Securing Data Transmission Using Blockchain Technology For IOT Platform: A Survey

1st Hatem M. Abd El-kader.
dept. Information systems
Faculty of computers and information
Menoufia University
hatem6803@yahoo.com

2nd Nirmeen A. El-Bahnasawy
dept. Computer Science and Engineering
Faculty of Electronic Engineering
Menoufia University
Nirmeena.el-bahnasawy@el-eng.menofia.edu.eg

3rd Asmaa S. El-daly
dept. Information systems
Faculty of computers and artificial intelligence
University of Sadat City
Asmaaseldaly@yahoo.com

4thAida A. Nasr
Faculty of computers and information
Tanta University, Egypt.
https://orcid.org/0000-0003-4996-5439
aida.nasr2009@gmail.com

Abstract—blockchain is a new direction for data protecting. The main idea behind using blockchain technology for hidden data is dividing data into small parts and store each part in block. The data block is related to the previous by hash code which makes the chain. Blockchain techniques are suitable for large and small amount of data. Since sensors collect much data all the time and send to receivers over edge computing devices, which have limited resources, researchers start to use blockchain as a light technique for protecting data transmission over the internet. Sensor communication over the internet platform called internet of things platform. In this paper we show some previous work of blockchain techniques based IOT platform. In addition challenges and future direction will be discussed.

Keywords: *Internet of Things (IoT), Security in IoT, Privacy, Block chain*

I. INTRODUCTION

Internet of Things (IoT) technology is used in different devices to interconnect each other and transfer data over the Internet for the purpose of remote control automatically. IOT leads to the creation and improvement of operations in the field of activities that contribute to increasing business, increase profitability and new opportunities for enterprises in activities related to solutions and innovations [1]. However, IOT platform faces many challenges.

One of challenges that faces the IoT platform is data protection issue. Because the specifications of IOT platform are very limited, IOT needs special techniques for data confidentiality. Traditional security approach are not suitable for IOT platform, because they need high powered resources. Blockchain technology is based on dividing data and make relation between the generated parts before applying any encryption or protection algorithm. This reduces time complexity and does not need high specifications. Thus, blockchain is used on IOT platform.

we present, in Section 2, overviews covering IoT technology . in Section 3, we present and discuss Blockchain technology ,its functions, nodes, and types. In Section 4, presents related work of blockchain for IoT.

II. INTENET OF THINGS STRENGTH AND CHALLENGES

Internet of things (IoT) is a network of heterogeneous devices, which are connected to each other and to the Internet. The architecture of IoT varies depending on the application where it has been employed. There are different types of IoT architectures, the three-layer architecture consisting of perception, network and application layers, is one of them and considered to be efficient, reliable, and the easiest to implement. The devices in the perception layer generate data and forward it to the next network layer via a sink node. From the network layer, the data are transferred to the cloud where it is analyzed and stored. Based on these data, various applications/services can be provided to the users as shown in fig 1.

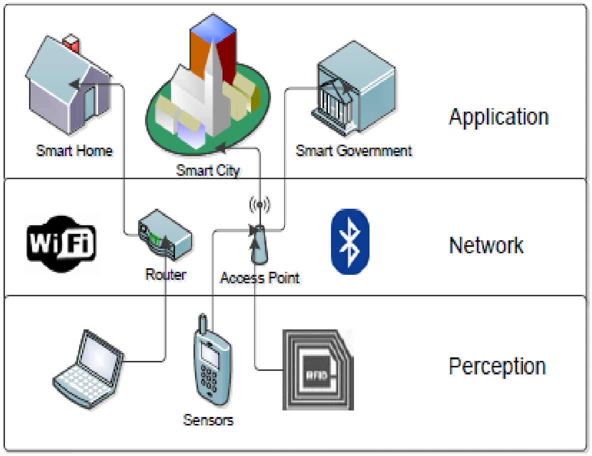

Fig 1. Basic three layer architectural framework of IoT

A. Strength of IoT

Due to the network of devices, a person can access data irrespective of their location making it convenient for people to use. When communications are not transparent, inefficiencies are caused, but with a network of interconnected devices, better communication is possible, because transferring data packets over connected network save time and money[5]. IoT not only helps to save time and money but achieve automation- the most important aspect in today's tech-life where all the tasks can be achieved without human intervention, with increasing quality of services.

