Technical aspects of blockchain and IoT

Hany F. Atlam[a,b], **Gary B. Wills**[a]
[a]Electronic and Computer Science Department, University of Southampton, Southampton, United Kingdom
[b]Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt

Contents

Abstract

Blockchain technology is getting a growing attention from various organizations and researchers as it provides magical solutions to the problems associated with the classical centralized architecture. Blockchain, whether public or private, is a distributed ledger with the capability of maintaining the integrity of transactions by decentralizing the ledger among participating users. On the other hand, the Internet of Things (IoT) represents a revolution of the Internet which can connect nearly all environment devices over the Internet to share their data to create novel services and applications for improving our

Advances in Computers
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2018.10.006

quality of life. Although the centralized IoT system provides countless benefits, it raises several challenges. Resolving these challenges can be done by integrating IoT with blockchain technology. To be prepared for the integration process, this chapter provides an overview of technical aspects of the blockchain and IoT. It started by reviewing blockchain technology and its main structure. Applications and challenges of the blockchain are also presented. This is followed by reviewing the IoT system by highlighting common architecture and essential characteristics. Various applications and challenges of the IoT system are also discussed.

1. Introduction

Before the invention of the blockchain, managing various activities and actions over the Internet was achieved through a centralized server to guarantee non-repudiation of data. A group of distributed entities could not verify transactions without using the centralized authority [1]. There was no trust between communicating parties, so a third party was needed to build the required trust and manage the communication process. This problem was known as the Byzantine Generals Problem (BGP) [2]. This problem supposed that there were three sections of the Byzantine army waiting outside an enemy city and planning to attack it. The army general of each section was independent; however, a common course of action should be achieved to be able to conquer the city. The army generals' capabilities to interconnect with one another were only allowed through a messenger service, and there was a traitor who corrupts generals' actions to make sure there is no chance to make a united attack [3].

To find a solution to the problem of Byzantine generals, the blockchain increases transparency and reliability by using a probabilistic approach to distribute data among several users of the network. Generally, blockchain is a distributed database/ledger of transactions used to manage a constantly increasing set of records. It provides an efficient way to maintain security and data integrity in which a transaction must be verified by the majority of participating users in the blockchain network to be eligible to add in the ledger [3,4]. The blockchain does not use a third party to store information instead, every participating user in the blockchain network holds a genuine copy of the ledger. So, if a user has breached and added a malicious transaction, the system will discard it, as it should be verified by all other network users. Also, there is a multi-signature protection to validate each transaction, which adds another layer of security [5]. Therefore, injecting the distributed ledger with false or malicious data by an intruder or malicious user is

significantly reduced. It is possible to happen but only if the intruder uses more computational power than the complete blockchain network, which is very rare to occur [6].

Another technology added significant developments to our community by having the capability to connect environment devices over the Internet to share their data and create new applications and services for improving our quality of life. This technology is known as the Internet of Things (IoT). The IoT is considered as an evolution of the Internet which involves both virtual and physical things of our environment, which are in billions [7]. Using a set of cheap sensors, the IoT enables several advantages to users by collecting relevant information that will ultimately change their lifestyles and improve their quality of life [8].

The next phase of developments is to merge the IoT with blockchain technology. Although the centralized IoT architecture provides various benefits, it raises severe challenges regarding costs, scalability and security. The blockchain provides a decentralized model that can process billions of operations between various IoT devices. This is, in turn, will reduce the costs associated with building and maintaining large centralized data centers. Moreover, in the absence of a third party, the security issues regarding the single point of failure will be eliminated [6].

To be prepared for the integration of IoT with blockchain, this chapter presents technical aspects of blockchain and IoT. It started by providing a discussion of the blockchain technology and its main components. Current applications and challenges of the blockchain are also presented. This is followed by providing an overview of the IoT system including its common architecture and essential characteristics. Various applications and challenges of the IoT system are also discussed.

This chapter is structured as follows; Section 2 provides the technical aspects of blockchain technology by discussing its history, structure, main characteristics, applications and challenges; Section 3 presents an overview of the IoT system by providing its definitions, architecture, essential characteristics, applications and challenges; and Section 4 is the conclusion.

2. Blockchain technology

This section provides a discussion of the technical aspects of blockchain technology. It discusses various definitions of blockchain with highlighting its essential characteristic and different types of the blockchain. Various applications and challenges of the blockchain are also presented.

2.1 An overview of blockchain

Blockchain is a distributed and decentralized ledger of transactions used to manage a constantly increasing set of records. To store a transaction in the ledger, the majority of participating users in the blockchain network should agree and record their consent. A set of transactions are grouped together and allocate a block in the ledger, which is chained of blocks. To link the blocks together, each block encompasses a timestamp and hash function to the previous block. The hash function validates the integrity and non-repudiation of the data inside the block. Moreover, to keep all participating users of the blockchain network updated, each user holds a copy of the original ledger and all users are synchronized and updated with newly change [4].

Blockchain has defined by many organizations from different perspectives. For instance, Coinbase, the world's largest cryptocurrency exchange, defined blockchain as "*a distributed, public ledger that contains the history of every bitcoin transaction*" [9]. This definition explains the blockchain from the cryptocurrency's perspective which does not consider the fact that the blockchain can be used in various applications independently. Whereas Oxford dictionary provides a more common definition for the blockchain. It stated "*a digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly*" [10].

In addition, a broader definition for the blockchain is provided by Webopedia. It stated "*a type of data structure that enables identifying and tracking transactions digitally and sharing this information across a distributed network of computers, creating in a sense a distributed trust network. The distributed ledger technology offered by blockchain provides a transparent and secure means for tracking the ownership and transfer of assets*" [11]. This definition provides a more detailed description of the blockchain by highlighting its essential features with confirming that the blockchain is not only a distributed technology but also a decentralized environment.

Moreover, highlighting the main elements of blockchain technology, Sultan et al. [12] provides a general definition for the blockchain. It stated "*a decentralized database containing sequential, cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model.*"

2.2 History of blockchain

The history of blockchain technology has their roots in the 1980s and 1990s in the 20th century. However, it became widely acknowledged in 2008 after

the discovery of the Bitcoin. According to Pilkington [13], the first notion of digital currency was invented based on a centralized server to avoid double-spending, which is the process of using the same bitcoins more than once. However, this perception failed to provide a solution for double-spending, anonymity and centralization problems.

The world remains several years to utilize the centralized architecture which use a third party to control and maintain the trust between communication parties until Szabo at the end of 1990 invented a decentralized digital currency which was called bit gold. After about 10 years, Bitcoin cryptocurrency was presented. Blockchain became broadly popular after the legendary paper of Nakamoto [6]. He proposed substituting the classical centralized architecture with a new technique based on a consensus mechanism. Initially, the technology was named as blockchain as two words "block" and "chain"; however, by 2016, two words are combined into one word to be what we all know now blockchain [14].

During the period from 2011 to 2013, blockchain has widely used in cryptocurrencies especially in currency transfer and digital payment. Nowadays, blockchain technology has emerged in various applications and services to make use of decentralization and immutability features. Fig. 1 depicts the history of blockchain technology from 1990 till now.

2.3 Building blocks of blockchain

Blockchain technology has the potential to deliver an effective way of storing transactions in the ledger with ensuring transparency, security and auditability. Although the blockchain still in the early stage of approval, the

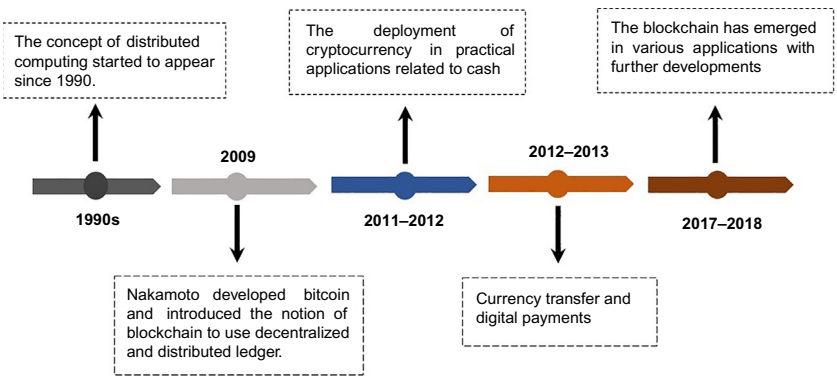

Fig. 1 History of the blockchain.

commercial community should adopt it for industries and businesses to avoid disruptive surprises or wasted chances.

The next section provides a brief discussion of significant building blocks of blockchain technology.

2.3.1 Database

A classical database is a data structure used for storing information. It uses a relational model to provide more composite ways of querying and collecting data by linking information from multiple databases. The information stored in databases can be organized using a DataBase Management System (DBMS). A simple database is stored in data elements called a table which contains fields. Each field contains columns to describe the field and rows to define a record stored in the database [15].

One of the main elements of the blockchain is the database. However, this is not a normal database containing rows and columns; instead, it is a ledger of all previous transactions for all participating users within the blockchain network. This type of databases is characterized by having a high-throughput, decentralized control, low latency, immutable data storage and built-in security.

2.3.2 Block

Block is the key storage element in the blockchain. It contains and perseveres data related to multiple transactions. The blocks are chained together by storing the hash of the previous block in the current block, which makes blocks chained as a circle for enclosure in the public ledger.

Blocks are typically divided into two segments, header and a group of transactions. The header contains the block metadata which is used to contain all details about the block in the ledger [16]. Fig. 2 shows the structure of a block and illustrates how blocks chained together with the block header information described as follows:

- *Version number*: 4 bytes to indicate the version number of the *block*.
- *Previous block hash*: 32 bytes to describe the hash of the previous block of the blockchain. It acts as a pointer between the current block and the previous block in the ledger.
- *Timestamp*: 4 bytes to record the time at which the block has been created.
- *Merkle tree*: 32 bytes which are a hash (SHA-256) of all transactions that are related to this block.
- *Difficulty target*: 4 bytes to identify the difficulty target of the block.
- *Nonce*: 4 bytes to create the block and compute different hashes.

