Intersections between IoT and distributed ledger

Chapter *in* Advances in Computers · January 2019

DOI: 10.1016/bs.adcom.2018.12.001

CITATIONS
2

READS
961

2 authors:

Hany F. Atlam
University of Southampton
26 PUBLICATIONS **223** CITATIONS

SEE PROFILE

Gary Wills
University of Southampton
644 PUBLICATIONS **3,285** CITATIONS

SEE PROFILE

Intersections between IoT and distributed ledger

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, Shebeen El-Kom, Egypt

Contents

Abstract

The Internet of Things (IoT) is growing exponentially. It allows not only humans but also all various devices and objects in the environment to be connected over the Internet to share their data to create new applications and services which result in a more convenient and connected lifestyle. However, the current centralized IoT architecture faces several issues. For instance, all computing operations of all nodes in the network are

Advances in Computers
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2018.12.001

carried out using a single server. This creates a single point of failure in which if the server goes down, the entire system will be unavailable. Also, the IoT centralized architecture is an easy target of various types of security and privacy attacks, since all IoT data collected from different devices is under the full authority of a single server. Therefore, adopting one of the Distributed Ledger Technologies (DLTs) for the IoT may be the right decision. One of the popular types of DLTs is the blockchain. It provides an immutable ledger with the capability of maintaining the integrity of transactions by decentralizing the ledger among participating nodes in the blockchain network which eliminates the need for a central authority. Integrating the IoT system with the blockchain technology can provide several benefits which can resolve the issues associated with the IoT centralized architecture. Therefore, this chapter provides a discussion of the intersection between IoT and DLTs. It started by providing an overview of the DLT by highlighting its main components, benefits and challenges. The centralized IoT system is also discussed with highlighting its essential limitations. Then, the integration of blockchain with IoT is presented by highlighting the integration benefits. Various application and challenges of integrating blockchain with IoT are also discussed.

1. Introduction

The Internet of Things (IoT) represents a revolutionary technology that enables almost everything everywhere to be connected over the Internet. The IoT enables various devices and objects around us in the environment to be addressable, recognizable and locatable via cheap sensor devices. These devices can be connected and communicate with each other over the Internet using either wired or wireless communication networks [1]. These devices 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 preferably using any path/network and any service [2].

Although the IoT system provides countless benefits in various domains, it faces several issues with the current centralized model in which all IoT devices and objects are identified, authenticated and controlled by a centralized server. This model faces many obstacles. For instance, it carries out all processing operations and controls all nodes in the network, which creates a single point of failure in which if the server goes down, the entire system will be unavailable [3]. Also, security is another issue for the centralized model since all sensitive information stored in one location and under the reasonability of a single server which makes it an easy target for various types of

attacks. Moreover, protecting the data privacy seems to be questionable, since the real-time data of IoT devices are collected and stored in a remote server outside the user control and with the authority of the centralized server only. In addition, the centralized architecture faces a scalability issue as it fits only for small businesses, but it will be an impractical solution for large organizations having many branches in a different location all over the world [4].

On the other hand, Distributed Ledger Technology (DLT) has gained a great attention in recent years as an innovative approach that provides a transparent and verifiable record of transactions. DLT combines a group of untrusted nodes in a distributed and decentralized environment. It has a massive potential to change how governments, organizations and institutions work. It can bring myriad advantages to various government activities such as tax collection, benefits associated with social security, passport issuance, licenses and voting. It can also provide several advantages to other applications such as music, finance, cyber security, public services, healthcare, etc. DLT provides an immutable ledger that cannot be changed or altered and eliminates the need for a centralized trusted third party [5].

With several limitations in the centralized IoT architecture, moving the IoT system into one of the distributed ledger technologies may be the right decision. One of the popular types of DLTs is the blockchain. It is defined as a distributed and decentralized ledger of transactions to manage a continuously growing group of records. To store a transaction in the ledger, the majority of participating nodes 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 [3]. To link the blocks together, each block encompasses a timestamp and hash function to the previous block. The hash function validates the integrity and nonrepudiation of the data inside the block. Moreover, to keep all participating nodes of the blockchain network updated, each user holds a copy of the original ledger and all nodes are synchronized and updated with newly change.

Integrating the IoT with blockchain will have many advantages. For instance, adopting the decentralized architecture for the IoT system can solve many issues especially security and single point of failure, since the blockchain provides a decentralized and distributed environment where there is no need for a central authority to manage the execution of operations and control communication between various nodes in the network. This, in turn, provides a trusted environment where participating nodes are the only entities to accept or discard a transaction based on their consent [6].

Moreover, the blockchain provides better security for various IoT applications since it provides an immutable and tamper-proof ledger to protect data against malicious attacks in which any data update or modification will not be added to ledger unless the majority of participating nodes verify it [7].

This chapter provides a discussion of the intersection between IoT and DLT. It started by presenting the main differences between centralized, decentralized and distributed systems. This followed by providing an overview of the DLT by highlighting its main components, advantages and challenges. The centralized IoT system by examining its essential limitations is also presented. Then, the integration of blockchain with IoT is presented by examining the benefits of the integration process. Various application and challenges of integrating blockchain with IoT are also discussed.

The remaining of this chapter is structured as follows; Section 2 presents the main differences between centralized, decentralized and distributed systems; Section 3 provides an overview of the DLT including its components, advantages and challenges; Section 4 discusses the centralized IoT system and its limitations; Section 5 discusses the intersection of blockchain with IoT with highlighting benefits, new applications and challenges resulted after integrating blockchain with IoT; Section 6 is the conclusion.

2. Centralized, decentralized and distributed systems

This section provides an overview of centralized, decentralized and distributed systems by presenting the main differences in the network structure, advantages and disadvantages of each approach.

2.1 Centralized system

The centralized system is built depending on a central server to manage a set of nodes. The nodes are simply nodes which can perform operations from neighboring nodes across the network. The central server handles all requests coming from various nodes and assigns tasks to various nodes in the network. Typically, the communication between various nodes and the central server is like Transmission Control Protocol (TCP) connection in which when a connection has been created, messages are sent between the central server and the connected node. These messages can be such as registering the node and getting node address [8].

The centralized system has several advantages. For example, the entire responsibility of the network is placed under the full control of the central server so, it is easier to manage, maintain and control. In addition, the use of

a central server saves the costs of having multiple hardware equipment. In other words, building a centralized system only need a central computer with the required hardware and software elements while other nodes could be just terminals. These terminals served only as an input/output method to connect various users to the central server. Also, if one terminal goes down, the user can simply use another terminal to access the stored files on the central server. Moreover, the centralized system provides better physical security since all data are stored in a central place, which makes it easier to protect against physical damage and reduces duplication and ensures data integrity since data are controlled by the central server which provides a uniform service for all nodes in the network.

On the other hand, the centralized system has multiple shortcomings. For example, since the central server carries out all processing operations and controls all nodes connected to it, if the server crash, the entire system will be unavailable. This problem is called a single point of failure so if the single point, central server, is failed, all the system will go down. Moreover, since all computing achieved across the central server, the hardware specification should be good enough to serve all nodes in the network, if not, the nodes may wait for a long time to get their job done. Also, the central system is unfeasible in large organizations which have many branches in different sites all over the world [9].

2.2 Decentralized system

A decentralized system is designed based on peer-to-peer communications between different nodes in the network without the need for a centralized server to manage operation execution and make decisions on behalf of other nodes. So, each node makes their own independent decision based on its targets which may collide with other nodes targets. Nodes can connect and communicate with each other to share information and provide various services to other nodes [10].

There are two basic structures for a decentralized system, pure decentralized structure and organizational structure. In the pure structure, all nodes are responsible for taking their own decisions without having any authority to manage communication and operations between communicating nodes. While the organizational structure has a supernode for a small network to manage communication and take decisions on behalf of this subnetwork. These supernodes are connected with similar nodes in the network to share information and make decisions [11].

The decentralized system has multiple advantages. For instance, it reduces the possibility of controlling and operating the entire system with only one central server, instead, it allows each node to take part in decision-making operations. In addition, the decentralized system carries decision-making operations closer to the scene of action which results in quick decisions that can save a lot of money. Also, the decentralized system is scalable and facilitate the expansion of organizations which results in opening a new business in different geographic locations. Moreover, in contrast to the centralized model, the failing of one node will not affect the entire system, so there is no single point of failure.

The decentralized system is not straightforward. It suffers some difficulties and challenges. For example, it increases costs as each node needs enough processing power and memory to execute operations and make decisions independently. Also, it increases the coordination problem between various subnetworks [3].

2.3 Distributed system

A distributed system is a set of autonomous nodes interconnected together to form a single and integrated coherent network with a huge processing and storage power to achieve a certain goal. The peers are communicated by passing messages to one another. The combination of storage and processioning capabilities allows the distributed system to perform complex and large tasks faster than other systems by dividing tasks into multiple subtasks and distributed it among network nodes which process and execute their subtasks and return the result to the main node to collect and constitute the final result [12].

The distributed system provides countless benefits. For instance, it increases the overall performance of the system by distributing the computational load across different nodes which provides less load at each node, which in turn increases the performance of the entire system. Also, it provides a reliable network of nodes where if a node goes down, the entire system will not be affected which eliminates the problem of single point of failure associated with the centralized system. In addition, since distributed systems operate with a diversity of different nodes, it provides a scalable system which can adjust their processing resources in light of assigned tasks and operations.

