Azerbaijan Journal of High Performance Computing, Vol 3, Issue 1, 2020, pp. 3-14
https://doi.org/10.32010/26166127.2020.3.1.3.14

A Security Model Based on BlockChain Smart Contracts for Improve Authentication on the Internet of Things

Mohammad Saeid Safaei[1], Shamsollah Ghanbari[1], Zhanat Umarova[2], Zhalgasbek Iztayev[2]

[1] Islamic Azad University, Ashtian Branch, Iran, saeidsafaei@gmail.com, myrshg@gmail.com
[2] South Kazakhstan state university, Shymkent, Kazakhstan, zhanat-u@mail.ru, zhalgasbek71@mail.ru

*Correspondence:
Mohammad Saeid Safaei,
Islamic Azad University,
Ashtian Branch, Iran,
saeidsafaei@gmail.com

Abstract

IoT is one of the most important and profitable projects proposed by Kevin Ashton since 1999. One of the most critical issues in maintaining communication between things and protecting the data is the security issue of IoT. So far, different strategies have been made to maintain safe security. In this paper, we provide a Five-Layers model by adding two security layers based on BlockChain. We show that blockchain smart contracts are a solution to enhance IoT security and prevent infiltration into the network.

Keyword: IoT, BlockChain, Security, Smart Contract, Distributed Ledger

1. Introduction

IoT is a concept to describe the future where physical objects are connected to the Internet one after another and are connected to other objects and thus transformed from simple machines to smart systems. With the current growth of communities and rapid evolution in wireless communication technologies, the unprecedented development of changes from real-world transformations to the digital world has led to an increase in the number of electronic devices in many areas. Therefore, using the current technology for a better understanding of the world, our way of interacting with one another and with the environment has changed. IoT has emerged as a collection of technologies from wireless sensor networks (WSN) to the radio frequency identify (RFID), which provides capabilities for the sense, employment, and communication of the Internet (Gokhale, P., Bhat, O., & Bhat, S., 2018; Gartner, 2016; Asadpour, F.,

Table 1: Three Layer Architecture of IoT

Layer No.	Layer Name	Usage and Duty
3	Application	The software beds required for the application of information
2	Cloud Computing (service-oriented)	Service-based processing processes to fully cover the Active equipment
1	Network of Things	Includes smart devices or activators

& Ghanbari, S., 2018). One of the fundamental problems of IoT is in all architectures of this technology. Traditional architecture, which is often used on the Internet, may not meet the needs of IoT. The traditional service-oriented architecture consists of the following three layers (Gia, T. N., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H., 2015).

• The first layer: This layer consists of Smart Devices or Activators. In this layer, we have equipment that enables connection to goods while also allowing for wireless connection with existing networks.

• The second layer: In this layer, we have a combination of different types of networks that can be used to fully cover the enabling equipment so that all objects can be connected to the Internet. The information collected by them is integrated into the central system. Third layer: In this layer, the software beds are described to utilize

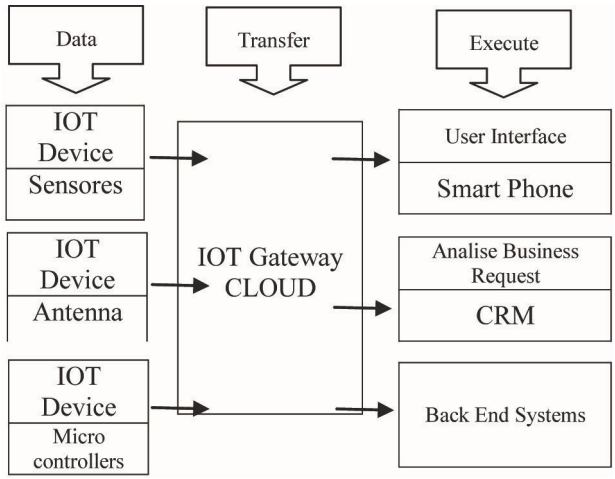

Fig.1 : IOT Traditional Approach

the collected data. These platforms, which act as an application interface, provide complete management of objects via the Internet portal.