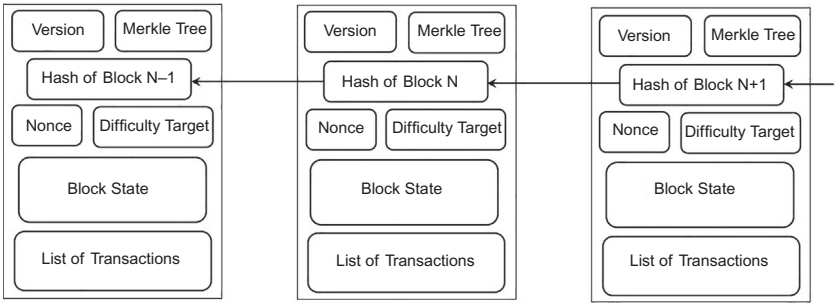

Fig. 2 Structure of block showing how blocks chained together with header information.

2.3.3 Hash

The hash function is a complex mathematical problem which the miners have to solve in order to find a block. The notion of hash function is used as a way to search for data in a database. Hash functions are collision-free, which means it is very difficult to find two identical hashes for two different messages. Hence, the blocks are identified through their hash, serving two purposes; identification and integrity verification [17].

For linking blocks together, each block encompasses the hash of its parent inside its own header which places a chain going all the way back to the first block which creates a sequence of hashes. The hash values are kept in a hash table which is a well-organized indexing mechanism to increase the performance of the search operations [18].

2.3.4 Minor

A CPU that tries to solve a computationally intense mathematical problem to discover a novel block is known as a miner. The miners can work either alone or in pools to try to find out the solution of the mathematical problem.

The process of finding a new block is started by broadcasting new transactions to all the users of the blockchain network. Each user collects new transactions into a block and works to find the block's proof-of-work. If a user finds it, the block will be broadcasted to all the users to verify it. The block will be verified only if all inside transactions are valid. The block can be considered as accepted from all the participating users in the blockchain network when they start working on generating the next block in the chain using the hash of the accepted block as the previous hash. In some cases, the transactions with the highest costs are first selected from minors, since the minor who finds the block earns the costs or fees of all the transactions in that block [17].

2.3.5 Transaction

A blockchain transaction can be defined as a small unit of task that is stored in public records. These records are implemented, executed and stored in the blockchain only after being verified by the majority of users involved in the blockchain network. Each previous transaction can be reviewed at any time but cannot be updated. The size of the transaction is significant for miners since larger transactions need more space in the block and consume more power, while smaller transactions are easier to validate and consume less power [18].

2.3.6 Consensus mechanism

Blockchain is a type of distributed ledger used to store a record of all previous transactions. It called distributed since it is stored across multiple computers over the network worldwide. The main operation of a distributed ledger is to guarantee that the entire network approves the contents of the ledger, which is done by using the consensus mechanism.

There are a number of consensus mechanisms. However, the most common blockchain consensus mechanisms are Proof of Stake (PoS) and Proof of Work (PoW). The key difference between various consensus mechanisms is the way they delegate and reward the verification of transactions [15].

PoW is a popular consensus mechanism used by the most widespread cryptocurrency networks like Bitcoin and Litecoin. The participant-user in the blockchain network is required to prove the work was done to qualify them to obtain the ability to add new blocks to the ledger. However, the mining process requires high energy consumption and processing time. PoS is another public consensus mechanism to provide a low-cost, low-energy consumption in comparison with the PoW mechanism. Also, it allocates the responsibility to the participant users in proportion to the number of virtual currency tokens held by it. However, this derives a downside as it encourages crypto-coin saving, instead of spending it [16].

2.4 Characteristics of blockchain

Blockchain can be considered as a decentralized architecture with built-in security to increase the trust and integrity of transactions. This section aims to provide a discussion of common characteristics associated with the blockchain. These features, as summarized in Fig. 3, include:

- *Decentralization*: In contrast to the centralized architecture which presents several issues including single point of failure and scalability, the blockchain uses a decentralized and distributed ledger to utilize the

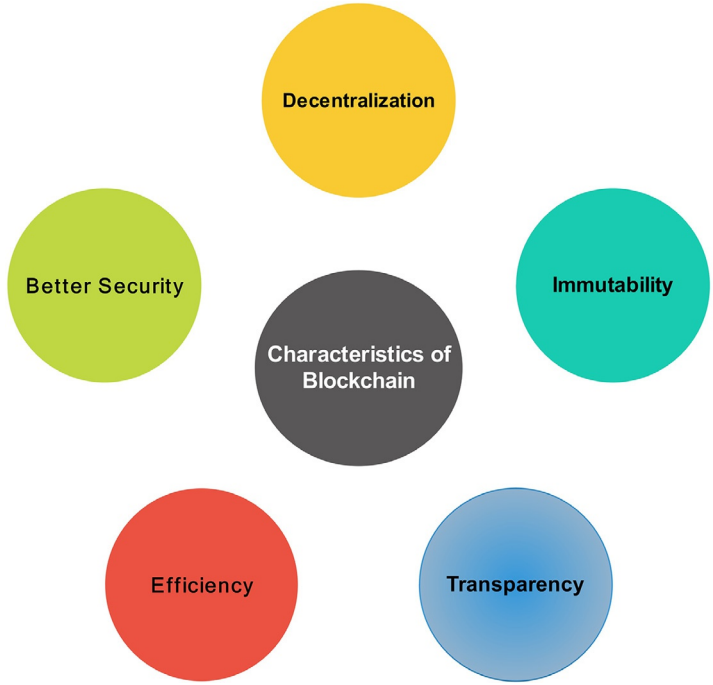

Fig. 3 Characteristics of the blockchain.

processing capabilities of all the participating users in the blockchain network, which reduce latency and eliminate the single point of failure.

- *Immutability*: One of the essential features of the blockchain is the ability to ensure the integrity of transactions by creating immutable ledgers. In traditional centralized architectures, databases can be altered and a trust with a third party needs to be created to guarantee information integrity. While in blockchain technology, since each block in the distributed ledger relates to the previous block constituting a chain of blocks, the blocks are permanently saved and never changed as long as the participating user continue to maintain the network [15].
- *Transparency*: Blockchain delivers a high level of transparency by sharing transaction details between all participants users involved in those transactions. In a blockchain environment, no need for a third party which improve business friendliness and guarantees a trusted workflow.
- *Better Security*: Although security represents an essential issue for most new technologies, blockchain provides better security since it uses public key infrastructure that protects against malicious actions to change data.

The participating users of the blockchain network place their trust in the integrity and security features of the consensus mechanism. In addition, blockchain eliminates the single point of failure which affects the entire system [12].

- *Efficiency*: Blockchain improves the classical centralized architecture by distributing database records between various users involved in the blockchain network. The distribution of transactions makes it more transparent to verify all records stored in the database. Blockchain is more efficient than the classical centralized architecture in terms of cost, settlement speed and risk management [19].

2.5 Types of blockchain

There are three types of blockchain; public, private and federated, as shown in Fig. 4.

- *Public Blockchain*: It is a blockchain that allows any anonymous user to be added to the blockchain network, sends a new transaction, verifies newly added blocks and reads the content of the blockchain. Public blockchain is open for all types of entities to participate in the network. Securing the public blockchain is done using cryptoeconomics which is a mixture of cryptographic verification and economic incentives using consensus

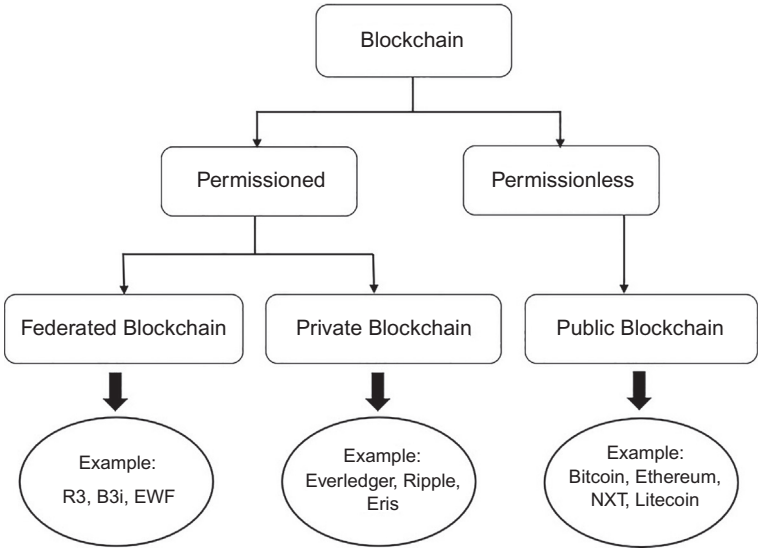

Fig. 4 Types of blockchains.

mechanisms such as PoW or PoS. There are many examples of public blockchains; however, the most common are Ethereum, Bitcoin and NXT [20].

- *Private Blockchain*: In this type of blockchains, only a specific organization has the authority to join the blockchain network, send a new transaction, and participate in the consensus mechanism. Users willing to participate have to gain their permissions from the organization before joining the blockchain network. Likely applications that used private blockchain include database management and auditing. Common instances of private blockchain are Ripple, Everledger and Eris [21]. In comparison with public blockchain, the private blockchain is easier since the number of participating users are small so that verifying the new blocks does not take huge processing power and time. Also, the private blockchain provides a better privacy as only users identified within the blockchain network can read the transactions.
- *Federated Blockchain*: It is considered as partly private blockchain. It is operated under the authority of a group of companies or organizations. So, it is a private blockchain for a specific set of organizations. Unlike public blockchain, federated blockchain is faster and delivers better scalability and privacy. Examples of federated blockchains are R3, EWF, and B3i [13].

Table 1 provides a comparison between public, private and federated blockchains in terms of access permission, speed of transaction execution, efficiency, security, immutability, consensus mechanism, network and asset.