On the other hand, the distributed system has some shortcomings. It has severe security and privacy issues since the system is based on sharing tasks

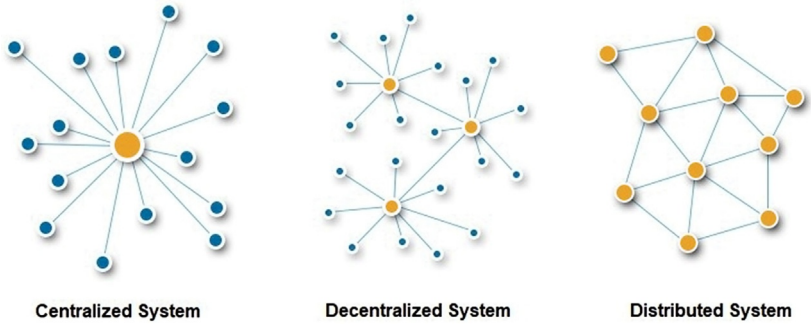

Fig. 1 Structure of centralized, decentralized and distributed systems.

Table 1 Comparison between centralized, decentralized, distributed systems.

Feature	Centralized system	Decentralized system	Distributed system
Scalability	Low	Moderate	Infinite
Security	High	Moderate	Low
Maintenance	Easy to maintain	Moderate	Difficult to maintain
Stability	Highly unstable	Possible recovery	Very stable
Complexity	Less complex	Moderate	Complex
Point of failure	Single point of failure	Finite number of failures	Infinite number of failures

and data between multiple nodes. If one of these nodes is malicious, it can cause serious issues. Also, the system communicates using messages which can be lost easily. Also, large data need a high bandwidth for data transmission which results in more costs to change existing network connections [13].

Fig. 1 shows the structure of centralized, decentralized and distributed systems. Also, Table 1 provides a comparison between centralized, decentralized, distributed systems in terms of scalability, security, maintenance, stability, complexity and point of failure.

3. Distributed ledger technology

Distributed ledgers are a multipurpose technology that is built to share data among different nodes in different locations all over the world. This technology provides several benefits to various applications. This section provides an overview of the DLT by discussing different definitions, main

elements and advantages of DLT. Then, presenting challenges of adopting this technology, distinguishing differences between blockchain and DLT and lastly discussing main technologies of DLT.

3.1 Definitions of DLT

DLT provides a universal data structure by combining a group of untrusted nodes in a distributed and environment. It provides an immutable ledger that cannot be changed or altered and eliminates the need for a centralized trusted third party. So, a centralized server is not required to manage operations and ensures trust between communicating parties instead, a distributed ledger is responsible for maintaining the trust by tracking the ownership of different nodes in the network. DLT has a huge potential to change how governments, organizations and institutions work. It can bring countless benefits to government activities such as tax collection, benefits associated with social security, passport issuance, licenses and voting. It can also provide several advantages to other applications such as music, finance, cyber security, public services, healthcare, etc. [14].

A distributed ledger is a form of database shared across multiple locations including organizations and countries. This ledger is shared and synchronized between different nodes of the network. It keeps all transactions of the participating nodes in the network [15]. There are other definitions for the DLT. For example, Investopedia [16] described the DLT as "*The technological infrastructure and protocols that allows simultaneous access, validation and record updating in an immutable manner across a network spread across multiple entities or locations.*" Also, Financial Conduct Authority [17] defined the DLT as "*A set of technological solutions that enables a single, sequenced, standardized and cryptographically-secured record of activity to be safely distributed to, and acted upon by, a network of varied participants.*" Also, Bank for International Settlements (BIS) [18] defined the DLT as "*the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes.*"

3.2 Components of DLT

Several governments started to adopt DLTs to provide various types of public services. This technology allows nodes to update their records in a shared database without the need for a central authority to validate the operation or even enforce their own standards. Also, this technology eliminates the issue

of single point of failure through the decentralization feature which provides an extensive increase in security regarding storing transactions and ensuring their integrity [19].

There are four components to implement a DLT, these components, as summarized in Fig. 2, include:

- Shared ledger: It is a shared database for storing all transactions that belong to nodes participating in the network. Since the ledger can be deployed at different locations, it has to be updated and synchronized with other copies of the ledger in the network in a very short time without noticeable latency.
- Cryptography: Transactions between two communicating nodes are recorded, maintained and secured cryptographically. Every node participating in the network can create a transaction in a secure way without the need for a central authority. Cryptography plays a vital part in the DLT through authenticating approved nodes, validating records and facilitating consensus on the ledger update. In other words, there is a cryptographic digital signature for each participating node to authenticate himself before adding or changing a transaction [18].
- Consensus Mechanism: This is the process used by all participating nodes in the network to validate the contents of the ledger.

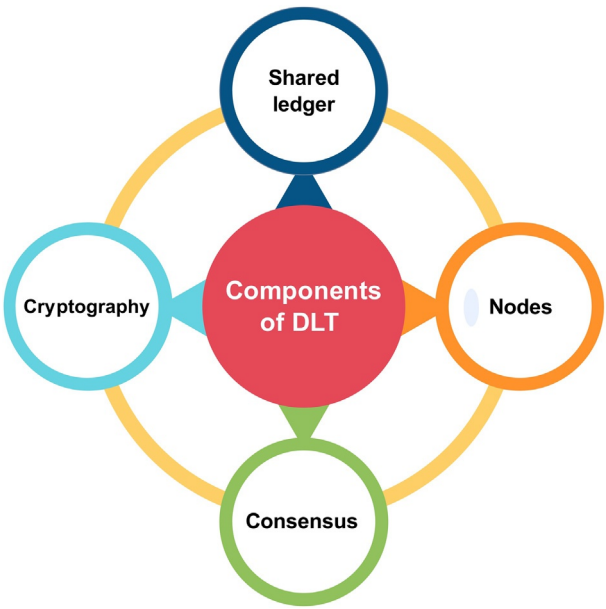

Fig. 2 Main components of the DLT.

Consensus generally includes two phases: validation and agreement on ledger update. There are multiple consensus mechanisms. However, the most common 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 a transaction [20].

- Nodes: They represent the participating users in the network. Nodes have different roles in the network including system administrator, asset issuer, proposer, validator and auditor. The system administrator role is used to control the access to the system and provides certain management services. While asset issuer role is permissioned to issue new assets. Proposer role is used to propose updates to the ledger, whereas validator role confirms the validity of a proposed change in the ledger. The lowest role is auditor which allows the user to only view the ledger without the ability to make changes or updates.

3.3 Advantages of DLT

DLT enables the participating nodes to store transactions in a shared database that can be accessed in a secure manner. These transactions are distributed between nodes in the network to access and use it without relying on a trusted central system. DLT as a new technology can add enormous advantages to different applications over the centralized ledger and other kinds of shared ledgers. This section provides potential benefits of the DLT, which are as follows:

- Availability: DLT provides a high level of availability as it can run on a continuous basis theoretically. The distributed and shared nature of the system facilitates the recovery of both data and processes in the case of an attack which can reduce the need for expensive recovery plans. However, the availability of the DLT remains untested, especially when large volumes are involved [14].
- Automation and Programmability: DTL supports automation in programming, so when a certain condition is verified, the programming actions are executed automatically. This feature relies on smart contracts which build digital contracts as a software code by implementing contracts terms as programming conditions and actions. Actions are automatically executed as soon as conditions were verified. Although smart contracts can be built on the centralized system, the actions cannot be executed only if they approved by the central system, which can take a long time [21].

- Immutability and verifiability: One of the critical advantages of the DLT is the ability to guarantee the integrity of transactions by creating immutable and verifiable ledgers. In the traditional centralized architecture, a trusted third party needs to exist for ensuring information integrity. Whereas in the DLT, the data cannot be changed until the majority of participating nodes in the network approve it [22].
- Decentralization: DTL is a decentralized technology in nature. It has a shared ledger giving all participating nodes the ability to hold an original copy of the ledger without the need to be controlled or managed through a single central authority. This gives the opportunity for all nodes to participate and transact equally. This also converted to a lower cost, better scalability and faster time for creating and validating a transaction.
- Transparency: DLT offers a high level of transparency by sharing transaction details between all participants nodes involved in those transactions. Also, there is no need for a central authority which improves business friendliness and guarantees a trusted workflow.
- Efficiency: DLT reduces the efforts needed to do reconciliation and handle disputes manually. The existing systems with separate ledgers can lead to inconsistent master and transaction data resulting in faulty and duplicated data. Also, identifying and correcting these data will take a significant loss of time. This not only slows down the process but also forms a source of contract uncertainty. While the DLT is expected to bring significant efficiencies to this process through distributed and immutability features [23].
- Security and Resilience: DLT delivers a good level of security since it uses a public key infrastructure that protects against malicious actions. The participating nodes of the network place their trust in the integrity and security features of the consensus mechanism. In addition, the use of distributed and decentralized ledger eliminates the single point of failure which affects the system resilience [24].
- Cost Reduction: DTL is based on a shared ledger which shares its contents with the participating nodes in the network in which each participating user holds a copy of the original ledger without the need for a central authority. This reduces costs associated with distributing and maintaining the ledger. In other words, the use of a distributed ledger eliminates maintenance costs of individual ledgers and reduces the need for costly business continuity plans [25]. Also, it reduces costs spent to ensure data integrity as the DLT is an immutable system in nature. According to Natarajan et al. [21], DLT could save about $15–20 billion per year for the financial industry only.