Given that the IoT beds such as cloud (resource-oriented) and Grid (Application-oriented) are decentralized, a collective wisdom-based security approach can be very effective in improving the IoT security. Based on the emergence and development of BlockChain, such a model is available (Androulaki, E., Barger, A., Bortnikov, V., Cachin, et al., 2018, April). The issue of trust in information systems is very complicated. There are no confirmation or evaluation mechanisms, mainly because these systems include sensitive information such as economic transactions with virtual currency. Accordingly, in 2008 Satoshi Nakamoto gave two fundamental concepts that reflect a great deal. The first concept of Bitcoin is a virtual encrypted currency that maintains its value without supporting any organization or centralized financial institution (Nakamoto, S., 2019). Indeed, Bitcoin was the Decentralized autonomous organization working with a set of rules and self-governing functions with a distributed consensus protocol (Nakamoto,

S., 2019). The second conception, the popularity of which is beyond itself, is the BlockChain, which comes after the collapse of smart agreements on the BlockChain. After smart contracts, DAO was introduced in general and in modern form. According to what was said in this chapter, the BlockChain is a brilliant and innovative invention—the idea of a person or group of people known as Satoshi Nakamoto. Nevertheless, since the BlockChain has been introduced, this technology has become a big one. The main question of many people is how is the BlockChain in this paper, after reviewing the work done in the management of the IoT security, systematic analysis of BlockChain and then a security-based security method for IoT security, is proposed.

2. Security of IoT

Security in IoT is one of the main concerns of the users and hardware and software producers as we can say that the main challenge for IoT is to spread across societies. The fear of possible attacks via the Internet, theft of information and the loss of privacy by any person or organization can cause irreparable damage to consumers and users, expanding the range of usage and making smartphones, as well as the ability to install defenses such as memory and information processing systems and to identify potential attacks and vulnerabilities through using the most effective methods to influence such abuses (Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P., 2017, March). According to Mosenia, A., & Jha, N. K. (2016), the following risks can be considered for the traditional IOT-based security models.

1. Preventive measures in Network of Things Layer
- Non-network side-channel attacks
- Policy-based mechanisms or IDS (intrusion detection systems)
- Circuit modification

2. Preventive measures in Cloud Computing Layer
- Reliable routing
- Role-based authorization
- Information flooding
- Cryptographic

3. Preventive measures in Application Layer
- Pretest
- Outlier detection

3. Bird's Eye View on BlockChain

3.1. Systematic Analisis of Blockchain Technology

Blockchain technology is essentially the integration of three traditional digital signatures technologies, peer-to-peer communication, and Common Sense, which is presented in a new way. Then This technology created a new type of Internet via the possibility of distributing digital information without copying it. Initially, it was designed

for digital money, but the technology community is now finding other potential applications for this technology. The BlockChain protocol method is summarized as follows:

- Every transaction is signed by the private key of the users.
- It will then be communicated to all members of the network by the peer-to-peer network.
- There are some who check this transaction and store it in a block and try to attach the block to the previous BlockChain.
- Moreover, eventually, give it to all members of the network (Everisnext, 2016).

Blockchain is a mechanism allowing for verification of transactions by a group of uncertain factors. A general general general ledger provides clear, transparent, and verifiable general ledger. Blockchain can be used as free and perfect for access to all trades that have been made since the first transaction in the system, and at any time, it is Applicable by any entity. The BlockChain protocol stores the data in a chain of blocks, which stores each block of trades that have been made at a given time with

Table 2: Bitcoin Nodes

Routing	Mining	Storage	Wallet	
X	X	X	X	Bitcoin Core
	X		X	Full Node
	X	X	X	Solo Miner
X			X	Light Wallet

the Bitcoin. The blocks are connected by reference to the previous block and form a chain. To support and work with BlockChain, the network factors should provide the following tasks: routing, Date Saving, wallet services, exploration, or exploration. Different types of nodes can be part of the network based on what they do. Table 2 summarizes the most common types of nodes in the Bitcoin network (Gupta, Y., Shorey, R., Kulkarni, D., & Tew, J., 2018; Antonopoulos, A. M., 2014; Nakamoto, S., 2008).

Routing work is required to participate in the peer-to-peer network, including the diffusion of block and transaction. The Storage task is responsible for maintaining a copy of the chain on the node (the entire chain for complete nodes, and only part of it for light nodes). Wallet services provide security keys that allow users to request transactions, i.e., Work with Bitcoin. Finally, the Mining task is responsible for creating new blocks by solving the problem (Gupta, Y., Shorey, R., Kulkarni, D., & Tew, J., 2018). Interestingly, the point in the recent 51 Percent attack on May 17, 2019, was that groups involved in the pursuit of a useful activity for the Crypto Currency ecosystem did. Indeed, their purpose was not to exploit or exploit the unauthorized property. Not all actors in the ecosystem have a belief in such a belief. For example, a developer of Kiarahpromises wrote an article about a 51 Percent

attack “To coordinate a reorg to revert unknown’s transactions. This is a 51Percent attack. The worst attack possible. It is there in the white paper. What about (miner and developer) decentralized and uncensorable cash? Only when convenient?”. It is a peer-to-peer technique that uses distributed infrastructure, and user activities can be recorded to enhance security in specific formats, in this paper, with methods based on BlockChain and changes in the management of 3 layers of IoT to enhance security in the integration of IoT (Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R., 2016).

