the form of a hash for a given block which is based on the work that came previously.

1.1.3 Generations of Blockchain

Currently we are witnessing a critical shift toward distributed applications. This enables decentralized data sharing via secure transactions. This section reviews

the emergence of blockchain in form generation starting from Blockchain 1.0 to Blockchain 4.0.

1.1.3.1 Blockchain 1.0: Bitcoin and Cryptocurrency

The first ever recognized generation of blockchain can be attributed to the rise of distributed ledger in form a virtual currency/coin, Bitcoin. The virtual coin enabled users to perform financial transactions over the internet. In addition, the currency is also referred to as "cryptocurrency" as it uses two keys to enable and authenticate the transaction:

Public Key: for verification of the legitimacy of the transaction
Private Key: for signing the transaction (enablement)

The Bitcoin ledger is composed of states of ownership of all existing bitcoin users informed of transactions between states, and output of any transaction state is essentially the transactional value if the transaction was successful. The copy of the above finite-length state transition system is maintained as a ledger record by the nodes of the network. The roles of third parties were eliminated in this decentralized and anonymous system as the proof of work is carried by hashing schemes based on Hashcash [9] and SHA-256 [10].

Figure 1.3 above illustrates the bitcoin transaction process, wherein the purchaser is referred by the entity to his signature which is a 16-digit encrypted code. The

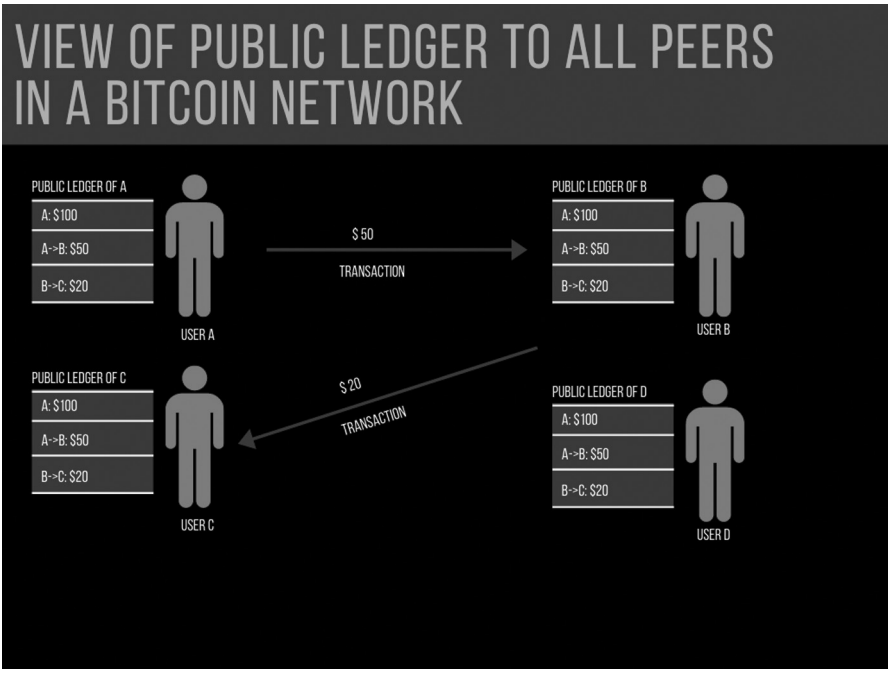

FIGURE 1.3 Public Ledger in a Bitcoin(BTC) network via State Transfer Function(STF).

signature is decoded by the purchaser at his receiving node, thus making the currency digital in nature over a decentralized and anonymous network.

1.1.3.2 Blockchain 2.0: Smart Contracts and Ethereum

The advent of Bitcoin (BTC) marked the rise of decentralization in computing, but the limited purview of BTC renders it unsuitable for general-purpose applications. This requirement of general application based systems was felt and in 2013 this was catered for to some extent with the launch of Ethereum. Ethereum is a blockchain coupled with an inbuilt Turing Complete programming language; this solved several scripting-based issues in BTC. This enabled users to create virtual ownership, the format for specific transactions and the state transfer function. This facilitated the growth of computer programs which existed and executed in a block chain—"Smart Contracts". These execute on their own in an autonomous manner through a set of predefined conditions. This resulted in reduction of the cost of verification and arbitration and enabled greater transparency in a transaction.

Figure 1.4 depicts the implementation of a smart contract on an Ethereum Blockchain. This includes a 20 B address and an STF. The contact code gets saved, authenticated and executed on a blockchain; each transaction comprises the following components:

