*I.J. Intelligent Systems and Applications,* **2018, 6, 40-48**
Published Online June 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2018.06.05

# Blockchain with Internet of Things: Benefits, Challenges, and Future Directions

**Hany F. Atlam**
Electronic and Computer Science Dept., University of Southampton, Southampton, UK
Computer Science and Engineering Dept., Faculty of Electronic Engineering, Menoufia University, Menoufia, Egypt
E-mail: hfa1g15@soton.ac.uk

**Ahmed Alenezi, Madini O. Alassafi, Gary B. Wills**
Electronic and Computer Science Dept., University of Southampton, Southampton, UK
E-mail: {aa4e15, moa2g15, gbw}@soton.ac.uk

Received: 04 November 2017; Accepted: 09 February 2018; Published: 08 June 2018

***Abstract*—**The Internet of Things (IoT) has extended the internet connectivity to reach not just computers and humans, but most of our environment things. The IoT has the potential to connect billions of objects simultaneously which has the impact of improving information sharing needs that result in improving our life. Although the IoT benefits are unlimited, there are many challenges facing adopting the IoT in the real world due to its centralized server/client model. For instance, scalability and security issues that arise due to the excessive numbers of IoT objects in the network. The server/client model requires all devices to be connected and authenticated through the server, which creates a single point of failure. Therefore, moving the IoT system into the decentralized path may be the right decision. One of the popular decentralization systems is blockchain. The Blockchain is a powerful technology that decentralizes computation and management processes which can solve many of IoT issues, especially security. This paper provides an overview of the integration of the blockchain with the IoT with highlighting the integration benefits and challenges. The future research directions of blockchain with IoT are also discussed. We conclude that the combination of blockchain and IoT can provide a powerful approach which can significantly pave the way for new business models and distributed applications.

***Index Terms*—**Blockchain, Blockchain with IoT, Internet of Things, Centralized, Decentralized.

## I. Introduction

The Internet of Things (IoT) has the ability to connect and communicate billions of things simultaneously. It provides various benefits to consumers that will change the way that users interact with the technology. Using a collection of cheap sensors and interconnected objects, information can be collected from our environment that will allow improving our way of living [1].

The IoT concept is not new. In 1999, Ashton, who is the founder of MIT auto-identification center has said, "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so"[2]. Later in 2005, the ITU officially define the IoT as "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" [3].

Current IoT systems are built on centralized server/client model, which requires all devices to be connected and authenticated through the server. This model would not be able to provide the needs to outspread the IoT system in the future [4]. Therefore, moving the IoT system into the decentralized path may be the right decision. One of the popular decentralization platforms is blockchain.

A blockchain is a distributed database of records that contains all transactions that have been executed and shared among participating parties in the network. This distributed databased is called distributed ledger. Each transaction is stored in the distributed ledger and must be verified by consent of the majority of participants in the network. All transactions that have ever made are contained in the blockchain. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology [5].

Integrating IoT with blockchain will have many benefits. The decentralization model of the blockchain will have the ability to handle processing of billions of transactions between IoT devices, which will significantly reduce the costs associated with installing and maintaining large centralized data centers and will distribute computation and storage needs across the billions of devices that form IoT networks. In addition, working with the blockchain technology will eliminate the single point of failure associated with the centralized IoT architecture [6]. Moreover, integrating blockchain with IoT will allow the peer-to-peer messaging, file distribution and autonomous coordination between IoT devices with no need for the centralized server-client model [4].

 

This paper provides an overview of integrating blockchain with the IoT system; this involves an examination of the benefits resulting from the integration process and the implementation challenges encountered. The ultimate goal of this work is to provide a detailed description of the benefits and the challenges that result from combing blockchain with IoT so as to make the decision whether to go with the decentralization for the IoT or not.

The remainder of this paper is organized as follows: Section II presents related work discussing integration blockchain with IoT applications; Section III discusses centralized IoT architecture; Section IV presents the blockchain technology and its structure; Section V introduces essential characteristics of the blockchain; Section VI discusses how the blockchain works; Section VII presents blockchain with IoT; Section VIII illustrates benefits of integrating blockchain with IoT; Section IX challenges of blockchain with IoT; Section X discusses future research directions, and Section XI is the conclusion.

## II. Related work

The integration of blockchain with IoT have investigated in a few papers. For instance, the IBM Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) project [7] leverages the blockchain to build a distributed network of devices. As for the ADEPT project, many other approaches are trying to design a solution that will be able to merge all the different blockchain based applications [8]. Also, Slock.it introduced the first implementation of IoT and Blockchain using the Ethereum platform [9]. It is so called Slocks to reflect real-world physical objects that can be controlled by the Blockchain. They use the Ethereum Computer which is a piece of electronics that brings Blockchain technology to the entire home, making it possible to rent access to any compatible smart object and accept payments without intermediaries.