B. Challenges in IoT

Some of the major IoT challenges include security issues, privacy issues, performance and scaling, and interoperability. These challenges are discussed in this section as follows:

- **Security**: Existing security mechanisms are not enough for reliable IoT application. Some of the challenges that are experienced while designing a secure IoT system are poor design, security adaptation, policy maintenance, and communication medium.

There are many security issues that can affect the IoT environment. As every layer is codependent on each other, identifying the security problems at every layer is critical as shown in Fig .2.

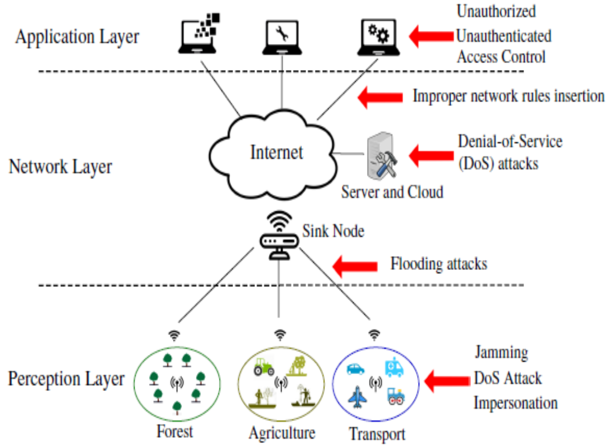

Fig 2. IoT security challenges

- **Privacy**: IoT has the potential to improve the quality of people's lives. However, the nature of the data (IoT users' location and movements, health conditions, and purchasing preferences, so on.) collected by IoT devices has serious privacy concerns.

- **Interoperability**: Heterogeneity has been a great challenge in distributed systems, as a variety of networks, hardware, different operating systems, and programming languages have to be in the same system.

- **Performance and scaling**: A scalable system with high performance continues to work effectively even when the number of resources and users are increased.

III. BLOCKCHAIN: TECHNIQUES AND IMPLEMENTATION

Blockchain is a distributed ledger technology (DLT) in which an append-only secure ledger database is shared and updated by all nodes/members, in a peer-to-peer (P2P) network. The participating nodes/members each store a copy of the ledger. BC technology offers a way of recording transactions or any digital interaction in a secure, transparent, resistant, auditable, and efficient way. The secure and decentralized property of BC has made it a strong field in the advancement of various fields of research such as IoT and artificial intelligence (AI).

A. Functioning of the Blockchain

To implement Blockchain technology, a P2P network needs to be created with the devices (users) that are interested to communicate through blockchain. Each participating device is referred to as a *node*. Two keys are generated for each node: namely, *public* and *private keys*. As the name implies, public key is acknowledged to all and private key is undisclosed, and is used by a user to produce a signature. In short, asymmetric cryptography is used to accomplish the security demand of the information. Private keys need to be kept protected to avoid possible misuse or tampering of data on a blockchain[7].

A node initiates the transaction and signing it with private key, then publishes it in the network for getting verified by the peer nodes. These verification methods used are known as *consensus algorithms*, and vary in different blockchain platforms, depending on the design objectives. After verification from peers, miner collects the transaction to create a block and that block gets appended to the blockchain with timestamp and unique ID (i.e. hash) to avoid further alterations[7]. Newly added block gets linked up with the earlier block using its hash and upcoming block will establish link with this block and so on as shown in Fig .3[8].