3.2. The Integration of BlockChain and IoT Technology

IoT makes the manual processes optimal for the digital era, providing a large amount of data that provides an unprecedented level of knowledge and knowledge. This knowledge facilitates the development of smart applications such as improving the management and quality of citizen’s life via digital services. Over the past few years, cloud computing technologies have helped to provide jobs for the IoT to analyze and process information and transform them into TimeLine knowledge. This unprecedented growth in IoT has created new opportunities, such as mechanisms for access and information sharing. The open data paradigm is the most obvious one. However, as in many scenarios, one of the most important vulnerabilities in these tasks is uncertainty. The focus structures, such as the structure used in cloud computing, have significantly contributed to the development of IoT. However, in terms of transparency, data acts as a black box, and the network participants do not know where and where they are being used (Vahid Rad, 2018). The communication process in the IoT has been centralized before 2005, and today, according to the work of the Cloud-focused Cloud, it is becoming peer-to-peer access to the data, thus making progress from a decentralized and decentralized cloud environment. Integration of renewable technologies such as IoT, BlockChain, artificial intelligence, and data mining that are named as big-four are considered valuable work (Vahid Rad, 2018). As such, we accept the enormous potential of BlockChain in the transformation of IoT. BlockChain can enrich IoT by providing a reliable service-sharing service. Data sources can be identified at any time, and during the time, the data will remain unchanged as a result of security. Among the projects that have been implemented in the project of IoT and BlockChain can be referred to as the Slock, which opened a bridge to BlockChain and the physical environment where people can lease the personal property to others. The Enigma project that works on Bitcoin offers a way to solve the privacy problem, and also tries to reduce processing too much. Alternatively, the ADEPT project, conducted by Samsung and IBM from 2015 on Etherium, balancing Manning’s process to the power and capacity of each miner (Vahid Rad, 2018).

3.3. Traditional approach of IoT

IoT makes it possible for the platform to provide the devices of a shared internet to save their information. A common language also offers machines to communicate with

each other, and people can benefit from them. Communication devices (sensors)are located in our everyday applications such as mobile, television, internal temperature control, electric appliances, cars, traffic lights, and industrial equipment. These sensors provide information on the location of the connected devices continuously and enable information exchange via the Internet. After that, the IoT Ins have analyzed data in order to extract important information and share them with other devices to start a new instruction or action (Vahid Rad, 2018; Ghanbari, A. M., Ghanbari, S., & Norouzi, Y., 2017) . One of the most well-known information-raiding attacks was the Mirai Botnet and DDOS attack that caused disturbances in closed-circuit cameras and DVR viewing almost all parts of the East Coast, including Twitter, Net-flix and Redit (Ghanbari, A. M., Ghanbari, S., & Norouzi, Y., 2017; Hallman, R., Bryan, J., et al., 2017). There are many challenges ahead for the integration of BlockChain and IoT, including the anonymity of nodes, the scalability, and authentication, where we will provide a solution to improve the authentication problem.

3.4. BlockChain Smart Contracts

Smart Contracts in BlockChain networks create an agreement for the machines that are implemented in the event of completion of certain conditions and cause them to work securely and independently. Therefore, the exchange of information less costly, more productive, and more independent (no third party would be required to monitor transactions). This smart deal can also prevent people who want to use this information to their own advantage. We recommend the security model using a distributed ledger book (Ledger)based on BlockChain for IoT. We also used the notation-based general ledger concept from Bitcoin. However, in our system, the symbols, instead of having monetary value, decide to distribute voting power between nodes and individual exchanges to prevent cross-service (DoS attacks in