2.6 How does blockchain work?

As said earlier, the blockchain is a decentralized and distributed ledger for maintaining the integrity of transactions. Before discussing how the blockchain works, let us talk about the classical ledger or centralized architecture. For a long time, ledgers were used as means for bankers and governments to store various transactions regarding land possession and other activities that require maintaining a record of the transaction. Maintaining and building a trust relationship between parties of a certain transaction were the major problem, so the bank or government office was used as a central authority to accomplish the required changes in the transactions and design contracts to define who possess what. Therefore, distinguishing between genuine and fake transactions are only done by the central authority.

The ledger manager (bank or government office) built the required trust, so people can sell and buy without having to worry since the centralized

Table 1 Differences between public, private and federated blockchain.

Item	Public	Private	Federated
Access	Read/write for anyone	Read/write for a single organization	Read/write for multiple selected organizations
Speed	Slower	Lighter and faster	Lighter and faster
Efficiency	Low	High	High
Security	Proof of work, proof of stake, and other consensus mechanisms	Pre-approved participants and voting/multi-party consensus	Pre-approved participants and voting/multi-party consensus
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Consensus process	Permissionless and anonymous	Permissioned and known identities	Permissioned and known identities
Network	Decentralized	Partially decentralized	Partially decentralized
Asset	Native Asset	Any Asset	Any Asset

manager controls the access to their information on the ledger. These ledgers are totally centralized in which a third-party person or organization is trusted by all users and has a full control over transactions management. Also, these ledgers are black-boxed since the ledger contents are only visible to the ledger manager.

On the other hand, blockchain provides similar functions in terms of storing and maintaining transactions but no third-party (ledger manager) is required. It solves the problem of the central authority that verifies transactions by decentralizing the ledger in which each participating user within the blockchain network holds a copy of the original ledger. In addition, any participating user can request to add a transaction; however, the transaction is added to the block only if the majority of participating users in the blockchain network verify it. An automatic checking is reliably done for each user to generate a fast and protected ledger that is significantly tamper-proof the transactions and blocks [22].

Once a transaction is verified, it will be added and linked with other transactions in a block, which is linked with previous blocks in the ledger through a timestamp and hash function. This forms chains of blocks, which create what is known as blockchain. Once the block is generated, all

participating users in the blockchain network start to look for the next block by trying to solve the complex mathematical function and generate a genuine encrypted block of transactions to add it to the ledger. This process is called mining, in which all users (minors) compete to generate the new block. The first minor to generate a genuine block and add it to the ledger is rewarded with the sum of fees for its transactions. Fees are applied to each transaction. Since blocks involve a large number of transactions which are added repeatedly, minors could collect multiple fees.

The ledger held by all participating users in the network is updated once a novel block is added. If the newly added block has been verified by all participating users and all its transactions are genuine, the block will be added and remains permanently in the ledger as a public record. If a conflict is discovered, the block will be discarded. Corrupting a classical ledger needs an attack on the third party (centralized manager). While the blockchain is immutable, so if there is a malicious attempt to alter the contact of any transaction, this will need repeated computations of PoW for the involved block and all other blocks afterward. These calculations are very difficult to accomplish unless most of the users in the blockchain network are malicious. Also, the possibility of having a fake ledger does not exist since all participating users have their own genuine copy of the ledger to compare with [23].

Fig. 5 shows the flow process of a typical financial transaction using the blockchain when a User A wants to send money to User B. The flow starts when User A requests to add a block to the ledger which contains information regarding his financial transfer transaction. After creating the block, it broadcasted between all participating users in the blockchain network to verify it. When the new block is verified by all participating users in the network, the block will be added to the ledger and the transfer operation will be completed. At last User B can receive the money.

2.7 Applications of blockchain

There are several applications that can benefit from various capabilities of blockchain technology. These applications include:

2.7.1 Music industry

Due to the evolution of the Internet and ease of accessibility to various streaming facilities over the Internet, the music industry has become one of the applications that can benefit from enormous benefits provided by blockchain technology. The music industry involves a variety of entities such as publishers, songwriters, artists, labels and streaming service providers. The music ownership has changed and become more difficult due to the

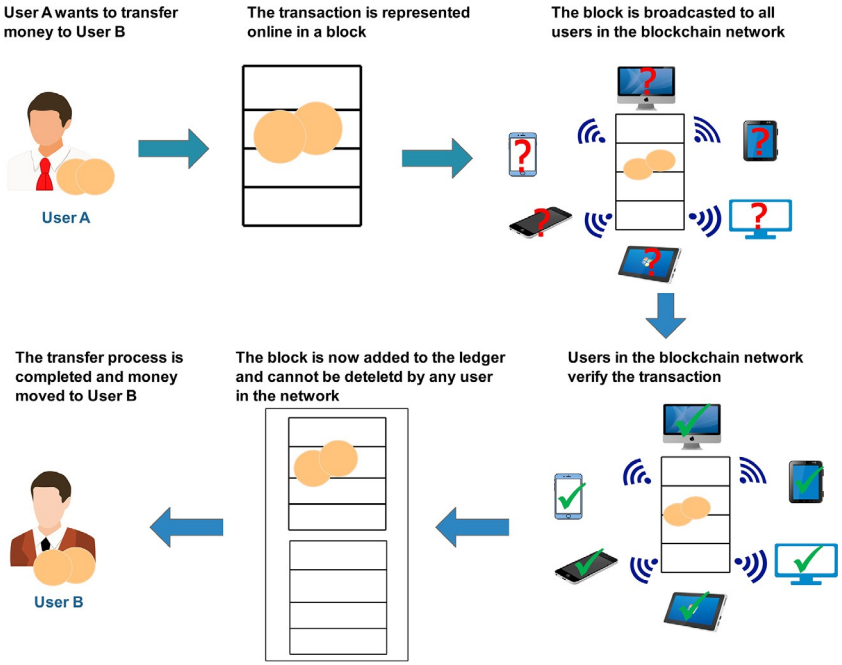

Fig. 5 The process of a financial transaction using the blockchain technology.

growth of the Internet. There is a need for transparency in the copyrights and ownership payments for songwriters and artists [24].

Integrating the music industry with blockchain technology can solve several issues regarding transparency and ownership payment. The blockchain can be used to create a precise distributed database to protect information of music rights in a ledger. Also, smart contracts can be used to provide a digital and secure contract for the music industry.

2.7.2 Education

Education is one of the applications that started to adopt the blockchain in interesting and innovative applications such as management of credentials and transcripts, proof of learning, management of reputation and management of student records. The blockchain can be used as a decentralized database to store different types of education information permanently. This, in turn, can help universities to adopt cryptographical-signed and confirmable certificate on the blockchain which allow both employers and students to access it easily [25].

Integrating the blockchain with learning societies can create innovative educational applications which build a new learning model where the exchange of ideas and concepts coupled with a tracking system for evaluating the learning results. The blockchain can be used in the regulation of contracts and payments to assess learning and record academic progress such as paying tuition fees by peer-teaching with other students.

2.7.3 Public services

Data generated by governmental organizations are internally fragmented and opaque to citizens and businesses. While with the use of blockchain technology, data records can be created and verified quickly with ensuring security and transparency of data. Blockchain features such as digital signatures and time-stamping are predicted to provide countless advantages in public services to allow citizens to handle transactions and generate accounts independently without the need for lawyers, government officials and other third parties.

Several governments started to adopt blockchain technology to support various public services to their citizens. For instance, the Estonian government has utilized blockchain technology to allow citizens to perform several tasks using their ID cards such as voting, register for their businesses, order medical prescriptions and pay taxes. In addition, the UK work and pensions department has started to adopt the blockchain in welfare payments. Also, Sweden has conducted tests to put real estate transactions on the blockchain [22].

2.7.4 Healthcare

Blockchain has great potentials to resolve interoperability problems of the existing healthcare systems. It can be utilized to enable healthcare objects and researchers to share their Electronic Health Record (EHR) in a safe and protected way. Also, it allows for improving medical care and doctor endorsement.

Managing the healthcare data whether by storing or analyzing is not an easy operation especially regarding data privacy. To provide a secure environment for the healthcare sector with blockchain, Healthcare Data Gateway (HDG) can be used to manage and control data storage and sharing easily. Also, improving privacy can be ensured by adopting the private blockchain which allows only specific persons to store or modify the medical information [26].

2.7.5 Cybersecurity

Security is one of the major issues for all current and new technologies. Popular companies faced many security problems. For instance, more than 50 million Facebook profiles have been breached by Cambridge Analytica to target them with personalized political advertisements which affected the US voters on their final decision on the presidential election. Also, in 2016, Yahoo, the famous search engine, faced a major attack and around one billion Yahoo accounts were compromised. When security companies did their research about common security vulnerabilities, they found that 65% of the data breaches were occurred because of weak, default, or stolen passwords. Also, they found phishing emails steal sensitive data such as username, password, and financial records [27].

Blockchain has several benefits that can be used to solve the cybersecurity issue. First, blockchain is a trustless system where people trust does not exist. It assumes that any insider or outsider can attack the system, so it is completely independent of human ethics. Second, blockchain is immutable, so anyone can store data and secure it with different cryptographic features such as hashing and digital signatures. As soon as data formed as a block in the blockchain, it cannot be altered or deleted. Third, blockchain involves multiple users in the network, so changing or adding a block needs to be verified by the majority of users which make the attack very difficult to achieve [16].

2.7.6 Voting

Voting is an important tool for any democratic government. It is a must process for all people; however, the traditional paper ballot system of voting faces several issues. For instance, the system cannot be automated, and people have to physically go to the venues where the ballot boxes are kept which make them wait in lines for long times. Also, counting the votes takes a long time and the election can be breached by inserting bogus ballot papers. Also, the cost and amount of papers wasted in the operation are very high [28].