1. Nonce
2. Ether Balance

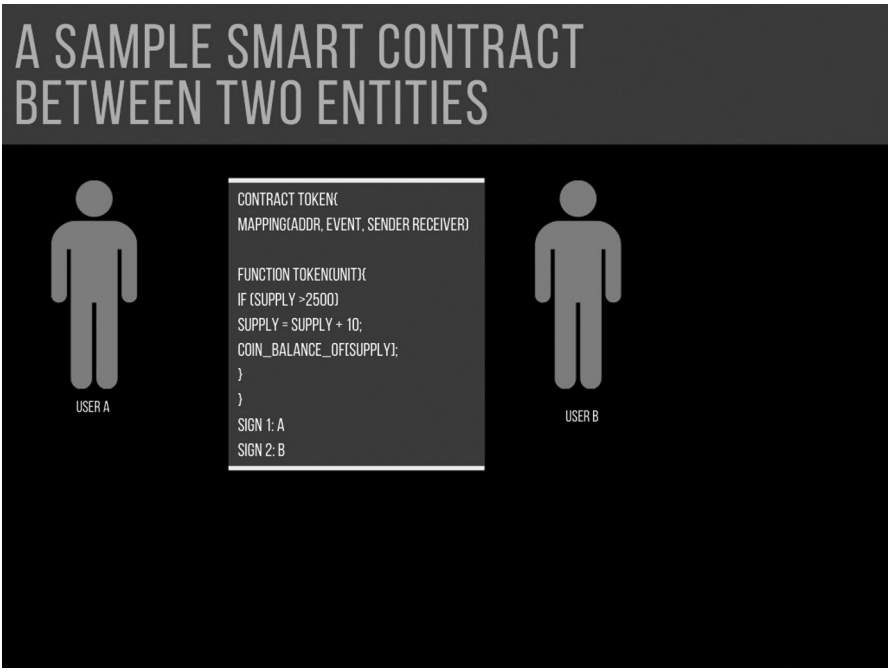

FIGURE 1.4 Illustration of a Smart Contract between two contracting entities.

3. Code Hash
4. Storage Root

1.1.3.3 Blockchain 3.0: Convergence toward Decentralized Applications

There is a lack of infrastructure evident as the existing technology is unable to sustain the volume of micro transactions with the prevalence of smart contracts. Consequently, there has been a shifting trend for blockchain toward decentralized networks and eventually a decentralized internet. This will integrate information storage, Smart Contract and communication networks. Thus there is a strong need for decentralized applications or D-App which have their backend enabled on Blockchain.

1.1.3.4 Blockchain 4.0: Seamless Integration with Industry 4.0

With the rise of decentralized applications there is a need for a common platform which will be a confluence of a myriad of applications and services that facilitate cross-platform communication. This enables entities to collaborate from distinct platforms to collate and work a single unit thus catering to the requirement of Industry 4.0. Industry 4.0 is used to label the trend in industry which emphasizes automation and confluence of cyber space with physical space in conjunction with IoT, Artificial Intelligence and cognitive computing.

1.2 IOT ARCHITECTURE AND SYSTEMIC CHALLENGES

1.2.1 Sensing Layer: Introduction and Challenges in End Nodes

Amidst the vast variety of IoT devices that surround humans, the most common are sensors, actuators, RFID readers, RFID tags, etc. These devices form a set of devices which are collectively termed as the sensing layer of IoT architecture. The critical contribution of this layer in IoT can be broadly summed up as sensing of ambient parameters and transmission of sensed data for processing in the next layers [8]. A few parameters that need to be considered in the sensing layer:

a) Cost, Resource and Energy consumption: The devices are equipped with minimal energy resources and memory in order to reduce cost.
b) Communication: The devices act as receiving ends of information and are designed to communicate with other devices on the network.
c) Networks: WSNs (Wireless Sensor Networks) and WMNs (Wireless Mesh Networks) connect a unique category of things in a complex; wireless and autonomous networks are employed for data acquisition, transmission and operation.

Figure 1.5 explains the fundamentals of service-oriented architecture in an IoT network and also its interaction with the other layers of IoT infrastructure.

Coupled with synchronized computing and communication capabilities, IoT is attributed to tapping into the potential offered by these individual sensors, turning them from classic to smart. In this regard, the security of the end nodes of the sensing layer of this network becomes of prime importance, particularly owing to

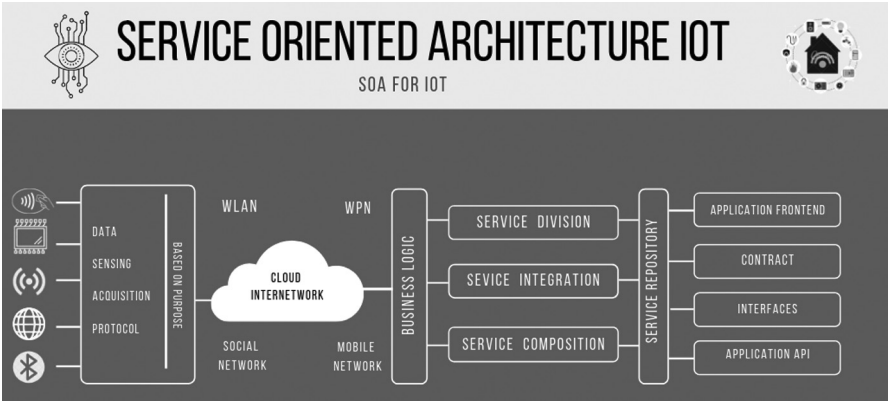

FIGURE 1.5 Service-Oriented Architecture IoT.

the uncertainty regarding data controlling. In this regard, the foremost prerequisite for the security mechanism in the Internet of Things is to have the rationale to take its own decisions which includes approving a command to accept, execute or terminate it. However, the confines of "Things" set up for minimal energy consumption and limited memory pose an extended range of security vulnerabilities at the sensing layer and end-node.

Upon classifying the various insecurities and threats that the sensing layer of IoT faces, it is essential to follow a few security preconditions; these include:

a) Security Prerequisites in IoT end nodes: confidentiality, integrity, privacy, access control, authentication, physical security protection and nonrepudiation.
b) Security Prerequisites in the IoT sensing layer: device authentication, authentication of information source, availability, integrity and confidentiality.