In addition, Dorri et al. [10] have proposed a new secure, private, and lightweight architecture for IoT, based on blockchain technology that eliminates the overhead while maintaining most of its security and privacy benefits was investigated on a smart home application as a representative case study for broader IoT applications. The proposed architecture was hierarchical, and consists of smart homes, an overlay network and cloud storages coordinating data transactions with blockchain to provide privacy and security.

Blockchain in healthcare IoT application has introduced as a solution for many challenges facing healthcare sector. For example, Gupta et al. [11] have proposed an approach to explain how Blockchain could enable an interoperable and secure electronic health records exchange in which health consumers are the ultimate owners. They have proposed a scenario to store only the metadata about health and medical events on the Blockchain. Otherwise the Blockchain infrastructure will have to scale massively to support complete health records. So, metadata such as patient identity, visit ID, provider ID, payer ID, etc. can be kept on a Blockchain, but the actual records should be stored in a separate universal health cloud.

Another study for Blockchain in Healthcare utilize Ethereum's smart contracts to create representations of existing medical records [12]. These contracts are stored directly within individual nodes on the network. They have proposed a solution called “MedRec” to structure the large amount of data into three types of contracts. The first one is Registrar Contract. It stores the participants’ identity with all the needed details and of course, the public keys. This kind of identity registration can be restricted only to certified institutions. The second contract is the Patient-Provider Relationship Contract. It is issued when one node stores or manages data for another node. The main usage will be when there is a smart contract between the care provider and patient. The last one is Summary Contract which helps the patient to locate her medical history. As a result of this contract, all previous and current engagements with other nodes in the system are listed.

## III. Centralized IoT Architecture

Basically, the IoT is the connection and communication of different devices over the Internet. These devices are composed of networking nodes whether serves or computer which are connected together to share their data. All devices are provided with sensors, which collect data that can be transmitted, stored, analyzed, and presented in a useful way [13].

There are many architectures for IoT, which is approved commonly. Different researchers and organizations proposed different architectures. According to the ITU, the IoT architecture is composed of four layers as shown in Fig.[3]:

- Application layer
- Service support and application layer
- Network Layer
- Device layer

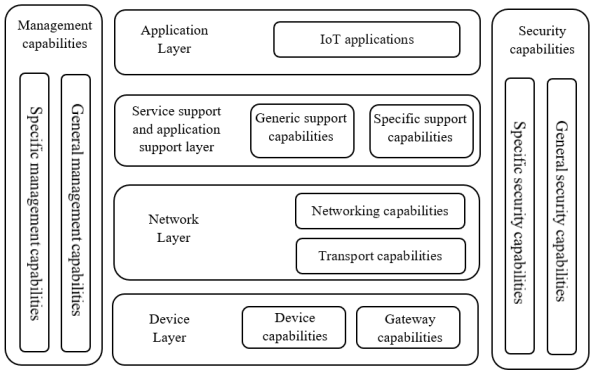


Fig.1. IoT reference model and architecture [3]

Application layer encompasses IoT applications. There are many IoT application such as healthcare, smart cities,

connected car, smart energy, smart agriculture and ...etc. Service support and application layer contains common capabilities which can be used by different IoT applications [14]. The Network layer includes devices such as routers, switches, gateways, and firewalls that are used to construct local and wide-area networks to provide Internet connectivity. In addition, it enables devices to communicate with one another and to communicate with application platforms such as computers, remote-control devices, and smartphones [13]. The device layer is similar to the physical layer of the Open System Interconnection (OSI) model of the network architecture. It is composed of physical devices and controllers that control objects. These objects represent things in the IoT that include a wide range of endpoint devices that send and receive a variety of information. For instance, sensors that collect information about the surrounding environment [15].

The current IoT architecture is built as a centralized model which is known as server/client model. In this model, all devices cannot talk to each other but talk to a centralized gateway instead. The centralized model has used to connect a wide range of computing devices for many years and will continue to support small-scale IoT networks, however, it will not be capable of providing the needs to extend the IoT system in the future [4].

The number of IoT devices will increase dramatically such that a network capacity will be at least 1,000 times the level of 2016. Cisco has reported that the number of IoT devices is about to reach 20 billion in 2020 [16]. Therefore, the amount of communication that needs to be handled will definitely increase costs exponentially. Even if costs and communication challenges are managed, the server/client model will still a point of failure that can interrupt the entire network [6].

