Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Review:

Cloud-based vs. blockchain-based IoT: a comparative survey and way forward*

Raheel Ahmed MEMON[†1,2], Jian Ping LI[†‡1], Junaid AHMED[3],
Muhammad Irshad NAZEER[2], Muhammad ISMAIL[2], Khursheed ALI[2]

[1]*School of Computer Science and Technology, University of Electronic Science and Technology of China, Chengdu 610031, China*
[2]*Department of Computer Science, Sukkur IBA University, Sukkur 65200, Pakistan*
[3]*School of Automation, University of Electronic Science and Technology of China, Chengdu 610031, China*
[†]E-mail: raheelmemon@iba-suk.edu.pk; jpli2222@uestc.edu.cn

Received May 30, 2018; Revision accepted Apr. 7, 2019; Crosschecked Mar. 30, 2020

Abstract: The Internet of Things (IoT) has been evolving for more than a decade. Technological advancements have increased its popularity, but concerns and risks related to IoT are growing considerably along with the increased number of connected devices. In 2013, a new cryptography-based infrastructure called blockchain emerged with the potential to replace the existing cloud-based infrastructure of IoT through decentralization. In this article, we provide a taxonomy of the challenges in the current IoT infrastructure, and a literature survey with a taxonomy of the issues to expect in the future of the IoT after adopting blockchain as an infrastructure. The two architectures are compared based on their strengths and weaknesses. Then a brief survey of ongoing key research activities in blockchain is presented, which will have considerable impact on overcoming the challenges encountered in the applicability of blockchain in IoT. Finally, considering the challenges and issues in both infrastructures and the latest research activities, we propose a high-level hybrid IoT approach that uses the cloud, edge/fog, and blockchain together to avoid the limitations of each infrastructure.

Key words: Internet of Things (IoT); Cloud; Blockchain; Data center; Taxonomy
https://doi.org/10.1631/FITEE.1800343 **CLC number:** TP393

1 Introduction

In considering the technologies of tomorrow, the Internet of Things (IoT) comes readily to mind. After 1995, it was the Internet that began to revolutionize several aspects of the modern world by digitizing mailing, banking, education, government systems, and business trends. Similarly, IoT has started to digitize everything around us, and it is expected that there will be 20.4 billion connected devices by 2020 (van der Meulen, 2017). In this case, technology will not discriminate by digitizing only a selected group of things; instead, a ubiquitous technological revolution will take place that connects everything to the Internet, even an automatic electric popup toaster, which has, in fact, not been upgraded since 1921 (Strite, 1920). The advantage of IoT is its barrier-free communication, where heterogeneous elements can be monitored and controlled remotely from any location. Currently, several smart devices like smart fitness shoes, surveillance cameras, home appliances to smart grids, industrial equipment, and traffic systems are connected and can be monitored or controlled remotely (Sun et al., 2017). The cloud has played a large role in providing such communication and the ability to

‡ Corresponding author
* Project supported by the National Natural Science Foundation of China (No. 61370073), the National High-Tech R&D Program of China (No. 2007AA01Z423), and the Science and Technology Department of Sichuan Province, China
ORCID: Raheel Ahmed MEMON, https://orcid.org/0000-0003-1206-3837; Jian Ping LI, https://orcid.org/0000-0003-2192-1450

communicate in a seamless fashion; the cloud has been around for a long time, but started to gain popularity when Amazon first announced its elastic computer cloud (EC2) in 2006 (Amazon, 2006).

In this article, we survey cloud- and blockchain-based IoT (referred to herein as CB-IoT and BB-IoT, respectively) to elucidate the underlying challenges involved in making a robust and trustworthy IoT. In the past couple of years, the cloud-based infrastructure of IoT has generated several debates which remain unresolved; these cover the losses and risks incurred due to various types of attacks, security issues, latency issues, energy ingestion, cost concerns, lack of payment methods, and scalability. In response to these challenges, huge effort has been made and some remarkable changes were implemented, such as IPv6 to improve scalability (Singh D et al., 2014) and fog clouds to reduce the burden on the main cloud and make computation power as local as possible (Cisco, 2015). Nevertheless, over time the risk of attack has also increased, and issues of data leakage, privacy, management, hardware upgrades, increasing number of devices, requirements of high bandwidth, energy consumption, unknown neighbor discovery, buffer failures, energy drain of devices, authentication, sinkholes, long communication paths, jamming, handling big data, payments, and trusted transactions persist because the cloud, as an intermediary itself, is a bottleneck for all processes, and a single point of failure (Granjal et al., 2015; Sicari et al., 2015; Wang YF et al., 2015; Yi et al., 2015; Li DR et al., 2017; Khan and Salah, 2018).

The purpose of the cloud data center in IoT was simply to provide services to end users in four basic service modes: public, private, community, and hybrid. However, the working paradigm has shifted and a user now has to request services from third-party providers such as cloud service providers (CSPs), attribute authorities (AAs), and third-party auditors (TPAs) (Singh I and Lee, 2018). In the current scenario, cloud services are more powerful than a user, and have more control over the user's data, which has led to several vulnerabilities such as cyberattacks and misuse of information in recent years, and thus clouds, CSPs, AAs, and TPAs are not considered to be reliable and trusted entities (Hur and Noh, 2011; Li JW et al., 2012; Singh I and Lee, 2018).

In the past few years, IoT has been running behind its predictions, and according to some new statements and literature surveys, there have been several predictions for the year 2020 (Sagiroglu and Sinanc, 2013; Juniper Research, 2015; Manral, 2015; Garai et al., 2016; Kshetri, 2017a; Marinakis et al., 2017; Moar, 2017; Qi et al., 2017; van der Meulen, 2017; Yang et al., 2017; Worldometer, 2018). Based on our survey, Fig. 1 shows the picture today and tomorrow for IoT, where the growth of IoT is predicted to be much more than what we have today; the number of devices and the average number of sensors per device will be almost twice what they are today (Garai et al., 2016; Marinakis et al., 2017; van der Meulen, 2017), and hardware and software updates will be three times what they are today (Sagiroglu and Sinanc, 2013). The data generated per year is accelerating much more rapidly, and by the year 2020, it is expected to be four times more than today (Yang et al., 2017), and it will eventually influence the bandwidth requirements; thus, the bandwidth demand will also increase by three times over today (Kshetri, 2017a). The astounding figure though is the prediction of losses and cyberattacks, which are predicted to be five times more than today (Juniper Research, 2015; Manral, 2015; Moar, 2017).

Recently, the launch of Bitcoin (a digital cryptographic currency) has achieved huge success in financial services technology with a remarkable growth rate in just a couple of years; the popularity of Bitcoin is because of its robust and unbreakable consensus on the underlying algorithm called blockchain (Kshetri, 2017a). Blockchain is based on a cryptographic signature key with an open ledger of transactions occurring in Bitcoin. The copy of the open ledger, also known as a distributed ledger, is shared among everyone in the network. Verification of a transaction is accomplished by a consensus algorithm such as proof-of-work (PoW). Breaking the consensus by tampering or collision is an extremely difficult or impossible task (Qi et al., 2017).

Nowadays, blockchain applications are not limited to financial services technology and digital cryptocurrencies. The IoT industry is also motivated to discover the potential of blockchain and several academic and industrial research groups have taken the initiative of adopting blockchain as a core technology. In September 2017, SAP with nine other companies announced they were making blockchain

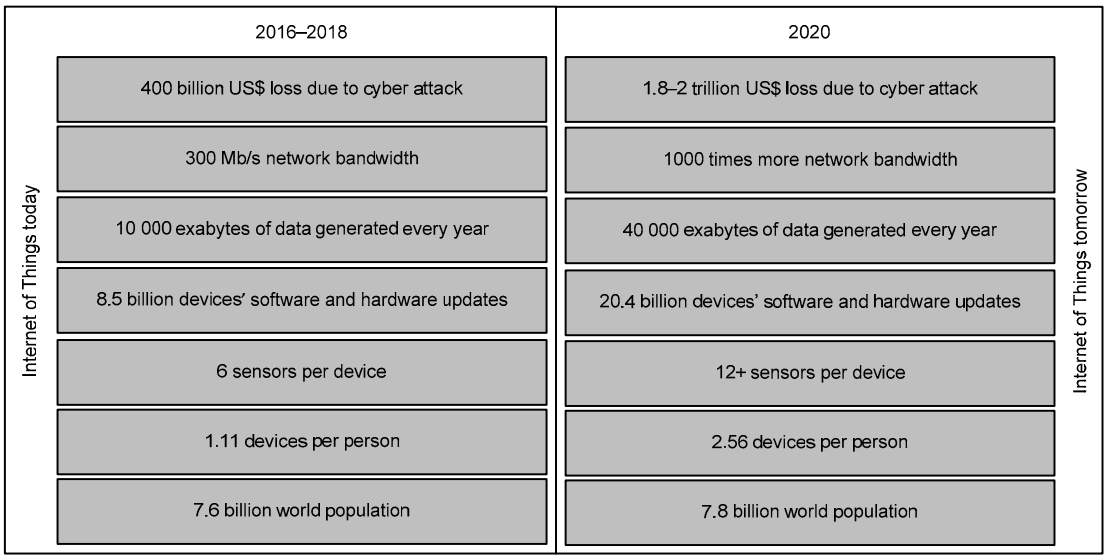

Fig. 1 IoT today and tomorrow

an integral part of IoT (SAP, 2017). IBM provides blockchain-based tracking for high-value items across their supply chain (https://www.ibm.com/supply-chain); the IBM Watson IoT platform provides the infrastructure of distributed peers that works to validate the transaction that has taken place by secure contracts (https://www.ibm.com/internet-of-things/trending/blockchain). Other startups have the goals of using blockchain to improve trust in the supply chain and creating business models to eliminate the need of an intermediary (Kshetri, 2017a); these include a filament initiated blockchain-based autonomous mesh network to control water flow and waste over an agricultural field called wireless sensor devices or taps (Kshetri, 2017a). Another group of large companies initiated a collaborative group effort to explore the potential of blockchain for IoT devices, applications, and networks (Brown, 2017). Blockchain has evolved with many good features resolving the issues of CB-IoT via a secure, transparent, and trusted infrastructure (Khan and Salah, 2018). It also has the potential to reduce or eliminate other issues such as a single point of failure and a central processing location that acts as a bottleneck. Because blockchain is now merging with IoT, it also has several new open research challenges, such as privacy (because of its transparency in nature) and latency (because of the time-consuming verification of transactions), flexibility in adopting new changes, and single security solution (cryptographic signature).

In this article, we review both architectures from an IoT perspective, and study the issues referenced in the literature; we will also discuss the recent research efforts to solve these problems and issues, and finally propose a reference architecture as a solution, which may be one of the possible solutions to resolve the existing issues in future research. Our main contributions can be summarized as follows: (1) cloud-based IoT: a taxonomy of issues; (2) blockchain-based IoT: a taxonomy of issues; (3) directions to pursue to overcome these challenges; (4) current key research projects; (5) possible solutions as a way forward.

2 Literature survey

2.1 Cloud-based Internet of Things (CB-IoT)

2.1.1 Overview and advantages of CB-IoT

Cloud computing or the "cloud," provides a tremendous amount of computational and storage resources with a virtualization-enabled environment, where any application or request can be processed using an infinite number of processors in a cloud center. In a nutshell, the cloud has evolved to facilitate the ability of devices to have low power, low computation, and small storage; because IoT devices are small with limited computational, storage, and battery power, the devices avail themselves of services from a third-party cloud to complete their tasks effortlessly (Formisano et al., 2015). The cloud infrastructure has

several advantages including pay-as-you go (PAYG), with no concerns for infrastructure, capacity, and computing resources, and an easier deployment of applications (Armbrust et al., 2010). The cloud platform has several types of services to offer, with the key services being software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). In service module SaaS, the multiple instances of applications are delivered to support the large base of customers simultaneously; these are also referred to as application service providers (ASPs) (Aulbach et al., 2008), and examples of SaaS are Google Apps, Microsoft Office 365, and GT Nexus. PaaS offers developers a readily available environment to develop applications, and it provides a complete and updated platform to develop, test, and deploy the created applications over the cloud in a matter of minutes (Rimal et al., 2009), examples of this type of service being AWS Elastic Beanstalk, Cloud Foundry, Google AppEngine, and OrangeScape. IaaS provides computing, storage, and database services as provisioned resources; it allows the scaling of computing and storage in real time on a per-usage basis (Rimal et al., 2009); examples of IaaS are Amazon Elastic Compute Cloud, Dyn DNS, HP Cloud Service, iland, and Joyent.