In order to achieve the above-mentioned requirements in the sensing layer of the IoT network, a few actions suggested include:

a) Creation of a trustworthy data sensing system and reinstating privacy and confidentiality of all devices in a network.
b) Identification of the source of users forensically as well as tracing them.
c) Designing the software or firmware at IoT to secure end nodes.
d) Administer security standards for all IoT devices.

1.2.2 Threat Based on Network Layer

For the optimum utilization of data procured in the sensing layer, it is equally important to transmit data among the IoT infrastructure. The network layer, therefore, provides the necessary medium to exchange information.

For smooth functioning and coordination among IoT devices, proper arrangement, organization and management of networks is important for which certain prerequisites include:

a) Effective network management such as wireless networks, fixed networks or mobile networks.
b) Energy efficiency within network layer.
c) QoS requirements.
d) Maintenance of privacy, confidentiality and security.
e) Mechanism for mining and searching.

Among the above-mentioned requirements, maintenance of privacy, confidentiality and security lies within the purview of the chapter and its importance is critical based on the complexity and mobility. Although existing security protocols and frameworks have provided security against threats and vulnerabilities until now, there exist a multitude of concerns that need to be addressed:

1) Broad security provisions: Provisions to ensure confidentiality, integrity and privacy for group authentication, protection of keys and availability of data.
2) Protection against privacy leakage: The location and complexity of certain devices in an IoT network often troubles the developers fearing the susceptibility of attacks upon sensitive data like user identity and credentials.
3) Secure communication: For an IoT system to exist, it must be fortified against attacks and reinforced with robustness, trustworthiness and confidentiality.
4) Fake network message: Creating fake signals corner and propagating miscommunication among devices from the entire network.
5) Overconnection: A highly connected network is also at risk due to two main reasons:
    a) High network congestion caused by signaling authentication on a bandwidth which may lead to a DoS attack.
    b) Intensive resource consumption caused by key operations and key security.
6) MITM attack: The attacks carried out independently by attackers over networks to forge a private connection while the attacker is controlling the entire conversation.

Although the innovations and technology available have been able to keep major threats at bay until recently, the growing influence of attackers has sent shockwaves across the globe. A series of steps in the following directions could help to provide greater security in the future:

a) Stringent authentication/ authorization process.
b) Secure transport encryption.

1.2.3 Service-Layer Based Threats

Upon sensing and transmission, the data procured requires operation while utilizing and integrating services of hardware and software platforms. The service layer hence aptly touted to be the middleware technology is designed according to the application requirements, application programming interface and service protocols to the standards of service providers, vendors and organizations. This layer is responsible for integration, analysis, security, management of UI and event-processing services [9] To render these services, the following steps are taken:

a) Service detection: Locating the optimum infrastructure necessary to conduct services efficiently;
b) Service combination and integration: To further broaden the scope of interaction among services and draw out more reliable ones is achieved by interaction by scheduling or recreating;
c) Authentication Management: Focus is laid upon verification of trusted devices through other services;
d) Service APIs: These help to improve interconnections between services.

To tackle the numerous challenges and threats, developers and corporations have contributed relentlessly to offer solutions to augment and improve services within the connected network. The ambitious SOCRADES integration architecture aims to ameliorate the interactions between application and service layers efficiently [11]. The "things" in the interconnection of devices are often limited to delivering services while exploiting these devices for discovery of networks, exchange of metadata and asynchronous publish and subscribe events [12]. In Peris-Lopez *et al.* (2006) [13], to increase the interoperability of loosely coupled devices and distributed applications, representational state transfer is set up. In Hernandez-Castro *et al.* (2013) [14], a service-provisioning process is introduced in the service layer that could strengthen ties and buttress cooperation between applications and services.

In light of the above-mentioned challenges and solutions offered to counter them, it is imperative to understand that certain security precautions, requirements and protocols, if undertaken, could shield against attacks in the service layer. A few of them are:

a) Dedicated authorization methods for service verification, authentication of groups, protection of privacy and integrity for the upkeep and storage of keys;
b) Protection against privacy leakage and location tracking;
c) Tracking services involving unauthorized use and unsubscribed services;
d) Prevention of potential threats like DoS attacks, node identification masquerade, replay attacks, service information manipulation and communication and services repudiation.

The solutions offered in this section broadly cover the solutions from major potential security threats.

In spite of the solutions offered, there remain a few open challenges that need to be addressed when creating an IoT application or services:

a) Securing data transference between layers;
b) Securing service management.

1.2.4 Application Interface Layer

This interface is the most visible and interactive layer of the IoT network and encompasses a myriad of utility-based implementations ranging from radio frequency identification based tracking to intelligent home management that are enabled via standardized protocols and other technologies [15]. Application maintenance requires certain security preconditions such as:

a) Safety-based isolation.
b) Secure methodologies for acquisition of software and updates.
c) Patches for augmenting security.
d) Verification means for the administrators.
e) Integrated platform for enhancement of security.

Different layers of IoT architecture require the following in order to sustain security in communication between the layers:

a) Maintaining the three tenets of security (privacy, confidentiality and integrity) for inter-layer communication.
b) Verification and approval of administrators cross layer.
c) Isolation of critical data.

The following regulations could prove to be helpful in designing security solutions:

a) The safety of these nodes should be attended carefully as most of the nodes in question are unsupervised.
b) Energy efficiency of nodes is of utmost importance while designing security solutions considering their large numbers.