In addition, the centralized model is vulnerable to data manipulation. Collecting real-time data does not ensure that the information is put to good and appropriate use. For example, if energy companies found that smart meter data analysis will be the evidence that might result in high costs or lawsuits. They will edit or delete these data [17].

A decentralized approach for the IoT would solve many of these issues. One of the popular decentralization techniques is blockchain. The next section discusses the blockchain technology.

## IV. Blockchain Technology

Blockchain technology provides an efficient way of recording transactions or any digital interaction in a way that makes it secure, transparent, highly resistant to outages, auditable. This technology is still new and changing very fast; adopting it in the commercial market is still a few years off. However, decision-makers across industries and business functions should pay their attention now and start to investigate applications of this technology to avoid disruptive surprises or missed opportunities [6].

In 2008, Satoshi Nakamoto has introduced the concept of Bitcoin. This was by releasing the popular paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" [18]. The paper presented a proposal for distributing electronic transactions rather than maintaining it dependent on centralized institutions for the exchange [19].

There are many definitions for the blockchain. According to [5], the blockchain is defined as " a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties". Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made [5].

A blockchain consists of two main elements [6], as shown in Fig.1:

- *Transactions*: are the actions generated by the participants in the system.
- *Blocks*: record the transactions and make sure they are in the correct sequence and have not been tampered with.

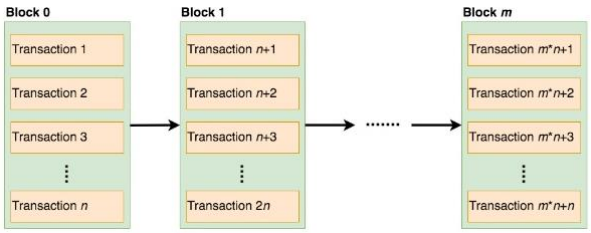


Fig.1. Structure of blockchain [13]

## V. Characteristics of Blockchain

The blockchain has many features that make it very attractive for the IoT to solve many of its issues. As shown in Fig.2, according to [10] blockchain characteristics include:

1. **Immutability**: Building immutable ledgers is one of the key value of blockchain. All centralized databases can be corrupted and commonly requires trust in a third party to keep the information integrity. Once you have agreed on a transaction and recorded it, it can never be changed.
2. **Decentralization**: The lack of centralized control ensures scalability and robustness by using resources of all participating nodes and eliminating many-to-one traffic flows, which in turn decreases latency and solve the problem of single point of failure that exists in the centralized model.
3. **Anonymity**: The anonymity provides an efficient way of hiding the identity of users and keeps their identities private.
4. **Better Security**: Blockchain provides better security because there is no single point of failure

 

to shut down the entire network.

5. **Increased Capacity**: One of the significant things about blockchain technology is that it can increase the capacity of an entire network. Having thousands of computers working together as a whole can have greater power than a few centralized servers.

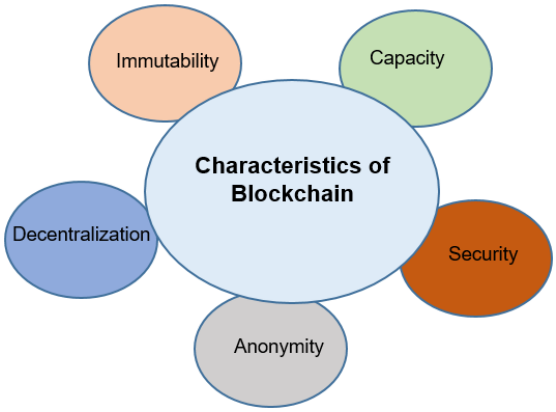


Fig.2. Characteristics of blockchain

## VI. How Blockchain Works?

Although the blockchain is still new and in experimenting stage, it is being perceived as a revolutionary solution that addresses modern technology issues such as decentralization, identity, trust, data ownership and data-driven decisions [7].

The blockchain is generally a database that stores all the transactions in blocks. When a new transaction is created, the sender broadcasts it to the Peer–to–Peer communication channel to all other nodes in the network. The transaction is still new and not verified. When the nodes receive the transaction, they validate it and keep it in their ledger [20].

