The Research of Blockchain Technology for Data Protection in IoT Devices

Mikhail G. Gorodnichev[1], Stanislav S. Makhrov [2], Elena N. Denisova[3]
[1,3]IT Department, [2] Department of Scientific Research
Moscow Technical University of Communications and Informatics
Moscow, Russia
[1]gorodnichev89@yandex.ru, [2]slavam4@yandex.ru,
[3]dummy.newmailbox@gmail.com

Ilya D. Buldin
Department of Economic Sciences
Higher School of Economics
Moscow, Russia
idbuldin@gmail.com

***Abstract*. The article presents a study aimed at determining an effective security model based on blockchain technology for IoT devices. It is completed a modification of the key features of the classical blockchain used for cryptocurrencies for adaptation to work in the network from the devices of the Internet of things, which requires minimal reaction time to the execution of control commands and knew the redemption of energy resources.**

***Key words:* blockchain, very careful registry, Internet of Things, data protection, information security.**

I. INTRODUCTION

The Internet of Things (IoT) represents one of the most significant disruptive technologies of this century. It is a natural evolution of the Internet (of computers) to embedded and cyberphysical systems, “things” that, while not obviously computers themselves, nevertheless have computers inside them. With a network of cheap sensors and interconnected things, information collection on our world and environment can be achieved at a much higher granularity [1].

IoT consists of devices that generate, process, and exchange vast amounts of security and safety-critical data as well as privacy-sensitive information, and hence are appealing targets of various cyber-attacks. Many new networkable devices, which constitute the IoT, are low energy and lightweight. These devices must devote most of their available energy and computation to executing core application functionality, making the task of affordably supporting security and privacy quite challenging. Traditional security methods tend to be expensive for IoT in terms of energy consumption and processing overhead. Moreover, many of the state-of-the-art security frameworks are highly centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, many-to-one nature of the traffic, and single point of failure [2].

Currently, IoT devices are a significant part of the total number of existing digital devices. According to Marketsandmarkets, by 2018, the global market of the Internet of things is about $200–250 billion. Expected that by 2022 it will reach $561.04 billion. Thus, the volume of the market of the Internet of things is constantly growing and an increasing number of digital devices belongs to the segment [3].

The privacy risks of IoT are exacerbated by the lack of fundamental security safeguards in many of the first generation IoT products on the market. Numerous security vulnerabilities have been identified in connected devices ranging from smart locks to vehicles [1]. IoT devices require protection of data from such basic types of vulnerabilities such as: data corruption, substitution of devices, hacking devices.

IoT is experiencing exponential growth in research and industry, but it still suffers from privacy and security vulnerabilities. Conventional security and privacy approaches tend to be inapplicable for IoT, mainly due to its decentralized topology and the resource-constraints of the majority of its devices [1].

One of the most promising modern methods of data protection today is the blockchain technology, which allows to control all transactions to perform authorization through the public key infrastructure.

Blockchain, a distributed append-only public ledger technology, was initially intended for the cryptocurrencies, e.g., Bitcoin. In 2008, Satoshi Nakamato introduced the concept of blockchain that has attracted much attention over the past years as an emerging peer-to-peer (P2P) technology for distributed computing and decentralized data sharing. Due to the adoption of cryptography technology and without a centralized control actor or a centralized data storage, the blockchain can avoid the attacks that want to take control over the system.

Combined with the blockchain technology, IoT systems benefit from the lower operational cost, decentralized resource management, robustness against threats and attacks, and so on. Therefore, the convergence of IoT and blockchain technology aims to overcome the significant challenges of realizing the IoT platform in the near future [4].

The study of the technology of the blockchain to determine an effective model of protection devices for the IoT is relevant and priority area of research.

II. PROBLEM DEFINITION

Existing methods for securing IoT devices are not always effective for protecting against the following types of threats:

- data corruption;
- device spoofing;
- breaking.

Protection against these types of threats can be provided by means of blockchain technology, which provides:

- audit logging of transactions;
- data encryption;
- public key authentication;
- execution and control over the execution of smart contracts.

Thus, the distortion of data substitution devices and hacking would be impossible in view of the specifics of the blockchain technology mentioned above. At the same time, the classic blockchain [5] is adapted for financial transactions and remuneration of miners for solving cryptographic problems. At the same time, the solution of problems is very resource-intensive to both computing resources and temporary resources. In turn, for IoT devices, these resources are critical because devices are typically Autonomous and must respond instantly to commands with minimal waiting [1].