1.2.5 Cross-Layer Challenges

Across all layers of IoT architecture through which the data is shared, certain standards are to be maintained to ensure that the network remains secure and fully interoperable. With the growing number of things in the network, it is the prerogative of the users to ascertain that their data is guaranteed protection against challenges among layers of the architecture.

The security needs across layers are virtually the amalgamation of the challenges faced across the IoT network:

a) Security protection in terms of design and execution time;

b) Ensuring high privacy standards to protect personal data through enhancement technologies;
c) Reinstating trust in IoT architecture

1.3 CHALLENGE TO IMPLEMENTATION OF BLOCKCHAIN IN IOT

1.3.1 Absence of IoT-Centric Consensus Protocol

A consensus protocol is a technique or a set of rules and regulations that make all the full nodes finalize on an arrangement over the sequence of transactions. There are various categories of consensus protocols being currently utilized in a variety of blockchain applications, for example, PoS, Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), etc. A few of the commonly used consensus protocols are deliberated upon in the following paragraphs of this chapter. Makdhoom [16] shows the contrariety of a few of the widely known and used blockchain consensus protocols in a thorough and exhaustive manner. The established consensus protocols such as Proof of Stake (PoS), Proof of Work (PoW), IOTA, Proof of Elapsed Time (PoET) are fabricated for permissionless blockchains, with an emphasis on financial transactions, whereas PoS and PoET have the potential to be used in permissioned blockchains.

The universal problem with these consensus protocols is the probabilistic nature of the consensus process and that it fails to terminate in a perdurable committed block. This further explains their vulnerability to blockchain forks [17]. One of the major contributors to deferred transaction verification is an absolute absence of consensus finality that is not at all sustainable for the various real / near-real-time IoT systems that demand instantaneous transaction verification and completion. Furthermore, examining the various consensus protocols, we find that a certain type of hardware is required by PoET in which the region allocating wait time necessitates being a trusted entity.

A number of ambiguities are yet to be resolved when it comes to IOTA since it is still in the open beta testing phase particularly regarding its performance efficacy and security. A number of questions pertaining to whether IOTA would be an effective micro-payment method or its compatibility with contracts as in HFB (Hyperledger-Fabric blockchains) and Ethereum and its capability of providing data confidentiality are still unanswered.

Meanwhile, a number of other consensus protocols like the Delegated Byzantine Fault Tolerance (DBFT), Practical Byzantine Fault Tolerance (PBFT), HoneyBadger *et al.* are based on the Byzantine Fault Tolerance (BFT) protocol which is a group of state machine reduplication protocols. By replicating the services on a multitude of nodes it provides security against arbitrary faults. Despite BFT being the preferred protocol for permissioned-type blockchains, it has several shortcomings. BFT-based protocols have a high vulnerability toward DoS attacks owing to their languid timing assumptions with the exception of HoneyBadger BFT [18]. Not only does the feeble synchrony negatively alters the system's productivity, but the liveness characteristic of languid synchronous protocols is also unsuccessful as the feeble timing assumptions get contravened when vitriolic networks launch DoS attacks.

Scalability pertaining to the number of validator nodes is another challenge that comes with BFT-based protocols as the testing mechanism is not usually implemented post 20 nodes [19]. This shortcoming can be overcome by executing Algorand [20] that implements a system of random selection of a small-sized committee for every step of the consensus protocol to address scalability. This random selection is done through the mechanism of Verifiable Random Functions (VRF). Committee size is contingent on two constraints in Algorand:

i. $1/2g + b \leq Tstep.\tau step$
ii. $g > Tstep.\tau step$

Where

g = number of honest committee members;
b = number of malicious committee members;
T = number of votes required for consensus;
τ = expected committee size.

Furthermore, BFT-based consensus protocols are proficient in obscuring non-deterministic faults that eventuate at $f = (n-1)/3$ replicas, where

f = number of faulty nodes
n = number of total nodes

Proof of Work (PoW) and BFT-based consensus protocols differ largely on the basis of availability which is an important necessity in IoT systems. On one hand where PoW does not determine whether a certain unresolved transaction will be present in the next bloc or not, PBFT on the other turns out to be particularly exorbitant when it comes to message complexity. Hence the sustainability of a huge number of IoT systems should be the focus of any future solution that is based on blockchain and should also be in accordance with the wireless communication rules of the particular country.

Transaction validation rules, fault tolerance and transmission complexity are some of the aspects that need to be enhanced if consensus-based protocols are to be applied in IoT-based systems.

1.3.2 Transaction Validation Rules

Figure 1.6 represents the transaction verification and completion procedure in bitcoin. The working protocol for this functions on a specific set of regulations encompassing the authentication of transaction format and correct signatures and then followed by a mechanism that checks whether the specified transaction has been previously spent or not [21]. In comparison, Ethereum has a different process for transaction validation. As Figure 1.7 depicts, Ethereum verifies signatures, gas, nonce, account balance of sender's account and the format.