Transaction validation is performed by running predefined checks on the structure and the actions of the transaction. Special node types called miners create a new block and include all or some of the available transactions from their transaction pool. Then the block is mined, which is a process of finding the proof of work using variable data from the new block's header [20]. Finding the proof of work is the continuous calculation of a cryptographic hash that fits the defined difficulty target. Mining requires a lot of processing power and the miners use a dedicated mining hardware. The miner that first finds a solution for its block is the winner. His candidate block becomes the new block in the chain. Because transactions are added in the mining block as they arrive, therefore, the latest block in the blockchain contains the latest transactions [4].

When a new block is created, it is time-stamped and propagated to all network nodes. Every node receives the block, validates it, validates the transactions, and adds the block to his ledger. When the majority of nodes accepted the block, it becomes authorized and non-reversible part of the blockchain. In addition to transactions, every block stores some metadata and the hash value of the previous block. So, every block has a pointer to its parent block. That is how the blocks are linked, creating a chain of blocks called blockchain [4].

The distributed ledger is available for everyone in the network to check the blocks and the transactions within. However, the users stay anonymous, they only identified by their public key as an address. Moreover, the transactions are encrypted. Invalid transactions are rejected and are not included in the blocks. Malicious attempt to make a change in the transactions will require repeated calculation of the proof of work for the attached block and all the blocks afterwards. These calculations are infeasible unless the majority of the nodes in the network are malicious [21].

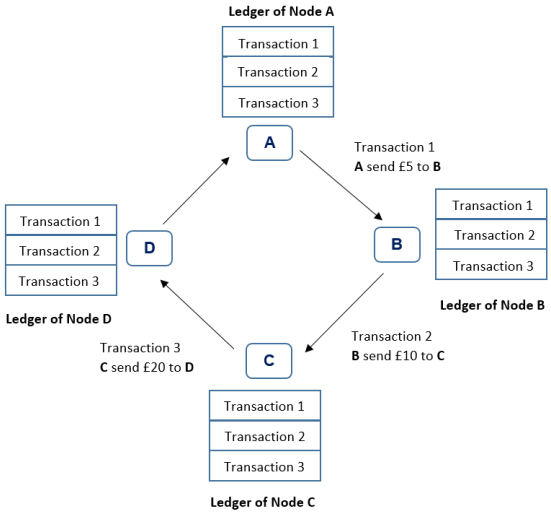


Fig.3. Simple example of blockchain technology

This section will discuss the blockchain with a simple example. Suppose that we have four nodes A, B, C and D who want to use the blockchain to transfer money, as it's known as Bitcoin. To transfer the money from one node to another node, there will be no intermediate third party to make the transfer process, which is the idea of decentralization. Therefore, if node A wanted to transfer money to node B, it will be transferred directly. As shown in Fig.3, suppose node A wants to send £5 to node B, then a transaction will be created and verified by all other nodes in the network to include it in the ledger. In addition, if node B wants to send £10 to node D, then a transaction will be created and verified by all other nodes in the network to include it in the ledger. This will be the same scenario when node C wants to send £20 to node D. All the transactions are chained together in what is called ledger. This ledger is distributed across all nodes in the network to make sure that all nodes have the same copy or version from the ledger, that is why it's called distributed ledger.

## VII. Blockchain with IoT

The IoT is an interesting developing system that

 

provides unlimited benefits, but there are many challenges with the current centralized IoT architecture such that all devices are identified, authenticated and connected through the centralized servers [4]. This model was used to connect a wide range of computing devices for many years and will continue to support small-scale IoT networks, however, it will not be capable of providing the needs to extend the IoT system in the future [22].

Table presents a comparison between blockchain and IoT. There are many advantages of both technologies, which can be combined, and get an improved outcome. The IoT has unlimited benefits and adopting a decentralized approach for the IoT would solve many issues especially security. Adopting a standardized peer-to-peer communication model to process the hundreds of billions of transactions between devices will significantly reduce the costs associated with installing and maintaining large centralized data centers and will distribute computation and storage needs across the billions of devices that form IoT networks. This will prevent failure in any single node in a network from bringing the entire network to a halting collapse [17,18].

Table 2. Comparison between blockchain and IoT

| Blockchain | IoT |
|---|---|
| Decentralized | Centralized |
| Resource consuming | Resource restricted |
| Block mining is time-consuming | Demands low latency |
| Scale poorly with large network | IoT considered to contains large number of devices |
| High bandwidth consumption | IoT devices have limited bandwidth and resources |
| Has better security | Security is one of the big challenges of IoT |

The decentralized, autonomous, and trustless capabilities of the blockchain make it an ideal component to become a foundational element of IoT solutions. It is no surprise that enterprise IoT technologies have quickly become one of the early adopters of blockchain technology. However, establishing peer-to-peer communications will present its own set of challenges especially security. IoT security is much more than just about protecting sensitive data. Therefore, the blockchain solutions will have to maintain privacy and security in IoT networks and use validation and consent of participants for transactions to prevent spoofing and theft [6].