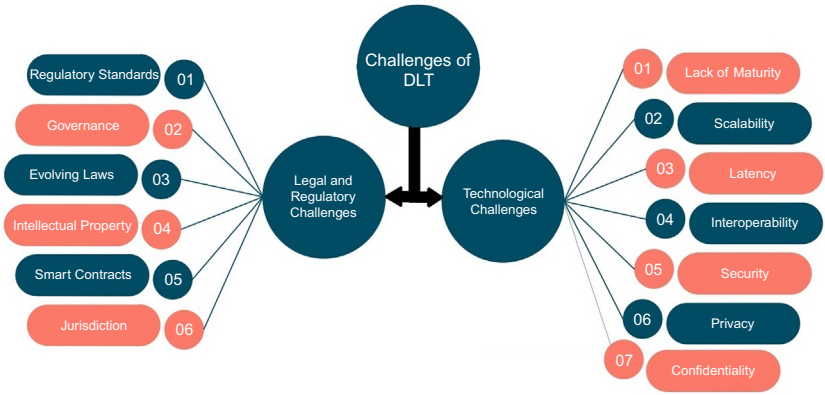

Fig. 3 Challenges of DLT.

3.4 Challenges of DLT

DLT is still in the first stage of approval, and there are many technological and legal issues that need to be addressed. This section provides a discussion of the most common challenges of DLT, as summarized in Fig. 3.

3.4.1 Technological challenges

The first type of DLT challenges is the technological issues which include lack of maturity, scalability, latency, interoperability, security and governance.

- Lack of Maturity: DLT is still in the early stage of evolution. There are serious concerns about the robustness and resilience of the DLT especially for large amount of transactions, availability of standardized hardware and software applications besides availability of skilled professionals. There is a lack of understanding among businesses, consumers and authorities about how the technology operates the potential use cases for DLT and the likely short- and medium-term market development potential. Although huge organizations like Microsoft and IBM started creating DLT products and services which can provide the necessary trust and confidence in the DLT and its huge expansion in various applications, there is still a big gap of research that needs to be handled to get the full benefits of such a revolutionary technology [26].
- Scalability: Current versions of distributed ledgers face concerns regarding the scalability of the DLT in terms of transaction volume and speed of verifications. Existing ledgers have limited transaction speed and block size. Although these issues can be resolved over time, the main issue that needs to be resolved is the capability of the system to handle the global

scale. The failure to handle this issue could result in expenses of a more centralized and less transparent platform, which can eliminate many of DLT benefits [21].

- Latency: With increasing number of transactions, the ledger is growing rapidly in size, which leads to slow transaction time. Also, the increase of participating nodes in the network adds more latency as internode latency logarithmically increases as each new user is added. Therefore, the DLT is incompetent to scale to process more transactions [27].
- Interoperability: There are different DLT systems that need to be interoperable with other ledgers. Also, the integration of the DLT with existing infrastructures will require not only large expenses but also extensive coordination and collaboration. Providing a solution that enables different systems to work efficiently with each other should be the main target to address the interoperability issue associated with the DLT [28].
- Security: The DLT eliminates the need for a centralized server by allowing all participating nodes in the network to hold an original copy of the ledger. However, this presents issues especially in the case of cyber attacks. Distributing access and management rights across multiple nodes may introduce a security threat. Also, the encryption level and network security may differ broadly, so if one user is breached, the entire network will be in danger. Hence, network security has to be very strong [29].
- Privacy: The DLT is built based on sharing information about various transactions between all participating nodes in the network. If the information in a transaction involves private or sensitive information such as medical data or an account number, it will be visible for all participating nodes in the network. Moreover, since nodes in the ledgers can be from different geographic locations, the transfer of data between these different locations will heavily depend on rules and requirement of each location, which create a legal issue that needs to be resolved.
- Confidentiality: It is a similar issue like privacy where information shared among participating nodes in the ledger become public and everyone can view this information. This applies to both public and private ledgers. So, if a company uses the distributed ledger to keep their confidential information, it will create a risk of a confidentiality attack or loss of trade secret protection. Therefore, there is a need to discover novel approaches to prevent confidential and sensitive information from being kept in the distributed ledger to protect it from any future confidentiality breach [30].

3.4.2 Legal and regulatory challenges

The second type of DLT challenges is the legal and regulatory issues which include regulatory standards, governance, evolving laws, intellectual property, smart contracts and jurisdiction.

- Regulatory Standards: Regulatory standards for several applications are necessary but are still in the early progress stages. A legal standard for the DLT is required to ensure the authenticity of data stored in the distributed ledger. Also, a standardized regulation is obligatory for data protection and authenticating the identity of legal nodes within the network. Although many regulators across the world are actively searching the technology, more regulatory standards for the DLT are yet to appear [19].
- Governance: In the DLT environment where no central entity is involved, there are several issues about ensuring active governance of the overall infrastructure. In the centralized infrastructure, regulators have used effective governance arrangements. But for the DLT whether permissionless or permissioned, it is unclear whom will have an issue and how to apply governance arrangements. The existence of administrator in permissioned DLT can be subject to specific governance arrangements but depending on the nature of the DLT.
- Evolving Laws: It is obvious that laws pause technology innovation, this is definitely the case with the DLT. Regulations regarding information sharing need to be changed to protect companies as well as their investors and their customers. The DLT provides an auditable and transparent environment for several applications and enables new products and services to grow significantly, but there is a lack of laws and regulations for such a technology.
- Intellectual Property: With the appearance of a new technology such as DLT, there are a 1000 patent applications by companies that utilize the benefits of this new technology. Although the core technology is open source, companies have built patented applications in which they require to protect their intellectual property rights, so there will be multiple patent infringement lawsuits as patent holders seek to enforce their exclusive rights to their patents. Therefore, adopters of the DLT need to be very careful as their application or implementation could potentially be violating an existing patent [31].
- Smart Contracts: There are several legal and law issues that appear with the emergent of new technologies, for example, a smart contract, which is based on a software code to implement the terms and conditions of a

contract. Smart contracts may contest the nature of traditional legal principles of contract law such as contract formation and termination. This will add more difficulty for courts to work with the new technology. Also, as smart contracts are software codes, their use may introduce enforceability questions if trying to investigate them within the traditional contract definition. Moreover, as smart contracts are built with the decentralized feature, resolving any future disputes arise over a contract will be another issue in the absence of a central authority [32].

- Jurisdiction: According to the Cambridge dictionary [33], Jurisdiction is defined as the authority of a court or official organization to make decisions and judgments. As DLT ledgers can connect different participating nodes from multiple jurisdictions around the world, it creates challenges from a jurisdictional perspective. The principles of a contract are different across jurisdictions, so defining the suitable governing law to resolve any future dispute will be very difficult.

3.5 Distributed ledger vs blockchain

Many people are confused about how to distinguish between DLT and blockchain. People often believe that they are the same thing, which is not the case. The reason behind this confusion is the popularity of the blockchain without mentioning the parent technology, DLT. The comparison between DLT and blockchain is simply like comparing an apple to a fruit. In simple terms, blockchain is one of the technologies that depends on the distributed ledger and other related features. There is an extensive variety of distributed ledger models, with different degrees of centralization and different types of access control for various business requirements.

There are a set of differences between distributed ledgers and blockchain. For instance, blockchain is a sequence of blocks chained together using hash functions and timestamp, while distributed ledgers do not need such a chain. Also, distributed ledgers do not require consensus mechanism and deliver better scalability. In summary, all blockchains are distributed ledgers, but not all distributed ledgers are blockchains.

3.6 Distributed ledger technologies

DLT refers to an innovative mechanism of storing and sharing data between multiple data storages. This technology enables transactions and data to be stored, shared, and synchronized across a distributed network of nodes. Each node acts as both a client and a server at the same time, holding the same

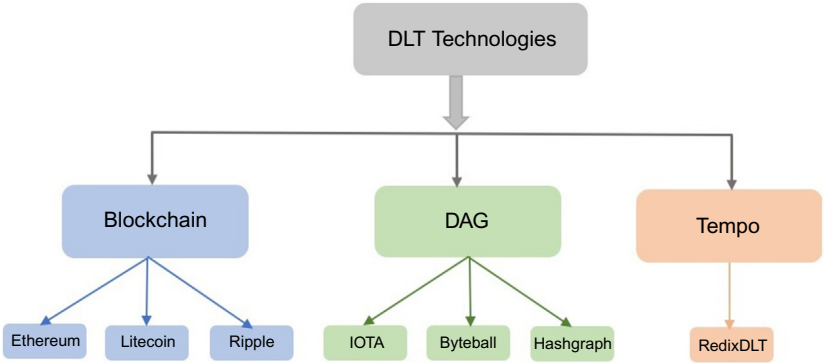

Fig. 4 DLT technologies and common applications of each technology.

copy of the distributed ledger. This technology enhances efficiency and eliminates reconciliation costs [21].

DLTs can be classified according to their applied data structure. Among various structures of the DLT, there are three main structures that have been widely adopted: blockchain, Directed Acyclic Graph (DAG) and Tempo, as shown in Fig. 4 [34].

3.6.1 Blockchain

The first and most popular type of the DLT is 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 nodes 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 nonrepudiation of the data inside the block. Moreover, to keep all participating nodes of the blockchain network updated, each user holds a copy of the original ledger and all nodes are synchronized and updated with newly change [3].

Blockchain delivers a high level of transparency by sharing transaction details between all participants nodes involved in those transactions. In a blockchain environment, no need for a third party which improve business friendliness, guarantees a trusted workflow and blockchain eliminates the single point of failure which affects the entire system. Moreover, blockchain provides better security since it uses public key infrastructure that protects against malicious actions. The participating nodes of the blockchain network place their trust in the integrity and security features of the consensus mechanism [24].

3.6.2 Directed acyclic graph (DAG)

The second type of the DLT is DAG. It is a directed graph data structure that uses a topological ordering. The sequence can only go from earlier to later. DAG is often applied to problems related to data processing, scheduling, finding the best route in navigation and data compression [14].