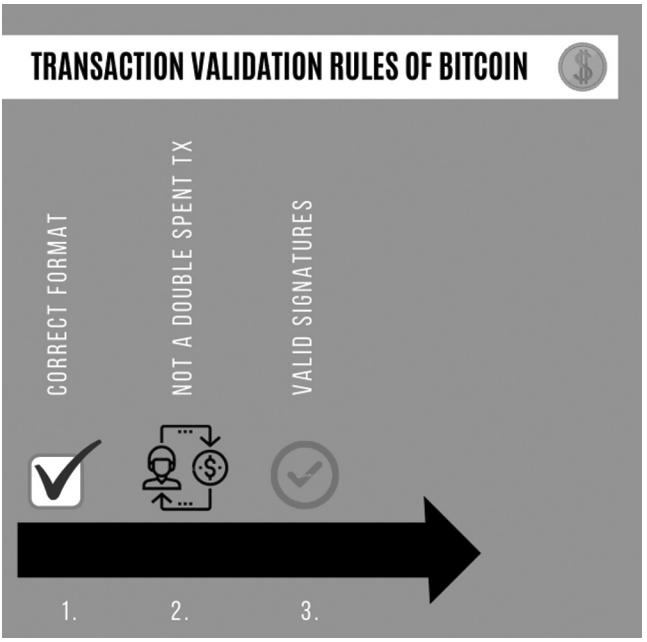

FIGURE 1.6 Transaction validation rules in Bitcoin.

Due to the vulnerability of IoT systems toward cyber attacks, it raises an important conundrum as to whether or not the present regulations for transaction verification of blockchain are compatible with the IoT system. This problem is further augmented due to the fact that IoT systems, for the most part, consist of heterogeneous devices and applications that send data in a distinct range of values. These devices being highly vulnerable can be infected even through generic malware attacks that would consequently also be used by a botnet for even more attacks. Hence, the transaction verification regulations of blockchain may not be appropriate for IoT systems.

1.3.3 Scalability Challenges

When it comes to discussing the challenges with respect to the scalability of integrating blockchain in IoT systems, two major issues arise—storage capacity and the inherent latency of blockchain. The scalability affects both the size and the consensus procedure. For instance, if the number of users increases it will directly result in the rise of transactions as well. Consequently, the consensus protocol affects the delay in transaction validation. These challenges are discussed at length in the following paragraphs of this chapter.

1.3.3.1 Storage Capacity

Typically, blockchain does not have the capacity to contain a huge amount of information, whereas a smart city IoT system containing hundreds and hundreds of end nodes has the ability to produce a large amount of data in a very small duration

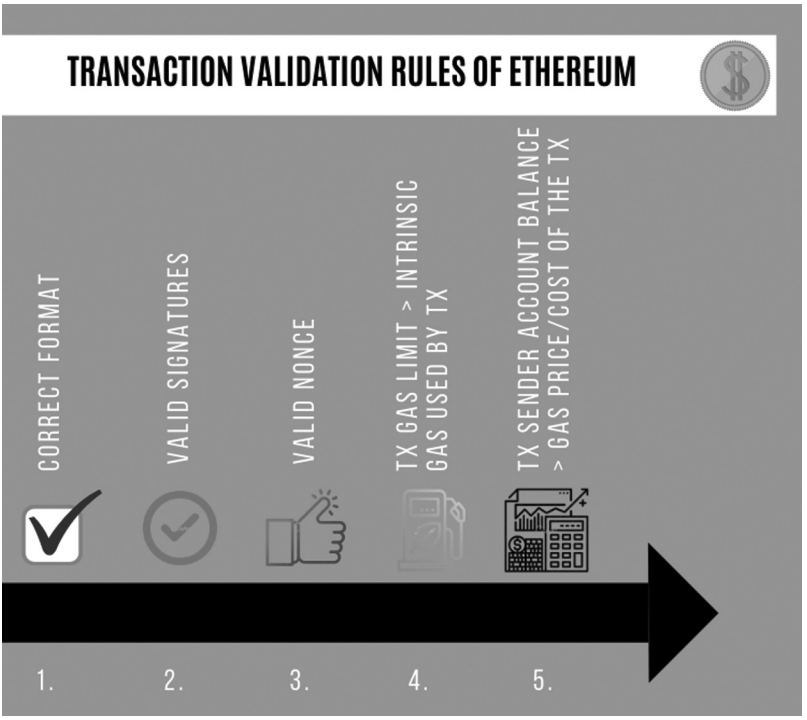

FIGURE 1.7 Transaction Validation Rules Ethereum.

of time which needs to be processed to extricate data for a multitude of uses. The integrability of IoT devices is further limited due to the necessity of storing the entire blockchain through the full and miner nodes. Furthermore, the impediments on resource-limited devices to perform as validator nodes is augmented with the perpetual expansion in blockchain's size which subsequently increases the storage necessities. The synchronization time rises as well, as each new user/device is added to the network. Hence it becomes extremely challenging to produce such a mechanism that encompasses both the constraint resources of IoT and the advantages of blockchain.

1.3.3.2 Inherent Latency Blockchain

The requirement for an enhancement in the transaction verification duration of real-time IoT systems like Industrial Control System (ICS), smart vehicles, Wireless Sensor Network (WSN), intelligent transportation systems, *et al.* without making concessions on its safety and efficiency has risen in demand.