With transparency and immutability features of the blockchain, the voting process can be much simpler and save the huge cost wasted in the classical paper ballot voting system. The voter can create a block, which is their vote, so once the vote is done, anyone can verify whether the signature is valid or not and make sure that none of the votes has been tampered with.

2.8 Challenges of blockchain

Blockchain is not straightforward. It raises several challenges with existing technologies that need to be resolved. These challenges are summarized in Fig. 6 and described as follows.

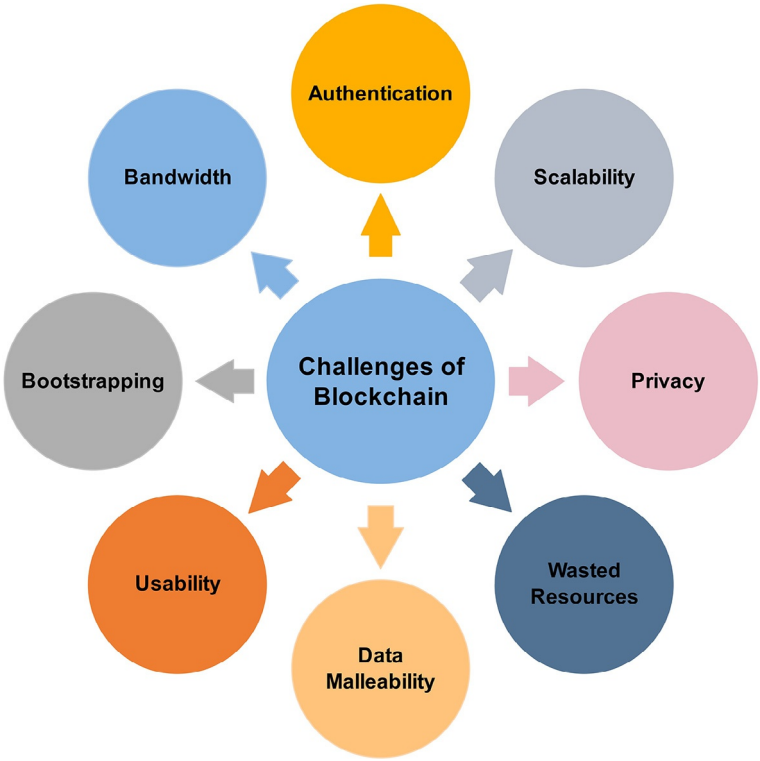

Fig. 6 Challenges of the blockchain technology.

- *Scalability*: As discussed earlier, every transaction is stored in the distributed ledger. These transactions are increasing every day. To validate a transaction, each user has to store it on the ledger to examine the source of the existing transaction. Moreover, creating a block faces several constraints regarding time and size. For example, Bitcoin can only create almost seven transactions per second, which cannot realize the processing needs of billions of transactions in real-time applications [21]. Also, the size of a transaction plays an important role in the execution order since minors prefer to generate blocks with large transaction size and high transaction fees. This leads to more latency for small transactions. Some research studies suggested solutions to the scalability issue. For instance, Bruce [29] proposed a storage optimization method for the blockchain to delete old transaction records from the ledger. However, more research is needed to address this challenge.
- *Privacy*: A certain amount of privacy can be protected through the blockchain technology. The user uses anonymous identity to create and verify transactions using their private and public key. However, since all participating users in the blockchain network can view values

of all transactions, the blockchain cannot guarantee transactions' privacy. Also, J. Barcelo indicated that the user's transaction can be linked to disclose user's personal information. Therefore, the privacy issue of blockchain technology needs more research to increase the adoption rate of blockchain in various applications.

- *Wasted Resources*: Till the moment, energy efficiency is one of the significant challenges in computer engineering that needs to be resolved. Regarding blockchain technology, the mining process needs a huge volume of computation power to compute and verify transactions in a secure manner. However, it is essential to reduce wasted resources in the mining process. Some researchers have proposed several solutions to resolve this problem. For example, Janish [30] has proposed a scheme to speed the mining process by using simultaneous Central Processing Units (CPUs) and Graphics Processing Units (GPUs) in individual machines in mining pools.
- *Data Malleability*: Maintaining the integrity of data is one of the critical aspects in the blockchain. Data should not be altered or tampered with when transmitted or verified. Malleability attack on data integrity indicates that the signature of transactions used to verify the possession of Bitcoin does not deliver any integrity assurance for signatures themselves. Consequently, an intruder can capture, alter, and rebroadcast a transaction which causes the transaction's creator to think that the transaction was not verified [31].
- *Usability*: The usability issue refers to the fact that the blockchain Application Programming Interface (API) is hard and difficult to use. The main target of all new technologies should involve providing usable and easy-to-use interfaces for both users and developers. Blockchain usability from the perspective of the cryptocurrency domain should allow users to analyze the blockchain. In the blockchain environment, blocks are generated continuously and validated by the participating users, which generate an exciting atmosphere of transaction flows. Therefore, it is critical to improve the blockchain usability by providing the required tools to allow users to analyze the entire blockchain network [32].
- *Bootstrapping*: Transferring the present business documents, contracts or frameworks to the novel blockchain based technology introduces multiple migration responsibilities which require to be performed. For instance, in the event of a land ownership, the existing forms require to be migrated and formatted to be equivalent for the blockchain form, which take time and cost.
- *Bandwidth*: The block size in blockchains determines the number of transactions needed for each block. To keep equality and give all users

of the blockchain network equal chances to become a leader in the next round, all users should be informed about newly blocks at the same time. The block size is generally restricted to the uplink bandwidth of users. For instance, the current block size in Bitcoin is 1 MB, which is around 1000 transactions [15]. Therefore, the block size and user's bandwidth should be considered when creating new blocks.

- *Authentication*: In the existing blockchain, once a user identity is created, there is no guarantee that the user requesting the identity is the correct owner of that identity and not a malicious one. There are some problems in the authentication of Bitcoin. For instance, there is a famous incident in Mt. Gox, where private keys of their users were breached. So, maintaining a strong authentication scheme is one of the fundamental priorities for the blockchain technology which needs more research and efforts to develop [32].

3. Internet of Things

The IoT allows different devices/objects around us in the environment to be addressable, recognizable and locatable via sensor devices. Also, it allows these devices to be controllable over the Internet using either wired or wireless communication networks. Everyday objects involve not only normal electronic devices or technological development products like vehicles, phones, etc., but also other objects such as food, animals, clothes, trees, etc. The key purpose of the IoT system is to allow various objects to be connected in anyplace, anytime by anyone ideally using any path/network and any service [33].

This section provides a discussion of technical aspects of the IoT system. It started by discussing the history of IoT and how it developed. This followed by presenting various definitions of the IoT which are suggested by various organizations and researchers. Architecture, essential characteristics, applications and challenges of the IoT system are also presented.

3.1 History of IoT

The concept of IoT is not new, it passed through several phases until reaches to what is known now. The IoT notion starts in 1982 when four students from Carnegie Mellon University invented the ARPANET-connected coke machine to indicate whether drinks contained in the coke machine are cold or not. Their main idea was to count how many coke bottles had remained in each row and for how long. If the loaded bottle is left for a long time in the machine, it is labeled "cold." All this data was then remotely available to customers via a finger interface. This experiment

had inspired a lot of inventors all over the world to create their own connected appliance [34].

In the early 1990s, IBM scientists presented and patented an Ultra-High Frequency (UHF) Radio Frequency Identification (RFID) that covers wider distance and provides faster data transfer. Although IBM performed few pilot experiments, it never commercialized this new technology. In the mid-1990s, IBM has suffered from tough financial problems which make them sell their patent to Intermec, a barcode system provider. Several applications are built using Intermec RFID systems, but due to the high cost of this technology at this time and low capacities of sales, this technology did not spread as was expected [35].

In 1999, Auto-IDentification Centre at the Massachusetts Institute of Technology (MIT) has funded through various organizations to involve UHF RFID in connecting various objects together. This occurred when two professors, David Brock and Sanjay Sarma, have proposed using RFID tags to track products through the supply chain. Their proposal was essentially to use only the tag's serial number to track products to save costs, since producing a more complicated chip with a large memory storage will be more expensive. Data linked with the RFID tag was kept in a database that can be accessed over the Internet [36].

Several research and publications confirmed that the term "Internet of Things" was first presented by Ashton, who is the executive director of MIT ID Centre in 1999 [37]. Ashton has said, "*The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so*" [37]. However, other researchers argued that Neil Gershenfeld is the first one who spoke about the idea of IoT in his book titled "*When Things Start to Think*" [38]. Table 2 presents the development phases of the IoT system starting from 1982 till 2021.

3.2 Definitions of IoT

The IoT concept describes the capacity of network connectivity of various types of objects in the environment, not just computers. These objects can act intelligently and exchange data with other devices with negligible human involvement. Although the popularity of the IoT system and high acceptance of this new technology globally, a precise definition does not exist. There are various definitions that focus on a specific view of the IoT. We will try to provide common definitions of the IoT from different perspectives [39].

Table 2 Summary of IoT development phases starting from 1982 till 2021.