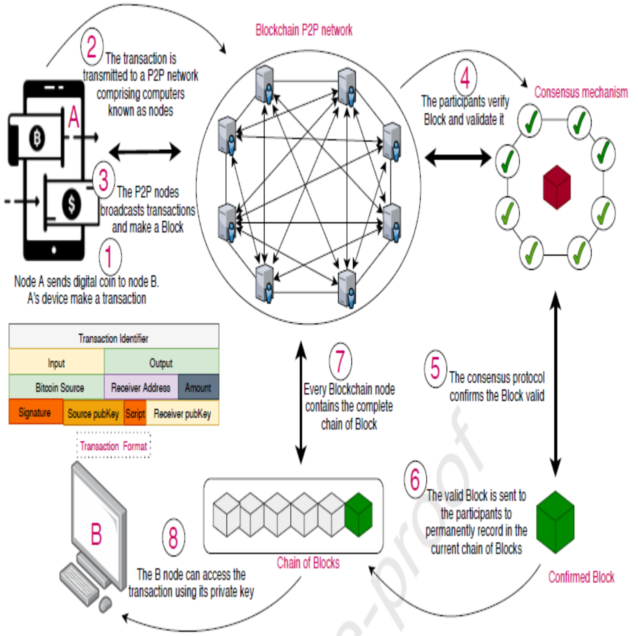
2 The transaction is transmitted to a P2P network comprising computers known as nodes
Blockchain P2P network
4 The participants verify Block and validate it
Consensus mechanism
A
3 The P2P nodes broadcasts transactions and make a Block
1 Node A sends digital coin to node B. A's device make a transaction
Transaction Identifier
Input
Output
Bitcoin Source
Receiver Address
Amount
Signature
Source pubKey
Script
Receiver pubKey
Transaction Format
7 Every Blockchain node contains the complete chain of Block
5 The consensus protocol confirms the Block valid
6 The valid Block is sent to the participants to permanently record in the current chain of Blocks
B
8 The B node can access the transaction using its private key
Chain of Blocks
Confirmed Block

Fig 3. given below depicts the general workflow of blockchain[8].

B. Consensus protocols

Consensus protocol is considered the heart of Blockchain technology because they maintain the integrity and security of the blockchain network, they ensure that no malicious transactions or changes can be made to the BC itself. It is a protocol by which network nodes of the blockchain arrive to a standard agreement on current records state of the ledger. Different blockchain platforms use different algorithms to reach the consensus and all of them differ in their operation and execution. Figure 4 shows the list of most popular consensus protocols used in different blockchain platforms.

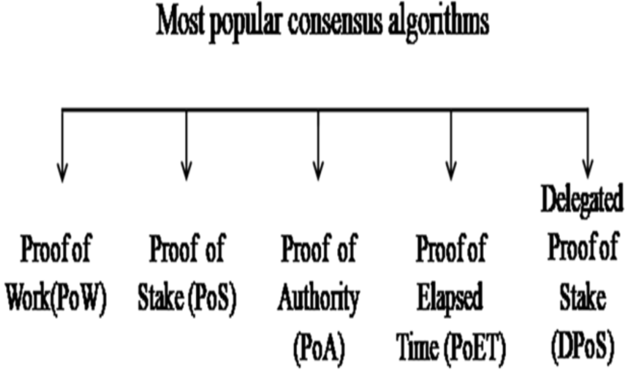
Most popular consensus algorithms
Proof of Work(PoW)
Proof of Stake (PoS)
Proof of Authority (PoA)
Proof of Elapsed Time (PoET)
Delegated Proof of Stake (DPoS)

Fig 4. Consensus protocols

C. Types of Blockchain

There are three blockchain (BC) types: public, private, and permissioned(hybrid) BC. In public BC, anyone can join the BC network without the approval of third parties. Anyone can act as node or as miner. In private BC, however, network access is restricted. It is a closed network in which only authorized nodes can maintain consensus, and the owner can control access of the nodes in the network[7]. Permissioned BC is a hybrid version of public and private BCs. It is not entirely open and is partially decentralized. As shown in table I

D. Blockchain nodes

A node is a device on a BC network. The BC nodes are distributed through a network, which are capable of carrying out a variety of tasks. The survival of any BC network is dependent on these nodes. The BC node can be general computer or other types of hardware devices having network connectivity, so it can be connected to the Internet with valid IP addresses. The main roles of a node are to store, process, and validate transactions that have occurred on the BC. ***Nodes are mainly of two types**: full nodes* and *partial nodes*. A full node stores the complete ledger locally. partial nodes store only the BC transactions, which are necessary and relevant to their operation.