After the evolution of cost-effective sensor-based processor systems empowered with communication technologies emerged, the new technological revolution of the IoT came into existence (Ray, 2016). IoT aims to provide direct machine-to-machine communication and bring these online over the Internet to become autonomous, intelligent, and self-organizing devices (Whitmore et al., 2015). Currently, IoT is gaining tremendous interest from business, government, medicine and healthcare, agriculture, mobile network providers, equipment vendors, device manufacturers, and research agencies (Qian and Zhang, 2010; Zhao JC et al., 2010; Foschini et al., 2011; Zhao W et al., 2011). To enable smooth interoperability between devices, the cloud infrastructure provides services as a middleware IoT platform over the Internet. There are several cloud platform service providers such as Amazon Web Services (AWS), GE Predix, Google Cloud IoT, Microsoft Azure IoT Suite, IBM Watson, and Salesforce IoT Cloud, which are considered the most reputable (Ning and Liu, 2015; Jagdeep and Meghna, 2017).

2.1.2 Limitations of CB-IoT

Besides its advantages, in the past decade the cloud infrastructure has also been singled out for a number of issues (Aazam et al., 2014). There are four basic building blocks in the existing IoT: things, gateways, network, and the cloud (Banafa, 2017). We consider the network and gateways to be part of the network infrastructure and present the underlying issues on the three other layers of CB-IoT, which are things, network infrastructure, and cloud infrastructure (Fig. 2).

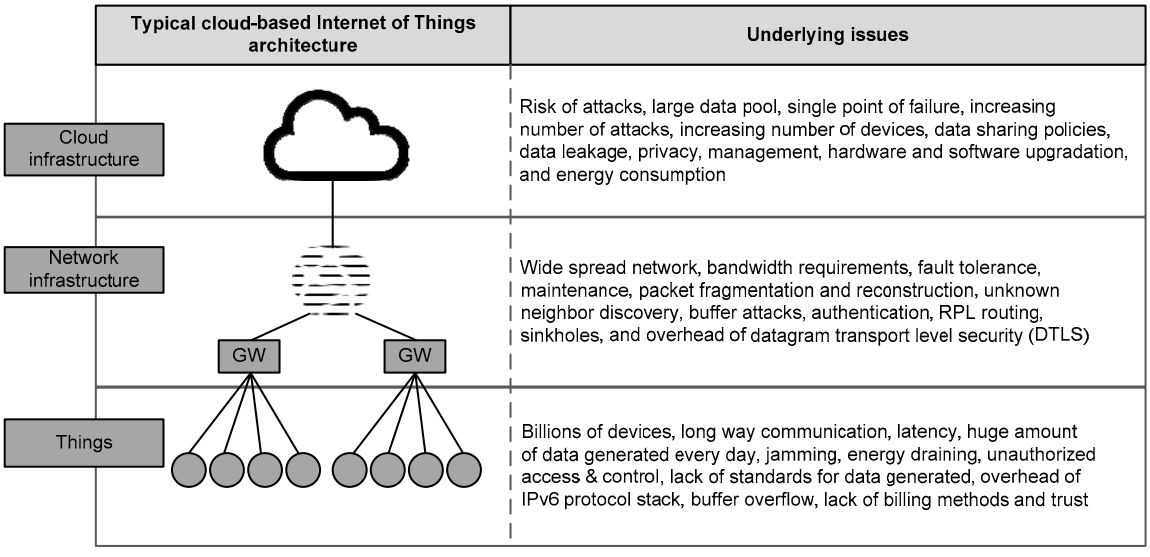

Fig. 2 Issues in a typical cloud-based IoT

Each layer has a number of issues related to historical losses, risks in the future, fear of attack, failure of timely responses, security issues between things and the cloud and within the cloud, data leaks, scalability, power consumption, responses and latency involved in real-time and non-real-time systems, cost, bandwidth, maintenance, trust, transactions, and billing. In this paper we present a taxonomy of issues in CB-IoT (Fig. 3) to categorically define the issues in the cloud infrastructure.

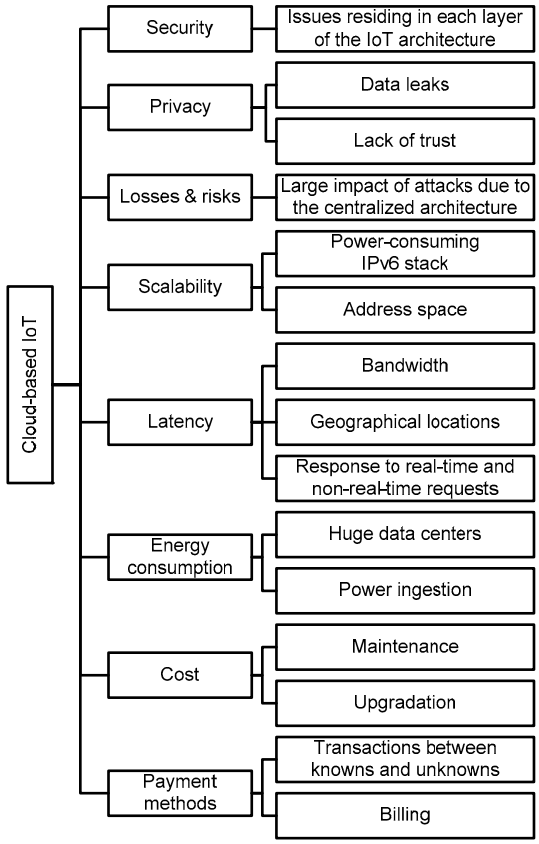

Fig. 3 Taxonomy of issues in cloud-based Internet of Things (CB-IoT)

1. Security

Security is foremost of all the issues in the current IoT. We generally categorize security issues according to the four layers of the IoT architecture, namely the perception layer, transport layer, service layer, and application layer. The literature on security issues of the cloud infrastructure is available for different viewpoints, such as security issues on the three tier IoT architecture, security issues in preserving privacy, trust management, data security, network security, and issues raised by intrusion at middleware (Granjal et al., 2015; Sicari et al., 2015; Wang YF et al., 2015; Yi et al., 2015; Khan and Salah, 2018). We define the underlying issues for architecture-level security, which considers not only the three layers but also keeps track of the "service layer" security issues that reside in the clouds and create opportunities for vulnerabilities such as multiple distributed-denial-of-service (DDoS) attacks in the case of Dyn, as discussed in the next section on losses and risks.

Perception layer: This layer is concerned with sensor- and actuator-level security (physical objects), from which a bad configuration can be initiated to communicate with the aim of misleading the user about the functionalities of IoT; there is also a lack of a standard format for data generation. The security threats at the perception layer can be jamming, energy drains, unauthorized access and control mechanisms, and Sybil attacks (Noubir and Lin, 2003; Xu et al., 2005; Chen et al., 2007; Xiao et al., 2009; Bhattasali and Chaki, 2011; Hong et al., 2013; Chae et al., 2014; Khan and Salah, 2018; Wang WB and Fan, 2018).

Transport layer: This layer is concerned with end-to-end transportation. It may suffer from fragmentation of packets, unverified neighbor inclusion in the network, reserve memory attacks by repeatedly sending garbage packets, depletion of resources, overhead of datagram transport level security (DTLS), and malicious nodes controlling the network. Threats like duplication, unknown neighbor discovery, buffer attacks, authentication, RPL (routing protocol for low-power and lossy networks) routing, and sinkholes are common flaws at the transport layer (Kim, 2008; Riaz et al., 2009; Brachmann et al., 2011; Dvir et al., 2011; Weekly and Pister, 2012; Granjal et al., 2013a; Hummen et al., 2013; Mahalle et al., 2013; Ahmed and Ko, 2016; Khan and Salah, 2018).

Service layer: This layer is concerned with services. Cloud-level security issues include server attacks, authenticated and authorized access, architecture of the cloud, data leakage, delay, location, data sharing policy, encryption, and increasing load. This may lead to threats like DoS (denial of service or distributed denial of service) attacks, access control, data vulnerabilities during processing and internal transmission, encapsulation, volume, velocity, and veracity (Soubra, 2012; Singh J et al., 2016; Henze et al., 2017; Zhou et al., 2017).

Application layer: This layer is concerned with the device application. Interfaces such as web, mobile, and machines are vulnerable and can have large impact on privacy, as well as software and firmware updates. Problems including multicast support in CoAP with IoT, interfacing, application and firmware updates, and communication in diverse environments are persistent (Conzon et al., 2012; Sethi et al., 2012; Granjal et al., 2013b; Liu et al., 2014; Khan and Salah, 2018).

2. Privacy

Confidentiality of data is important and is one of the main reasons for the lack of trust in cloud environments (Li DR et al., 2017). Due to a history of data leaks, privacy concerns have had a serious impact on the cloud in recent years, especially due to the lack of privacy protection and authentication mechanisms (Stergiou et al., 2018). Cloud storage and processing are usually spread over multiple locations, which results in privacy leaks. In mobile applications, there are several nefarious ways to collect personal data, including contacts, media, hobbies, and locations, which are common threats now for normal users (Mollah et al., 2017).

3. Losses and risks

IoT is all about a huge number of devices that are tiny, simple, and inexpensive with little processing and small operating systems, and thus they cannot afford to have sophisticated security approaches. On 21st October 2016, a multiple DDoS attack hits popular services like Twitter, Netflix, *New York Times*, and PayPal across the United States by targeting the domain name system (DNS) provider Dyn (Hilton, 2016). The current IoT model is a centralized broker communication one, also known as a client/server model, where the cloud works as a server and provides intermediary services for authentication and identification of devices. Each communication carries through all of the levels of the CB-IoT infrastructure as shown in Fig. 2, even if the devices are only a few feet distant from each other. With the massive growth in IoT devices, a centralized cloud service will remain a bottleneck and point of failure that can disrupt an entire IoT communication network (Banafa, 2017).

It is unavoidable that with the emergence of IoT, new vulnerable entry points would also emerge, and as the number of connected devices increases, new cyber threats will also arise. Ingra Beale, Chief Executive Officer of Lloyd's, a British insurance company specializing in mitigating risk, states that "Lloyd's estimates that cyber-attacks cost the business as much as 400 billion US dollars a year" (Manral, 2015). Juniper predicts that business losses due to cybercrime will grow every year, and it will be over 2 trillion US dollars by 2021 (Juniper Research, 2015; Moar, 2017). Thus, not only cost but also the risks to privacy are issues that are a large constraint in the evolution of IoT.

4. Scalability

The increasing numbers of sensors and actuators in different sectors of the industrial deployment of IoT have affected the challenge of scalability; thus, industry and cloud hosting services are interested in scalable solutions for upcoming Internet technologies (Bellavista and Zanni, 2016). The issues related to the address space are the main concerns in producing scalable solutions for IoT. IPv6 is considered a key enabler technology for address space issues. It is a 16-byte address space with 2^{128} (about 3.4×10^{38}) addresses (Singh D et al., 2014). Yet, IoT applications are small in memory and computation power, so running them over IPv6 requires confirmation of device communication on the IEEE 802.154 standards, in which packet fragmentation is carried out (Hummen et al., 2013). The reconstruction of packet fragments on 6LoWPAN may give rise to issues like depletion of resources, buffer overflow, and even device restarts (Kim, 2008).

5. Latency

Faster response is the key requirement in several critical fields of IoT such as smart cities, autonomous vehicles, traffic management, and e-healthcare, as they are considered real-time systems. These systems are time critical and should be able to react rapidly. However, the convergence of the cloud in IoT has raised latency issues due to three main reasons: first, there are an increasing number of connected devices; second, there is distribution of nodes across widespread geographical locations; third, there is limited bandwidth. It is due to these limitations that the cloud is considered a bottleneck. The cause of the issues is the long distance of the communication, and the scheduling and processing of the incoming stream from different locations (Bonomi et al., 2012). According to one survey, the number of connected devices is going to be 20.4 billion by 2020 (van der

Meulen, 2017), Furthermore, 10 000 exabytes of digital data were generated in the year 2015, and the explosion of data generated is expected to be even greater in 2020, and according to the literature, it is going to surpass 40 000 exabytes of digital data by 2020 (Yang et al., 2017). Thus, centralized IoT or CB-IoT is not sufficiently capable of meeting the needs of the upcoming tsunami of IoT, where every bit on earth desires a response in real time.