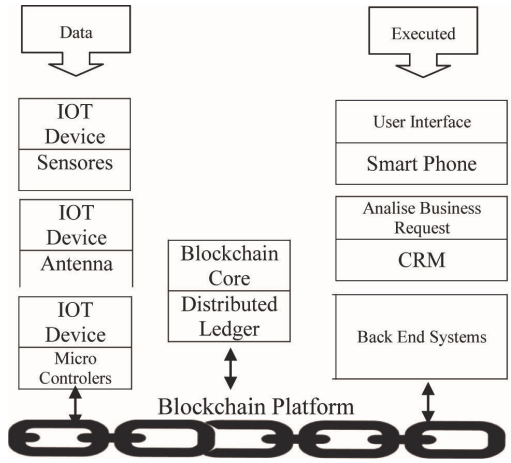

Fig. 2: Example modified by BlockChain

transmitting the information. The transaction is also included in every form of financial transaction or any communication between devices.

Table 3: Five- Layer Architecture of IoT and BlockChain

Layer No.	Layer Name	Usage and Duty
5	Application	The software beds required for the application of information
4	BC- Application	IoT Security Construct
3	BC Protocol	Consensus, Mining
2	Cloud Computing (service-oriented)	Service-based processing processes to fully cover the Active equipment
1	Network of Things	Includes smart devices or activators

4. The Proposed Model

We propose a Five-Layer Model Based on BlockChain Smart Contracts for providing security in IoT. This section will explain how the IoT security improvement process can be improved by the BlockChain protocol layer and the BlockChain application layer after describing the proposed model. Essentially a three-layer architecture for IoT security was proposed by Yash Gupta. This paper improves the mentioned architecture with two extra layers. The proposed layers have appeared in layers 3 and 4. The proposed method consists of the following five phases.

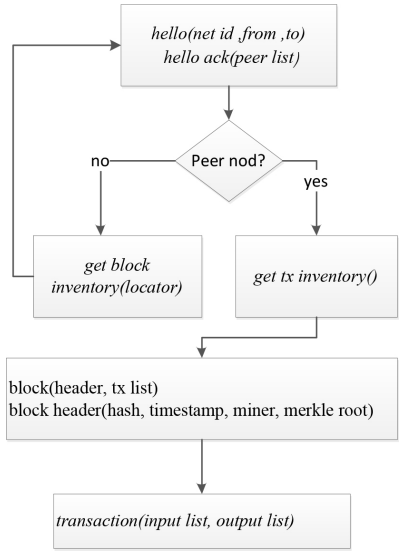

Fig. 3: Flowchart of BlockChain Protocol Layer

• Phase I: By removing the IoT gateway, we actively create a Peer to Peer linkage between devices (Fig. 2).

• Phase II: By providing the scattered general ledger (Ledger), for setting smart contracts in a decentralized manner, we provide an unchanging structure to record information.

• Phase III: Insert BlockChain Protocol Layer and BlockChain Application Layer to the IoT layer 3-layer models (Table 3).

• Phase IV: In the BC-Protocol, we propose a consensus algorithm for establishing data transmission among the nodes in the network. That is, the decision to use the BlockChain Platform. This layer covers a consensus algorithm for accepting or rejecting the transaction between the nodes in the network. We define a set of messages in this layer to assist in achieving a shared view of BlockChain among all participating nodes (Fig. 3). The BlockChain protocol layer encompasses the consensus algorithm for nodes in the network. We define certain categories of messages in this layer to help achieve a common view of the BlockChain among all participating nodes.

Now, we explain the details of the Flowchart of BlockChain Protocol Layer, which was demonstrated in Fig 3.

hello (net id, from, to), hello ack(peer list): Allows the nodes to discover peers.

get block inventory(locator)-Request for the inventory of blocks available with a node's peers, with "locator" summarizing its own block inventory.

get tx inventory(): Request for transactions in the mempool (i.e., not yet mined into a block)

block (header, tx list), block header(hash, timestamp, miner, merkle root)

transaction (input list, output list): Transactions have a list of inputs which it is spending and a list of outputs which it creates. Certain categories of transactions may be allowed without any input to create or "mine" new tokens.

To ensure that all IOT nodes have a uniform view of the BlockChain, we define the rules that the BlockChain protocol layer follows to achieve consensus. A summary of these rules is as follows.

On receiving a transaction, each node stores it in its memory pool and broadcasts it further.

Once every clock tick, a node tries to mine a new block based on its mining token balance b, difficulty d, timestamp t, new block's merkle root m, and mining condition:

$$hash(prevblk|m|t) \leq elapsedtime * b/d \qquad (4.1)$$

Upon generating a new block, the node updates its view of the BlockChain and broadcasts it to its peers.