In addition, blockchain technology is considered the key solutions to solve privacy and reliability issues in the IoT. It can be used in tracking billions of connected devices, enabling the processing of transactions and coordination between devices; this allows for significant savings for IoT industry manufacturers[24]. Moreover, this decentralized approach would eliminate single points of failure, creating a more resilient system for devices to run on. The cryptographic algorithms used by blockchains would make consumer data more private [25].

In an IoT network, the blockchain can keep an immutable record of the history of smart devices. This feature enables the autonomous functioning of smart devices without the need for centralized authority [26]. As a result, the blockchain will open a series of IoT scenarios that were difficult, or even impossible to implement without it. For example, by leveraging the blockchain, IoT solutions can enable secure, trustless messaging between devices in an IoT network [27]. In this model, the blockchain will treat message exchanges between devices similar to financial transactions in a bitcoin network. To enable message exchanges, devices will leverage smart contracts which then model the agreement between the two parties [20].

One of the most exciting capabilities of the blockchain is the ability to maintain a duly decentralized, trusted ledger of all transactions occurring in a network. This capability is essential to enable the many compliances and regulatory requirements of industrial IoT (IIoT) applications without the need to rely on a centralized model [6].

Many large organizations have started to adopt blockchain with IoT systems to get all benefits of the blockchain. For instance, IBM in partnership with Samsung has developed a platform ADEPT (Autonomous Decentralized Peer- To- Peer Telemetry) that uses elements of the bitcoin's underlying design to build a distributed network of devices, a decentralized IoT. ADEPT uses three protocols-BitTorrent ( file sharing), Ethereum ( Smart Contracts) and TeleHash ( Peer-To-Peer Messaging)-in the platform [28].

## VIII. Benefits of Integrating Blockchain with IoT

There are many benefits of adopting blockchain with IoT, as shown in Fig.4. These benefits can be summarized as follows:

1. **Publicity**: All participants have the ability to see the all the transactions and all blocks as each participant has its own ledger. The content of the transaction is protected by participant's private key [19], so even all participants can see them, they are protected. The IoT is a dynamic system in which all connected devices can share information together and at the same time protecting users' privacy.
2. **Decentralization**: The majority of participants must verify the transactions in order to approve it and add it to the distributed ledger. There is no single authority that can approve the transactions or set specific rules to have transactions accepted. Therefore, there is a massive amount of trust included since the majority of the participants in the network have to reach an agreement to validate transactions [28]. Therefore, the blockchain will provide a secure platform for IoT devices. In addition, eliminating centralized traffic flows and single point of failure of the current centralized IoT architecture.

 

3. **Resiliency**: Each node has its own copy of the ledger that contains all transactions that have ever made in the network. So, the blockchain is better able to withstand attack. Even if one node was compromised, the blockchain would be maintained by every other node [29]. Having a copy of data at each node in the IoT will improve information sharing needs. However, it introduces new processing and storage issues.
4. **Security**: Blockchain has the ability to provide a secure network over untrusted parties which is needed in IoT with numerous and heterogeneous devices [10]. In other words, all IoT network nodes must be malicious to perform an attack.
5. **Speed***:* A blockchain transaction is distributed across the network in minutes and will be processed at any time throughout the day [16].
6. **Cost saving***:* Existing IoT solutions are expensive because of the high infrastructure and maintenance cost associated with centralized architecture, large server farms, and networking equipment. The total amount of communications that will have to be handled when there are tens of billions of IoT devices will increase those costs substantially [30].
7. **Immutability**: Having an immutable ledger is one of the main advantages of blockchain technology. Any changes in the distributed ledger must be verified by the majority of the network nodes. Therefore, the transactions cannot be altered or deleted easily [14, 25]. Having an immutable ledger for IoT data will increase security and privacy which are the major challenges in this technology and all new technologies.
8. **Anonymity**: To process the transaction, both buyer and seller use anonymous and unique address numbers which keep their identity private. This feature has been criticised as it increases the use of cryptocurrencies in the illegal online market. However, it could be seen as an advantage if used for other purposes, for example, electoral voting systems [14, 26].