6. Energy consumption

The high energy ingestion of huge data centers is a big research challenge: cloud data centers consume high amounts of electricity and leave a carbon footprint in the ecosystem, making data centers responsible for 2% of the overall global CO_2 emissions in the environment (Khosravi and Buyya, 2018). There have been several research projects working to reduce this energy consumption, including the GreenSlot Scheduler which works on a prediction algorithm that suspends batch jobs in the absence of solar energy (Goiri et al., 2011a). The free lunch architecture migrates virtual machines (VMs) from one data center to another with minimal downtime. This migration is done to minimize the cost of electric power using a site that is already working on renewable energy (Akoush et al., 2011). Data center intelligent placement is used to select the best location for data centers (Goiri et al., 2011b). Several other projects have been proposed in the last decade (Khosravi and Buyya, 2018), but high energy consumption is still one of the big challenges of a cloud-based infrastructure.

7. Cost

Handling the growth of IoT is also a big challenge: 1000 times more network bandwidth will be required to support the technological revolution by the year 2020 (Kshetri, 2017a). In an ever-expanding digital world, from the manufacturer's point of view, high maintenance costs, frequent software and hardware updates for billions of devices, and security concerns are the most costly segments of a centralized model. From the consumer's point of view, the demand is for inexpensive solutions, faster response, trust, and security through transparency (Christidis and Devetsikiotis, 2016).

8. Payments and billing

Imagining IoT without a digitally integrated payment system would be to envision an unfinished model in the current technological era. To the best of our knowledge, IoT lacks billing methods; while a few types of micropayment methods have been proposed, unfortunately none of them fit the needs of IoT well (Wilusz and Rykowski, 2013). Well-known micropayment systems are Amazon flexible payment service and GeldKarte (Stormer and Meier, 2012), but these systems are prepaid types of payment systems, and are limited to aggregating multiple payments into a single payment, where micropayments are merged and paid as a single macropayment (Wilusz and Rykowski, 2013). This solution is not suitable in an IoT environment because of two reasons: first, shopping trends can be irregular and incidental; second, in a centralized payment system, keeping track of where service providers or an intermediary stores each transaction leads to a system that can never be trusted to carry out financial transactions (Sherif, 2016).

2.2 Blockchain-based Internet of Things (BB-IoT)

Blockchain is a digital ledger technology, first introduced by Satoshi Nakamoto in 2008 (Nakamoto, 2008), who later in 2009 presented its implementation as the underlying engine of Bitcoin, the first digital currency. Bitcoin is a crypto/digital currency based on a peer-to-peer network of nodes. In Bitcoin, financial transactions of digital currency take place directly (one-to-one) using the cryptographic signature as an identifier without an intermediary like an admin (bank, agent, or any central repository) (Nakamoto, 2008; Brito and Castillo, 2013; Yao, 2018). In the last 10 years, blockchain has proven to be the only robust architecture for a distributed system that has never been hacked or faced any downtime (Wang J et al., 2017). Since then, several digital currencies have been launched subsequently, among which Ether, Litecoin, Nxt, Ripple, and Peercoin are only a few (Nakano, 2018). The scope of blockchain is not limited to digital currencies; in fact, it is receiving a great deal of attention in several other fields, as provided in a scoping survey of blockchain showing that it has also been applied to revolutionize several different fields like medicine, software engineering, IoT, and many others (Li Y et al., 2018).

2.2.1 Technical overview of blockchain

In blockchain, a block is a container data structure that assembles the transactions from the entire network for a limited size within a limited time frame.

Blockchain can be considered a linked list type of data structure where each block has a hash pointer pointing to the previous block except the genesis block, which is the first block in the chain with no previous reference (Bahga and Madisetti, 2016). Each block contains metadata, the hash of the block, hash of the previous block, timestamp, and nonce (Fig. 4). Every new block is signed with a time consuming cryptographic hash signature, which is solved by the mining operation. If the mining process goes successful and a new block qualifies to find the exact nonce, then the data block is broadcasted over to the network and a copy is added to the local chain of the miner; however, it is ignored if getting failed. In mining a block, the use of the hash signature is to verify and validate the digest of inherited information by reproducing the nonce. The difficulty of the mining operation for reproducing the nonce therefore lies in maintaining the time interval in between the block generation process; in case of Bitcoin, it is revised every two weeks to maintain an interval of 10 min (Memon et al., 2019a). However, the nonce itself is challenge of an arbitrary number called "number used once" or "number once," which is used with the timestamp to add another level of difficulty. Also, note that in digital currencies, the chances of double spending (an issue with the banking sector) are eliminated by use of timestamp (Nakamoto, 2008).

2.2.2 Distributed consensus algorithms

The consensus algorithm is used to reach a decision to add a new block to the distributed ledger, and there are several variations of consensus algorithms, but they all fall into two categories, proof-of-work (PoW) and proof-of-stake (PoS). PoW was first given by Castro and Liskov (2002). Later, it was proposed to eliminate the double spending problem from the backbone of blockchain, where a distributed consensus protocol reaches an agreement by mining, which involves the majority of honest nodes (51% of nodes from the whole network) (Bahga and Madisetti, 2016); there are miners in the network who resolve the complex mathematical puzzles and come to a consensus. Miners are nodes in the network who compete for performing the complex calculations faster; the one that wins receives some incentives to perform that task; the produced block is then verified by other miners for validity (Bahga and Madisetti, 2016). PoW has some well-known issues, including high energy consumption and a need for high computation power; thus, only a number of selected nodes with high computation power can participate in the mining process. These limitations eventually lead to a decrease in the number of miners and also a decrease of the difficulty level of mathematical computation of the system, so the idea of decentralization moves in the opposite direction of that scenario (Thakur, 2017).

In contrast, there is PoS, where instead of racing through the mining job to win the reward, a miner is chosen randomly from the mining pool to solve the mathematical puzzle. If mining is effective, the miner obtains a reward for the stake, and if it fails, another miner is chosen from the pool (Seibold and Samman, 2016). The main advantages of PoS are that it has a simple mathematical puzzle, requires less energy and less computation, and is more decentralized to beat the 51% chance of attack (Seibold and Samman, 2016).

Considering the crypto-secure, transparent, and distributed ledger properties of blockchain, it has begun to gain popularity in the IoT industry as a potential candidate technology to further strengthen IoT from the threats of the future. The Trusted IoT Alliance, a consortium of companies like IBM Watson,

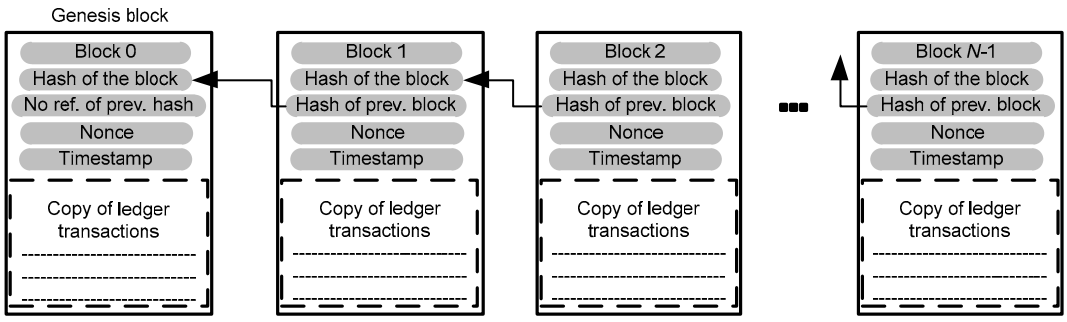

Fig. 4 Blockchain distributed ledger technology

Samsung, Cisco, Bosch, BNY Mellon, Foxconn, Gemalto, bitSE, Chronicled, Ledger, Consensys (Consensus Systems), IOTA, and many others, is heavily investing in blockchain to build an IoT ecosystem that will be secure, interoperable, and scalable with the ability to make fearless transactions of trillions of dollars (https://www.iiconsortium.org/; Kshetri, 2017b). Some startups like Slock.it, FILAMENT, CHRONICLED, and Ambisafe are also progressing towards the same goal (Brown, 2017; https://www.ambisafe.co/; https://slock.it/). On the other hand, two notable distributed ledger technology (DLT) frameworks, Ethereum and Hyperledger Fabric, have come into play to strengthen blockchain in multiple fields of IoT (Underwood, 2016).

2.2.3 Blockchain-based frameworks

Ethereum was designed by Buterin (2013) and it is an open-source blockchain-based framework to be used with the help of smart contracts for building decentralized applications, also known as DApps for creating peer-to-peer exchanges (Warren and Bandeali, 2017); currently, it supports 10 000 contracts, which are worth million dollar coins called ETHs (Luu et al., 2016a; Lin and Liao, 2017; Warren and Bandeali, 2017). Performing financial transactions is only one application of Ethereum; it also opens up the power of blockchain to beyond transferring money. Ethereum has a grand vision to become a shared "World Computer" by combining millions of accounts (Dhillon et al., 2017). As in blockchain, instead of using PoW, Ethereum uses PoS to perform the mining work, which increases the efficiency of the blockchain (Lin and Liao, 2017).

The smart contract used by Ethereum as its building block was initially introduced by Nick Szabo in 1996 as a protocol for ecommerce to sign an electronic contract among strangers (Szabo, 1996). A smart contract is a logical decentralized program running on an Ethereum virtual machine (EVM), which is a runtime environment for smart contracts. The Ethereum smart contract is written in a high-level language called Solidity, and the written contract code compiles in EVM to generate bytecode, which then runs on an Ethereum client (Dhillon et al., 2017). Unlike transactions in blockchain, Ethereum Smart Contracts are more flexible in nature in terms of dealing with objects, subjects, actions, and conditions to perform the desired transfer of ownership (Drescher, 2017).

Another framework came into play in the year 2015 by Linux Foundation called Hyperledger Fabric (https://www.hyperledger.org/). Unlike the previous implementations of blockchain, Hyperledger does not have any kind of digital currency; it is an open-source project for supporting cross-industry blockchain-based distributed ledger frameworks. Hyperledger Fabric is one of the implementations of the Hyperledger project (github.com/hyperledger/fabric) for running smart contracts and other familiar and proven technologies with pluggable modules in the form of functions (Cachin, 2016).

2.2.4 Limitations of BB-IoT

Blockchain is a highly technical and sophisticated creation with a natural flow, but there is no perfect system that does not have limitations and challenges. While blockchain provides many attractive features, it has also several problems. Fig. 5 shows the issues in blockchain.

There are some important points that need to be evaluated before implementing BB-IoT. These points are related to things, services, and the user; things are the devices containing sensors and actuators to monitor the real world, services are related to security, efficiency, network architecture, and upgrades and amendments to underlying systems. Finally, the user relates to faster response with minimized latency and no down time. The expected issues in BB-IoT can be categorically divided into several areas such as security, privacy, scalability, latency and energy consumption, and flexibility. Fig. 6 shows the proposed taxonomy of issues in BB-IoT.