The difficulty value for the next block is updated such that the average expected time for finding the next block (taken over some fixed number of last blocks) is equal to a set value.

Upon receiving a new block, the node verifies that the block satisfies all protocol rules and that all transactions in the block follow the protocol and application rules.

After verifying a received block, the node updates its view of the BlockChain, clears included transactions from the mempool, and broadcasts the block further.

- Eventually, all nodes have a uniform view of the BlockChain (Nakamoto, S., 2008).

Phase V: In the BC-Application layer, we establish special security exchanges in IoT and define how each transaction is made for higher layers. Trust is a full risk assessment of the risk between different groups. In the digital world, it is often necessary to establish trust in the authentication and to obtain permits. In short, we want to ensure that you are the person you say? And, " Are you capable of doing what you promised? In technology, the encrypted private key provides a powerful ownership tool that meets the requirements for authentication. Having a private key means ownership. However, authentication is insufficient, having a license, having sufficient credit for transactions,etc. need to trust, and to do so requires a distributed network such as such a distributed network that prevents corruption. The security of the distributed network must be guaranteed. Authentication is the result of the implementation of protocol rules by all networks. BC-Application Layer provides special security exchanges on the Internet and defines how they transaction for higher layers. The main function that is provided by our proposed user model is authentication for machines in IoT networks. We define a node in the IoT network by the tuple (id, Kpu, Kpr, Пnonce, firmware, Kpu), where (Kpu,Kpr) is the public-private key pair for the node, id is a shorter version of the public key; nonce,firmware,Kpu is a proof-of-firmware generated by the node using hardware root of trust (such as Physically Unclonable Functions (PUFs)), to prevent Sybil attacks on the network. Пnonce,firmware,Kpu is a function of the private key, the firmware contents, and a nonce value derived from the Block Chain's latest block. This is to provide dynamic authentication and avoid replay attacks on the network. We define the following transactions for the BlockChain application layer:

join net (id, Kpu, Пnonce, firmware, Kpu), leave net (…): A node can join the BlockChain with a join net transaction. Join net is allowed to have a sister output of pay token, which pays a set number of token to the newly joined node's id. The node uses these newly issued tokens for all further actions which require the node to be joined to the network. leave net indicates that the node has left the network, and must spend all the tokens issued by join net.

begin session(idA,idB,…), end session(…): These transactions are used by a member node to initiate and end authenticated and authorized communication session with another node in the network. Begin session must spend at least 1 token issued by the join net of the session initiating node. This spent token is then either released by a corresponding end session tx or after a set timeout in the number of blocks.

add to group(id, group), remove from group(…): These transactions are used to add a node to a group for access control management.

add rule(group, resource, action), remove rule(): These transactions are used to add/ remove domain-specific access control rules for the IoT node sessions.

pay token(id, amount, type): This transaction is used to pay tokens of a given "type" to node id. New tokens can only be generated along with a join net() transaction.

pay mining token(id, amount, type): Mining tokens are a special token type which grant mining privilege to the nodes which hold them. Mining tokens reduce the difficulty of mining blocks for a node. Only the first block of the BlockChain can generate new mining tokens, which are then transferred to different nodes in subsequent blocks for the decentralization of trust.

5. Discussion And Case Study

Suppose that four hybrid cars are moving along a road and are not able to charge from the source between source and destination, and Cars require charging each other to continue moving. In order to validate the charging values in the machines and the charging transaction, we use the BlockChain model (Bitcoin model). If the transaction is stored behind each other in blocks and all nodes have access to the blocking and approval of the block (Table 4).

Table 4: Explaining a case study

No#	Event
1	Charging of the Car a = 10.
2	Car a gives the Car a number of five units.
3	In the continuation of the Car b it charges the Car c to the 3-unit Car (confirmed and recorded in the third block).
4	Car c to Car d charge 1 unit (confirmed and recorded in the fourth block).
5	Car a to Car d charge 15 units. It is not confirmed because, in the first block, a Car has 10 charging units, so it cannot give more to another node so that it is impossible to insert the item in order considering that all nodes are witnessing every transaction. The block does not appear to be recorded (Fig. 4).