For instance in the Proof of Work (PoW) based blockchain, the transaction verification duration is reduced if the block production duration lessens. However, a transaction needs to wait for more verifications to realize the identical strength of security because of the reduced complications in mining the block. Furthermore, a rise in the dissipation of computational resources is incurred due to the increase in the stability

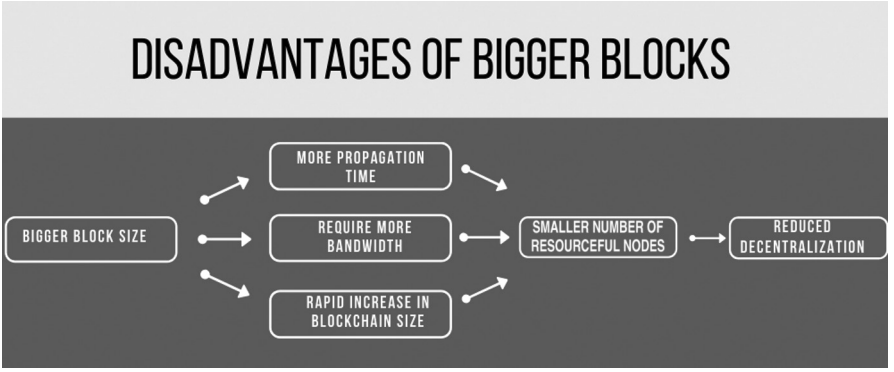

FIGURE 1.8 Disadvantages of Bigger Block.

of blocks. It is believed that the throughput of a bitcoin blockchain can be augmented if the block size compounds from 1 MB to 2 MB. However, it is the larger block that utilizes a larger duration of time to transmit in the network.

Figure 1.8 illustrates the disadvantages of implementing bigger blocks. Furthermore, the number of full nodes is influenced by the expansion in the block size as an increased amount of resources are hence necessitated to store the entire blockchain which consequently factors into a swift development of the blockchain size. To conclude, it can be said that there is a clear trade-off between the degree of reliability and execution efficacy. A distributed network will have performance issues and a centralized network will harbor trust issues.

1.3.4 IoT Device Integration Challenges

Even though only Ethereum and Hyperledger-Fabric are a few of the only blockchain techs that incorporate smart contracts and distributed applications, they have a major shortcoming vis-à-vis execution of smart contracts in an Ethereum Virtual Machine (eVM) does not transmit in a direct fashion with the rest of the world. Hence, we make use of the web3.js library as an interfacing mechanism. Consequently, a safe decentralized database is one of the useful utilizations of blockchain.

As the present situation is with regard to the threats in IoT devices as they can be undermined without much difficulty, the integrity of IoT systems will always remain a matter of concern. Furthermore, the data can be further compromised due to an infectious code implemented remotely or simply due to a software/hardware malfunction or even human interference. These errors are not determined by the system unless they are specifically tested for such kinds of failures, modifications or misconfigurations. At present, the sole accessible solution is Orcalize [22] which takes information from third-party sources like IPFS and WolframAlpha. The provision of a Proof-Of-Authentication is mandated to establish the authenticity of the data provided.

Unfortunately, Orcalize is not compatible with IoT devices and hence their integration becomes even more difficult. Therefore, the requirement of an additional client-interfacing software between blockchain and the IoT device will introduce more

computational and memory expenditure. Hence, a lot of attention needs to be paid to ensure that an IoT device can have a vast variety of interchanges with blockchain.

1.3.5 Protection of Devices against Malware and Content Execution Attacks

The protection of devices against malware and content execution attacks has a dual aspect to it—ransomware and malware. Ransomware, however, has minimal effect on a distributed ledger as the network contains the error-free copy of the ledger even though some of the nodes may get affected. On the other hand, malware has the capacity to infiltrate the network with counterfeit/unauthentic data through a compromised node. Since the sensors have situation-based data which is challenging to authenticate with older transactions as opposed to in bitcoin, it becomes extremely difficult for the nodes to verify any transaction/data. Henceforth, for the detection of malicious and counterfeit nodes, the existence of malware detection software is a necessity in such blockchain-based IoT systems.

1.3.6 Secure and Synchronized Software Updates

IoT devices and their applications continue to be in operation for an extended period of time due to their analytical functionalities with the absence of any software or firmware upgrades and hence are very prone to cyber attacks. Even though because of the localized and distributed framework of blockchain, at present, synchronized firmware and software updates cannot be assured, the need for such a mechanism is increasing day by day.

1.4 APPLICATION OF BLOCKCHAIN IN IOT SECTOR

1.4.1 Autonomous Decentralized Peer-to-Peer Telemetry

In 2015, the International Business Machines Corporation released the Proof of Concept (PoC) for a Decentralized Peer-to-Peer Telemetry System (DePT) that is autonomous in its functionality in order to utilize blockchain's ability to perform smart contracts on the verification of transactions [23].

The objective of DePT is to execute and administer a localized, distributed, safe, independent, expandable and powerful architecture for IoT that does not contain singular vulnerable failure functions. The suggested architecture makes use of the TeleHash protocol for peer-to-peer data transfer and BitTorrent as the mechanism for distributed sharing. This suggested system endeavors to solve several issues pertaining to the traditional IoT systems concerning privacy, failure points, safety regarding centralized entity and problems introduced due to human interference. An autonomous decentralized telemetry system also aims to proffer user and data protection, identification management and the peer-controlled access to data.

A major void that exists with regards to its implementation is that this system is a Proof of Concept (PoC) and hence it needs testing and development to determine its dependability pertaining to safety and functioning efficacy.

1.4.2 Blockchain-Enabled Security for Smart Cities

A multitude of challenges regarding the problems faced during data sharing from heterogeneous applications occurs due to the non-existence of a universal protocol for smart devices in a traditional environment. This further hampers their integration and the provision for cross-functionality characteristics. Examining the synopsis of a security system based on blockchain for reliable transmission among smart city units presented in Muthukkumarasamy and Biswas [24] states that smart cities aiming to provide a shared environment for secure transmission require integration of its devices with blockchain. Furthermore, an incorruptible log of transfers will be available for auditing purposes due to the use of blockchain in such a system.