1. Security

In blockchain, the only security measure is the cryptographic signature (known as a hash key). The hash key, which is used in blockchain, is considered to be a powerful security measure, but losing that signature by means of data leak or theft can lead to a severe security breach. There are several other possible issues related to the security perspective of blockchain, such as if a group has 51% computing power, then it can find the nonce (solution of the mathematical puzzle) faster than everyone else, and this kind of attack is known as a majority attack (or 51% attack) (Courtois and Bahack, 2014; Eyal and

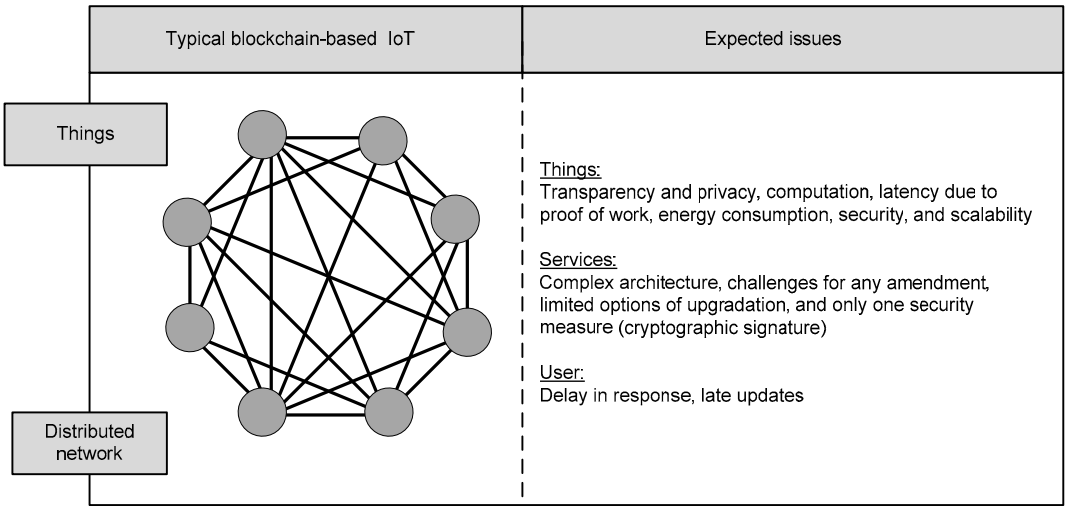

Fig. 5 Issues in blockchain-based IoT

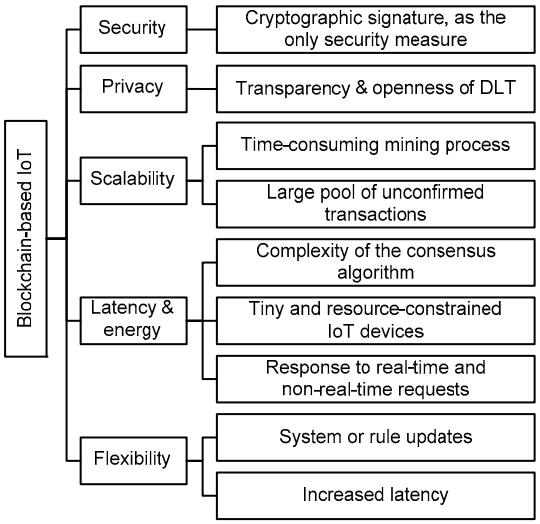

Fig. 6 Taxonomy of issues and concerns in blockchain-based Internet of Things (BB-IoT)

Sirer, 2018). Another issue is the forking problem, which is a problem of agreement on the software upgrade (compatibility issue); forks also occur in centralized systems, but with decentralized systems, forks are trickier to deal with. In the case of blockchain, a fork will not activate until it has upgraded the majority of nodes. There are two types of forks: hard fork and soft fork. A hard fork is the incompatibility of old nodes with new version or agreement rules, so the old chain does not accept it, and it is divided into two independently working chains. A soft fork is the incompatibility of new nodes with the version or agreement rules of the old node, and thus they continue with both rules on the same chain (Lin and Liao, 2017). This situation may create difficulty in dealing with the security agreements of the system.

2. Privacy

Blockchain is a purely distributed network of nodes connected in a peer-to-peer manner, and transparency and openness are two of the key features of blockchain; however, the openness and lack of privacy may not favor several IoT applications. Creating an entirely satisfying mechanism like a black box obfuscation is mathematically impossible as stated by Buterin (2016); there is always something beyond the output, which can uncover the original source. However, there has been ongoing research in blockchain to improve privacy within blockchain-based IoT, and one very good framework proposed in Dorri et al. (2017a) is called the lightweight secure blockchain (LSB) for IoT. In LSB the devices in a smart home use a private immutable ledger (IL) of local communications, and thus it is a small-scale blockchain managed by the smart home edge device (a miner), which can help improve privacy in the network.

3. Scalability

As discussed in CB-IoT, the address space is a big concern for industries involved in IoT, and that issue does not exist in blockchain (Khan and Salah, 2018). However, in Bitcoin, recently the response time and issues of managing big networks and performing mining operations for various nodes have been considered poor (Memon et al., 2019a, 2019b). There are two main causes of this issue: throughput

(rate to process transactions) and latency (time taken for a transaction to be inserted in the blockchain) (Bano et al., 2017b). Because mining itself is a time-consuming process, the unconfirmed transactions are being pooled and waiting for a long time (Bano et al., 2017a). Scaling the blockchain-based distributed network for large-scale applications may very well create new challenges.

4. Latency and energy

The latency of any operation can be measured by factors like computational effort and the overall time taken to respond to a request, while the energy consumption is the power consumed during performing a task by a system. PoW is considered to be a time- and energy-consuming operation, which is why it takes place in an interval of 10 min (Gervais et al., 2016). Because each transaction stored on a blockchain has a high validation cost, each consequently has an extremely low throughput and high latency (Gaetani et al., 2017). Because processing time depends on the complexity of the hash code puzzle, this ultimately affects the above factors and results in a delayed response system.

5. Flexibility

Blockchain is a very complex construct with a sophisticated set of protocols. Therefore, any amendment in the ecosystem will be a challenging job because it may lead to multiple forks. Once deployed, there is a lack of options to upgrade the underlying mechanism of the blockchain, or if upgraded, the mining process may become affected because of the multiple chains of transaction (Lin and Liao, 2017).

Table 1 presents a summary and comparison of these two technologies. Although the cloud technology in IoT is quite well explored and is mature at this time, and blockchain is very young and immature, the comparison is conducted equally based on the literature available to date. Table 1 compiles all the issues of both architectures discussed earlier, and opinion is provided in the form of comments about which one might have the potential to address a particular challenge.

The issues of security, privacy, and losses are very serious with regard to the cloud; on the other hand, blockchain is very reliable in terms of security, privacy, and historical losses. However, a concern that may be worth noting is that blockchain has only one security measure, which is its cryptographic signature, or maybe the mining process to validate the transaction can be considered another security measure. However, some issues may be encountered in the future with the growth of the blockchain network, including the 51% attacks and forking as discussed earlier. The scalability and flexibility issues of blockchain have some limitations such as the throughput and latency of the overall communication due to the complexity of the mining process. Furthermore, the latency issue with both architectures is very critical. The energy consumption of the data center is much higher than in blockchain, but in blockchain, latency and energy consumption are interrelated, so if the complexity of mining is reduced and the miner is moved to the access level in the form of a private blockchain, then the latency and energy consumption problems can be solved.

The cloud in comparison to blockchain is a very costly solution. Establishing huge data centers, maintenance and other expenses mean that it is a very expensive approach. Blockchain is cost-effective in regular tasks, but expensive in industrial or business processing, while the cloud for business processing is much cheaper. If regular communication is executed at the device level over a blockchain network and business processes are accomplished using cloud data centers, the issue of cost can be addressed. Finally, with regard to payment methods, because digital currency has already started to revolutionize the overall economy, it can be said that blockchain is very well established compared to the cloud in the area of payment methods.

From Table 1, we can see that blockchain has the potential to provide security and protect against losses and risks, and also helps preserve privacy. Blockchain also has very robust payment methods available, while the cloud has advantages in scaling the network and combating the forking issues of blockchain. Thus, a fusion of these two approaches could solve the issues with each architecture. However, the issues of scalability, flexibility, latency, cost concerns, and energy consumption require more attention from the research community. In the next section we will first discuss ongoing research projects to solve the issues addressed in Table 1, and then present a hybrid-IoT architecture as one possible solution.

Table 1 Summary of issues in CB-IoT and BB-IoT

Issues in both architectures	Cloud-based IoT	Blockchain-based IoT	Comments
Security	The cloud has multiple security measures, but is still insecure and has been found to have a number of issues in recent years (Granjal et al., 2015; Sicari et al., 2015; Wang YF et al., 2015; Yi et al., 2015; Khan and Salah, 2018).	Blockchain depends only on its cryptographic signature (Courtois and Bahack, 2014; Eyal et al., 2015). It is considered to be tamperproof because of the cryptographic signature, which is unique for each block, and also because of the validation of the consensus algorithm (Kshetri, 2017b).	Blockchain is very secure and shows no evidence of issues, but two major concerns can be found in the literature, i.e., the 51% attack issue and the forking issue.
Privacy	There are several solutions for privacy, but issues such as financial risks and losses as estimated by Lloyd's may cross 400 billion US$ in coming years, and availability of data centers over different locations may increase the chance of data leaks, which develops the lack of trust in centralized approaches (Soubra, 2012; Singh J et al., 2016; Henze et al., 2017; Mollah et al., 2017; Zhou et al., 2017; Stergiou et al., 2018).	Transparency and openness are building blocks of blockchain. Thus, privacy may also be considered an issue with this approach (Kshetri, 2017b; Ourad et al., 2018).	Improvements have been proposed to strengthen privacy in blockchain, the private and consortium blockchain with an immutable ledger (Dorri et al., 2017a), as discussed in Section 3.
Losses and risks	This approach has a history of huge financial losses and data leaks due to third-party involvement, and it is expected that this will grow with time (Juniper Research, 2015; Manral, 2015; Hilton, 2016; Moar, 2017).	Since its inception, the blockchain core algorithm has had no history of attacks that breached the security of the network (Kshetri, 2017a).	Blockchain is very robust due to its consensus algorithm and hash key to protect against losses and maintain trust.
Scalability	The IPv6 protocol stack has a huge overhead at the individual device level; address space is also a big concern for industry (Kim, 2008; Singh D et al., 2014; Bellavista and Zanni, 2016).	The overhead for GUID is much less than that for IPv6; also, it provides 4.3 billion more address space than IPv6 (Khan and Salah, 2018). However, scaling the blockchain to be as huge as the Internet is a challenge, because throughput and latency will become very high (Bano et al., 2017a).	The cloud approach is capable of efficiently managing a network spread over a wide geographical location.
Latency	Request and response time is very high and also depends on several factors such as speed of the network and the geographical location (Bonomi et al., 2012; Yang et al., 2017). One good solution introduced by Cisco is fog computing, which brings computing, communication, and processing close to the user (Almadhoun et al., 2018). The fog is discussed further later in Section 3.	Mining is a heavyweight and time-intensive process when solving the mathematical puzzle (PoW) in peers over a blockchain network (Dorri et al., 2017a).	Both approaches have challenges with latency. An in-between approach could be obtained to solve the latency issue. Local miners at the access level could be considered a potential solution (Dorri et al., 2017b).

To be continued

Table 1

Issues in both architectures	Cloud-based IoT	Blockchain-based IoT	Comments
Energy consumption	Huge data centers are ingesting high amounts of energy, and this is increasing day by day with an increased number of connected devices and applications (Shveta and Pandey, 2014; Hameed et al., 2016).	The mining process is considered to be inefficient in terms of energy consumption (Dorri et al., 2017b; Lin and Liao, 2017).	A cloud data center has a big impact on the environment; therefore, blockchain deployed with local miners at the access level could be a solution to this problem.
Cost	This approach is a very costly solution in terms of bandwidth, maintenance, and updating of hardware and software (Shveta and Pandey, 2014).	In terms of bandwidth consumption, maintenance, and upgrade costs, blockchain is a more feasible solution than the cloud. However, the cost of business process execution is twice that of the cloud (Rimba et al., 2017).	A private distributed network with blockchain can be efficient in handling common requests and responses, e.g., scheduling a washing machine, paying bills, and obtaining a shopping list, but heavy industrial processing can be conducted over the cloud.
Payment	This approach is very limited in the methods of payments, and the available modes of payment are rarely used (Stormer and Meier, 2012; Wilusz and Rykowski, 2013).	Bitcoin is already a very popular example of digital currency (Underwood, 2016; Drescher, 2017). Alternatively, there are several other choices for cryptocurrencies based on the DLT of blockchain, including Ether, Litecoin, Nxt, Ripple, and Peercoin (Buterin, 2013; Nakano, 2018).	Undoubtedly, digital currency is the future currency; it may be Bitcoin or something else.
Flexibility	Forking with a centralized system is much easier to deal with (Lin and Liao, 2017).	Dealing with forks in a decentralized system is difficult. In blockchain, hard and soft forks may degrade the rating of a miner (Lin and Liao, 2017).	The cloud, due to its centralized architecture, can efficiently handle synchronizing upgrades simultaneously across all nodes to deal with different types of forks.

