# On Application of Distributed Ledgers for Internet of Things in Russia

Konstantin Mironov [1,2]
[1] *Ural Federal University*
Ekaterinburg, Russia
[2] *Ufa State Aviation Technical University*
Ufa, Russia
mironovconst@gmail.com

Sergey Trishin
*Ufa State Aviation Technical University*
Ufa, Russia
igres28@gmail.com

Amir Makhmutov
*Ufa State Aviation Technical University*
Ufa, Russia
makhmutovamir15@gmail.com

Vadim Kartak
*Ufa State Aviation Technical University*
Ufa, Russia
kvmail@mail.ru

Thilo Sauter
*Institute of Computer Technology*
*Technische Universität Wien*
Vienna, Austria
Thilo.sauter@tuwien.ac.at

***Abstract* — In this article we consider tasks related to ensuring the integrity and availability of information in the Internet of Things (IoT) sphere. Such systems include sensors and similar devices, which are the sources of data, access points, which transmit data from sensors to the Internet and servers, which store received data and grant access to users. When storing data on a server and providing access to it, it is necessary to ensure its integrity and availability to users. To this end, it is proposed to apply a distributed ledger technology (DLT). One of the applications of DLT for data protection is energetics. Here we consider a system for processing and storing data on the production and consumption of electricity in a decentralized power grid. A review of currently existing projects related to the use of distributed ledger technologies in the energy sector is carried out. An important obstacle to the use of DLT in the IoT is the contradiction between, on the one hand, high memory computational requirements of the DLT, and, on the other hand, limited resources of IoT nodes. Further research directions are proposed that are associated with overcoming this obstacle in applying distributed ledger technologies in the energetics.**

***Keywords— Distributed ledger technology, energy systems, lightweight cryptography, internet of things.***

## I. Introduction

Distributed ledger technology (DLT), particularly the blockchain are attracting more and more attention around the world, including Russia. Distributed ledger systems are included in the list of nine major cross-cutting digital technologies of the “Digital Economy of the Russian Federation” program [1]. Since the emergence of the Bitcoin system in 2008–2009, most blockchain projects have been developed by enthusiasts and business structures. At the same time, very little fundamental research is being conducted to assess the applicability of this technology for various tasks, to explore advantages and issues that may arise during the implementation and operation of distributed ledger systems. Therefore the significant part of the referred sources are not scientific articles but supporting documentation of initiative projects (so-called white papers).

This article focuses on the use of the DLT to ensure the integrity of data in an information system using the Internet of Things (IoT) technology. As an example of a protected information system, a system for processing and storing data on the production and consumption of electricity in a decentralized power grid is considered. The aim of our research project is to build a system for protecting information that received from smart electricity meters using DLT. As known, there are 3 main aspects of information security: confidentiality, integrity and availability of information. Here we pay our attention to the last two aspects.

In case of distributed production of electricity using the Smart Grid technology, many consumers and producers of electricity can be connected to a single power supply network (with a centralized production, there is only one manufacturer). Accounting for the production and consumption of energy is carried out using smart meters. Processing data from multiple meters allows determining how much specific consumers should pay for electricity and how this amount should be distributed among producers. Distributed platforms for interaction between producers and consumers of electricity are actively developing in the USA and EU [2]. In Russia, this trend is less relevant because there is a limited number of producers which are engaged in the production of electricity and have little interest in a decentralized system. The regulatory framework for such decisions is only being formed; the basis for this is the Federal Law No. 261 “On Energy Saving and Improving Energy Efficiency” [3]. However, for consumers in remote areas in which the supply of electricity is associated with unreasonably high costs or is impossible, the proposed concept of building distributed energy generation systems is relevant. Examples of such areas are remote settlements of Siberia, the Far East and the North of Russia. As part of our work, it is supposed to enter information on the production and consumption of electricity recorded by smart meters into a distributed ledger.

The use of distributed ledger technology allows the exchange of information in the absence of trust between the producer and the consumer and without organizing an additional interaction environment. The analysis of existing projects based on the use of distributed ledger technology in the energy sector is given in the second part of this article. The third section provides the rationale for the existing technical limitations.

## II. Distributed ledger systems

Historically, the first form of a distributed ledger is the blockchain. Blockchain as a structure for data storage is characterized by the following features:

1. Stored data is a set of records, each of which is signed by the electronic signature of the author.

2. The set of records consists of subsets - blocks arranged chronologically, with each next block containing a cryptographic hash function of the previous one.