The purpose of this study is to determine an effective protection model based on blockchain technology for IoT devices.

III. THEORY

A. Algorithm of consensus

The technology of the blockchain is concluded the algorithm of consensus. A consensus algorithm is required to select a node whose recent transaction data (represented as the last block of transactions) will accept all other nodes and add them to its block chain. This algorithm allows you to prevent the possibility of conflicting transactions in the network by multiple nodes by selecting only one node, the transaction block of which will be considered relevant and correct. The classic blockchain [5] solves the problem of double spending of funds from one wallet.

After the consensus algorithm is executed, all nodes in the network will update their block chain to match what they receive from the node that was selected by the consensus algorithm. At the same time, when updating the block chain, the receiving nodes check the correctness of the consensus algorithm. If the consensus algorithm can take a long time to execute, the check is instantaneous.

The classical blockchain [5; 6] uses the proof-of-work algorithm as a consensus algorithm (Proof of Work, PoW). The essence of the algorithm is that the miner node should be the first in relation to all other nodes to solve some mathematical problem. As a mathematical problem can be calculated from an arbitrary number of such a hash, which at the end will be 5 zeros. The solution of such a problem takes a lot of time and computing resources.

Other variants of the consensus algorithm are also known, in particular [6]:

- Proof of Activity (PoA);
- Proof of Stake (PoS);
- Proof of Capacity (PoC);
- Proof of Importance;
- Proof of Authority (PoAuthority).

Each of these, as well as other consensus algorithms, are mainly focused on operations with monetary transactions [6] and are not suitable for adaptation to work in the network from IoT devices.

To enable the use of blockchain technology in IoT devices, it is proposed to use such a proof-of-work algorithm to determine the node with the correct and relevant data instantly. In view of the absence of the need to reward miners for their work, and accordingly, the need to perform this work by the miners themselves, the consensus algorithm can be determined by the simplest generation of a random number:

$$proof = random\left(list, H_{PREV\_BLOCK}\right) \quad (1)$$

According to the formula (1), the value of the proof consensus algorithm is calculated as a random number from the $list = \{miner_1, \ldots, miner_z\}$ miners list and the calculated hash value from the previous H_{PREV_BLOCK}. A random number will be in the list of miner node numbers range of the *list.* Therefore, without spending a lot of time and computing resources, the node whose transaction block will be accepted as correct and up-to-date will be determined. Introduction in the formula (1) of the consensus algorithm hash of the previous block H_{PREV_BLOCK} will allow the nodes to upgrade chain to see if it made a substitution blocks node miner.

B. Blockchain block contents

The result of the consensus algorithm cannot be faked because the hash value of the previous block is involved in calculating the hash of each new block:

$$H_{BLOCK} = SHA256\begin{pmatrix} index + H_{PREV\_BLOCK} + \\ H_{MPROG} + timestamp \\ + proof + \sum_{k=1}^{p} transaction_k \end{pmatrix} \quad (2)$$

According to the formula (2) hash each transaction block is calculated as the hash-function *SHA256* of the following arguments: index block *index*, *hash* H_{PREV_BLOCK} from the previous block, hash H_{MPROG} code from the firmware executable on the node, timestamp of creation timestamp of the block, the result of the consensus algorithm proof and the amount of the transaction.

Introduction in the formula (2) H_{MPROG} hash code of the firmware is another difference from the classical blockchain [5] and allows to protect the network nodes of the Internet of things from breaking by controlling the integrity of the firmware. If the

firmware hashes are different, this will signal that the node is not trusted and communication with it should be terminated.

C. Data transmission and addressing of nodes

Data transfer and addressing of IoT nodes can be done through the public key infrastructure. Two keys are created – *PrivateKey* and *PublicKey*, which are used for different purposes..

The *PrivateKey* is used for the following tasks:

- creating a *PublicKey*;
- the digital signature of transactions;
- decryption of received data.

The *PublicKey* is used for the following tasks:

- addressing nodes by the *PublicKey*;
- for generating the host address: a *PublicKey* hash is generated by hash function SHA256. The resulting hash value is then hashed again using the RIPEMD160 function. The final hash of RIPEMD160 is Base64 encoded;
- validation of the digital signature of the received transaction;
- encryption of transmitted data.