Year	Contribution
1982	Four students from Carnegie Mellon University invented the ARPANET-connected coke machine
1989	Tim Berners-Lee proposed the World Wide Web
1990	John Romkey introduced a toaster connected to the Internet
1999	Neil Gershenfeld talked about foundations of the IoT in his book titled "*When Things Start to Think*"
1999	Kevin Ashton introduced the concept of "Internet of Things" for the first time
2000	LG announced the world's first Internet-enabled refrigerator
2004	The concept of IoT becomes more popular. There were enormous publications in newspapers and magazines about the IoT
2005	The Internet-connected device Nabaztag appeared. It was a small robot for consumer use, manufactured to connect to Wi-Fi networks to gather weather information, news and stock market changes, and read them aloud to the owner
2008	The first international conference on the IoT which took place in Zurich, Switzerland
2008	The IoT has been notified as one of the "Disruptive Civil Technologies" by US national intelligence council with possible effects on US interests out to 2025
2008	Cisco reported that the IoT was born since there were more connected devices than people population
2009	Google starts testing self-driving cars. Using sensor-enabled devices on the car deck, Toyota Prius was able to detect pedestrians, cyclists, road work, and other valuable objects
2010	China picks the IoT as a key industry. Chinese Premier Wen Jiabao considered the IoT as a significant industry domain for China
2011	IPv6 public launch. Several organizations have motivated the Internet providers to be prepared for the transition from IPv4 to IPv6
2013	Google announced smart glasses. It featured a display that had the ability to show information hands-free, and a natural language voice recognition module to connect to the Internet via spoken commands
2015	Mattel produces IoT-enabled toys. They produced a Barbie with an embedded Wi-Fi module and a toy house with built-in interactive features such as voice-controlled light bulbs and a toy oven with fire

Continued

Table 2 Summary of IoT development phases starting from 1982 till 2021.—cont'd

Year	Contribution
2016	Apple introduced products home kit to provide the developers with comprehensive tools for developing smart home appliances' software
2016	Google releases Google Home which allows for integrating third-party services to enable users with a wide field of interaction
2017	Microsoft launches Azure IoT edge that enables small devices to utilize cloud services even if they are not connected to the cloud
2017	Google releases Cloud IoT Core that allows devices to connect to the cloud more easily
2018	Governments started to think about the security of IoT devices and encourage manufacturers to adopt security by design
2020	According to Cisco, there will be around 50 billion connected devices
2021	BMW, Ford, Volvo say that there will be fully autonomous cars

The International Telecommunication Union (ITU) in 2012 has provided a common definition for the IoT which has been adopted by several researchers. It stated "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*" [40]. While the Internet Architecture Board (IAB) describes the IoT as "*Internet of Things denotes a trend where a large number of embedded devices employ communication services offered by the Internet protocols. Many of these devices, often called 'smart objects,' are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment*" [41].

There were other views from various researchers. For instance, Atzori et al. [42] have suggested the fundamental idea of the IoT is the universal existence of diversity of things such as sensors, RFID tags, actuators and mobile phones which can interact with each other to achieve a common goal. In addition, Ma [43] has proposed a definition for the IoT which stated as "*The IoT can enable the interconnection and integration of the physical world and the cyberspace; representing the trend of future networking while leading the third wave of the IT industry revolution.*"

Similarly, Gubbi et al. [44] have defined the IoT system from the perspective of a smart environment. It described the IoT as "*interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for*

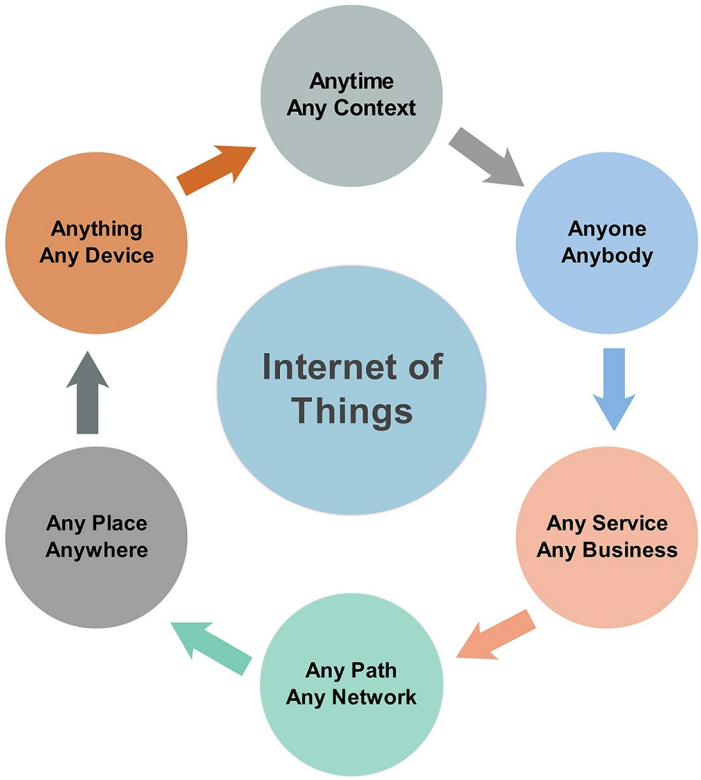

Fig. 7 The IoT can connect anything in anywhere using any path.

enabling innovative applications." Also, Guillemin and Friess [45] have defined the IoT in simple terms, as shown in Fig. 7. It stated: "*The Internet of Things allows people and things to be connected Anytime, Anyplace, with anything and anyone, ideally using any path/network and any service.*"

3.3 IoT expansion

The IoT refers to a huge network of devices and sensors that able to capture and share data with one another. These devices involve both physical and virtual objects that are interconnected together over the Internet. There are huge technological developments that extended the IoT to include other technologies such as Cloud computing and Wireless Sensor Networks (WSNs) [45]. The IoT has the capability to primarily modify business models and value chains in different organizations. It is not just a smart oven connected to the Internet. In some stage, all products will have the ability to connect to the Internet in an economic way.

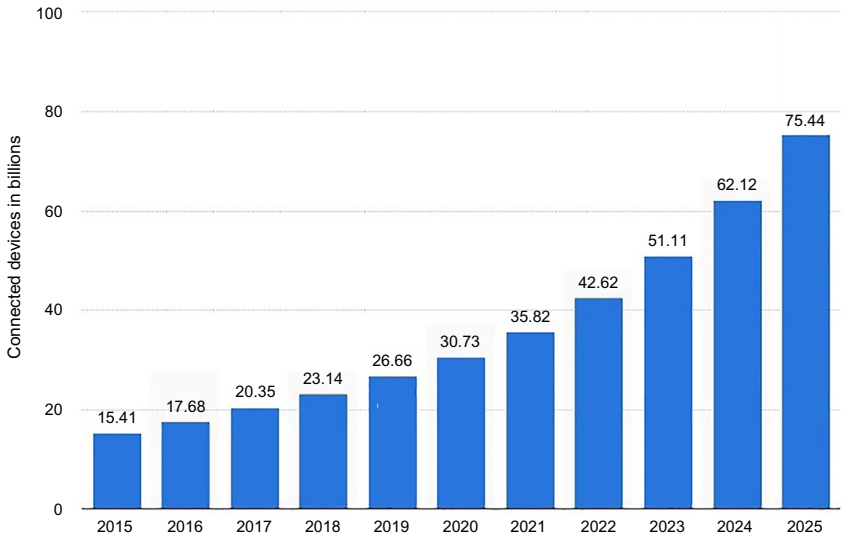

Fig. 8 Expectation of IoT growth from 2015 to 2025 [47].

The number of connected devices exceeds the population worldwide from 2008 and with unlimited capabilities of the IoT system, novel applications and services can be created every day using this fascinating technology. The number of IoT devices is increasing every day. Regarding Statista, the number of IoT devices is expected to reach about 31 billion worldwide at the end of 2020. This number will significantly increase to about 75 billion devices at the end of 2025 [46], as shown in Fig. 8. In addition, the IoT has an expected revenue estimated to reach about $1.8 trillion by 2026.

One of the major issues standing as a barrier to adopting various IoT products is the security and privacy challenges. The growth of IoT devices creates new services and applications, but at the same time, it creates several security vulnerabilities that became more apparent. Manufacturers of IoT devices are not considering security in their priorities [48]. With low public awareness about security and privacy, IoT devices could lead to severe problems that could literally lead to losing our lives. The governments should encourage manufacturers of IoT devices to adopt new security measures in their products. Also, manufacturers should employ the concept of security by design to implement built-in security algorithms within their products to ensure minimum security and safety for various consumers.

3.4 Architecture of IoT

There are different architectures for the IoT system that represent various perspectives about the IoT and its functions. However, the most common

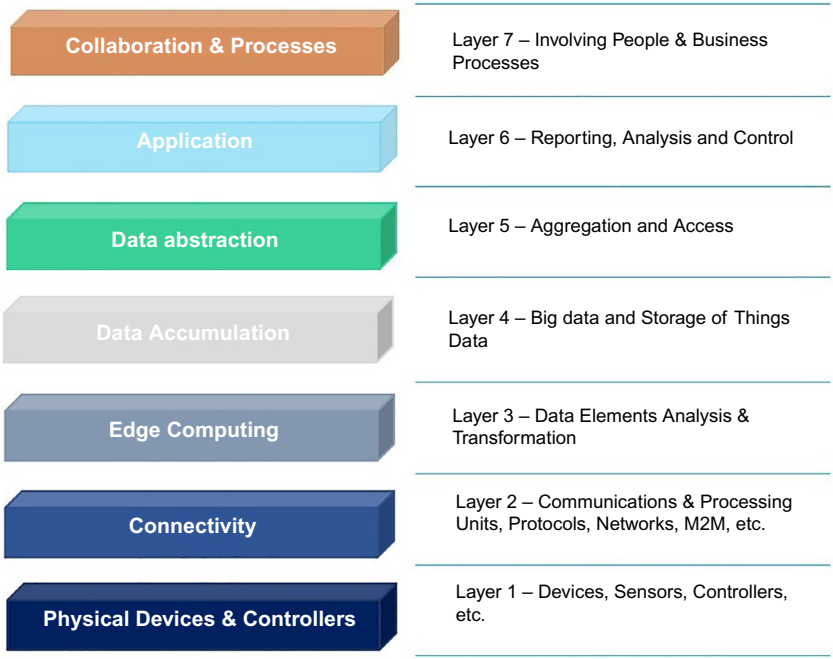

Fig. 9 The IoT reference model according to IWF.

architecture for the IoT is the one made by IoT World Forum (IWF) architecture committee in October 2014 [49]. This reference model provides a common framework to allow deploying the IoT easily and quickly in the industry. Similar to Open System Interconnection (OSI) reference model of the network, the IoT reference model is divided into seven layers to promote the association and expansion of IoT deployment models, as shown in Fig. 9. It identifies where various kinds of processing are operated through different layers of the IoT reference model and enables various manufacturers to produce compatible IoT products working with each other smoothly and efficiently. Also, this architecture model converts the IoT from a conceptual model into a real and approachable system [50].