DAG is simply involving multiple nodes connected to each other with edges. An edge is a connection between nodes with a specific direction. DAG is a noncircular structure, so it is not possible to face the exact node twice when moving from node to node by edges.

Blockchain adds blocks sequentially to constitute what is called chain of blocks, while DAG uses blocks' acyclic graph which parallelizes the validation process which results in higher throughput. In addition, DAG transactions are connected from one to another in which each transaction confirms the next one, while blockchain requires proof of work from minors for each transaction [35]. Fig. 5 shows the structure of blockchain and DAG.

DAG has several advantages over blockchain. First, DAG is a zero-transaction fee since there is no need for minors to compete to create or approve a transaction. Second, DAG provides a higher level of scalability, as it becomes faster and more secure with the growth of network boundaries. Third and lastly, DAG is a partition tolerant, which allows a portion of the network to split off the main network for a period of time and continue to run without the Internet connectivity. These portions can be reconnected to the main network when the Internet connection was established.

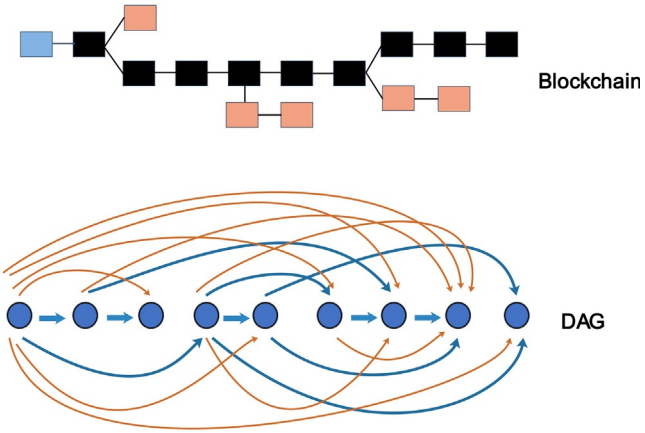

Fig. 5 Blockchain consists of blocks chained together using hash function while DAG transactions are connected from one to another in which each transaction confirms the next transaction.

This feature is very beneficial for areas around the world that have limited Internet connectivity or an unreliable electricity supply [36].

Although DAG provides countless benefits, it is not straightforward and associated with some flows. For example, DAG requires loads of traffic to operate efficiently which will be a big problem for small business networks. Also, the DAG network becomes more vulnerable to attacks with decreasing network traffic. Moreover, although one of the main benefits of DAG over blockchain is scalability, it does not be approved at a large scale since it's a quite new technology [14].

There are several applications that use DAG such as IOTA, Byteball, and Raiblocks, Hashgraph and Hylochain. IOTA is the most popular application among DAG applications. It is a cryptocurrency built for IoT. It is so-called as it is built to facilitate transactions of IoT. IOTA solves challenges associated with blockchain regarding transaction fees and scalability. It gets rid of blocks and chaining process of blocks of the blockchain in which a user can send a transaction to the IOTA ledger only if the user verifies the previous two transactions [37].

3.6.3 Tempo

Tempo ledger is an essential part of Redix [38], which is a DLT platform that works efficiently with the IoT. Tempo uses partitions of the ledger to accomplish the appropriate ordering of actions that occur in the whole network. The Tempo ledger comprises of three main elements; a networked cluster of nodes, a global ledger database which is distributed across the nodes and an algorithm for generating a cryptographically secure record of temporally ordered events [39].

The Tempo ledger involves events which are represented by objects, which are called atoms. It is a distributed database that keeps all atoms in the network. It is built to be horizontally scalable, supports semistructured data, and can update entries.

Table 2 provides a comparison between three main technologies of the DLT in terms of data structure, verification time, applications and projects for each technology, scalability, transaction fees, mining process, energy consumption and popularity.

4. Centralized IoT system

The IoT system allows almost all devices and objects in the environment to be connected and communicates with each other using either wired or wireless technologies. Since each object generates data about

Table 2 Comparison between blockchain, DAG and tempo.

Item	Blockchain	DAG	Tempo
Data structure	Distributed ledger with blocks chained together using the Hash function	Directed graph data structure that uses a topological ordering	Tempol Ledger consisting of a distributed database and consensus algorithm
Verification time	Several minutes	Minutes	<5 Seconds
Applications	Bitcoin, Litecoin, Ripple, Ethereum, etc.	IOTA, Byteball, and Raiblocks, Hashgraph and Hylochain	RedixDLT
Scalability	Less scalable	Scalable but untusted	Scalable but untusted
Transaction fees	High	Low	Low
Mining process	Mining is required	No mining is required	No mining is required
Energy consumption	High energy consumption for mining process	Less energy consumption since no mining is involved	Less energy consumption since no mining is involved
Popularity	Very well known, first launched 2008	Not well known yet, launched 2017	Not well known yet, launched 2018

their surroundings, these data can be integrated with other data from other devices to provide a meaningful information for various services and applications. Although the IoT notion is simple, it provides countless benefits that create new applications and services to facilitate our way of living [40].

This section provides a discussion of the centralized IoT system and its structure by highlighting limitations of the centralized model in the context of IoT.

4.1 Structure of centralized IoT

Currently, the majority of IoT solutions are based on the centralized client-server approach in which all IoT devices and objects are connected and authenticated through cloud servers. Every connection between different

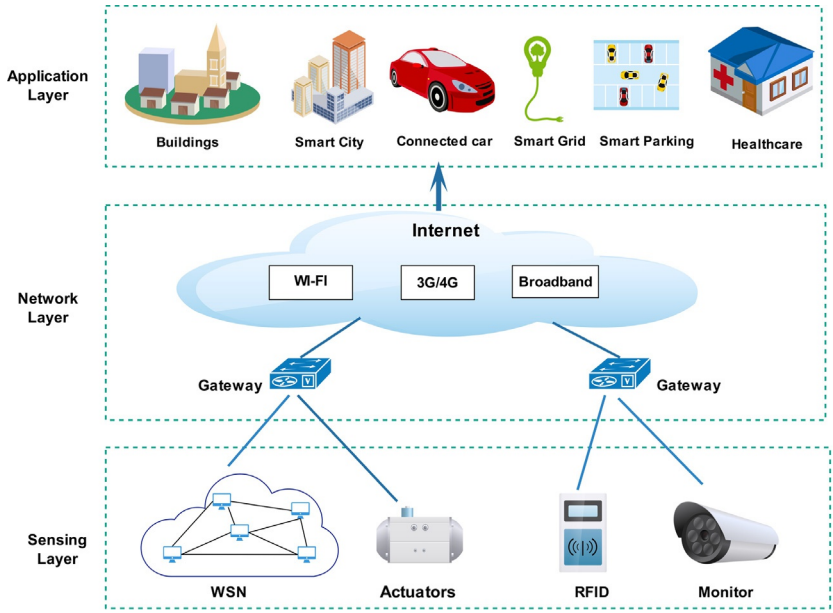

Fig. 6 Structure of centralized IoT system.

devices must be achieved through centralized servers. According to Fernández-Caramés and Fraga-Lamas [4] and Lu et al. [41], the centralized IoT architecture consists of three main layers: sensing, network and application layer, as shown in Fig. 6.

The basic layer of the IoT architecture is the sensing layers which involves different types of sensors, RFIDs, actuators and Wireless Sensors Networks (WSNs). This layer collects all relevant data about the surrounding environment to provide a meaningful information about our physical world. All devices and objects in the sensing layer are not connected to each other directly, but with a centralized gateway instead [42]. The network layer is used to connect all IoT objects and devices to the Internet. It contains gateways that act as interlayer communication points between the sensing layer and network layer. Several communication technologies and protocols are used in the layer, such as 3G/4G, ZigBee, Wi-Fi, Bluetooth and Broadband to transport data between the sensing layer and the application layer. The application layer involves various IoT applications that can benefit from data collected by sensors such as smart city, healthcare, connected cars, smart parking, smart grid and other.

4.2 Limitations of centralized IoT model

The centralized architecture of the IoT system provides a good start for connecting a wide range of various objects and devices all over the world under the responsibility of a centralized server which manages and control all communication between devices and provides the required identification and authentication for different devices and objects. However, it is unable to support large-scale IoT networks which need to be extended in the near future especially with the huge increase of adopting IoT solutions [43].

The number of IoT devices is increasing every day and there are several indications that this increase will continue especially with integrating IoT system with new technologies that can deliver more improvement for IoT services and applications. Cisco has reported that the number of IoT devices is about to reach 50 billion in 2020 [44]. Therefore, with these expectations, the constraints associated with the centralized architecture of the IoT system need to be addressed to continue the adoption of IoT solutions in the future.

There are several limitations associated with the IoT centralized architecture. These limitations include:

- Scalability: It is a major issue for the centralized system since it based on managing and controlling all processes using a central authority. This system structure can scale well but only for small networks. Deploying a centralized system for large business organizations with many branches in different locations will be impractical. It will be hard to transport decisions to different locations based on the management hierarchy. In the IoT context, since there is a massive increase in the number of IoT devices, there are many doubts about the capability of the centralized architecture of the IoT to scale and operate efficiently with the increasing demands [45].
- Cost: Since all computing operations are executed through the central server, the hardware and software capabilities should be good enough to serve all nodes in the network. There is a huge amount of communications between nodes and the centralized server which need to be handled which require high processing power to serve multiple nodes at the same time. Also, it requires maintaining large data storages that able to store data of different devices in the network. In the IoT context, there are high costs related to the deployment and maintenance of centralized servers which increased with increasing number of IoT devices in the network [4].