3. Multiple nodes store synchronized copies of the blockchain. This condition is not mandatory, if it is not met, the data structure is called "centralized blockchain." However, a centralized blockchain, strictly speaking, is not a distributed ledger.

This structure allows ensuring the integrity of information: to change a block, one need to change all subsequent blocks in the chain, since the hash function of each block depends on the hash function of the previous block. Thus, to replace a block, it will be necessary to collude with all users who sent their records to the blockchain after this block, since the hash functions of each record are signed by the sender. Since the blockchain is a distributed structure, well-meaning nodes will refuse to acknowledge changes. To make such changes, an attacker would need to gain control over more than half of all network nodes.

An alternative way to build a distributed ledger is the concept of DAG (Directed acyclic graph). In this concept, the nodes of the graph are blocks, and the directed arcs are their hash functions. The main difference from the blockchain is that in the blockchain each block refers strictly to the previous one, and in the DAG each block can refer to random ledger blocks. When writing a new block, its author looks at the list of those ledger blocks whose hash functions are not contained in any other block. Then he chooses several (usually 2) blocks and adds their hash functions to his block.

We consider that the definition of such a form of a distributed ledger by the term “directed acyclic graph” is redundant and inconvenient. On the one hand, it is not possible to build a distributed ledger on a graph with cycles, or on a undirected graph (arcs of a graph in a distributed ledger indicate the previous record is signed by the previous record and therefore directed from the subsequent to the previous one), on the other hand, directed acyclic graphs are used not only in the DLT. Therefore, we use the terms “chain ledger” and “graph ledger” instead of blockchain and DAG, respectively. From our point of view, they are fairly brief and intuitive.

In comparison with chain ledger, graph ledger has less stringent requirements for network synchronization. If two nodes at different ends of the network simultaneously generate a new block, in chain ledger this will lead to a conflict between the two versions of the chain ledger (the one that more users will accept first is selected correctly). When using graph ledger, both blocks will be successfully written to the ledger. For this reason, the graph ledger concept seems to be preferable for the Internet of Things, in which the bandwidth of the communication channels is limited, which means that there can be significant delays in data transmission between nodes. There is a cryptocurrency named as iota [4] which is based on graph ledger technology and positioned as a cryptocurrency for the Internet of Things.

Nevertheless, all known to us projects of building DLT in the energy industry use chain ledger technology. Next we look at them in more detail.

The authors of [5] identify 9 main areas of use of the chain ledger in the energy:

1. Distributed trading

2. Charging stations for electric vehicles

3. Remuneration for the production of renewable energy

4. Differential payments

5. Payment for electricity with cryptocurrency

6. Energy wholesales

7. Network load stabilization

8. Ecology assets trading

9. Data Exchange Platforms

Directions 1 and 9 are the most interesting for our project. The purpose of creating distributed marketplaces is to form a decentralized system through which small producers, such as owners of solar panels or wind turbines, will be able to sell electricity to nearby consumers directly, without attracting large energy suppliers, and consumers in turn are able to choose a supplier and buy energy at the most economical tariff. As a rule, platforms are created within a quarter or district, for example, projects of Brooklyn Microgrid and Allgau Microgrid of LO3 Energy [6] use a distributed trading platform for residents of small communities. Many companies create their own smart meters that record energy consumption and interact with the chain ledger for transactions. For example, the meter developed by Grid+ [7] combines the chain ledger and machine learning technologies, it is able to effectively plan electricity consumption, buy and sell at its best price. Other similar projects: PowerLedger [8], Greeneum [9], Wepower [10], Electrify.Asia [11].

Developing platforms for sharing data about used energy use the chain ledger to create mechanisms by which manufacturers, regulators, utilities and consumers can interact with each other and transmit information about electricity. Such platforms are being created as part of the Energy Web Foundation [12] projects, the GridSingularity platform, Clearwatts [2], ElectriCChain [13]. in Russia Qiwi, in cooperation with Tavrida Electric, planned to use chain ledger to store data on energy supply contracts [14], but at the moment there is no new information about the development of the project.

Table 1 presents basic information about the most famous projects. As can be seen, Ethereum is the most popular platform, more than 40% [2] of projects use it. Thanks to the smart contract mechanism and the Ethereum virtual machine, it becomes possible to create various distributed applications and use the chain ledger in different areas. However, the public type of chain ledger and mining, built on the “proof of work” limit its use.