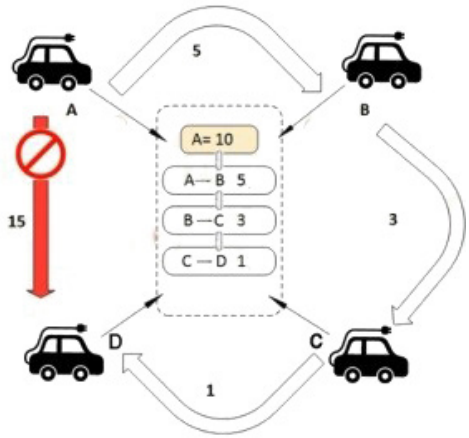

Fig. 4: Case Study image implementation

Given the addition of the recommended layers to the core layers of IoT, which we discussed in Chapter 4, the following assumptions will be made.

• The IoT application layer: Nodes start meetings with the time between exchange and end.

• The BC-Application Layer: Transaction between the internal nodes of the network is established by this authentication layer and ensures packet transmission from the source to the destination.

• The BC-Protocol Layer: the internal nodes of the network are involved in the creation of new blocks, whereas the leaf nodes only confirm the incoming blocks.

• Cloud computing layer: We assume the underlying transportation is a reliable package.

• Network layer: The tree topology is assumed for the network.

6. Conclusion

BlockChain is a relatively unexplored area in the IoT security space, and we show that it is a viable solution to the IoT security problem. The key properties of tamper resistance and decentralized trust allow us to build a secure authentication and authorization service that does not have a single point of failure. It is to be noted that the work in this paper is a preliminary attempt to understand the implementation challenges of BlockChain in an IoT network. At this point, we do not have detailed results on the scalability or the performance of BlockChain in an IoT network. The critical contribution of this work is in the application of BlockChain to provide an authentication and authorization service in IoT networks to:

• Secure the network from remote and local adversaries

• Provide visibility in the form of BlockChain history of active nodes and sessions

• Detect and prevent outlier behavior from certain nodes

Further, we validate the stability and performance of our proposed model using simulations. We also show that our model's stability or performance does not degrade significantly on a lossy wireless network. IoT has a wide range of attacks and vulnerabilities. IoT can cover more attacks and cover specific IoT applications. The proposed model can also be modified to operate on the low-energy Bluetooth link (Bluetooth), unreliable transport layer protocols such as UDP, and optimized to meet the real-time system's performance requirements.

References

Androulaki, E., Barger, A., Bortnikov, V., Cachin, et al. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conf*erence (pp. 1-15).

Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies.* " O'Reilly Media, Inc."

Asadpour, F., & Ghanbari, S. (2018, February). Presenting a New Method of Au-

thentication for the Internet of Things Based on RFID. In *International Conference on Soft Computing and Data Mining* (pp. 506-516). Springer, Cham.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Everisnext (2016). Block Chain disruptive use cases. Retrieved from: https://everisnext.com/2016/05/31/Block Chain -disruptive-use-ases

Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016). Bitcoin-ng: A scalable blockchain protocol. In *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)* (pp. 45-59).

Gartner (2016). Report on IOT security spending, Gartner Newsroom.

Ghanbari, A. M., Ghanbari, S., & Norouzi, Y. (2017, November). A new approach to architecture of human-computer interaction. In *2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)* (pp. 1-4). IEEE.

Gia, T. N., Rahmani, A. M., Westerlund, T., Liljeberg, P., & Tenhunen, H. (2015, April). Fault tolerant and scalable IoT-based architecture for health monitoring. In *2015 IEEE Sensors Applications Symposium (SAS)* (pp. 1-6). IEEE.

Gokhale, P., Bhat, O., & Bhat, S. (2018). Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology, 5*(1), 41-44.

Gupta, Y., Shorey, R., Kulkarni, D., & Tew, J. (2018, January). The applicability of blockchain in the Internet of Things. In *2018 10th International Conference on Communication Systems & Networks (COMSNETS)* (pp. 561-564). IEEE.

Hallman, R., Bryan, J., Palavicini, G., Divita, J., & Romero-Mariona, J. (2017). IoDDoS-the internet of distributed denial of sevice attacks. In *2nd international conference on internet of things, big data and security. SCITEPRESS* (pp. 47-58).

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586-602.

Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Retrieved from: https://bitcoin.org/bitcoin.pdf, 2008.

Nakamoto, S. (2019). *Bitcoin: A peer-to-peer electronic cash system.* Manubot. Retrieved from: https://bitcoin.org/bitcoin.pdf.

Vahid Rad (2018). Ten Great Blessing of Blockcain Technology. Retrieved from: https://arzjoo.com/blogs/847/.

Submitted 10.03.2020
Accepted 12.05.2020