Layer 1 is the physical layer. It is the hardware layer which collects data from the physical world and transfers it to the upper layer. This layer involves physical objects and sensors. Essentially, the purpose of this layer is to identify different objects and collect information about the surrounding environment such as temperature, humidity, pressure, water quality, motion detection, amount of dust in the air, etc. [51].

Layer 2 is connectivity. This layer is used to interconnect different IoT things with each other using interconnection devices such as switches,

gateway and router. It also transfers gathered data securely from sensors to the upper layer for processing. Layer 3 is edge computing. This layer takes data coming from the connectivity layer and converts it into information appropriate for storage and higher-level processing. At this layer, the processing components work with a huge amount of data which could execute some data transformation to reduce the size of data.

Data accumulation occurs in layer 4. The main function of this layer is to store data coming from layer 3. It absorbs a huge amount of data and places them in storages to be accessible by upper layers. So, it simply changes event-based data to query-based processing information for upper layers. Layer 5 is data abstraction. This layer combines data coming from different sources and converts stored data into the appropriate format for applications in a manageable and efficient manner [47].

Layer 6 is the application layer. This layer is concerned with the information interpretation of various IoT applications. It includes various IoT applications such as healthcare, smart city, smart grid, smart home, connected car, smart agriculture, etc. [49]. Layer 7 is collaboration and processes. This layer identifies individuals who can communicate and collaborate to make use of the IoT data efficiently. It provides other functionalities like creating graphs and business models and other based on data retrieved from the application layer. It also assists managers to make precise choices about their business based on their data analysis [52].

3.5 Characteristics of IoT

The basic notion of the IoT is to provide an autonomous system capable of sharing useful information between uniquely identifiable real-world objects using RFID tags and WSNs. The IoT system shows common characteristics. This section provides common characteristics that better describe the IoT system, as summarized in Fig. 10.

- *Large Scale*: As explained earlier, the IoT system expanded to reach about 30 billion devices at the end of 2018. Cisco expected that this number will increase to reach about 50 billion devices at the end of 2020. This large number of connected devices creates a large-scale network to share their collected information and cooperate together to enhance existed services and generate novel applications capable of handling daily life problems of IoT users [53].
- *Intelligence*: The notion of integrating sensors, computers and communication networks to collect and observe information has found for

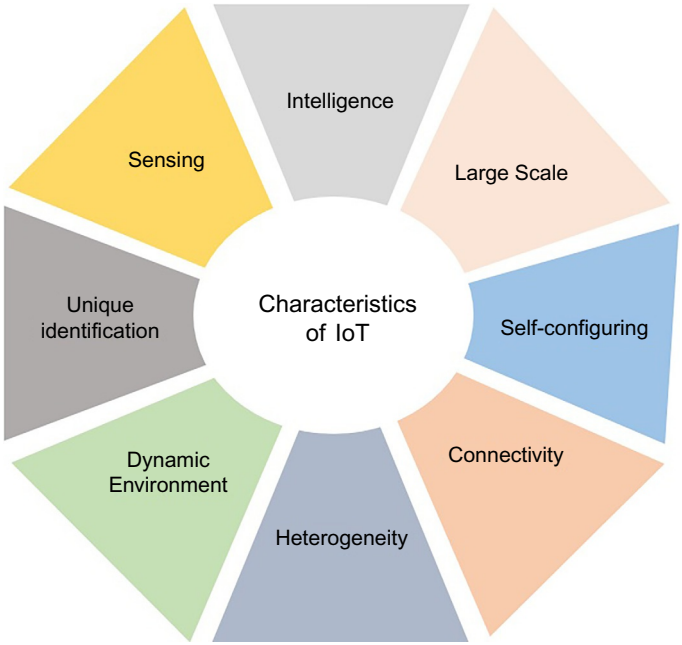

Fig. 10 Common characteristics of the IoT system.

decades. The modern developments aim to make IoT objects acting intelligently and make autonomous decisions. Most IoT devices act regarding their predetermined actions, but with the convergence of sophisticated hardware and software algorithms, IoT objects become able to respond intelligently and correctly according to different situations and contexts [33].

- *Sensing*: Sensors are one of the main elements of the IoT system, which are used to sense, perceive, and gather information about the surrounding environment. The collected information can be resulted from their recording or after their interaction with the environment. Sensing techniques deliver various abilities to consider human susceptibility about the surroundings. Also, the sensing feature is important aspect toward context awareness which allows devices to adjust themselves to various situations and contexts depending on their operating circumstances [44].
- *Unique Identification*: Each IoT device involves an RFID tag which provides a unique identity for each device. These identities given to IoT devices are used by the manufactures to upgrade devices' software. The IoT system with billions of connected devices needs a naming

architecture that provides unique identities to IoT devices to establish communication paths between different types of devices [54].

- *Dynamic Environment*: The IoT is a dynamic system in nature which makes various things can adapt to environmental changes and act intelligently based on the context. Also, IoT devices gather data with considering dynamic changes in the environment. The status of these devices changes dynamically based on surrounding conditions such as connected or disconnected, sleeping or running [55].
- *Heterogeneity*: There are several manufacturers who want to produce many devices to leverage their connectivity over the Internet. However, they face a problem when it comes to managing the heterogeneity of their devices. The IoT system involves several devices with different hardware platforms, networks, communication protocols and operating systems. Although the heterogeneity of these devices causes many problems, they still able to communicate with each other using different communication networks [56].
- *Connectivity*: The IoT system involves multiple devices that need to be connected to share their information. The IoT has the ability to link and interconnect different objects in the environment to offer new market opportunities for generating new applications and services to help humans in different domains [41].
- *Self-configuring*: The large-scale feature of IoT devices creates a severe problem for various service providers and manufacturers to maintain and update their devices. With the self-configuring features for the IoT, devices can work with each other to deliver a specific operation. Also, these devices could configure themselves and search for the newest software update in association with the device manufacturer with negligible efforts [57].

3.6 IoT Applications

The IoT system can interconnect almost all physical and virtual objects in our environment that yield new services and applications. These applications can be adopted in different domains to increase our quality of life. This section provides a discussion of common IoT applications.

3.6.1 Home automation

Smart home is one of the most popular applications of the IoT system. Thanks to sensor and actuation technologies along with WSNs, people can connect a variety of smart appliances inside their homes to resolve their

interests. In a smart home, there are several sensors to enable smart and automated services which operate with minimal human efforts. Also, sensors are used to maintain security and safety [58].

Although the benefits supported by smart home are countless, it introduces some issues regarding security and privacy since all actions and events occurred in the home are being recorded. If an attacker has succeeded to breach the system, it may make the system to act maliciously. So, smart home should be protected in a way that allows smart devices to notify the owner regarding any abnormal action. Also, reliability is another challenge since no administrator is existed to observe the system behavior [59].

3.6.2 Healthcare

The IoT has proven it can provide several benefits for the healthcare domain by creating new application and services that help patients and keep the field innovative. There are multiple wearable devices developed to monitor and track patient's health conditions. These devices allow older patients to live independently without fear. Also, these devices can be utilized to constantly observe and store patients' health conditions and send warning messages in abnormal situations. If the situation is minor, the device itself can recommend a treatment for the patient. While if it is a major situation, the device can send urgent messages to the hospital or ambulances to be immediately dispatched [51].

3.6.3 Smart agriculture

With the existence of multiple sensors within the IoT environment, farmers can use collected data to produce a better return on the investment. The soil parameters such as humidity, salt level and temperature can be collected and measured using the available sensors to increase agriculture production. Furthermore, with the existence of several wireless technologies such as geographical information system and remote sensing, there are many chances to collect relevant information about the soil quickly and efficiently which can help to substitute human effort with automatic machinery to increase agricultural production [60].

There is a significant growth in the adoption of IoT devices in the agriculture domain. It is predicted that the number of IoT devices in agriculture will reach about 75 million by the end of 2020 [61]. There are several advantages for integrating IoT solutions in agriculture. For example, sensors can be used to monitor soil quality, crop's growth progress and weather conditions besides staff performance and equipment efficiency. Also, the IoT system can

help to automate various operations across the crop life cycle and accomplish better management over the production method and ensure advanced standards of crop quality [62].

3.6.4 Supply chain and logistics

The IoT system attempts to facilitate real-world operations in business and information systems. Using sensor technologies such as RFID and Near Field Communication (NFC), products can be tracked from the manufacturer to the distribution location. RFID tags attached to the products are used to uniquely identifies each product and collect relevant information automatically to convey it in real-time along with location information. These tags are used to transmit messages showing exactly what products, sizes and style variations as well as temperature and humidity of products. In addition, automated data capture gives real-time visibility of stock and avoids manual counting and human errors. In simple words, the IoT is set to revolutionize the supply chain with both operational efficiencies and revenue opportunities [63].

3.6.5 Smart city

The notion of smart cities refers to the adoption of IoT devices such as sensors, meters, lights, etc., to monitor and collect information about the surrounding city. This information is used to improve public services and city infrastructure. IoT solutions are involved in many areas of smart cities such as smart street lighting, trash management, smart parking and traffic management [64].

For smart traffic, collected sensor information about traffic can be sent to citizens' phones to monitor traffic in real-time and allow drivers to choose the best road to save driving efforts and time. Also, drivers can be warned in the case of accidents to redirect away from congestion. For trash management, IoT sensors are deployed across trash bins to send messages to specific authorities to report bins need to be emptied. Also, these sensors can be used to optimize trash trucks to reduce emerge usage [65].

3.6.6 Smart grid

Using energy efficiently and ultimately saving more money can be achieved through the use of IoT sensors to collect relevant information about energy consumption in the home, for example, suggesting better ways to save energy. Also, IoT sensors information can be used to deliver consumers

all relevant information about various energy suppliers in an automated way for choosing the best for consumers.