IV. RELATED WORK OF BLOCKCHAIN FOR IOT

Rresearchers proposed a variety of new IoT architectures combined with characteristics of the blockchain including the application of the smart contract , distributed technology and the data integrity of blockchain . Also The advantages of blockchain are consolidating the IoT, there are many security problems in IoT that need to be solved urgently. Table II shows the features and challenges of blockchain in IoT applications.

Decentralized systems such as Blockchain and smart contracts have been regarded as a potential means of addressing these problems. The authors designed Blockchain that requires low computational costs for smart city infrastructure. All IoT devices' communications on a P2P Blockchain networks are tagged as transactions and securely stored in Cloud storage. **Ali et al. [5]** implemented a Blockchain-based behavioral verification system for smart-IoT. The system demonstrated a degree of trust level for the external devices that want to join the smart home network. Blockchain was deployed in the IoT behavior controller system to store, track, and identify

There are many applications of IoT using Blockchain such as smart home devices. A smart city is referred to as an interconnected network consisting of computer servers, system administrations and other equipment such as IoT devices for capturing and processing all forms of data generated by city dwellers. Thanks to the nature of IoT devices, the design of smart cities infrastructure remains challenges, including ensuring anonymity, completeness, and bottleneck issues.

IoT devices to safeguard IoT devices from malicious attacks. Sensor level filter has been utilized to prevent the malicious sensor from joining the network. **Lee et al.[6]** developed a Blockchain-based smart home architecture to solve the problems of the existing centralized smart home network and face future attacks against the smart Gateway. They used Ethereum Blockchain to make sure the smart home data was authenticated and confidential. **Singh et al. [4]** proposed a smart home appliance management and controlling system utilizing Proof of Authority consensus mechanism of the Blockchain.

Table I: Types of Blockchain

	Public Blockchain	**Private Blockchain**	**Permissioned Blockchain**
Aim	Used to solve efficiency, security problems with traditional financial institutions.	Mostly used in database management and for tasks to a single company, by setting up groups and participants who can verify the transactions internally.	Operate under the leadership of a group. But no entity having access to the Internet can involve in transaction verification.
Type	Open and decentralized	Restricted	Controlled and restricted(hybrid)
Operation	anyone can join the BC network without the approval of third parties. Anyone can act as a simple node or as miner.	network access is restricted. It is a closed network in which only authorized nodes can maintain consensus, and the owner can control access of the nodes in the network.	It is not entirely open and is partially decentralized. .
Features	Transactions are anonymous and transparent, secured by game theoretic mechanisms, with no infrastructure costs.	Existence of state compliance of data privacy rules, but there is a risk of security breaches like in a centralized system.	Reduced transaction costs and data redundancies, and replaces legacy systems ,and simplifying document handling

Table II: Features and challenges of Blockchain in IoT applications

	Features	challenges
Blockchain	Decentralization	The trade-off between power consumption, performance, and security
	Reduced Cost	Compromising between concurrency and throughput
	Greater Transparency	IoT device connectivity issue
	High Security	Limited scalability
	Data Privacy	Handling Big data in the Blockchain
	Improved Traceability	Compromising between transparency and privacy

Table III**:** Blockchain in IoT applications: some of smart cities/home studies

Authors	Blockchain type	Access control	Scalable	Tools/Simulator	Contributions	Remarks
Ali et al.[3]	PrB	x	x	Tensorflow and Keras libraries	A behavior capturing, and verification procedures in Blockchain supported smart-IoT system were introduced. Blockchain was deployed in the IoT behavior controller system to store, track, and identify IoT devices to safeguard IoT devices from malicious attacks	Performance on the Blockchain has not been conducted.
Lee et al.[4]	PrB	x	√	Mininet, Amazon EC2, Ethereum Bridge, Truffle development suite	A Blockchain-based smart home network architecture was proposed to overcome recent problems in current centralized security network architecture and combat future attacks on the smart homes Gateway.	The Gateway is vulnerable to a point of failure and no approach was designed to tackle this problem
Singh et al.[2]	CoB	√	√	Cooja and Netsim, Amazon EC2	The Blockchain technology was used in a smart home network to manage system transactions and adopted green Cloud computing, which hosts a green broker to minimize the environmental impact of the model	Blockchain configuration and simulators have not described in detail.