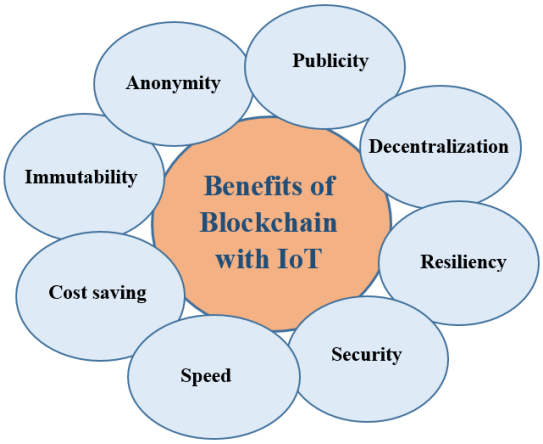


Fig.4. Benefits of integrating blockchain with IoT

## IX. Challenges of Blockchain with IoT

There is no doubt that integrating blockchain would have many advantages. However, the blockchain technology is not a perfect model which has its own flaws and challenges, as shown in Fig.5. These challenges can be summarized as follow:

1. **Scalability**: Scalability issues in the blockchain might lead to centralization, which is casting a shadow over the future of the cryptocurrency. The blockchain scales poorly as the number of nodes in the network increases. This issue is serious as

IoT networks are expected to contain a large number of nodes [28].

2. **Processing Power and Time***:* The processing power and time needed to achieve encryption for all the objects included in a blockchain system. IoT systems have different types of devices which have very different computing capabilities, and not all of them will be able to run the same encryption algorithms at the required speed [14, 27].
3. **Storage***:* One of the main benefits of blockchain is that it eliminates the need for a central server to store transactions and device IDs, but the ledger has to be stored on the nodes themselves [33]. The distributed ledger will increase in size as time passes and with increasing number of nodes in the network. As said earlier, IoT devices have low computational resources and very low storage capacity [34].
4. **Lack of skills**: The blockchain technology is still new. Therefore, a few people have large knowledge and skills about the blockchain, especially in banking. In other applications, there is a widespread lack of understanding of how the blockchain works [6]. The IoT devices exist everywhere, so adopting the blockchain with IoT will be very difficult without public awareness about the blockchain.
5. **Legal and Compliance***:* The blockchain is a new technology that will have the ability to connect different people from different countries without having any legal or compliance code to follow, which is a serious issue for both manufacturers and service providers. This challenge will be the major barrier for adopting blockchain in many businesses and applications [35].
6. **Naming and Discovery***:* The blockchain technology has not been designed for the IoT, meaning that nodes were not meant to find each other in the network. An example is the Bitcoin application in which the IP addresses of some "senders" are embedded within the Bitcoin client and used by nodes to build the network topology. This approach will not work for the IoT as IoT devices will keep moving all the time which will change the topology continuously [23].

 

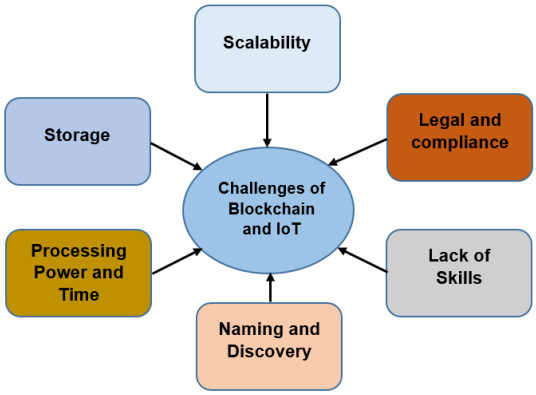


Fig.5. Blockchain and IoT challenges

## X. Future Research Directions

The blockchain has changed the concept of centralized authorities. The integration of blockchain with IoT will be the starting point for opening new businesses and applications. This section discusses future research directions of blockchain with IoT. This can be summarized as follows:

### A. Smart Contracts

Smart contracts are scripts stored on the blockchain. They are so powerful because of their flexibility. They can encrypt and store data securely, restrict access to data to only the desired parties and then be programmed to utilize the data within a self-executing logical workflow of operations between parties. Smart contracts translate business process into the computational process, greatly improving operational efficiency [5].

Using smart contracts within the IoT systems will provide an efficient way to improve security and Integrity of IoT data. The research questions that need to be addressed regarding conducting smart contracts within IoT systems are:

Q1: Are the smart contracts able to execute all event functions of IoT devices, which are in billions?

Q2: How the smart contract will respond to changing environmental conditions of the IoT as it is a dynamic system?

Q3: What is the appropriate platform to implement smart contracts within IoT systems?