- Privacy: The centralized system is vulnerable to data manipulation. Collecting real-time data of different devices and store it in one place with the authority of the centralized server can violate the data privacy. The collected data may contain sensitive information about nodes such as their financial accounts, passwords, etc. Since these data are stored in one place, it can be easily breached. On the other hand, there are several examples of privacy violation by service providers. For example, some service providers sell information about their customers to marketing companies that can use this information to analyze nodes' behavior. Also, if an energy company found that their smart meter data analysis will be the evidence that might result in high costs or lawsuits. They will edit or even delete these data [46]. Therefore, privacy is another issue in the centralized IoT system that needs to be handled.
- Security: Security is a nightmare for any system. It is a major issue in the centralized system since all data stored in one location and all operations are executed through a central server which makes it an easy target for various types of attacks especially to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The enormous increase of IoT devices in our environment leads to increasing the chances to exploit security vulnerabilities within IoT devices which are poorly secured. Therefore, both IoT devices (source of data) and centralized cloud server (data storage location) are an easy target for security attacks [47].
- Single Point of Failure: Since the centralized server carries out all processing operations and controls all nodes connected to it in the network. This creates a single point of failure in which if the server goes down, the entire system will be unavailable. Avoiding this issue can be done by adding redundant switches, network connections and servers as a backup to provide an alternative path when the original server goes down. However, this solution creates problems with synchronization between the original server and backup as well as it requires high expenses to install a backup server.
- Access and Diversity: Nodes can access the network for different needs. However, centralized systems require their nodes to access the information on the network consistently using identical processes. This kind of networks may not provide the flexibility needed by various nodes with diverse needs. In addition, a centralized system uses a single operating system for the whole network. While this can have advantages for some nodes, it limits diversity within the network and can prevent some nodes from accessing the network. Since the IoT system is dynamic and

heterogeneous in nature with diverse devices and objects, so ensuring access of various heterogeneous devices should be a fundamental priority for the centralized IoT architecture [48].

- Inflexibility: Since the centralized server carries out all processing operations and controls all nodes connected to the network, there are huge workloads coming from different nodes in the network. Although the centralized server schedules the workload to avoid peak-load concerns when people across an organization need to use it simultaneously, the tight schedule and delay associated with this process limit the flexibility of the user while doing their own work.

5. Intersection of blockchain with IoT

This section provides a discussion of integrating IoT with blockchain by highlighting benefits of the integration process. Applications and challenges of integrating IoT with blockchain will also be discussed.

5.1 Integration of blockchain with IoT

The IoT system facilities the development of various applications and services by allowing different devices and objects to share their data over the Internet which enhance people quality of life through digitization of various services. Over the last few years, Cloud computing technologies have provided the IoT system with the required functionality to analyze and process information to convert it into real-time actions and knowledge.

The extraordinary progress of the IoT has unlocked novel opportunities in different domains; however, one of the major concerns that stand as a barrier for the promised distribution of IoT devices is the lack of trust and confidence. This is because the existing IoT architecture relies on a centralized system in which a third-party or service provider manages and controls all data collected from IoT devices without clear boundaries about how the collected data is being used. The centralized server acts as a black box and the network participants do not have a pure vision of where and how their data is being utilized [49].

On the other hand, blockchain provides autonomous, distributed, decentralized and trustless environment. In contrast to the centralized architecture which presents several issues regarding single point of failure and scalability, the blockchain uses a decentralized and distributed ledger to utilize the processing capabilities of all the participating nodes in the blockchain

network which provide more efficiency. Also, as there is no need for a third party or a central authority, this improve business friendliness and guarantees a trusted workflow. In addition, blockchain delivers a high level of transparency by sharing transaction details among all participants nodes involved in those transactions.

There are several similarities and differences between IoT and blockchain. Table 3 provides a summary of comparison between IoT and blockchain.

Integrating the IoT with blockchain can bring several benefits to both technologies. For instance, adopting the decentralized architecture for the IoT system can resolve many issues particularly security. The peer-to-peer communication model can be used to process billions of transactions between IoT devices which can critically decrease the costs regarding installing and maintaining large centralized data centers and distribute computation and storage among billions of IoT devices. The decentralization feature will also eliminate the whole network from being unavailable if one node goes down [19]. Fig. 7 shows the centralized architecture of the IoT system and the decentralized IoT system after integrating IoT with blockchain.

Blockchain has the capability to provide an easy infrastructure for two nodes to directly convey a piece of property such as money or data between one another with a secured and reliable time-stamped contractual handshake. By the use of smart contracts, the agreement between communicating

Table 3 Comparison between IoT and blockchain.

Items	Blockchain	IoT
System structure	Decentralized	Centralized
Resources	Resource consuming	Resource restricted
Privacy	Ensures the privacy of the participating nodes	Lack of privacy
Latency	Block mining is time-consuming	Demands low latency
Scalability	Scale poorly with a large network	IoT considered to contains a large number of devices
Bandwidth	High bandwidth consumption	IoT devices have limited bandwidth and resources
Security	Has better security	Security is one of the big challenges of IoT

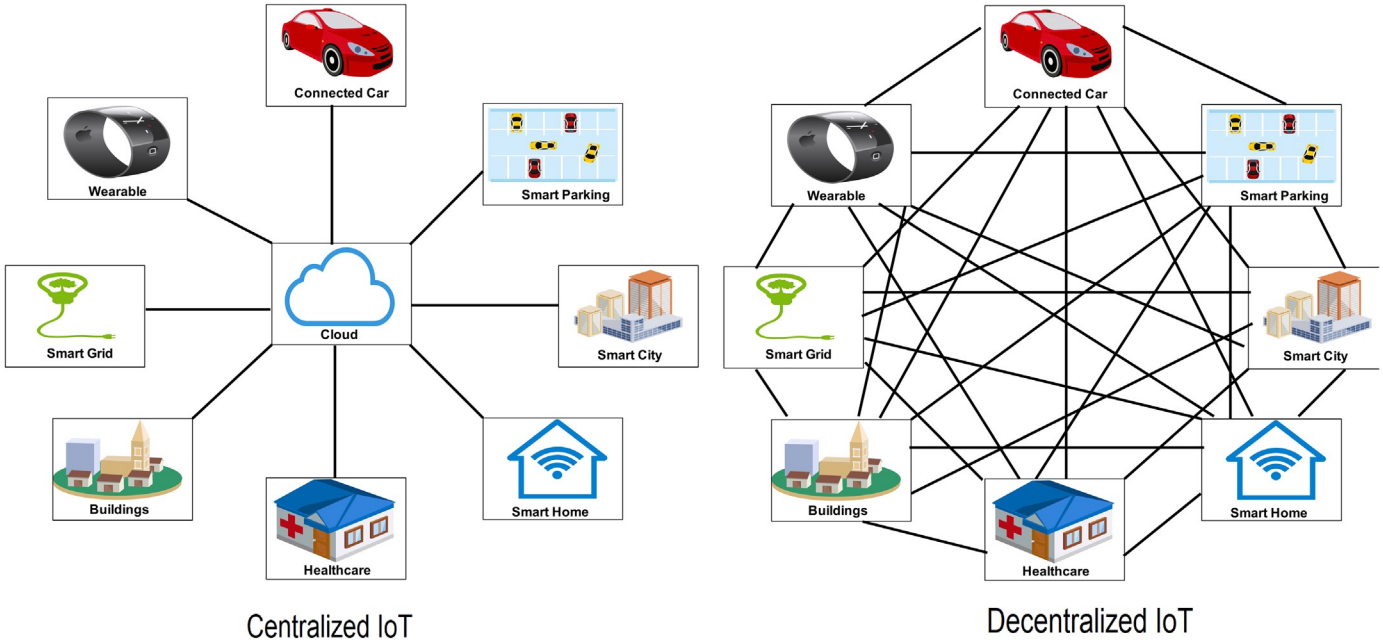

Fig. 7 Centralized IoT where a central authority manages and controls all operations of the communicating nodes and after integrating blockchain with IoT and build decentralized IoT where no central authority or a single point of failure.

Table 4 How blockchain can address the challenges of IoT.

IoT challenge	How blockchain can address the challenge
Security	Blockchain provides an immutable and secure environment for various types of IoT devices. It also ensures data integrity since any change should be verified by the majority of participating nodes in the blockchain network [45]
Point of failure	Blockchain uses decentralized and distributed communication between participating nodes in the network which eliminates the issue of single point of failure.
Third party authority	Blockchain provides a decentralized and distributed environment for the IoT devices so there no need for a centralized server or service provider to build the required trust between communicating nodes in the IoT system
Address space	In contrast to IPv4 with 32-bit and IPV6 with 128-bit address space, blockchain has 160-bit address space which allows blockchain to generate and allocate addresses for about 1.46×10^{48} IoT devices offline [51]
Susceptibility to manipulation	Since blockchain provides a decentralized and immutable environment which allow to detect and prevent any malicious action. The update is only approved after the consent of most participating nodes in the blockchain network
Ownership and identity	Blockchain can provide a trustworthy, authorized identity registration, ownership tracking and monitoring. It has been used in monitoring and tracking products, goods and assets successfully [51]
Data Integrity	Blockchain provides an immutable and tampered-proof ledger that cannot be updated unless the majority of participating nodes provide their consent and verify the update
Authentication and access control	The blockchain smart contracts have the capability of providing decentralized authentication rules and logic that can enable an efficient authentication for IoT devices
Flexibility	With various commercial and open source choices for blockchain, it's possible for IoT organizations to use it to realize several targets without spending a huge amount of money on research and development
Costs and capacity constraints	Since there is no need for a centralized server in the blockchain, IoT devices can communicate securely, exchange data with each other and carry out actions automatically through smart contracts [6]

parties can be formulated and stored as an immutable record of history which enables autonomous functions with no need for a centralized authority [50]. As a result, the blockchain will unlock a sequence of IoT situations that were hard, or even impossible to perform without it.