3 Way forward

It is evident that researchers are paying considerable attention to solving the problems encountered in both architectures, but a heuristic approach for overcoming the maximum number of challenges is required. The possible solution to those problems can be the combination of these two architectures. Based on the survey conducted in Section 2, we can say that a hybrid-IoT architecture is tomorrow's technology. There may be a conflict of opinion on the working paradigms, but it is certain that the upcoming IoT architecture will be some sort of hybrid approach. In this section we will discuss the ongoing research activities and some key projects to overcome the challenges, and later propose a possible hybrid approach as a way forward to overcome the challenges. It could be one of the possible solutions to the existing issues with both architectures.

3.1 Recent research projects

As we can see from Table 1, the security and privacy issues with the cloud are very serious, while blockchain, on the other hand, has proven to be the most secure and privacy-oriented model since 2009. The integration of blockchain at the perception and transport layers can provide security and privacy in data collection and data transmission. The transmission can be initiated by blocks using a telehash to broadcast in the network (Biswas and Muthukkumarasamy, 2016). The smart contract functionality of Ethereum can also be used by the BitTorrent protocol to form a peer-to-peer network (Biswas and Muthukkumarasamy, 2016). At the service layer, instead of storing data on the cloud, the distributed ledger can be used, which is one of the best solutions to eliminate the risk of single-point failure and data leaks. Moreover, the consensus algorithms like PoW and PoS are

the key protocols to discourage DoS/DDoS and spam attacks in a network (Dwork and Naor, 1993; Jakobsson and Juels, 1999). Confidentiality of data can be achieved by discouraging existing server-based application development, and trends should move toward developing decentralized software applications to avoid hosting important information on central servers, for example, no need for signup on payment services such as PayPal, no need to worry about customer credentials. An example of such a type of application development platform is Ethereum DApp (Singhal et al., 2018). DApp is an open-source model for building decentralized applications, and nearly a thousand DApps have been created on Ethereum (https://www.stateofthedapps.com/).

From the loss and risk perspectives, the main cause behind the history of losses is the central gigantic pool of valuable data residing in costly data centers and presenting an opportunity for attacks by bad actors. In contrast, blockchain is distributed in nature, and every node in the network holds the same copy of the ledger; thus, leaving behind the centralized paradigm of IoT, blockchain may help create an unhackable distributed system to connect every bit of the world without involvement of any third party as an intermediary (Kshetri, 2017a).

Scalability and latency in blockchain are considered challenging because of throughput and latency. On the other hand, cloud-based IoT provides efficient management of a widespread network of connected devices. In terms of latency, the distributed network of BB-IoT means that the communication and processing are as local as possible. Nevertheless, this is not straightforward; there is a need to come up with new strategies by exploiting the characteristics of the distributed architecture of blockchain (Dorri et al., 2017a), such as the case of Storj launched in 2014. It is a distributed peer-to-peer blockchain-based storage system that works like torrents to create a worldwide distributed storage, and instead of hosting the data on the cloud, it is shredded into encrypted pieces and spread redundantly over the network, while the key is kept with the owner only. The encrypted small pieces of data cannot be decrypted by anyone, and can be retrieved only by the owner at any time; the retrieval speed is much higher than that of the cloud because the data comes from multiple nodes in the network (Wilkinson et al., 2014). Several methods have been introduced to overcome the on-chain scalability and latency challenges of blockchain. Key approaches are Sharding, Multiple Blocks per Leader, Collective Leaders, and Parallel Blockchain Extension (Bano et al., 2017a). Sharding is an approach for creating a group of nodes called committees, where each committee manages a subset (shard) of transactions (Luu et al., 2016b). In Multiple Blocks per Leader, one elected leader is provided a time slot (epochs) to perform PoW and append multiple transactions on the blockchain. When epochs are over, a new leader is elected (Eyal et al., 2015). Using the Collective Leaders approach, multiple leaders are hired to jointly decide if a block can be appended over to the blockchain (Kokoris-Kogias et al., 2016). Parallel Blockchain Extension has been introduced to parallelize the mining process of blockchain; in this approach, multiple leaders are given different parts of the blockchain to solve, where each transaction validates two previous (parent) transactions (Bano et al., 2017b).

The cost concern and energy consumption in establishing huge data centers are inevitable, where massive energy ingestion, large bandwidth requirements, and maintenance and updating of hardware and software are foreseeable. Pursuing the blockchain approach could be the best solution to distribute the computation over the network in nearby proximity of IoT devices. Yet, processing of large industrial data is expensive with blockchain, as it is almost twice that of the cloud (Rimba et al., 2017). Thus, a greedy approach can be used regarding the cost concern. One possible approach could be fusion of the cloud and blockchain; blockchain resolves regular communication queries, while the cloud responds to industrial big data processing.

The micropayments in IoT should be an integral part of the future Internet. In the upcoming years, most transactions will take place between machines, for example, using the reserved pool of money or a coupon for utilities will automatically pay the utility bills in a smart home scenario. The billing issue has been treated in IoT as micropayments, but never received much attention because IoT is still in the experimentation phase. If we consider blockchain for micropayments in IoT, then it can serve as a marketplace to easily enable financial transactions between two parties or things (Christidis and Devetsikiotis,

2016), for example, smart utility meter(s) at home, recharging an electric vehicle, renting a house, and shopping. Because the blockchain already has a robust and trusted solution for financial transactions, it can serve as a billing layer in between a distributed network of heterogeneous devices. For example, currently the Ethereum smart contracts based German startup, Slock.it (Smart Lock), is the first Ethereum blockchain platform based on real-world smart objects. Slock introduces the benefits of blockchain such as payments, transparency, security, and auditability in property-sharing applications (https://slock.it/; Liao et al., 2017). Slock is also encouraging some trends, such as sharing bicycles, cars, washing machines, lawn mowers, or any unused smart object that can be used to generate revenue by renting them in an easy, secure, safe, and smart way without an intermediary agent (https://slock.it/; Christidis and Devetsikiotis, 2016).

Another issue with blockchain is forking. In the decentralized network architectures of blockchain, a valid block might get generated by multiple nodes simultaneously known as a fork, and this creates a new branch of blocks (new chain) over the existing one (Mosakheil, 2018). In the case of frequent forks, the multiple branches of a chain may delay the mining process to finish the job, and this can also lead to forking attacks known as Goldfinger attacks (Bonneau et al., 2015). Blockchain can solve this problem by adopting Practical Byzantine Fault Tolerance (PBFT) as done by ByzCoin (Kokoris-Kogias et al., 2016). On the other hand, the cloud architecture is centralized, and it is easier to deal with forking than in distributed systems (Elham et al., 2012).

Currently, a number of research projects are ongoing to overcome the challenges discussed in Section 2 using the methods examined above. Table 2 presents some of the latest key research projects that might be helpful in further addressing these issues. The approaches of Dorri et al. (2017b), Samaniego and Deters (2017), and Xiong et al. (2017) use a local miner at the access level to solve the complex mathematical puzzle of blockchain. The security solutions at the device level are F-Secure and access control and authentication management. F-Secure offers a solution which is a middle box, called a "secure Wi-Fi router" in between the IoT devices and Internet gateway to protect a home or business from hazards (https://www.f-secure.com/en_US/web/home_us/sense). The access control and authentication management system is a blockchain-based authentication system for secure interactions with IoT devices (Ourad et al., 2018). Another security solution listed is a proactive approach for defense against DDoS attacks in the cloud by distributing the control layer (Bawany et al., 2017). As discussed earlier in this section regarding sharding, Storj implements the sharding method to secure the data over a distributed network of blockchain. It encrypts and shards the data into small pieces and distributes them on the peers of a network, which results in reduced latency while retrieving data, but it also increases security and privacy.

There are also several other projects ongoing to overcome the issues encountered in the implementation of blockchain for IoT, but a comprehensive architecture is required that can address the existing issues and provide a reliable, secure, fearless, fast, cheap, energy-efficient, and scalable solution for tomorrow's IoT. Next, we will see a hybrid approach which may be one of the feasible solutions to overcome the existing challenges.

3.2 Hybrid-IoT architecture

We propose a hybrid IoT approach as one of the possible ways to overcome the challenges with both architectures. Hybrid IoT is a three-tiered architecture: from bottom to top, the first element is things, then the fog/edge, and at the top the cloud. There are three basic configurations of hybrid IoT, and these are the different modes of communication. Fig. 7 shows the high-level architecture of the proposed hybrid IoT approach.

1. Things layer

The first tier of the proposed architecture is things. Things are the objects or devices deployed into a smart environment. All the smart objects must have the capability of collecting, storing, and communicating data over the network. In the proposed architecture, things are connected using a blockchain-based peer-to-peer communication network, where the things communicate with each other using a global unique identifier (GUID) or public key. The encrypted communication between devices enables the trust among all objects of the network. The first time registration of a device in a blockchain network is done by the edge node.

Table 2 Key research projects

Project	Purpose	Mechanism	Entities involved
Scalability, mining, and energy consumption			
Blockchain meets edge computing (Xiong et al., 2017)	For resource-constrained devices, it reduces both the burden of computation and energy consumption.	It uses edge servers to compute the complex puzzle, e.g., PoW, to create consensus between mobile nodes.	Edge service provider and mobile nodes
Blockchain as a service for IoT (Samaniego and Deters, 2017)	It evaluates the latency issues of the network for the cloud and edge, and suggests possible solutions for a hosting environment for blockchain.	It performs experiments on latency to uncover the fact that if blockchain data is hosted on the edge, the edge can outperform the cloud in latency, but the edge is limited in computation and storage compared to the cloud.	Edge and the cloud
BC-based smart home framework (Dorri et al., 2017b)	It is a framework for resource-constrained IoT devices to create a manageable, secure, and privacy-oriented method for the future IoT.	The smart home case study shows that every home can have a local blockchain network of IoT devices, and the smart home miner (gateway or standalone PC-like device) could be used for the mining operation.	IoT devices and local miner
Security and privacy			
F-Secure	The secure Wi-Fi router protects the entire home network and devices from security threats.	It has a middle box that acts as intermediary between IoT devices and the Internet gateway.	IoT devices, middle box, and gateway
Blockchain-based IoT access control and authentication management (Ourad et al., 2018)	It is a blockchain-based solution to authenticate users to enable a secure approach to IoT devices. It focuses on devices with low computation power.	It is a different approach for performing authentication in a decentralized way, while the existing approach auth0 involves a third-party authentication server. In the case of the proposed work, the user authenticates to the smart contract to verify identity. If authenticated, then the user can interact with devices via any preferred method, SSH, http, https, etc.	User, smart contract, and IoT device
Proactive DDoS defense framework (Bawany et al., 2017)	It is a proactive approach for detecting DDoS attacks in the cloud.	It implements an adaptive DDoS protection mechanism by a distributed controller layer to increase the reliability and scalability of huge data centers.	Application and distributed controller layer
Distributed storage with low latency			
Storj.io (Wilkinson et al, 2014)	Instead of cloud storage, it uses distributed file storage, which is faster, cheaper, and more private.	Storj is a blockchain-based peer-to-peer cloud storage system. It works like torrents; it encrypts data, shreds it into encrypted small pieces, and spreads them redundantly over hundreds of disks across a network. On retrieval, the owner knows only about the addresses and hash keys of shards. An audit algorithm ensures data integrity and availability over time.	Peer-to-peer network of nodes

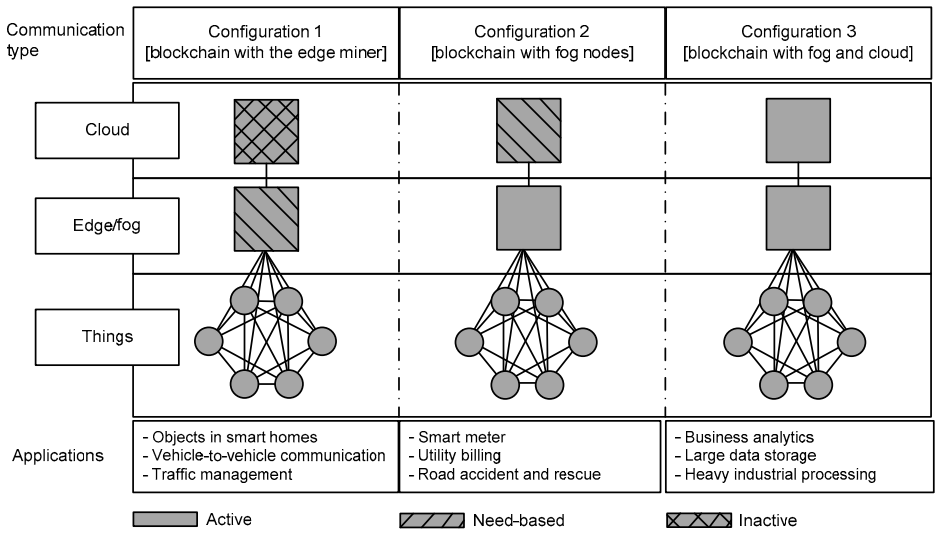

Fig. 7 Proposed hybrid IoT

2. Middle layer (fog/edge)

The application of the edge node in the hybrid-IoT architecture is to register IoT devices with the blockchain network by sharing the public key with each other. Each device first needs to perform a genesis transaction, and the edge validates the transaction by generating a shared key to encrypt the communication between devices. The key generated is then assigned to the first genesis block. Once the communication is established, all existing devices in the network will start to recognize the new device. The registration to enable device-to-device communication is achieved using one of the consensus algorithms (PoW or PoS), and due to transient and limited resources, this mining process is outsourced to a locally available miner at the access level. In a smart home environment, we call it the edge node, and in a smart city or smart industry, it is the fog node.