D. Registration and transfer of data between network nodes

Let we have a node $node_T$, that is required to register in a network consisting of n standard $node_{1,\dots,}node_n$ and z miner nodes $miner_{1,\dots,}miner_z$. While $n>z$. Node $node_T$ generated 2 key $PrivateKey[node_T]$ and $PublicKey[node_T]$. The last key (public) is sent to all nodes of the $node_{1,\dots,}node_n$ and $miner_{1,\dots,}miner_z$, which by means of this key will be able to verify the authenticity of the digital signature of transactions received from the $node_T$, and will also be able to transmit data to the $node_T$. node in encrypted form. Digital signature of transaction by far identified the sender. In response to the public key received from $node_T$ the nodes send them their public keys $PublicKey[node_1],\dots,PublicKey[node_n]$, $PublicKey[miner_1],\dots,PublicKey[miner_z]$ to perform similar functions.

If you want to control the issuance of digital signature certificates, this function can be assigned to the miner nodes $miner_{1,\dots,}miner_z$.

IV. Experimental Prototype And Results

The model described in the theoretical part is implemented in practice in the Python programming language on the hardware basis of the IoT module Onion Omega2+ [7] (Fig. 1).

Fig. 1. IoT module Onion Omega2+

The Onion Omega2+ module has the following features:

- processor: MIPS32, 580 MHz;
- memory: 128 MB;
- flash memory: 32 MB;
- USB: one 2.0 port;
- SD-slot for 1 MicroSD card;
- support WiFi: b/g/n;
- number of GPIO: 15;
- support PWM, UART, I2C, SPI, I2S.

As part of the experiment, the code of the blockchain model was recorded on 7 devices, each device was a miner at the same time. The following types of attacks on the network from IoT devices were used:

- node substitution;
- listen to traffic;
- change the firmware code to create a backdoor in it;
- units change the chain on the nodes.

As a result of implementation of all listed attacks, the network revealed each attempt of influence and successfully resolved all conflict situations.

V. Conclusion

The developed model of data protection and its practical implementation using IoT-modules Onion Omega2+, showed that through the blockchain technology, Internet of things devices can be protected from the following vulnerabilities:

- Control over the distortion of information, hacking devices is provided by storing transactions on all nodes (transaction audit) and checking them by Consensus algorithm, for distortion of the previous information and the introduction of malicious code in the original firmware code.
- Protection against spoofing and introduction of phantom devices into the network is provided by applying a digital signature for each transaction received from the node.
- Data privacy is guaranteed by encrypting traffic according to the public key infrastructure. The information is protected and available only to the parties involved in a particular transaction.

The model provides the ability to authenticate users through a decentralized or centralized public key infrastructure. Also, through this model can be implemented proof of warranty, if the blockchain network nodes will be entered data on the manufacturer of electronic components.

The disadvantages of the model include the inability to update the software, because when you add a new block to the blockchain, the hash from the H_{MPROG} firmware is compared with its value in the previous blocks of the blockchain.

VI. REFERENCES

[1] Dorri A., Kanhere S.S., Jurdak R. Blockchain in internet of things: Challenges and Solutions. URL: https://arxiv.org/abs/1608.05187.

[2] Dorri A., Kanhere S. S., Jurdak R. et al. Blockchain for IoT security and privacy: The case study of a smart home // 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). Kona, 2017. P. 618-623. doi: 10.1109/PERCOMW.2017.7917634.

[3] Marketsandmarkets.com: Internet of Things (IoT) Market by Software Solution (Real-Time Streaming Analytics, Security Solution, Data Management, Remote Monitoring, and Network Bandwidth Management), Service, Platform, Application Area, and Region - Global Forecast to 2022. URL: https://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html.

[4] Ferrag M.A., Derdour M., Mukherjee M. et al. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. URL: https://arxiv.org/abs/1806.09099.

[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf.

[6] Nguyen T., Kim K. A survey about consensus algorithms used in Blockchain // Journal of Information Processing Systems. 2018. Vol. 14. P. 101–128. 10.3745/JIPS.01.0024.

[7] Omega 2 - The Invention Platform for the Internet of Things. URL: https://onion.io/omega2/.