The Integration of blockchain with IoT provides a good solution for many issues of the IoT system. Table 4 provides a summary of IoT challenges and how integrating blockchain with IoT can solve these issues.

Integrating blockchain with IoT will create a system with more benefits and fewer issues. According to Tapscott and Tapscott [52], the integration of blockchain with IoT will create a system with the following features.

- Responsive, working in different situations and adapt to changing conditions.
- Resilient without a single point of failure.
- Robust with an ability to contain billions of nodes and transactions without affecting the performance of the network.
- Reductive with optimized costs and increased efficiency.
- High availability in real-time and provide a smooth data flow.
- Revenue-generating, providing opportunities to new business models.
- Radically openness, endlessly evolving and capability of updating the network with new inputs.
- Reliable, ensuring data integrity and trustworthiness of nodes.

Adopting blockchain with IoT is not a theoretical assumption. It practically occurs when IBM with a partnership with Samsung has designed a platform called ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry) which utilize the design of bitcoin to construct a distributed network of devices [53]. In addition, there are many other practical projects that investigate the potential of integrating blockchain with IoT. For example, Chain of Things [54] which provides an integrated blockchain and IoT hardware solution to solve IoT challenges regarding identity, security, and interoperability. Also, Slock.it [55] provides the transparency and auditability features to the IoT objects by integrating blockchain with IoT. It resolves the problem of connecting a device to the blockchain and improves the essential features for nonblockchain designers working on IoT systems by providing an interoperable and decentralized platform. Moreover, Waltonchain [56] provides a trustworthy and traceable business network with complete data sharing and absolute information transparency. It is designed by integrating RFID and blockchain technologies.

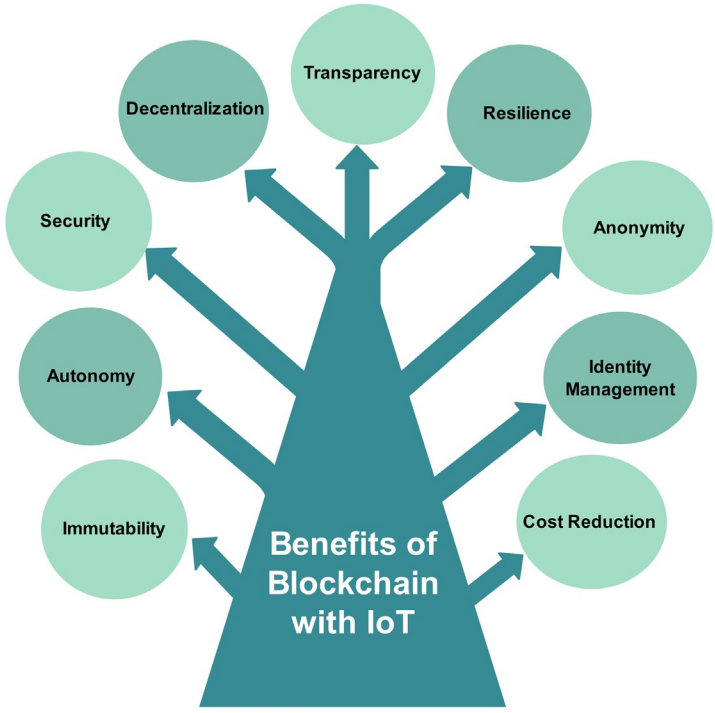

Fig. 8 Benefits of integrating blockchain with IoT.

5.2 Benefits of integrating blockchain with IoT

There are many benefits of adopting blockchain with IoT such as publicity, immutability, decentralization, resiliency, etc. This section provides a summarized discussion of advantages of integrating blockchain with IoT, as indicated in Fig. 8.

- Transparency: There is a high level of transparency in the blockchain network by allowing all the participating nodes to view transactions and blocks in the distributed ledger without any modification since the content of a transaction is protected by the participant's private key. Since the IoT is a dynamic and heterogeneous system in nature, the transparency feature will allow various devices to share their data with other devices in the network and at the same time data integrity is guaranteed.
- Decentralization: Blockchain provides a decentralized and distributed environment where there is no need for a central authority to manage the execution of operations and control communication between

various nodes in the network. There is no centralized authority to verify a transaction or put certain rules to accept a transaction. This, in turn, provides a trusted environment where participating nodes in the network are the only entities that will decide to accept or discard a transaction based on the agreement of the majority of participating nodes [53].

- Security: It is one of the main challenges standing as a barrier for the successful implementation of IoT devices. But with integrating IoT with blockchain, this issue will be significantly reduced, as blockchain provides better security since it uses public key infrastructure that protects against malicious actions. The participating nodes 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 [57].
- Autonomy: The blockchain technology allows the development of new generation of devices with the capability to provide smart autonomous assets and hardware as a service. For example, autonomous cars which need the blockchain to provide a secure environment and data tamper-proof to increase safety and security since cyber-attack is one of the essential issues of adopting autonomous cars. Adding the autonomy feature to the IoT system with the huge development in machine learning techniques will enable the appearance of novel autonomous IoT applications [6].
- Identity Management: The IoT system with a growing number of devices and objects is suffering from identity theft that allows malicious entities to steal legal owner's identities and exploit their sensitive information. Integrating blockchain with IoT can solve this issue since the blockchain technology has the potential to control and manage the user identity and credentials of nodes easily and in a more secure manner. In addition, blockchain can provide trusted distributed authentication and authorization of devices for IoT applications [58].
- Immutability: Blockchain provides a tamper-proof capability in which if a participating user request to add a transaction, the transaction is only added to the block if the majority of participating nodes 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. The traditional security solutions applied on the centralized server in the IoT system do not protect data integrity, but with the immutability feature of the blockchain, data integrity will be guaranteed [59].

- Resilience: Blockchain provides a resilient environment where transactions are stored in different locations. In addition, blockchain allows each participating user in the network to hold an original copy of the distributed ledger that encompasses all transactions which have ever made in the network. Therefore, blockchain is better to handle and tolerate an attack, since if a user is compromised, it will not be affected as blockchain will be maintained by every other user in the network. Holding a copy of data for each IoT data will enhance the information sharing; however, it presents new processing and storage challenges [60].
- Anonymity: Although the blockchain is a public and distributed ledger among various nodes in the network, it can provide an anonymous identity for nodes to keep their privacy. For example, the buyer and seller can use an anonymous and unique address number to process a transaction to keep their identities uncovered. Although this feature has caused a lot of problems for blockchain especially it can provide a cover for criminals and malicious nodes in money laundering and other suspicious activities, it can provide several advantages for many other applications like electoral voting systems [61].
- Cost Reduction: Since blockchain is a decentralized technology, it has the potential to reduce costs associated with installing and maintaining large centralized servers and other networking equipment. Adopting peer-to-peer communication to process billions of transactions between IoT devices will distribute computing and storage requirements across billions of devices that form IoT networks [29].

5.3 Applications of blockchain with IoT

The decentralized, autonomous and trustless attributes associated with the blockchain technology provide several benefits for various IoT applications. This section provides a discussion of common IoT applications that can be strengthened through the blockchain technology.

5.3.1 Smart city

A smart city is built to provide various services to citizens using new information and communication technologies to provide a better lifestyle and enhance the quality of life. This achieved by having a network of sensors and smart objects that sense the surrounding environment and collect relevant data to create new services and applications for citizens.

With newly built intelligent and interconnected services at cities, it becomes a desirable target for attackers. Since the existing centralized architecture stores all data in one location, centralized server, in which if the

attacker has breached the server, all data will be under his own malicious behavior. So, the malicious attack on smart cities' services can cause serious issues that can result in real damage to the citizens' lives. Therefore, efficient security measures should be applied to mitigate against these attacks [62].

The integration of blockchain with IoT specifically in the smart city context can provide a solution to this problem. The decentralized feature of the blockchain can be used to split data into multiple chunks and distribute them across several smart devices in the smart city network and make the owner is the only one who can rebuild the original data. Also, blockchain can be used to provide certification of the data produced by IoT devices [63].

5.3.2 Smart home

A smart home is generally a home with integrated home automation system to improve quality of life by providing a safe, secure and comfortable place to live in. Also, it enables the owner to control home's appliances without being physically at home. IoT devices at a smart home collect a huge amount of data that can be utilized to enhance the owner's experience. The collected data can be subjected to powerful algorithms of machine learning to enable IoT devices to learn from the collected data and make autonomous decisions based on their surrounding conditions without requiring manual input from the owner. Therefore, with machine learning, IoT devices can constantly enhance themselves and provide highly efficient services [43].

Although smart home provides magnificent services which really improve people life, there is still a security nightmare in which an attacker can access smart devices and tamper their data or functions that can cause real problems that can literally cause the owner to lose his life. Since smart devices come with poor built-in security measures besides smart homeowners tend to work with default or weak passwords which can be easily breached. To solve this issue, the blockchain provides a magical solution by making IoT devices immutable and tamper-proof. This, in turn, protects data collected by IoT devices and control data to be accessed by other third parties. A common case of using blockchain for smart home is Comcast which uses a permissioned ledger to enable the homeowner to grant or deny access permissions remotely through a mobile application [64].