The fog is the idea of a substantial computing resource available locally to IoT devices, and it was first announced by Cisco (2015). Fog is an extension of cloud computing where mini public clouds are distributed closer to end devices to provide processing, storage, and controlling capabilities to deal with requests locally in real time. The fog nodes at the access level of the network are also used to offload the computation burden from clouds (https://www.openfogconsortium.org/; Bonomi et al., 2012; Ficco et al., 2017; Almadhoun et al., 2018). However, in the proposed hybrid-IoT architecture, the fog or edge node performs four functions: (1) speeding up the mining process; (2) saving the energy of IoT devices; (3) reducing the latency; (4) filtering the incoming requests like the message queuing telemetry transport (MQTT) protocol (Andersen et al., 2017). Filtering the incoming requests means deciding the job nature from the type of content and volume of data, and no matter whether it is to be performed locally or sent to the cloud, this can be achieved using the publish/subscribe model of the MQTT protocol of IoT (Cohn et al., 2014). For example, in smart industry, there could possibly be all configurations of the three tiers of the hybrid architecture working simultaneously and sharing the same resources; deciding if a request should be published over a blockchain network, performing small local processing, or forwarding it to the cloud would all be accomplished by the fog node.

3. Cloud data center layer

The third tier of the proposed architecture is the cloud data center, which is similar to the existing technology, but instead of forwarding all incoming requests to the cloud as in CB-IoT, here only the selected applications would communicate with the cloud to perform industrial tasks like big data analysis and big data storage.

As shown in Fig. 7, the three-tiered architecture offers three different network configurations, Configurations 1–3. All of the configurations represent the modes of communication in the network, where the configuration gets enabled and disabled by altering the states of the components in the network. There

are three states in all the components of the network (Fig. 7), active, need-based (or event-based), and inactive. The active components are the nodes in the working mode, the need-based components are the event-based nodes, and they are activated or deactivated by the tags in the packets received, while the inactive components remain inactive in a particular type of configuration.

Configuration 1 The first configuration facilitates local communication. It is like a blockchain-based local area network (BB-LAN), and it works at the things and device levels, such as appliances in a smart home environment. In this configuration, the devices usually communicate with each other in a trusted environment. When registering a new device, the edge component is activated by a signup request, which performs the mining process to validate the new device. Once validated, the device can be identified by the whole network. Applications of Configuration 1 could be in a smart home network, smart parking lots, and for sharing of the unused items.

Configuration 2 This works similar to Configuration 1. The change in this configuration is that every communication goes through the fog node, where all the data traffic can be monitored. An example of this kind of configuration is in a smart city environment, where the actions related to security, traffic management, collision detection on roads, ensuring newly imposed rules, and smart metering are the activities in which a trusted third party like government is involved. In this configuration, the fog node is monitored and controlled by city management. While the objects of a smart city would still be communicating using a blockchain-based peer-to-peer network, the orchestration and monitoring are conducted at the fog nodes. This configuration also has the ability to communicate with the cloud for data analysis or history preservation, but not all the information flows through the cloud.

Configuration 3 In this configuration, all the tiers of communication are active, and it is not necessary to send all the collected data to the cloud, but the configuration has ability to do so. It incorporates Configurations 1 and 2 plus an ability for communicating with cloud (as in the existing CB-IoT architecture). Its applications would include smart industry, where at the production line, devices communicate with each other in a trusted network of blockchain, but the registration of new devices and other lightweight routine tasks can be performed at the fog node, while the large volume data storage and analysis is performed on the cloud.

Table 3 shows a comparison of CB-IoT, BB-IoT, and the proposed hybrid IoT for the required features of a future IoT. There are some features suitable for the cloud, while others are performed well by blockchain. The hybrid approach maximizes the benefits of each by adopting a middle ground approach and comes up with a solution to overcome the limitations of CB-IoT and BB-IoT as shown in Table 1. Furthermore, a set of more optimized communication protocols for the enabling technologies and a clear categorization of rules and operations need to be developed.

Table 3 Cloud and blockchain fusion to reform IoT

Challenge	CB-IoT	BB-IoT	Hybrid IoT
Security	Weak	Strong	It uses blockchain at the device level to ensure the security of the IoT ecosystem.
Scalability	Strong	Weak	Configuration 1 can be used to create private networks of blockchain, which provides security and preserves privacy in building area networks (BLANs).
Privacy	Weak	Strong	
Losses and risks	Weak	Strong	The use of blockchain at the device level will resolve the risk of attacks by restricting it to trusted members only, and thus the fear of losses would be mitigated.
Latency	Weak	Strong	The latency, energy ingestion, cost of bandwidth consumption, and capital or operational expenses of huge data centers will be dramatically reduced if regular communication occurs in Configurations 1 and 2, and only industrial data storage and analysis are performed over the cloud in Configuration 3.
Energy consumption	Weak	Strong	
Cost effectiveness	Weak	Strong	
Payment methods	Weak	Strong	Bitcoin is a very good example of the payment method; there could also be alternatives for payment systems. In the past few years, more than a dozen of new digital currencies have been introduced using blockchain.
Flexibility	Strong	Weak	Forking is easy to deal with if there is an edge node involved in the mining process.

4 Conclusions

In this article we reviewed the existing cloud-based IoT (CB-IoT) and presented a taxonomy of issues that, in sharp contrast to the literature survey, we expect to grow further in a couple of years beyond what they are today. As a consequence, CB-IoT will become more vulnerable to cyberattacks and will eventually report financial and data losses up to five times greater than those of today. To cope with the consequences of CB-IoT, blockchain-based IoT (BB-IoT) has the potential to overcome the underlying issues in CB-IoT. However, considering that the merging of new technologies always has downsides, we proposed a taxonomy of issues expected in BB-IoT. We found that there are some good features in both CB-IoT and BB-IoT, so instead of shifting to an entirely new infrastructure, it would be better to come up with something in between rather than a full migration.

To realize this strategy, we proposed a hybrid-IoT approach with the help of a survey of current key research activities in blockchain. Hybrid IoT addresses the shortcomings of both infrastructures and adheres to the requirements of the future IoT. Hybrid IoT operates on three communication configurations for different kinds of applications. Configuration 1 is a blockchain-based local area network that works in tandem with edge nodes, and it would have potential applications in smart homes. Configuration 2 is another kind of blockchain-based metropolitan area network with fog nodes, and it can be used to facilitate a smart city environment. Configuration 3 can operate over the multiple layers of the proposed ecosystem. This configuration can be used by industrial and business applications for big data storage and analysis. Furthermore, for effective implementation of this approach, a set of new policies and standards would be required to ensure a robust, secure, and distributed IoT.

Contributors

Raheel Ahmed MEMON, Junaid AHMED, and Muhammad ISMAIL performed literature survey and processed the collected information. Raheel Ahmed MEMON and Junaid AHMED drafted the manuscript. Muhammad Irshad NAZEER and Khursheed ALI helped organize the manuscript. Jian Ping LI supervised the overall work.

Compliance with ethics guidelines

Raheel Ahmed MEMON, Jian Ping LI, Junaid AHMED, Muhammad Irshad NAZEER, Muhammad ISMAIL, and Khursheed ALI declare that they have no conflict of interest.

References

Aazam M, Khan I, Alsaffar AA, et al., 2014. Cloud of Things: integrating Internet of Things and cloud computing and the issues involved. Proc 11th Int Bhurban Conf on Applied Sciences and Technology, p.414-419. https://doi.org/10.1109/IBCAST.2014.6778179

Ahmed F, Ko YB, 2016. Mitigation of black hole attacks in routing protocol for low power and lossy networks. *Secur Commun Netw*, 9(18):5143-5154. https://doi.org/10.1002/sec.1684

Akoush S, Sohan R, Rice A, et al., 2011. Free lunch: exploiting renewable energy for computing. https://www.usenix.org/events/hotos/tech/final_files/Akoush.pdf [Accessed on Sept. 22, 2018].

Almadhoun R, Kadadha M, Alhemeiri M, et al., 2018. A user authentication scheme of IoT devices using blockchain-enabled fog nodes. IEEE/ACS 15th Int Conf on Computer Systems and Applications, p.1-8. https://doi.org/10.1109/AICCSA.2018.8612856

Amazon, 2006. Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta. https://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/ [Accessed on Jan. 18, 2018].

Andersen MP, Kolb J, Chen KF, et al., 2017. Wave: a decentralized authorization system for IoT via blockchain smart contracts. https://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-234.pdf [Accessed on May 29, 2019].

Armbrust M, Fox A, Griffith R, et al., 2010. A view of cloud computing. *Commun ACM*, 53(4):50-58. https://doi.org/10.1145/1721654.1721672

Aulbach S, Grust T, Jacobs D, et al., 2008. Multi-tenant databases for software as a service: schema-mapping techniques. Proc ACM SIGMOD Int Conf on Management of Data, p.1195-1206. https://doi.org/10.1145/1376616.1376736

Bahga A, Madisetti VK, 2016. Blockchain platform for Industrial Internet of Things. *J Softw Eng Appl*, 9(10): 533-546. https://doi.org/10.4236/jsea.2016.910036

Banafa A, 2017. IoT and blockchain convergence: benefits and challenges. http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html [Accessed on Feb. 23, 2018].

Bano S, Al-Bassam M, Danzis G, 2017a. The road to scalable blockchain designs. *Winter*, 42(4):31-36.

Bano S, Sonnino A, Al-Bassam M, et al., 2017b. SoK: consensus in the age of blockchains. https://arxiv.org/pdf/1711.03936.pdf [Accessed on Sept. 27, 2018].

Bawany NZ, Shamsi JA, Salah K, 2017. DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arab J Sci Eng*, 42(2):425-441. https://doi.org/10.1007/s13369-017-2414-5

Bellavista P, Zanni A, 2016. Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP. IEEE 2nd Int Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow, p.1-6. https://doi.org/10.1109/RTSI.2016.7740614

Bhattasali T, Chaki R, 2011. A survey of recent intrusion detection systems for wireless sensor network. In: Wyld DC, Wozniak M, Chaki N, et al. (Eds.), Advances in Network Security and Applications. Springer Berlin Heidelberg, p.268-280. https://doi.org/10.1007/978-3-642-22540-6_27

Biswas K, Muthukkumarasamy V, 2016. Securing smart cities using blockchain technology. IEEE 18th Int Conf on High Performance Computing and Communications, p.1392-1393. https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

Bonneau J, Miller A, Clark J, et al., 2015. SoK: research perspectives and challenges for Bitcoin and crypto-currencies. Proc IEEE Symp on Security and Privacy, p.104-121. https://doi.org/10.1109/SP.2015.14

Bonomi F, Milito R, Zhu J, et al., 2012. Fog computing and its role in the Internet of Things. Proc 1st Edition of the MCC Workshop on Mobile Cloud Computing, p.13-16. https://doi.org/10.1145/2342509.2342513

Brachmann M, Garcia-Morchon O, Kirsche M, 2011. Security for practical CoAP applications: issues and solution approaches. 10th GI/ITG KuVS Fachgespraech Sensornetze, p.1-4. https://www.researchgate.net/profile/Michael_Kirsche/publication/265973615_Security_for_Practical_CoAP_Applications_Issues_and_Solution_Approaches/links/5583f51c08ae4738295c2028.pdf [Accessed on Feb. 24, 2018].