At present, there does not seem to be a computational inclusive quantitative and qualitative analysis of blockchain-enabled smart city entities; however, it is quite ambiguous which platform, transaction technique or consensus protocol will be the most suitable for efficient implementation.

1.4.3 Blockchain-Enabled Smart Home Architecture

A safe, personal and lightweight framework for Smart Home Applications based on blockchain has been advocated by A. Dorri, S. Kanhere and R. Jurdak in [25] and [26]. What we need to understand here is that a Smart Home blockchain differs from a traditional Bitcoin blockchain in a multitude of ways. The owner operates the smart home blockchain alone as opposed to in bitcoin and hence, the owner has complete control over the transactions inside his Smart Home. Furthermore, it also proffers limited access to IoT data that guarantees information integrity, availability and confidentiality and also safeguards against DDoS threats. A blockchain-enabled Smart Home architecture intends to solve other challenges like the strenuous computations, latent transaction verification and power consumption through imitating Proof Of Work (PoW) in the process of block mining. The suggested framework makes use of cloud storage space to reduce the strain of memory necessities on smart home appliances.

There are a number of problems when it comes to the implementation of a Blockchain-enabled Smart Home. The distinguishing feature of blockchain is its distributed network but in a smart home environment, the Home-Miner or the owner solely has control over the entire network. This introduces a single juncture failure at both the Home-Miner level and the cloud storage space level. Secondly, the absence of a verification mechanism on a consensus basis as the home-miner has complete control. Furthermore, if the home-miner itself is malicious or corrupted, then the integrity of the transactions cannot be determined. Also, in this case, the home-miner determines if a new block will be added whereas, in the conventional blockchain, it is a consensus decision.

1.4.4 Blockchain-Based Self-Managed VaNeTs

In order to address the challenges posed by a centralized traditional Vehicle Ad-Hoc Network (VaNeT), such as the single juncture failure and vulnerability toward

attackers and reduced user privacy, Leiding [18] has advocated for a distributed Self-Managing VaNeT based on Ethereum Blockchain that has a challenge-response verification mechanism. The entire framework is run by appliances based on Ethereum that administer the regulations for proffering a multitude of services. The identification mechanism for every node is its Ethereum address. Each node makes a payment in ethers if it intends to use any Ethereum-based service which in turn becomes a funding mechanism for the network platform. This funding provides the necessary incentive for various merchants to continue manufacturing such applications and services based on Ethereum. Such an Ethereum account has the potential to make self-operating transactions; for insurance, registration and fines in case of violation of traffic rules.

A number of dilemmas are still unanswered pertaining to this suggested framework such as—What kind of data will be visible on the blockchain, Who will be mining the said block, What shall be the mechanism for V2V transmission and the inherent latency in it. An important point to be noted is that latency is an intrinsic characteristic of the blockchain technology but in traffic and road situations, real-time information is of paramount significance for nodes connected to a VaNeT.

1.4.5 Security and Privacy of Data

Nathan and Zyskind [27] propose a data management prototype for a distributed network that provides protection and safeguard measures on problems related to data proprietorship, transparency and auditability. Ethos is a bitcoin-based system for transmission of personal information manufactured by Viral Communications, MIT Media Lab [28]. Ethos's compatibility for its use in IoT systems is something that presently still needs evaluation. A distributed computational protocol named Enigma has also been developed with the purpose of preserving privacy [29]. Enigma further allows very limited access to the entire data by its nodes through the deployment of a multi-entity computation that has a secret-sharing validation protocol. This type of system has the added advantage of decentralized storage and reduced memory necessity for embedded devices.

For its efficacious execution in IoT systems, Enigma still necessitates analyses for the overhead transmission and computation. It is important that any solution for decentralized computation and safe data transmission are in accordance with the respective country's law for wireless communication since most of the IoT devices transmit through wireless media only. Even though such decentralized computational schemes seem quite efficacious, their productivity with respect to bandwidth efficiency still requires evaluation. In conclusion, any future data transmission and sharing systems based on blockchain should keep in mind these shortcomings.

1.5 CONCLUSION AND FUTURE SCOPE OF WORK

Technologies such as blockchain have disrupted the entire fintech market and even though it has created a lot of controversies, the technology is going to get more and more integrated into our lives. The advantages of integrating blockchain with IoT

should hence be assessed very carefully and with the utmost caution, because without determining its risks and applying it in situations where the costs do not overpower the improvements is an easy trap to fall into. This chapter summarizes the challenges that come with blockchain and IoT and hence collective work must be done in order to address these problems. We have also been able to identify where this technology has the potential to enhance IoT applications.

Furthermore, we have provided a feasibility check on using the blockchain technology with IoT appliances where existing frameworks have been analyzed, conditions for future solutions identified and the current scenario of the blockchain-IoT paradigm exhaustively addressed. Moreover, special caution has been put on the need for future solutions to be contingent with the respective country's laws. This integration of technologies should hence become part of the government's framework which would subsequently speed up interactions with citizens as well.

The dual aspect of data integrity and framework supervision is of utmost importance. The privacy of users and security concerns affect how the citizens will perceive this integration. The challenges of storage space, scalability and consensus protocols will play an integral role in how this process moves forward. This integration of IoT devices with blockchain technology is bound to exponentially increase the applications and use of blockchain and establish its prominence at a similar level as in the current fiduciary money market.