5.3.3 Supply chain

Supply chain is one of the IoT applications that involves integrated planning and performing several operations. This includes material flow, information flow as well as financial capital flow. The management of flow process of

goods, products, services, and information involving the storage and movement of raw materials as well as full-fledged finished goods from one point to another is called as supply chain management [65].

While this process seems easy in theory, but practically there is a huge amount of paperwork involved for each transaction between a supplier and retailer. This creates a big problem especially with growing the business size. Blockchain along with smart contracts can solve issues of the supply chain and reduce costs, time and efforts. It delivers the required scalability for supply chain by providing a large database that can be accessed from multiple locations around the world. Also, the blockchain technology can be adopted in a private manner to maintain data integrity across multiple participants. It also provides higher standards of security and the ability to be customized according to the data feed [5].

5.3.4 Healthcare

With the existence of connected devices and objects, real-time monitoring can save lives especially in emergency situations such as diabetes, asthma attacks, heart failure, etc. With a smartphone application, the patient real-time data can be collected and transferred to the doctor on a regular basis to monitor the patient remotely and independently. Also, these smart devices can be programmed to take autonomous decisions. For example, in emergency situations, it can call the ambulance or the doctor of the patient, while in less emergency situations, it can provide a suitable prescription for the patient [66].

The existing healthcare system faces several issues especially in security and privacy of healthcare data collected and transmitted in real-time. Adopting the blockchain technology in the healthcare sector can add numerous improvements. For instance, blockchain can provide an immutable ledger of medical records that cannot be altered once it created and signed. This, in turn, can increase the integrity of medical records. Another benefit of the blockchain is the consent management. Since the existing healthcare system has different privacy and consent regulations at every stage, the blockchain can be utilized to store the patient consent for purposes of data sharing, so any third-party can check the blockchain to decide whether to share the patient information or not [67].

5.3.5 Smart grid

Smart grid is one of the critical applications of the IoT system. It is a part of the IoT framework that is used to monitor and track lighting, parking spaces,

traffic signals, road warnings, traffic congestion, and early detection of things such as earthquakes and extreme weather. By definition, a smart grid is a network of transmission lines that involves transformers, smart meters, sensors, distribution automation and software that are deployed to businesses and homes across the city. Providing a bidirectional communication between connected devices and hardware to sense and quickly reflect the user requirements should be one of the main targets of the IoT smart grid [1].

Since smart grids are based on automation and remote access, they become a target for security issues in which attackers can access the devices and cause serious damage for either devices or homes. The adoption of the blockchain can resolve this issue by providing a shared and encrypted ledger which is immutable to changes made by malicious nodes or attackers. It can also be utilized to verify identities and authorize the access by storing and recording transactions in the immutable ledger and make data exchanges between distributed gadgets smooth and cost-efficient [68].

5.4 Challenges of blockchain with IoT

Although the convergence of blockchain with IoT brings countless benefits, it also faces several challenges that need to be addressed to increase the adoption of the blockchain technology in various IoT applications. This section provides common challenges standing in the way of integrating blockchain with IoT, as summarized in Fig. 9.

5.4.1 Security

As the IoT system contains billions of heterogeneous devices and objects connected over the Internet with poor built-in security measures. This makes it a desirable target for most security attacks. To improve the security of the IoT system, most security experts and researchers have confirmed that integrating blockchain with IoT can resolve this issue; however, one of the key challenges of providing a secure IoT system is the reliability of the data generated by IoT devices. Indeed, blockchain provides an immutable and tamper-proof ledger that ensures data integrity; however, if the data are corrupted before storing it in the blockchain, it will stay corrupted. The data can be corrupted either by a malicious intruder or the devices themselves and their sensors fail to work correctly from the start. Therefore, IoT devices need to be tested before their integration with the blockchain and apply appropriate techniques to detect device failures immediately [69].

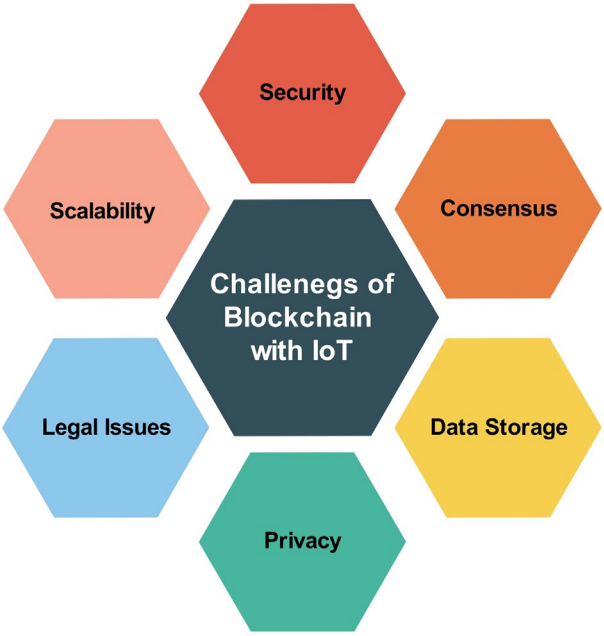

Fig. 9 Challenges of Integrating blockchain with IoT.

5.4.2 Scalability

One of the main challenges of integrating blockchain with IoT is the capability of the blockchain to scale to meet the security requirements of a dynamic network containing billions of devices. Although the integration between blockchain and IoT provides myriad benefits such as authentication, data integrity, fault tolerance and security, it comes at the price of scalability. The existing blockchain platforms such as Bitcoin and Ethereum can process only seven and 20 transactions per second, respectively. This processing speed cannot handle the processing requirements of the IoT system with billions of transactions. Also, the limited bandwidth associated with the blockchain technology cannot enable real-time transaction processing. Although there were several proposed blockchain scaling solutions over the last years, the scalability is still the major issue facing the convergence of blockchain with IoT [53].

5.4.3 Privacy

Several IoT applications collect and work with sensitive and classified data, for example, e-health connected devices that track and monitor the patient healthcare data. These data should be anonymously stored and protected

against any data modification. The integration of blockchain with IoT has promised to provide a secure and immutable environment; however, the data privacy faces several issues especially in transparent and public blockchains where all participating nodes in the blockchain network can view values of all transactions, so the blockchain cannot guarantee transactions' privacy [70]. Also, as indicated by Barcelo [71], the user's transaction can be linked to disclose user's personal information. Therefore, the privacy issue of the blockchain needs more research.

5.4.4 Data storage

In the IoT system, there are billions of devices that create Terabytes of data in real-time which needs to be stored for processing to extract meaningful information. Indeed, the integration of blockchain with IoT eliminates the need for a centralized authority to store and process the IoT collected data [72]. However, blockchain is not designed to store large amounts of data like those produced in the IoT system. The storage capacity is considered one of the big problems of the blockchain technology, but with integrating blockchain with IoT, this issue will become much greater. Also, as distributed ledger keeps all transactions that have ever made in the network, the size of the ledger will increase with increasing number of participating nodes in the network. The storage issue is still one of the biggest challenges for the integration of blockchain with IoT; therefore, more research and new approaches are needed to resolve this issue [4].

5.4.5 Legal issues

The IoT is a dynamic system in nature which have expanded over the boundaries of countries to connect and communicate data between various devices all over the world. Like all new technologies, the IoT is affected by the country's laws or regulations regarding data privacy. However, most existing laws do not cope with technological developments and became obsolete and need to be reviewed. Creating novel laws and standards can facilitate the certification of security features of devices to build a more secure and trusted IoT network. In this sense, laws that deal with information privacy and information handling are still a big challenge to be tackled in the IoT and will be an even bigger challenge after integrating blockchain with IoT. The blockchain can collect various nodes from different countries without having any legal or compliance code to follow, which is a serious issue that needs to be handled by issuing the appropriate laws which can cope with technological progress of both IoT and blockchain [49].

5.4.6 Consensus

The IoT system involves billions of devices and objects with limited resources such as computing power and storage. These resource-constrained devices cannot participate in the consensus mechanisms such as PoW and PoS associated with the blockchain technology that require high processing power for the mining process. Since the mining process is a complex operation that needs a huge amount of energy, integrating sophisticated Artificial Intelligence (AI) techniques with blockchain can be very efficient in optimizing energy consumption. So, therefore, more research is needed to investigate how to adopt consensus mechanisms in the IoT system [6].

6. Conclusion

The IoT has proven it can provide several benefits in various domains. It has evolved to include the perception of realizing a global infrastructure of interconnected networks of physical and virtual objects. These objects are interconnected using either wired or wireless networks to share information between various IoT devices to create novel applications and services. However, the current IoT centralized architecture faces many issues regarding security and scalability. One of the recommended solutions to resolve these challenges is the blockchain technology. It uses a decentralized and distributed ledger to utilize the processing capabilities of all the participating nodes in the blockchain network, which reduce latency and eliminate the single point of failure. Integrating the IoT system with blockchain can bring countless benefits. For instance, the decentralization feature of blockchain can process billions of transactions between IoT devices. This chapter provided a discussion of the intersection between IoT and DLTs. It started by providing an overview of DLT by highlighting its main components, benefits and challenges. The centralized IoT system is also discussed with highlighting its essential limitations. Then, the integration of blockchain with IoT is presented by highlighting the benefits of the integration process. Various application and challenges of blockchain with IoT are also discussed.

References

[1] 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.

[2] 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.