### B. Regulatory Laws

Regulatory Laws are the procedures created by authorities and local administrative agencies to define legal ways of working with a product or technology within a certain country or region. As said earlier, the blockchain is a new technology which has not any legal or compliance code to follow. The research question that needs to be addressed regarding blockchain legal and compliance issues is:

Q1: What are regulatory rules that ensure the best practice of blockchain in IoT globally?

### C. Security

For all new technologies, the security is still the most challenging topic that takes the attention of researchers and organizations. Integrating blockchain with IoT can improve security as it uses use consent of the majority of participants to validate transactions to prevent spoofing and theft. However, IoT devices have low computational resources and storage space that cannot be able to process cryptographic algorithms. The research questions that need to be addressed regarding security are:

Q1: What is the optimum platform for IoT to integrate with blockchain?

Q2: How to overcome low capabilities of IoT devices to provide a secure IoT system?

### D. IOTA

IOTA is a new generation of public and distributed ledger that uses a concept called “Tangle”. The Tangle is a new data structure that based on a Directed Acyclic Graph (DAG). IOTA provide an efficient, secure, lightweight, and real-time transaction without fees. It is open-source, decentralized cryptocurrency, designed specifically for the IoT [36].

As IOTA is designed specifically for the IoT, it may be more appropriate to different IoT applications. However, it’s still under construction. The research questions that need to be addressed regarding IOTA are:

Q1: What the appropriate decentralization technology for the IoT, blockchain or IOTA?

Q2: What are major challenges with IOTA?

## XI. Conclusion

The IoT technology has extended that reached to every home in the universe. It has the ability to connect everyday objects to the Internet. Through cheap sensors, a lot of information can be collected from the surrounding environment that results in improving our life. However, current IoT architecture that based on server/client model has many issues that need to be addressed especially scalability and security. One of the solutions to address IoT issues is blockchain. Blockchain provides distributed peer-to-peer communication network where non-trusting nodes can interact with each other without a trusted intermediary, in a verifiable manner. In this paper, we provided an overview of integrating blockchain with IoT with highlighting benefits and challenges. The discussion also focused on future research directions. At the end, we can conclude that integrating blockchain with IoT can bring many advantages that improve many of IoT issues but at the same time, it introduces new challenges that should be addressed. There is still need more research to investigate implementing blockchain with IoT in more details.

## Acknowledgment

We acknowledge Egyptian cultural affairs and missions sector and Menoufia University for their

 

scholarship to Hany Atlam that allows the research to be funded and undertaken.

## REFERENCES


[1] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, 2017, pp. 254–260.

[2] K. Ashton, "That 'Internet of Things' Thing," *RFiD J.*, p. 4986, 2009.

[3] ITU, "Overview of the Internet of things," *Ser. Y Glob. Inf. infrastructure, internet Protoc. Asp. next*-generation *networks - Fram. Funct. Archit. Model.*, p. 22, 2012.

[4] E. Karafiloski, "Blockchain Solutions for Big Data Challenges A Literature Review," in *IEEE EUROCON 2017 -17th International Conference on Smart Technologies*, 2017, no. July, pp. 6–8.

[5] 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.

[6] A. Banafa, "IoT and Blockchain Convergence: Benefits and Challenges," *IEEE IoT Newsletter*, 2017. [Online]. Available: http://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html.

[7] IBM, "ADEPT: An IoT Practitioner Perspective," 2015.

[8] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, "CoinParty: Secure Multi-Party Mixing of Bitcoins," in *Proceedings of the 5th ACM* Conference *on Data and Application Security and Privacy - CODASPY '15*, 2015, no. August, pp. 75–86.

[9] C. Jentzsch, "Decentralized Autonomous Organization to Automate Governance," *white Pap.*, pp. 1–30, 2016.

[10] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," *arXiv1608.05187 [cs]*, no. August, 2016.

[11] N. Gupta, A. Jha, and P. Roy, "Adopting Blockchain Technology for Electronic Health Record Interoperability," 2016.

[12] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare:'MedRec' prototype for electronic health records and medical research data," *Proc. IEEE Open Big Data Conf.*, pp. 1–13, 2016.

[13] W. Stallings, "The Internet of Things: Network and Security Architecture," *Internet Protoc. J.*, vol. 18, no. 4, pp. 2–24, 2015.

[14] A. Torkaman and M. A. Seyyedi, "Analyzing IoT Reference Architecture Models," *Int. J. Comput. Sci. Softw. Eng.* ISSN, vol. 5, no. 8, pp. 2409–4285, 2016.

[15] Cisco, "The Internet of Things Reference Model," *White* Pap., pp. 1–12, 2014.