Brito J, Castillo A, 2013. Bitcoin: a Primer for Policymakers. Mercatus Center at George Mason University.

Brown J, 2017. Companies forge cooperative to explore blockchain-based IoT security. https://www.ciodive.com/news/companies-forge-cooperative-to-explore-blockchain-based-iot-security/435007/ [Accessed on Feb. 23, 2018].

Buterin V, 2013. Ethereum white paper. GitHub Repository.

Buterin V, 2016. Privacy on the blockchain. Available from https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ [Accessed on Sept. 27, 2018].

Cachin C, 2016. Architecture of the Hyperledger Blockchain Fabric. IBM Research. https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf [Accessed on Feb. 24, 2018].

Castro M, Liskov B, 2002. Practical Byzantine fault tolerance and proactive recovery. *ACM Trans Comput Syst*, 20(4):398-461. https://doi.org/10.1145/571637.571640

Chae SH, Choi W, Lee JH, et al., 2014. Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone. *IEEE Trans Inform Forens Secur*, 9(10):1617-1628. https://doi.org/10.1109/TIFS.2014.2341453

Chen YY, Trappe W, Martin RP, 2007. Detecting and localizing wireless spoofing attacks. 4th Annual IEEE Communications Society Conf on Sensor, Mesh and Ad Hoc Communications and Networks, p.193-202. https://doi.org/10.1109/SAHCN.2007.4292831

Christidis K, Devetsikiotis M, 2016. Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4:2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

Cisco, 2015. Fog computing the Internet of Things: extend the cloud to where the things are. White Paper. https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview.pdf

Cohn RJ, Coppen RJ, Banks A, et al., 2014. MQTT version 3.1. https://www.oasis-open.org/committees/download.php/52951/mqtt-v3.1.1-csd06.pdf [Accessed on May 29, 2019].

Conzon D, Bolognesi T, Brizzi P, et al., 2012. The VIRTUS middleware: an XMPP based architecture for secure IoT communications. 21st Int Conf on Computer Communications and Networks, p.1-6. https://doi.org/10.1109/ICCCN.2012.6289309

Courtois NT, Bahack L, 2014. On subversive miner strategies and block withholding attack in Bitcoin digital currency. https://arxiv.org/abs/1402.1718 [Accessed on Sept. 16, 2018].

Dhillon V, Metcalf D, Hooper M, 2017. Blockchain enabled applications: understand the blockchain ecosystem and how to make it work for you. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-3081-7_1

Dorri A, Kanhere SS, Jurdak R, et al., 2017a. LSB: a lightweight scalable blockchain for IoT security and privacy. https://arxiv.org/pdf/1712.02969.pdf [Accessed on Sept. 14, 2018].

Dorri A, Kanhere SS, Jurdak R, et al., 2017b. Blockchain for IoT security and privacy: the case study of a smart home. IEEE Int Conf on Pervasive Computing and Communications Workshops (PerCom Workshops), p.618-623. https://doi.org/10.1109/PERCOMW.2017.7917634

Drescher D, 2017. Blockchain basics. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-2604-9

Dvir A, Holczer T, Buttyan L, 2011. VeRA-version number and rank authentication in RPL. IEEE 8th Int Conf on Mobile Ad-hoc and Sensor Systems, p.709-714. https://doi.org/10.1109/MASS.2011.76

Dwork C, Naor M, 1993. Pricing via processing or combatting junk mail. In: Brickell EF (Ed.), Advances in Cryptology—CRYPTO' 92. Springer Berlin Heidelberg, p.139-147. https://doi.org/10.1007/3-540-48071-4_10

Elham H, Lebbat A, Medromi H, 2012. Enhance security of cloud computing through fork virtual machine. IEEE Int Conf on Complex Systems, p.1-4. https://doi.org/10.1109/ICoCS.2012.6458569

Eyal I, Sirer EG, 2018. Majority is not enough: Bitcoin mining

is vulnerable. *Commun ACM*, 61(7):95-102. https://doi.org/10.1145/3212998

Eyal I, Gencer AE, Sirer EG, et al., 2015. Bitcoin-NG: a scalable blockchain protocol. https://arxiv.org/abs/1510.02037

Ficco M, Esposito C, Xiang Y, et al., 2017. Pseudo-dynamic testing of realistic edge-fog cloud ecosystems. *IEEE Commun Mag*, 55(11):98-104. https://doi.org/10.1109/MCOM.2017.1700328

Formisano C, Pavia D, Gurgen L, et al., 2015. The advantages of IoT and cloud applied to smart cities. 3rd Int Conf on Future Internet of Things and Cloud, p.325-332. https://doi.org/10.1109/FiCloud.2015.85

Foschini L, Taleb T, Corradi A, et al., 2011. M2M-based metropolitan platform for IMS-enabled road traffic management in IoT. *IEEE Commun Mag*, 49(11):50-57. https://doi.org/10.1109/MCOM.2011.6069709

Gaetani E, Aniello L, Baldoni R, et al., 2017. Blockchain-based database to ensure data integrity in cloud computing environments. Italian Conf on Cybersecurity. https://eprints.soton.ac.uk/411996/ [Accessed on Sept. 27, 2018].

Garai Á, Attila A, Péntek I, 2016. Cognitive telemedicine IoT technology for dynamically adaptive eHealth content management reference framework embedded in cloud architecture. 7th IEEE Int Conf on Cognitive Infocommunications, p.187-192. https://doi.org/10.1109/CogInfoCom.2016.7804547

Gervais A, Karame GO, Wüst K, et al., 2016. On the security and performance of proof of work blockchains. Proc ACM SIGSAC Conf on Computer and Communications Security, p.3-16. https://doi.org/10.1145/2976749.2978341

Goiri Í, Beauchea R, Le K, et al., 2011a. Greenslot: scheduling energy consumption in green datacenters. Proc Int Conf for High Performance Computing, Networking, Storage and Analysis, p.1-11. https://doi.org/10.1145/2063384.2063411

Goiri Í, Le K, Guitart J, et al., 2011b. Intelligent placement of datacenters for Internet services. 31st Int Conf on Distributed Computing Systems, p.131-142. https://doi.org/10.1109/ICDCS.2011.19

Granjal J, Monteiro E, Sá Silva J, 2013a. End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. IFIP Networking Conf, p.1-9. http://ieeexplore.ieee.org/abstract/document/6663530/ [Accessed on Feb. 24, 2018].

Granjal J, Monteiro E, Sá Silva J, 2013b. Application-layer security for the WoT: extending CoAP to support end-to-end message security for Internet-integrated sensing applications. *LNCS*, 7889:140-153. https://doi.org/10.1007/978-3-642-38401-1_11

Granjal J, Monteiro E, Sá Silva J, 2015. Security for the Internet of Things: a survey of existing protocols and open research issues. *IEEE Commun Surv Tutor*, 17(3): 1294-1312. https://doi.org/10.1109/COMST.2015.2388550

Hameed A, Khoshkbarforoushha A, Ranjan R, et al., 2016. A survey and taxonomy on energy efficient resource allocation techniques for cloud computing systems. *Computing*, 98(7):751-774. https://doi.org/10.1007/s00607-014-0407-8

Henze M, Wolters B, Matzutt R, et al., 2017. Distributed configuration, authorization and management in the cloud-based Internet of Things. IEEE Trustcom/ BigDataSE/ICESS, p.185-192. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.236

Hilton S, 2016. Dyn analysis summary of Friday October 21 Attack. Company News. https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ [Accessed on Feb. 24, 2018].

Hong YWP, Lan PC, Kuo CCJ, 2013. Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. *IEEE Signal Process Mag*, 30(5):29-40. https://doi.org/10.1109/MSP.2013.2256953

Hummen R, Hiller J, Wirtz H, et al., 2013. 6LoWPAN fragmentation attacks and mitigation mechanisms. Proc 6th ACM Conf on Security and Privacy in Wireless and Mobile Networks, p.55-66. https://doi.org/10.1145/2462096.2462107

Hur J, Noh DK, 2011. Attribute-based access control with efficient revocation in data outsourcing systems. *IEEE Trans Parall Distrib Syst*, 22(7):1214-1221. https://doi.org/10.1109/TPDS.2010.203

Jagdeep K, Meghna S, 2017. Extending IoTs into the cloud-based platform for examining Amazon web services. Examining Cloud Computing Technologies Through the Internet of Things, p.216-227.

Jakobsson M, Juels A, 1999. Proofs of work and bread pudding protocols (extended abstract). In: Preneel B (Ed.), Secure Information Networks. Springer, Boston, MA, p.258-272. https://doi.org/10.1007/978-0-387-35568-9_18

Juniper Research, 2015. Cybercrime will cost businesses over $2 trillion by 2019. Press Releases. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion [Accessed on Feb. 24, 2018].

Khan MA, Salah K, 2018. IoT security: review, blockchain solutions, and open challenges. *Fut Gener Comput Syst*, 82:395-411. https://doi.org/10.1016/j.future.2017.11.022

Khosravi A, Buyya R, 2018. Energy and carbon footprint-aware management of geo-distributed cloud data centers: a taxonomy, state of the art, and future directions. https://www.igi-global.com/chapter/energy-and-carbon-footprint-aware-management-of-geo-distributed-cloud-data-centers/189954 [Accessed on Sept. 22, 2018].

Kim HG, 2008. Protection against packet fragmentation attacks at 6LoWPAN adaptation layer. Proc Int Conf on Convergence and Hybrid Information Technology, p.796-

801. https://doi.org/10.1109/ICHIT.2008.261

Kokoris-Kogias E, Jovanovic P, Gailly N, et al., 2016. Enhancing Bitcoin security and performance with strong consistency via collective signing. https://arxiv.org/abs/1602.06997

Kshetri N, 2017a. Can blockchain strengthen the Internet of Things? *IT Prof*, 19(4):68-72. https://doi.org/10.1109/MITP.2017.3051335

Kshetri N, 2017b. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun Pol*, 41(10): 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Li DR, Shen X, Chen NC, et al., 2017. Space-based information service in Internet plus era. *Sci China Inform Sci*, 60(10):102308. https://doi.org/10.1007/s11432-016-9164-1

Li JW, Jia CF, Li J, et al., 2012. Outsourcing encryption of attribute-based encryption with mapreduce. *LNCS*, 7618: 191-201. https://doi.org/10.1007/978-3-642-34129-8_17

Li Y, Marier-Bienvenue T, Perron-Brault A, et al., 2018. Blockchain technology in business organizations: a scoping review. Proc 51st Hawaii Int Conf on System Sciences. https://doi.org/10.24251/HICSS.2018.565

Liao CF, Bao SW, Cheng CJ, et al., 2017. On design issues and architectural styles for blockchain-driven IoT services. IEEE Int Conf on Consumer Electronics, p.351-352. https://doi.org/10.1109/ICCE-China.2017.7991140

Lin IC, Liao TC, 2017. A survey of blockchain security issues and challenges. *Int J Netw Secur*, 19(5):653-659. https://doi.org/10.6633/IJNS.201709.19(5).01

Liu CH, Yang B, Liu TC, 2014. Efficient naming, addressing and profile services in Internet-of-Things sensory environments. *Ad Hoc Netw*, 18:85-101. https://doi.org/10.1016/j.adhoc.2013.02.008

Luu L, Chu DH, Olickel H, et al., 2016a. Making smart contracts smarter. Proc ACM SIGSAC Conf on Computer and Communications Security, p.254-269. https://doi.org/10.1145/2976749.2978309

Luu L, Narayanan V, Zheng CD, et al., 2016b. A secure sharding protocol for open blockchains. Proc ACM SIGSAC Conf on Computer and Communications Security, p.17-30. https://doi.org/10.1145/2976749.2978389

Mahalle PN, Anggorojati B, Prasad NR, et al., 2013. Identity authentication and capability based access control (IACAC) for the Internet of Things. *J Cyber Secur Mob*, 1:309-348.