REFERENCES

1. Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. "Internet Of Things: A Survey On Enabling Technologies, Protocols, and Applications". *IEEE Communications Surveys & Tutorials* 17 (4): 2347–2376. doi:10.1109/comst.2015.2444095.
2. R. van Kranenburg. *The Internet of Things: A Critique of Ambient Technol- ogy and the All-Seeing Network of RFID*. Amsterdam, The Netherlands: Institute of Network Cultures, 2007.
3. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, *IEEE Communications Surveys & Tutorials*, 17 (4) (2015) 2347–2376.
4. S. A. Kumar, T. Vealey, H. Srivastava, Security in Internet of Things: Challenges, Solutions and Future Directions, in: Proceedings of the IEEE 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5772–5781.
5. M. Khari, M. Kumar, S. Vij, P. Pandey, Vaishali, Internet of Things: Proposed Security Aspects for Digitizing the World, in: Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2165–2170.
6. R. Khan, S. U. Khan, R. Zaheer, S. Khan, Future Internet: The Internet Of Things Architecture, Possible Applications and Key Challenges, in: Proceedings of the IEEE 10th International Conference on Frontiers of Information Technology (FIT), 2012, pp. 257–260.
7. T. Qiu, N. Chen, K. Li, M. Atiquzzaman, W. Zhao, How Can Heterogeneous Internet of Things Build Our Future: A Survey, IEEE Communications Surveys & Tutorials.

8. Editors, MIT. 2019. "Explainer: What Is A Blockchain?". *MIT Technology Review*. www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/.
9. A. Back, "Hashcash – A Denial of Service Counter- Measure," 2002, available at: www.hashcash.org/papers/hashcash.pdf
10. D. Eastlake, 3rd and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)," RFC 6234 (Informational), May 2011, available at: www.ietf.org/rfc/rfc6234.txt.
11. Choi, J., Li, S., Wang, X., Ha, J., 2012. A General Distributed Consensus Algorithm For Wireless Sensor Networks. Paper presented at the Wireless Advanced (WiAd), 2012
12. Fielding, R. and Taylor, R. (2002). Principled Design of the Modern Web Architecture. *ACM Transactions on Internet Technology*, 2(2), pp.115–150.
13. Kranenburg, R.V., Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., Ratto, M., 2011. The Internet of Things. Paper presented at the 1st Berlin Symposium on Internet and Society (Versión electrónica). Consultado el.
14. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A., 2006. M2ap: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags. Ubiquitous Intelligence and Computing. Springer, Heidelberg, pp. 912923.
15. Hernandez-Castro, J.C., Tapiador, J.M.E., Peris-Lopez, P., Li, T., Quisquater, J.-J., 2013. Cryptanalysis of the SASI Ultra-Light Weight RFID Authentication Protocol. arxiv.
16. I. Makhdoom, M. Abolhasan, H. Abbas and W. Ni, Blockchain's adoption in IoT: The challenges, and a way forward in: Journal of Network and Computer Applications, 2019, vol. 125, pp. 251-279.
17. EconoTimes, Blockchain project antshares explains reasons for choosing dbft over pow and pos (2017)
18. A. Miller, Y. Xia, K. Croman, E. Shi, D. Song, The Honey Badger of BFT Protocols, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, ACM, 2016, pp. 31–42.
19. M. Vukolic, The Quest for Scalable Blockchain Fabric: Proof-of-work vs. BFT Replication, in: Proceedings of the International Workshop on Open Problems in Network Security, Springer, 2015, pp. 112–125.
20. Y. Gilad, R. Hemo, S. Micali, G. Vlachos, N. Zeldovich, Algorand: Scaling Byzantine Agreements for Cryptocurrencies, in: Proceedings of the 26th Symposium on Operating Systems Principles, ACM, 2017, pp. 51–68.
21. V. Buterin, et al., A next-generation smart contract and decentralized application platform, white paper.
22. Oraclize Is Now Provable Things". 2019. *Oraclize.It*. www.oraclize.it.
23. 2019.*Cryptonomics.Show*.https://cryptonomics.show/wp-content/uploads/2018/08/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.pdf.
24. K. Biswas, V. Muthukkumarasamy, Securing smart cities using blockchain technology, in: Proceedings of the IEEE 14th International Conference on Smart City High Performance Computing and Communications, 2016, pp. 1392–1393.
25. A. Dorri, S. S. Kanhere, R. Jurdak, Blockchain in internet of things: Challenges and solutions, arXiv preprint arXiv:1608.05187.
26. A. Dorri, S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IOT Security and Privacy: The Case Study of a Smart Home, in: Proceedings of the IEEE 2nd Workshop on security, privacy, and trust in the Internet of things (PERCOM), Hawaii, USA, 2017.

27. G. Zyskind, O. Nathan, et al., Decentralizing Privacy: Using Blockchain to Protect Personal Data, in: Proceedings of the IEEE Security and Privacy Workshops (SPW), 2015, pp. 180–184.
28. MIT-Media-Lab, Ethos (2014. Last accessed 26 July 2018). URL http://viral.media.mit.edu/projects/ethos/
29. G. Zyskind, O. Nathan, A. Pentland, Enigma: Decentralized Computation Platform with Guaranteed Privacy, CoRR abs/1506.03471.