IIV. CONCLUDING REMARKS

Internet of things technology is the future of connecting different devices, places and organizations for data analysis and device control. So, researchers turn to develop communication security for IOT. In the environment of the IoT, the number of heterogeneous terminal connections and the amount of data transmission are very large. The entry of blockchain can solve the existing problems of IoT security. In this paper we, show the previous work in this field to show the advantages and disadvantages of applying blockchain on IOT platform. This clarifies a big picture of combination between IOT and blockchain. From the comparison of the previous algorithms, we find that the decentralized architecture of blockchain reduces the pressure of the old central computing of the IoT, and provides more possibilities for the innovation of the organizational structure of the IoT.

REFERENCES

[1] Bhanu, K. N., Mahadevaswamy, H. S., & Jasmine, H. J. (2020, July). IoT based Smart System for Enhanced

Irrigation in Agriculture. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 760-765). IEEE.

[2] Stoyanova, Maria, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K. Markakis. "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues." IEEE Communications Surveys & Tutorials 22, no. 2 (2020): 1191-1221.

[3] Md.Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, Venki Balasubramanian. A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions, 30 January 2021

[4] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, and Sukumar Nandi. Managing smart home appliances with proof of authority and blockchain. In International Conference on Innovations for Community Services, pages 221–232. Springer, 2019.

[5] Jawad Ali, Ahmad Shahrafidz Khalid, Eiad Yafi, Shahrulniza Musa, andWaqas Ahmed. Towards a secure behavior modeling for iot networks using blockchain. arXiv preprint arXiv:2001.01841, 2020.

[6] Younghun Lee, Shailendra Rathore, Jin Ho Park, and Jong Hyuk Park. A blockchain-based smart home gateway architecture for preventing data forgery. Human-centric Computing and Information Sciences, 10(1):1–14, 2020.

[7] Blockchain for IoT Access Control, Security and Privacy:A Review Pradnya Patil1 · M. Sangeetha1 · Vidhyacharan Bhaskar2, Accepted: 29 October 2020, © Springer Science+Business Media, LLC, part of Springer Nature 2020.

[8]M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions, Blockchain: Research and Applications, https:// doi.org/10.1016/j.bcra.2021.100006.

[9]. Chaabouni, N.; Mosbah, M.; Zemmari, A.; Sauvignac, C.; Faruki, P. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Commun. Surv. Tutor. 2019, 21, 2671–2701. [CrossRef]

[10]. Li, D.; Deng, L.; Lee, M.; Wang, H. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manag. 2019, 49, 533–545. [CrossRef]

[11]. Casado-Vara, R.; Prieta, F.D.L.; Prieto, J.; Corchado, J.M. Blockchain framework for IoT data quality via edge Comp]uting. In Proceedings of the BlockSys'18: 1st Workshop on Blockchain-enabled Networked Sensor System 2018, Shenzhen, China, 4 November 2018. [CrossRef]

[12]. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Gener. Comput. Syst. 2018, 82, 761–768. [CrossRef]

[13]. Duong, T.; Todi, K.K.; Chaudhary, U.; Truong, H. Decentralizing Air Trac Flow Management with Blockchain-based Reinforcement Learning. In Proceedings of the IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki, Finland, 23–25 July 2019; pp. 1795–1800. [CrossRef]

[14]. Calvaresi, D.; Dubovitskaya, A.; Calbimonte, J.P.; Taveter, K.; Schumacher, M. Multi-Agent Systems and lockchain: Results from a Systematic Literature Review. In Proceedings of the International Conference on Practical Applications of Agents and Multi-Agent Systems, Toledo, Spain, 20–22 June 2018.

[15]. Kapitonov, A.; Lonshakov, S.; Krupenkin, A.; Berman, I. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. In Proceedings of theWorkshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), Linkoping, Sweden, 3–5 October 2017; pp. 84–89. [CrossRef]

[16]. Santos, L.; Rabadao, C.; Goncalves, R. Intrusion detection systems in Internet of Things: A literature review. In Proceedings of the 13th Iberian Conference on Information Systems and Technologies (Cisti), Caceres, Spain, 13–16 June 2018