Manral J, 2015. IoT enabled insurance ecosystem—possibilities, challenges and risks. http://arxiv.org/abs/1510.03146

Marinakis YD, Walsh ST, Harms R, 2017. Internet of Things technology diffusion forecasts. Portland Int Conf on Management of Engineering and Technology, p.1-5. https://doi.org/10.23919/PICMET.2017.8125435

Memon RA, Li JP, Ahmed J, 2019a. Simulation model for blockchain systems using queuing theory. *Electronics*, 8(2):234. https://doi.org/10.3390/electronics8020234

Memon RA, Li JP, Ahmed J, et al., 2019b. Modeling of blockchain based systems using queuing theory simulation. 15th Int Computer Conf on Wavelet Active Media Technology and Information Processing, p.107-111. https://doi.org/10.1109/ICCWAMTIP.2018.8632560

Moar J, 2017. Cybercrime & the Internet of Threats. White Paper, Juniper Research.

Mollah MB, Azad MAK, Vasilakos A, 2017. Security and privacy challenges in mobile cloud computing: survey and way ahead. *J Netw Comput Appl*, 84:38-54. https://doi.org/10.1016/j.jnca.2017.02.001

Mosakheil JH, 2018. Security threats classification in blockchains. http://repository.stcloudstate.edu/msia_etds/48 [Accessed on Sept. 25, 2018].

Nakamoto S, 2008. Bitcoin: a peer-to-peer electronic cash system. https://bitcoinsv.io/bitcoin

Nakano SM, 2018. Cryptocurrency and Blockchain Blueprint for Beginners: All You Need to Know about Bitcoin, Ethereum, Ripple, Litecoin and other Popular Cryptocurrencies. CreateSpace Independent Publishing Platform, USA.

Ning HS, Liu H, 2015. Cyber-physical-social-thinking space based science and technology framework for the Internet of Things. *Sci China Inform Sci*, 58(3):1-19. https://doi.org/10.1007/s11432-014-5209-2

Noubir G, Lin GL, 2003. Low-power DOS attacks in data wireless LANs and countermeasures. *ACM SIGMOBILE Mob Comput Commun Rev*, 7(3):29-30. https://doi.org/10.1145/961268.961277

Ourad AZ, Belgacem B, Salah K, 2018. Using blockchain for IoT access control and authentication management. *LNCS*, 10972:150-164. https://doi.org/10.1007/978-3-319-94370-1_11

Qi RM, Feng C, Liu Z, et al., 2017. Blockchain-powered Internet of Things, E-governance and E-democracy. In: Vinod KT (Ed.), E-Democracy for Smart Cities. Springer, Singapore, p.509-520. https://doi.org/10.1007/978-981-10-4035-1_17

Qian XC, Zhang JD, 2010. Study on the structure of "Internet of Things (IoT)" business operation support platform. IEEE 12th Int Conf on Communication Technology, p.1068-1071. https://doi.org/10.1109/ICCT.2010.5688537

Ray PP, 2016. A survey of IoT cloud platforms. *Fut Comput Inform J*, 1(1-2):35-46. https://doi.org/10.1016/j.fcij.2017.02.001

Riaz R, Kim KH, Ahmed HF, 2009. Security analysis survey and framework design for IP connected LoWPANs. Proc Int Symp on Autonomous Decentralized Systems, p.29-34. https://doi.org/10.1109/ISADS.2009.5207373

Rimal BP, Choi E, Lumb I, 2009. A taxonomy and survey of cloud computing systems. 5th Int Joint Conf on INC, IMS, and IDC, p.44-51. https://doi.org/10.1109/NCM.2009.218

Rimba P, Tran AB, Weber I, et al., 2017. Comparing blockchain and cloud services for business process

execution. IEEE Int Conf on Software Architecture, p.257-260. https://doi.org/10.1109/ICSA.2017.44

Sagiroglu S, Sinanc D, 2013. Big data: a review. Int Conf on Collaboration Technologies and Systems, p.42-47. https://doi.org/10.1109/CTS.2013.6567202

Samaniego M, Deters R, 2017. Blockchain as a service for IoT. IEEE Int Conf 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), p.433-436. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

SAP, 2017. SAP announces first co-innovation customers, partners in blockchain initiative for Internet of Things. https://news.sap.com/sap-announces-first-co-innovation-customers-partners-in-blockchain-initiative-for-internet-of-things/ [Accessed on Feb. 24, 2018].

Seibold S, Samman G, 2016. Consensus immutable agreement for the Internet of Value. Technical Report. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

Sethi M, Arkko J, Keränen A, 2012. End-to-end security for sleepy smart object networks. 37th Annual IEEE Conf on Local Computer Networks, p.964-972. https://doi.org/10.1109/LCNW.2012.6424089

Sherif MH, 2016. Protocols for Secure Electronic Commerce (3rd Ed.). CRC Press, Boca Raton, USA.

Shveta, Pandey A, 2014. Energy conservation and security issues in cloud computing: a review. *Int J Adv Comput Sci Cloud Comput*, 2(1):57-60.

Sicari S, Rizzardi A, Grieco LA, et al., 2015. Security, privacy and trust in Internet of Things: the road ahead. *Comput Netw*, 76:146-164. https://doi.org/10.1016/j.comnet.2014.11.008

Singh D, Tripathi G, Jara AJ, 2014. A survey of Internet-of-Things: future vision, architecture, challenges and services. IEEE World Forum on Internet of Things, p.287-292. https://doi.org/10.1109/WF-IoT.2014.6803174

Singh I, Lee SW, 2018. Comparative requirements analysis for the feasibility of blockchain for secure cloud. In: Kamalrudin M, Ahmad S, Ikram N (Eds.), Requirements Engineering for Internet of Things. Springer, Singapore, p.57-72. https://doi.org/10.1007/978-981-10-7796-8_5

Singh J, Pasquier T, Bacon J, et al., 2016. Twenty security considerations for cloud-supported Internet of Things. *IEEE Int Things J*, 3(3):269-284. https://doi.org/10.1109/JIOT.2015.2460333

Singhal B, Dhameja G, Panda PS, 2018. Building an Ethereum DApp. In: Beginning Blockchain. Apress, Berkeley, CA, p.319-375. https://doi.org/10.1007/978-1-4842-3444-0_6

Soubra D, 2012. The 3Vs that define Big Data. https://www.datasciencecentral.com/forum/topics/the-3vs-that-define-big-data

Stergiou C, Psannis KE, Kim BG, et al., 2018. Secure integration of IoT and cloud computing. *Fut Gener Comput Syst*, 78:964-975. https://doi.org/10.1016/j.future.2016.11.031

Stormer H, Meier A, 2012. ePayment. In: eBusiness & eCommerce. Springer Berlin Heidelberg, p.181-202. https://doi.org/10.1007/978-3-642-29802-8_7

Strite CP, 1920. Bread-Toaster. US1394450A. https://patents.google.com/patent/US1394450 [Accessed on Feb. 23, 2018].

Sun L, Li Y, Memon RA, 2017. An open IoT framework based on microservices architecture. *China Commun*, 14(2):154-162. https://doi.org/10.1109/CC.2017.7868163

Szabo N, 1996. Smart contracts: building blocks for digital markets. http://www.alamut.com/subj/economics/nick_szabo/smartContracts.html [Accessed on Feb. 24, 2018].

Thakur M, 2017. Authentication, authorization and accounting with Ethereum blockchain. https://helda.helsinki.fi/bitstream/handle/10138/228842/aaa-ethereum-blockchain.pdf [Accessed on Sept. 11, 2018].

Underwood S, 2016. Blockchain beyond Bitcoin. *Commun ACM*, 59(11):15-17. https://doi.org/10.1145/2994581

van der Meulen R, 2017. Gartner Says 8.4 Billion Connected "Things" will be in use in 2017, up 31 Percent from 2016. Gartner Press Release.

Wang J, Wu P, Wang XY, et al., 2017. The outlook of blockchain technology for construction engineering management. *Front Eng Manag*, 4(1):67-75. https://doi.org/10.15302/J-FEM-2017006

Wang WB, Fan SQ, 2018. Attacking OpenSSL ECDSA with a small amount of side-channel information. *Sci China Inform Sci*, 61(3):032105. https://doi.org/10.1007/s11432-016-9030-0

Wang YF, Uehara T, Sasaki R, 2015. Fog computing: issues and challenges in security and forensics. IEEE 39th Annual Computer Software and Applications Conf, p.53-59. https://doi.org/10.1109/COMPSAC.2015.173

Warren W, Bandeali A, 2017. 0x: an open protocol for decentralized exchange on the ethereum blockchain. https://0x.org/pdfs/0x_white_paper.pdf [Accessed on Feb. 24, 2018].

Weekly K, Pister K, 2012. Evaluating sinkhole defense techniques in RPL networks. 20th Int Conf on Network Protocols, p.1-6. https://doi.org/10.1109/ICNP.2012.6459948

Whitmore A, Agarwal A, Da XL, 2015. The Internet of Things—a survey of topics and trends. *Inform Syst Front*, 17(2):261-274. https://doi.org/10.1007/s10796-014-9489-2

Wilkinson S, Boshevski T, Brandoff J, et al., 2014. Storj—a peer-to-peer cloud storage network. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.693.785 [Accessed on Sept. 15, 2018].

Wilusz D, Rykowski J, 2013. The architecture of coupon-based, semi-off-line, anonymous micropayment system for Internet of Things. In: Camarinha-Matos LM, Tomic S, Graça P (Eds.), Technological Innovation for the Internet of Things. Springer Berlin Heidelberg, p.125-132. https://doi.org/10.1007/978-3-642-37291-9_14

Worldometer, 2018. World Population Projections. http://www.worldometers.info/world-population/world-population-projections/ [Accessed on Sept. 15, 2018].

Xiao L, Greenstein LJ, Mandayam NB, et al., 2009. Channel-based detection of Sybil attacks in wireless networks. *IEEE Trans Inform Forens Secur*, 4(3):492-503. https://doi.org/10.1109/TIFS.2009.2026454

Xiong ZH, Zhang Y, Niyato D, et al., 2017. When mobile blockchain meets edge computing. https://arxiv.org/abs/1711.05938?context=cs

Xu WY, Trappe W, Zhang YY, et al., 2005. The feasibility of launching and detecting jamming attacks in wireless networks. Proc 6th ACM Int Symp on Mobile Ad Hoc Networking and Computing, p.46-57. https://doi.org/10.1145/1062689.1062697

Yang C, Puthal D, Mohanty SP, et al., 2017. Big-sensing-data curation for the cloud is coming: a promise of scalable cloud-data-center mitigation for next-generation IoT and wireless sensor networks. *IEEE Consum Electron Mag*, 6(4):48-56. https://doi.org/10.1109/MCE.2017.2714695

Yao Q, 2018. A systematic framework to understand central bank digital currency. *Sci China Inform Sci*, 61(3): 033101. https://doi.org/10.1007/s11432-017-9294-5

Yi SH, Qin ZR, Li Q, 2015. Security and privacy issues of fog computing: a survey. In: Xu K, Zhu H (Eds.), Wireless Algorithms, Systems, and Applications. Springer, Cham, p.685-695. https://doi.org/10.1007/978-3-319-21837-3_67

Zhao JC, Zhang JF, Feng Y, et al., 2010. The study and application of the IoT technology in agriculture. 3rd Int Conf on Computer Science and Information Technology, p.462-465. https://doi.org/10.1109/ICCSIT.2010.5565120

Zhao W, Wang CW, Nakahira Y, 2011. Medical application on Internet of Things. IET Int Conf on Commun Technology and Application, p.660-665. https://doi.org/10.1049/cp.2011.0751

Zhou J, Cao ZF, Dong XL, et al., 2017. Security and privacy for cloud-based IoT: challenges. *IEEE Commun Mag*, 55(1):26-33. https://doi.org/10.1109/MCOM.2017.1600363CM