[16] Nir Kshetri, "Can blockchain Strengthen the Internet of Things?," *IEEE Compu ter So ciet y*, no. August, pp. 68–72, 2017.

[17] M. Conoscenti, D. Torino, A. Vetr, D. Torino, and 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.

[18] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.

[19] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," *2017 IEEE Technol. Eng. Manag. Conf.*, no. 2016, pp. 137–141, 2017.

[20] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," *2016 IEEE/ACS 13th Int. Conf. Comput. Syst. Appl.*, pp. 1–6, 2016.

[21] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. , M 1st ed. Sebastopol, CA, USA: O'Reilly Media, Inc., 2014.

[22] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. (PerCom Work.*, pp. 618–623, 2017.

[23] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini, "*CONNECT*: CONtextual NamE disCovery for blockchain-based services in the IoT," *IEEE Int. Conf. Commun.*, 2017.

[24] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and 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, no. June, pp. 655–661.

[25] A. Boudguiga *et al.*, "Towards Better Availability and *Accountability* for IoT Updates by means of a Blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2017, pp. 50–58.

[26] H. F. Atlam, A. Alenezi, A. Alharthi, R. Walters, and 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, no. June, pp. 670–675.

[27] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an Adaptive Risk-based Access Control Model for the Internet of Things," *I.J. Comput. Netw. Inf. Secur.*, no. January, pp. 26–35, 2018.

[28] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," *2016 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, pp. 433–436, 2016.

[29] D. Geist, "Using the Bitcoin Blockchain as a Botnet Resilience Mechanism," 2016.

[30] K. Christidis and G. S. Member, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[31] S. Huh, S. Cho, and S. Kim, "Managing IoT Devices using Blockchain Platform," in *The 19th IEEE International Conference on Advanced Communications Technology (ICACT 2017)*, 2017, pp. 464–467.

[32] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain," in *2017 IFIP/IEEE International Symposium on Integrated Network Management (IM2017):*, 2017, pp. 772–777.

[33] A. Alenezi, N. H. N. Zulkipli, H. F. Atlam, R. J. Walters, and 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.

[34] H. F. Atlam, G. Attiya, and N. El-Fishawy, "Integration of Color and Texture Features in CBIR System," *Int. J.*

*Comput. Appl.*, vol. 164, no. April, pp. 23–28, 2017.
[35] Diana Asatryan, "4 Challenges to Blockchain Adoption From Fidelity CEO," 2017. .
[36] H. F. Atlam, M. O. Alassafi, A. Alenezi, R. J. Walters, and G. B. Wills, "XACML for Building Access Control Policies in Internet of Things," in *in Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*, 2018, pp. 1–6.

## Authors' Profiles

**Hany F. Atlam** has born in Menoufia, Egypt in 1988. He has completed his Bachelor of Engineering and computer science from Faculty of Electronic Engineering, Menoufia University, Egypt in 2011, then completed the master's degree in computer science from the same university in 2014. He joined the University of Southampton as a Ph.D. student since January 2016. Hany's now is a lecturer in Faculty of Electronic Engineering, Menoufia University, Egypt and a Ph.D. candidate at the University of Southampton, UK.

He has large experiences in networking as he holds international Cisco certifications, Cisco Instructor certifications, and database certifications. He also 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 areas include IoT security and privacy, Cloud computing security, Blockchain, Big data, digital forensics, computer networking and image processing.

**Ahmed Alenezi** a lecturer at Northern Border University, Saudi Arabia and a Ph.D. candidate at the University of Southampton, UK. Ahmed is interested in multidisciplinary research topics that related to computer science. His research interests include Parallel Computing, Digital forensics, Cloud Forensics, Cloud Security, Internet of Things Forensics and Internet of Things Security.

**Madini O. Alassafi** born in Saudi Arabia. Alassafi received Bachler's degree in Computer Science from King Abdul-Aziz University in Saudi Arabia, 2006, and his master's degree in Advanced Computer Science from California Lutheran University, Thousand Oaks, USA, 2013. He works as a lecturer at King Abdul-Aziz University, Saudi Arabia. Now he is a Ph.D. candidate at the University of Southampton, UK. His current research interested in multidisciplinary research topics to pertain to computer science, which includes and not limited to Cloud Computing, Security, Risks, Cloud Migration Project Management and Cloud of Things, Security Threats.

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

**How to cite this paper:** Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi, Gary B. Wills, "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions", International Journal of Intelligent Systems and Applications(IJISA), Vol.10, No.6, pp.40-48, 2018. DOI: 10.5815/ijisa.2018.06.05

 