The concept of smart grids adds intelligence at the power flow cycle from supplier to consumer. This type of intelligence can be used to help consumers to be aware of power consumption and dynamic pricing [66]. Also, one of the main applications of the smart grid is a smart meter which collects, records and analyzes power consumption at different times of the day. This information can be used by consumers to adjust their power consumption and change their lifestyles to reduce costs.

3.6.7 Connected car

Smart car or what it called connected car started to be deployed into our community. This type of cars can access the Internet and share their data with other devices. The number of cars equipped with this facility is increasing every day, which will allow the appearance of several applications for connected cars in the near future [67]. The connected car provides several advantages over the normal one. It can reduce car accidents and decrease car drivers' errors by allowing the driver to operate the car remotely. These driverless cars also can save time and reduce driving stress. Several car manufacturers such as BMW, Ford and Volvo have confirmed that there will be fully autonomous cars by the end of 2021 [62].

3.6.8 Wearables

Wearables have a huge interest in markets all over the world. Many companies started to produce these devices with huge quantities to satisfy increased demands such as Google and Samsung. According to Statista, the number of connected wearable devices is expected to reach 830 million at the end of 2020 [46]. Wearable devices are equipped with sensors and have the ability to connect to the Internet for data sharing. These sensors collect data about the user which is later processed to extract meaningful information. Most common wearable devices are in fitness, health and entertainment [68].

3.7 Challenges of IoT

Although IoT solutions provide countless benefits, they raise many challenges that need to be resolved. Most common issues of the IoT system including Big Data, networking, scalability, heterogeneity, interoperability and security and privacy are discussed in this section. They also summarized in Fig. 11.

Fig. 11 Challenges of IoT.

3.7.1 Big data

Big Data is a quite novel expression that indicates the massive quantity of data whether structured or unstructured, which is hard to process with classical database methods and software techniques. It characterized by what is called 5V's, volume, variety, variability, value and velocity. Big Data has a huge interest from multiple organizations as a new industry domain such as online social networks (Twitter, Facebook, and Instagram) since there is a huge amount of data collected through social networks. For instance, in 2010, Twitter produced in average about 10 terabytes of data per day [69].

With billions of devices and objects, the IoT is one of the major sources of big data. Although Cloud computing can be used to store data permanently, processing this huge quantity of data is an extensive problem especially the performance of various IoT applications is based on the data management service. Also, this huge amount of data raises security and privacy issues since ensuring the data integrity will be a very difficult task to achieve [70].

3.7.2 Networking

The key driver of the IoT system is to connect all objects/devices to share their information. These devices are different in shape and structure which make it use different communication networking protocols [71].

Implementing a networking protocol for the IoT should be built with taking consideration of system performance and usability. This is because the network protocol has a major impact on the behavior of the network. So, choosing the appropriate networking protocol is an issue that needs to be addressed. Furthermore, selecting the appropriate network topology for the protocol is another challenge [59].

3.7.3 Heterogeneity

The IoT is one of the popular examples that describes the heterogeneity issue since it involves billions of different devices in their nature. The main target of the IoT system is to build a common method to abstract the heterogeneity of these devices and accomplishing the best exploitation of their functionality [72].

Since the IoT system is growing significantly, the search for applications that can adapt itself with varying hardware and software of IoT devices will continue to achieve the maximum efficiency for the IoT system. Service providers have to take into their consideration the widespread diversity of network connectivity options, protocols, and communication methods when implementing a service for the IoT system [53].

3.7.4 Interoperability

The interoperability refers to the capability of the system components to cooperate with each other in an efficient manner regardless of their technical specifications. Although the interconnection of IoT heterogeneous devices allows sharing their information which results in creating novel services, it comes at a price. As the acceptance of the IoT system increased and the number of connected objects and networks expands, the interoperability becomes a fundamental priority to interconnect various things efficiently [73].

Despite the presence of several proposed results to address the interoperability problem like open source frameworks, data-over-sound technology and creating common IoT services layer, the interoperability is still a big challenge that needs to be addressed [74].

3.7.5 Scalability

Scalability is one of the significant challenges of the IoT system that requires to be handled to contain the massive increase of connected devices. Scalability signifies the system capability to deal with the potential growth of the system in an efficient manner without affecting the system performance.

Being scalable is a mandatory operation for the IoT system to satisfy the varying requirements since people interest varies with time and environmental situations [75]. Therefore, the scalability issue needs more research to test potentials of the IoT system when increasing number of connected devices.

3.7.6 Security and privacy

The enormous increase of IoT devices in our environment leads to increasing the chances to find security vulnerabilities within IoT devices which are poorly secured without any built-in security measures. Exploiting these vulnerabilities results in stealing user information and may put their lives in danger. Also, as IoT sensors are distributed in our surroundings which allow it to collect our sensitive information, marketing behavior, habits and other information which violates our privacy [76].

Therefore, handling security challenges in the IoT system should be a fundamental priority to increase adoption of IoT applications among consumers. Also, IoT users need to be fully confident about the security of their IoT devices and related applications, as they become more integrated into people daily lives activities [77].

4. Conclusion

Recently, blockchain technology has received widespread attention. It has the potential to be involved in almost every industry even if it still in the first stage of approval and still multiple challenges need to be addressed. Blockchain refers to a tamper-proof distributed ledger which enables transactions to be executed in a decentralized environment. It has the capability to solve the main problems of the traditional centralized model. On the other hand, the IoT has emerged as a new evolution of the Internet. It enables different objects and devices in the environment to be connected over the Internet. With the help of sensors and actuators, it collects meaningful information from these objects/devices to improve human productivity and efficiency. The integration of the IoT with blockchain should be the next stage of developments. To be ready for this integration, this chapter presented a discussion of the technical aspects of blockchain and IoT. It started by providing a review of the blockchain technology. Applications and challenges of the blockchain are also discussed. This is followed by providing an overview of the IoT system including its common architecture and essential characteristics. In addition, various applications and challenges of the IoT system were presented.

References

[1] A. Stanciu, Blockchain based distributed control system for Edge Computing, in: 21st International Conference on Control Systems and Computer Science Blockchain, 2017, pp. 667–671.

[2] L. Lamport, R. Shostak, M. Pease, The byzantine generals problem, ACM Trans. Program. Lang. Syst. 4 (3) (1982) 382–401.

[3] E. Khudnev, Blockchain: Foundation technology to change the world, Int. J. Intell. Syst. Appl. (2017)

[4] H.F. Atlam, A. Alenezi, M.O. Alassafi, G.B. Wills, Blockchain with Internet of Things: benefits, challenges, and future directions, Int. J. Intell. Syst. Appl. 41 (10) (2018) 40–48.

[5] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecomm. Policy 41 (10) (2017) 1027–1038.

[6] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Available:http://www.bitcoin.org/bitcoin.pdf, 2009.

[7] K. Xu, Y. Qu, K. Yang, A tutorial on the internet of things: from a heterogeneous network integration perspective, IEEE Netw. 30 (2) (2016) 102–108.

[8] H.F. Atlam, A. Alenezi, R.J. Walters, G.B. Wills, An overview of risk estimation techniques in risk-based access control for the Internet of Things, in: Proceedings of the 2nd International Conference on Internet of Things, 2017, Big Data and Security (IoTBDS), 2017, pp. 254–260.

[9] Coinbase, What Is the Bitcoin Blockchain?, [Online]. Available: https://support.coinbase.com/customer/portal/articles/1819222-what-is-the-blockchain, 2017. Accessed 20 October 2018.

[10] Oxford, Blockchain | Definition of Blockchain in English by Oxford Dictionaries, [Online]. Available:https://en.oxforddictionaries.com/definition/blockchain, 2018. Accessed 20 October 2018.

[11] F. Stroud, Blockchain, [Online]. Available:https://www.webopedia.com/TERM/B/blockchain.html. Accessed 5 October 2018.

[12] K. Sultan, Conceptualizing blockchain: characteristics & applications, in: U. Ruhi, R. - Lakhani (Eds.), 11th IADIS International Conference Information Systems, 2018, pp. 49–57.

[13] M. Pilkington, Blockchain technology: principles and applications, in: F. Xavier Olleros, M. Zhegu, E. Elgar (Eds.), Handbook of Research on Digital Transformations, 2016.

[14] S.A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, Enabling Blockchain Innovations With Pegged Sidechains, 2014, Applied Energy. https://blockstream.com/sidechains.pdf.

[15] J.J. Sikorski, J. Haughton, M. Kraft, Blockchain technology in the chemical industry: machine-to-machine electricity market, Appl. Energy 195 (2017) 234–246.

[16] M. Ahmad, K. Salah, IoT security: review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018) 395–411.

[17] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, Bitcoin and Cryptocurrency Technologies, 2016.

[18] G.W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money, in: P. Tasca, T. Aste, L. Pelizzon, N. Perony (Eds.), Banking Beyond Banks and Money, New Economic Windows, Springer, Cham, 2016, pp. 239–278.