[3] H.F. Atlam, A. Alenezi, M.O. Alassafi, G.B. Wills, Blockchain with Internet of Things: benefits, challenges, and future directions, Int. J. Intell. Sys. Appl. 10 (2018) 40–48.
[4] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2018) 32979–33001.
[5] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, J. Tazelaar, A distributed ledger for supply chain physical distribution visibility, Information 8 (4) (2017) 137.
[6] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Futur. Gener. Comput. Syst. 88 (2018) 173–190.
[7] E. Karafiloski, A. Mishev, Blockchain solutions for big data challenges: a literature review, in: 17th International Conference on Smart Technologies, 2017, pp. 763–768. July.
[8] M.Å. Hugoson, Centralized versus decentralized information systems: a historical flash-back, IFIP Adv. Inf. Commun. Technol. 303 (2008) 106–115.
[9] M. Tommasi, F. Weinschelbaum, Centralization vs. decentralization: a principal-agent analysis, J. Public Econ. Theory 9 (2007) 369–389.
[10] K. Kawano, M. Orimo, K. Mori, Autonomous decentralized system test technique, in: Conference Proceedings of the Thirteenth Annual International Computer Software & Applications, 1989, pp. 52–57.
[11] 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.
[12] L. Swierczewski, The Distributed Computing Model Based on the Capabilities of the Internet, arXiv Prepr. (2012). arXiv1210.1593.
[13] J. Rehman, What Are Advantages and Disadvantages of Distributed Operating Systems, IT release, 2018. [Online]. Available: http://www.itrelease.com/2015/09/what-are-advantages-and-disadvantages-of-distributed-operating-systems/. [Accessed: 26-Oct-2018].
[14] F.M. Benˇ, I.P. Žarko, Distributed ledger technology: blockchain compared to directed acyclic graph, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018, pp. 1569–1570.
[15] M. Hancock, E. Vaizey, Distributed Ledger Technology: Beyond Blockchain, UK Government Office for Science, 2016.
[16] Investopedia, Distributed Ledger Technology, 2018. [Online]. Available: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp. [Accessed: 25-Oct-2018].
[17] Financial Conduct Authority, Discussion Paper on Distributed Ledger Technology, Discussion Paper DP17/3, 2017, www.fca.org.uk/publication/discussion/dp17-03.pdf, [Accessed 30-Oct -2018].
[18] B. Cœure, Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework, 2017. [Online], Available: https://www.bis.org/cpmi/publ/d157.pdf. [Accessed 30-Oct-2018].
[19] P. Ferraro, C. King, R. Shorten, Distributed ledger technology for smart cities, the sharing economy, and social compliance, IEEE Access 6 (2018) 62728–62746.
[20] J.J. Sikorski, J. Haughton, M. Kraft, Blockchain technology in the chemical industry: machine-to-machine electricity market, Appl. Energy 195 (2017) 234–246.
[21] H. Natarajan, S.K. Krause, H.L. Gradstein, Distributed Ledger Technology (DLT) and Blockchain, World Bank Group, Washington, D.C., 2017.
[22] 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.
[23] 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: IoTBDS 2017—Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, 2017.

[24] K. Sultan, U. Ruhi, R. Lakhani, Conceptualizing blockchain: characteristics & applications, in: 11th IADIS International Conference Information Systems, 2018, pp. 49–57.
[25] ESMA, The Distributed Ledger Technology Applied to Securities Markets, 2016. [online], Available: https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf. [Accessed 30-Oct-2018].
[26] A. Deshpande, K. Stewart, L. Lepetit, S. Gunashekar, Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards, British Standards Institution, 2017.
[27] W. Meng, E.W. Tischhauser, Q. Wang, Y. Wang, J. Han, When intrusion detection meets blockchain technology: a review, IEEE Access 6 (2018) 10179–10188.
[28] 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: IoTBDS 2018—Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, vol. 2018, 2018. March.
[29] K. Christidis, G.S. Member, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.
[30] 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.
[31] W.-T. Tsai, L. Feng, H. Zhang, Y. You, L. Wang, Y. Zhong, Intellectual-property blockchain-based protection model for microfilms, in: 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), 2017, pp. 174–178.
[32] M. Alharby, A. van Moorsel, Blockchain based smart contracts: a systematic mapping study, Comput. Sci. Inf. Technol. (2017) 125–140.
[33] Cambridge Dictionary, Jurisdiction | Cambridge English Dictionary, [Online]. Available: https://dictionary.cambridge.org/dictionary/english/jurisdiction. [Accessed: 31-Oct-2018].
[34] E. Benos, R. Garratt, P. Gurrola-Perez, The Economics of Distributed Ledger Technology for Securities Settlement, Bank of England, 2017. Staff Work Paper no 670.
[35] S. Cho, T. Elhourani, S. Ramasubramanian, Independent directed acyclic graphs for resilient multipath routing, IEEE/ACM Trans. Networking 20 (1) (2012) 153–162.
[36] M. Kalisch, B. Peter, Estimating high-dimensional directed acyclic graphs with the PC-algorithm, J. Mach. Learn. Res. 8 (2007) 613–636.
[37] IOTA, The Next Generation of Distributed Ledger Technology, 2018. [Online]. Available: https://www.iota.org/. [Accessed: 04-Nov-2018].
[38] Radix, [Online]. Available: https://www.radixdlt.com. [Accessed: 04-Nov-2018].
[39] D. Hughes, Radix-Tempo, Radix White Pap, 2017.
[40] H.F. Atlam, R.J. Walters, G.B. Wills, Fog computing and the internet of things: a review, Big Data Cogn. Computing 2 (2) (2018) 1–18.
[41] L. Yueming, Y. Li, S. Yin, Design and implementation of IoT centralized management model with linkage policy, in: Third International Conference on Cyberspace Technology (CCT 2015), 2015, pp. 5–9.
[42] 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.
[43] 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, pp. 1–8.
[44] N. Kshetri, Can Blockchain Strengthen the Internet of Things? IEEE Computer Society, 2017, pp. 68–72.
[45] H. Halpin, M. Piekarska, Introduction to security and privacy on the blockchain, in: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017, pp. 1–3.

[46] M. Conoscenti, D. Torino, A. Vetr, D. Torino, J.C. De Martin, Peer to peer for privacy and decentralization in the internet of things, in: 2017 IEEE/ACM 39th IEEE International Conference on Software Engineering Companion Peer, 2017, pp. 288–290.
[47] H.F. Atlam, G.B. Wills, IoT security, privacy, safety and ethics, in: Digital Twin Technologies and Smart Cities, Springer International Publishing AG (in press), 2019.
[48] 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), 2017, pp. 655–661.
[49] N. Fabiano, Internet of things and blockchain: legal issues and privacy. The challenge for a privacy standard, in: Proceedings—2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017, vol. 2018, 2018, pp. 727–734.
[50] 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), 2017, pp. 670–675. June.
[51] M. Ahmad, K. Salah, IoT security: review, blockchain solutions, and open challenges, Futur. Gener. Comput. Syst. 82 (2018) 395–411.
[52] D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Penguin Random House, New York, 2016.
[53] M. Samaniego, R. Deters, Blockchain as a service for IoT, in: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016, pp. 433–436.
[54] Chain of Things, [Online]. Available: https://www.chainofthings.com/. [Accessed: 09-Nov-2018].
[55] Slock.it, [Online]. Available: https://slock.it/. [Accessed: 09-Nov-2018].
[56] Waltonchain, [Online]. Available: https://waltonchain.org/. [Accessed: 09-Nov-2018].
[57] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in Internet of things: challenges and solutions, arXiv1608.05187. 2016.
[58] E.F. Jesus, V.R.L. Chicarino, C.V.N. De Albuquerque, A.A.D.A. Rocha, A survey of how to use blockchain to secure internet of things and the stalker attack, Secur. Commun. Netw. 2018 (2018), 9675050.
[59] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (4) (2016) 1–24.
[60] X. Liang, J. Zhao, S. Shetty, D. Li, Towards data assurance and resilience in IoT using blockchain, in: Proceedings—IEEE Military Communications Conference MILCOM, 2017, pp. 261–266.
[61] E. Heilman, F. Baldimtsi, S. Goldberg, Blindly signed contracts: anonymous on-blockchain and off-blockchain bitcoin transactions, in: International Conference on Financial Cryptography and Data Security, 2016, pp. 43–60.
[62] A. Panarello, N. Tapas, G. Merlino, F. Longo, A. Puliafito, Blockchain and IoT integration: a systematic survey, Sensors 18 (8) (2018) 1–37.
[63] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, IEEE Trans. Dependable Secure Comput. 15 (5) (2018) 840–852.

[64] S. Williamson, How IoT, Blockchain, and AI Can Join Forces to Improve the Smart Home Experience, 2018. [Online]. Available: https://medium.com/swlh/how-iot-blockchain-and-ai-can-join-forces-to-improve-the-smart-home-experience-7cdbdab75214. [Accessed: 10-Nov-2018].
[65] B. Bhandari, Supply chain management, blockchains and smart contracts. SSRN Electron. J. (2018). https://doi.org/10.2139/ssrn.3204297.
[66] 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. 10 (2018) 26–35.
[67] 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. 40 (2016) 218–225.
[68] M. Mylrea, S.N.G. Gourisetti, Blockchain for smart grid resilience: exchanging distributed energy at speed, scale and security, in: 2017 Resilience Week (RWS), 2017, pp. 18–23.
[69] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.
[70] H.F. Atlam, G. Attiya, N. El-Fishawy, Integration of color and texture features in CBIR system, Int. J. Comput. Appl. 164 (2017) 23–28.
[71] J. Barcelo, User Privacy in the Public Bitcoin Blockchain, White Paper. 2014.
[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.

About the Authors

Hany F. Atlam is a PhD Researcher at the University of Southampton, UK and lecturer at 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 is a Cisco Certified Network Associate (CCNA) and a Cisco Certified Academy Instructor (CCAI). 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 Honors 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.