[19] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[20] M. Samaniego, R. Deters, Blockchain as a service for IoT, in: IEEE International Conference on Internet of Things and IEEE Green Computing and Communications IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2016 2016, pp. 433–436.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: 2017 IEEE 6th International Congress on Big Data, 2017, pp. 557–564.
[22] P. Boucher, S. Nascimento, M. Kritikos, How Blockchain Technology Could Change Our Lives, European Parliamentary Research Service, 2017.
[23] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, first ed., O'Reilly Media, Inc., Sebastopol, CA, 2014.
[24] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, V. Kalyanaraman, Blockchain Technology Beyond Bitcoin, 2015.
[25] C. Holotescu, Understanding blockchain technology and how to get involved, in: The 14th International Scientific Conference eLearning and Software for Education Bucharest, 2018, pp. 1–8 (April).
[26] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. (2016) 218–225.
[27] H.F. Atlam, R.J. Walters, G.B. Wills, Fog computing and the Internet of Things: a review, Big Data Cogn. Comput. 2 (10) (2018) 1–18.
[28] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things, in: IEEE Access, vol. 4, 2016, pp. 2292–2303.
[29] J. Bruce, The Mini-Blockchain Scheme, [Online]. Available:http://cryptonite.info/files/mbc-scheme-rev3.pdf, 2014.
[30] J. Janish, Bitcoin mining acceleration and performance quantification, in: 2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), 2014, pp. 1–6.
[31] C. Decker, R. Wattenhofer, Bitcoin transaction malleability and MtGox, in: Computer Security DESORICS, Lecture Notes in Computer Science, vol. 8713, Springer International Publishing, 2014, pp. 313–326.
[32] J. Yli-huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—a systematic review, PLoS One (2016) 15–27.
[33] H.F. Atlam, R.J. Walters, G.B. Wills, Internet of Things: state-of-the-art, challenges, applications, and open issues, Int. J. Intell. Comput. Res. 9 (3) (2018) 928–938.
[34] M.U. Farooq, M. Waseem, A review on Internet of Things (iot), internet of everything (ioe) and internet of nano things (IoNT), Int. J. Comput. Appl. 113 (1) (2015) 1–7(0975 8887).
[35] M. Roberto, B. Abyi, R. Domenico, Towards a Definition of the Internet of Things (IoT), IEEE Internet Things, 2015.
[36] H.F. Atlam, R.J. Walters, G.B. Wills, Intelligence of things: opportunities & challenges, in: IEEE 2018 Cloudification of the Internet of Things (CIoT), 2018.
[37] K. Ashton, That 'internet of things' thing, RFiD J. (2009).
[38] K.K. Patel, S.M. Patel, Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges, Int. J. Eng. Sci. Comput. 6 (5) (2016) 6122–6131.
[39] H.F. Atlam, A. Alenezi, A. Alharthi, R. Walters, G. Wills, Integration of cloud computing with Internet of Things: challenges and open issues, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), June, 2017, pp. 670–675.
[40] ITU, Overview of the Internet of things, in: Ser. Y Glob. Inf. Infrastructure, Internet Protoc. Asp. Next-Generation Networks—Fram. Funct. Archit. Model, 2012.
[41] RFC 7452, Architectural Considerations in Smart Object Networking, Computer Networks, 2015.
[42] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[43] H. Ma, Internet of Things: objectives and scientific challenges, J. Comput. Sci. Technol. 26 (2011) 919–924.
[44] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Futur. Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[45] P. Guillemin, P. Friess, Internet of Things strategic research roadmap, Eur. Comm. Inf. Soc. Media, Luxemb. (2009).
[46] Statista, Internet of Things (IoT) Connected Devices Installed Base Worldwide From 2015 to 2025 (in Billions), [Online]. Available:https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2018. Accessed 15 October 2018.
[47] H.F. Atlam, A. Alenezi, R.J. Walters, G.B. Wills, J. Daniel, Developing an adaptive Risk-based access control model for the Internet of Things, in: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), June, 2017, pp. 655–661.
[48] H.F. Atlam, R.J. Walters, G.B. Wills, Internet of nano things: security issues and applications, in: 2018 2nd International Conference on Cloud and Big Data Computing, 2018, pp. 71–77.
[49] W. Stallings, The Internet of Things: network and security architecture, Internet Protoc. J. 18 (4) (2015) 381–385.
[50] S.H. Shah, I. Yaqoob, A survey: Internet of Things (IOT) technologies, applications and challenges, in: 2016 IEEE Smart Energy Grid Engineering, vol. i, 2016, pp. 381–385.
[51] Cisco, The Internet of Things Reference Model, White Paper, 2014.
[52] M. Muntjir, M. Rahul, H.A. Alhumyani, An analysis of Internet of Things (IoT): novel architectures, modern applications, security aspects and future scope with latest case studies, Int. J. Eng. Res. Technol. 6 (6) (2017) 422–447.
[53] H.F. Atlam, G. Attiya, N. El-Fishawy, Integration of color and texture features in CBIR system, Int. J. Comput. Appl. 164 (April) (2017) 23–28.
[54] P.P. Ray, A survey on Internet of Things architectures, J. King Saud Univ. Comput. Inf. Sci. (2016) 1–29.
[55] H.F. Atlam, G. Attiya, N. El-Fishawy, Comparative study on CBIR based on color feature, Int. J. Comput. Appl. 78 (16) (2013) 975–8887.
[56] M. Adda, J. Abdelaziz, H. Mcheick, R. Saad, Toward an access control model for IOTCollab, in: The 6th International Conference on Ambient Systems, Networks and Technologies, vol. 52, 2015, pp. 428–435.
[57] I. Chatzigiannakis, et al., True self-configuration for the IoT, in: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2012, pp. 545–551.
[58] I.I. Pătru, M. Carabaş, M. Bărbulescu, L. Gheorghe, Smart home IoT system, in: Netw. Educ. Res. RoEduNet Int. Conf. 15th Ed. RoEduNet 2016—Proc., 2016, pp. 365–370.
[59] B.L. Risteska Stojkoska, K.V. Trivodaliev, A review of Internet of Things for smart home: challenges and solutions, J. Clean. Prod. 140, pp (2017) 1454–1464.
[60] K.L. Krishna, O. Silver, W.F. Malende, K. Anuradha, Internet of Things application for implementation of smart agriculture system, in: Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), vol. 25(15), 2017, pp. 54–59.
[61] M.A. Akkaş, R. Sokullu, An IoT-based greenhouse monitoring system with Micaz motes, in: International Workshop on IoT, M2M and Healthcare (IMH 2017), vol. 113, 2017, pp. 603–608.
[62] L. Da Xu, W. He, S. Li, Internet of Things in industries: a survey, IEEE Trans. Ind. Inf. 10 (4) (2014) 2233–2243.

[63] Z. Guo, Z. Zhang, W. Li, Establishment of intelligent identification management platform in railway logistics system by means of the Internet of Things, Procedia Eng. 29 (2012) 726–730.
[64] a. Zanella, N. Bui, a. Castellani, L. Vangelista, M. Zorzi, Internet of Things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[65] R. Khatoun, S. Zeadally, Cybersecurity and privacy solutions in smart cities, IEEE Commun. Mag. 55 (3) (2017) 51–59.
[66] H.F. Atlam, M.O. Alassafi, A. Alenezi, R.J. Walters, G.B. Wills, XACML for building access control policies in Internet of Things, in: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), 2018.
[67] M. Kalmeshwar, N. Prasad, Internet of Things: architecture, issues and applications, Int. J. Eng. Res. Appl. 07 (06) (2017) 85–88.
[68] S. Cirani, M. Picone, Wearable Computing for the Internet of Things, IEEE Computer Society, 2015, pp. 35–41.
[69] J. Lin, C. Chen, C. Lin, Integrating QoS awareness with virtualization in cloud computing systems for delay-sensitive applications, Futur. Gener. Comput. Syst. (2013) 478–487.
[70] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and IoT: a big picture, Futur. Gener. Comput. Syst. 49 (2015) 58–67.
[71] M. Chen, J. Wan, F. Li, Machine-to-machine communications: architectures, standards and applications, KSII Trans. Internet Inf. Syst. 6 (2) (2012) 480–497.
[72] A. Alenezi, N.H.N. Zulkipli, H.F. Atlam, R.J. Walters, G.B. Wills, The impact of cloud forensic readiness on security, in: Proceedings of the 7th International Conference on Cloud Computing and Services Science (CLOSER 2017), 2017, pp. 511–517.
[73] H.F. Atlam, A. Alenezi, R.K. Hussein, G.B. Wills, Validation of an adaptive risk-based access control model for the Internet of Things, Int. J. Comput. Netw. Inf. Secur. (2018) 26–35.
[74] D. Bubley, Data over sound technology: device-to-device communications & pairing without wireless radio networks, Int. J. Comp. Intell. Res. (2017).
[75] A. Gupta, R. Christie, P.R. Manjula, Scalability in Internet of Things: features, techniques and research challenges, Int. J. Comput. Intell. Res. 13 (7) (2017) 1617–1627.
[76] R.K. Hussein, A. Alenezi, H.F. Atlam, M.Q. Mohammed, R.J. Walters, G.B. Wills, Toward confirming a framework for securing the virtual machine image in cloud computing, Adv. Sci. Technol. Eng. Syst. 2 (4) (2017) 44–50.
[77] M.A. Iqbal, O.G. Olaleye, M.A. Bayoumi, A review on Internet of Things (Iot): security and privacy requirements and the solution approaches, Glob. J. Comput. Sci. Technol. E Network, Web Secur. 16 (7) (2016).

About the Authors

Hany F. Atlam is a PhD candidate at the University of Southampton, UK and assistant lecturer in Faculty of Electronic Engineering, Menoufia University, Egypt. He was born in Menoufia, Egypt in 1988. He has completed his Bachelor of Engineering and Computer Science in Faculty of Electronic Engineering, Menoufia University, Egypt in 2011, then completed his master's degree in computer science from the same university in 2014. He joined the University of Southampton as a PhD student since January 2016. He has several experiences in networking as he holds international Cisco certifications and Cisco Instructor certifications. Hany is a member of Institute for Systems and Technologies of Information, Control and Communication (INSTICC), and Institute of Electrical and Electronics Engineers (IEEE). Hany's research interests include and not limited to: Internet of Things Security, Cloud Security, Cloud and Internet of Things Forensics, Blockchain, and Big Data.

Gary B. Wills is an Associate Professor in Computer Science at the University of Southampton. He graduated from the University of Southampton with an Honours degree in Electromechanical Engineering, and then a PhD in Industrial Hypermedia system. He is a Chartered Engineer, a member of the Institute of Engineering Technology and a Principal Fellow of the Higher Educational Academy. He is also a visiting associate professor at the University of Cape Town and a research professor at RLabs. Gary's research projects focus on Secure System Engineering and applications for industry, medicine, and education. Gary published more than 200 publications in international journals and conferences.