Tobalaba [12] is a chain ledger platform created by the Energy Web Foundation. It is a private chain ledger with permissions of various levels (Private Permissioned chain ledger) based on Ethereum and intended for use by companies in the energy sector. HyperledgerFabric [16] implements distributed ledger technology to create a platform for closed chain ledger managed by LinuxFoundation organizations. The platform uses smart contracts called Chaincode. Tendermint [17] is a protocol consisting of two main components: a mechanism for achieving consensus and a universal application interface. The rights to create a new block is assigned in a pseudo-random manner, and the block is added by multi-step voting.. BigchainDB [18] is a platform that combines chain ledger properties (decentralization, immutability, controlled assets) and database capabilities (high transaction processing, low latency, the ability to index and query structured data). BigchainDB was introduced in 2016, and in 2018 it was updated to version 2.0. The new version uses the Tendermint protocol, which solves the problem of the Byzantine generals and accelerates the network.

## III. Issues and Proposals

The main restrictions on the use of the IoT devices as nodes of a distributed ledger are associated with the memory costs of storing the ledger and the cost of computational resources for calculating hash functions and setting electronic signatures. In the existing works and projects on the application of a distributed ledger in the energy sector, issues of these restrictions are poorly considered. Projects either require the use of more expensive smart meters with high computing resources or did not work with smart meters at this stage of development. For example, within the framework of the LO3 Energy project that came to practical implementation [6], data for meter is entering manually by consumers, which nullifies the main advantage of the chain ledger - the lack of trust between participants in the system; most other projects have not come to practical use at all.

Depending on the computational capabilities of the smart meters, we propose 3 options for their interaction with the ledger:

1. Meters do not have neither memory nor computational power to work with the ledger, therefore, trusted nodes with sufficient resources work with the ledger on behalf of the meters. It is assumed that meters and trust nodes completely trust each other and exchange information via communication channels protected by means of lightweight cryptography.

2. Meters calculate hash functions and put their digital signatures on ledger records, but do not store a copy of the entire ledger.

3. Meters are full-fledged ledger nodes: they keep a copy of the ledger in their memory, calculate and validate hash functions and digital signatures.

TABLE I. BASIC INFORMATION ABOUT THE MOST FAMOUS PROJECTS

| **Project name** | ***Area of use*** | ***Type of chain ledger*** | ***Hash function and electronic signature algorithm*** |
|---|---|---|---|
| LO3 Energy<br>(Brooklyn Microgrid) [6] | Distributed trading | Ethereum | Keccak-256<br>ECDSA |
| Grid+ [7] | Distributed trading | Ethereum | Keccak-256<br>ECDSA |
| PowerLedger [8] | Distributed trading | Ethereum | Keccak-256<br>ECDSA |
| Greeneum [9] | Distributed trading | Ethereum/<br>Hyperledger/<br>Tendermint | Keccak-256 / SHA-256<br>ECDSA |
| Wepower [10] | Distributed trading | Ethereum | Keccak-256<br>ECDSA |
| Electrify.Asia [11] | Distributed trading | Ethereum | Keccak-256<br>ECDSA |
| Energy Web Foundation [12] | Data Exchange Platforms | Tobalaba | Keccak-256<br>ECDSA |
| Clearwatts [2] | Data Exchange Platforms | BigchainDB | Keccak-256<br>ECDSA |
| Enerchain [15] | Energy wholesales | Tendermint | SHA-256 |

The third option is hard to implement on most available devices: the built-in memory of controllers is not enough to store all ledger entries if it will be used by a large system for a long period of time: for example, the size of Ethereum's open chain ledger exceeded 176 GB [19]. This version might be implemented with the use of a Raspberry Pi alike microcomputer smart meter with the ability to use external memory cards. However, this option will increase the cost of the end device several times; at the same time, the physical dimensions of the meters and their own energy consumption will significantly increase.

The second option contains a significant complexity, which is the high requirements for computing power when self-calculating a smart counter digital signatures. It is possible to compute signatures on the meters themselves, however, this will significantly increase their cost, since the need to replace hardware with more powerful ones.

Signing the record consists of two operations - the calculation of the hash function of the record and the calculation of the digital signature based on this hash function. Both operations are quite resource-intensive: the hardware implementation of the SHA-256 hash function [20, 21] takes about 10,000 logical elements, as well as the hardware implementation of elliptic curve cryptography with a key length equivalent to a 113-bit key with symmetric encryption (while calculating the signature in such a compact implementation will take considerable time [22]). Alternative Keccak hash is fast on 64-bit systems (12.5 cycles per byte on systems with Intel Core 2 Duo) [23], however, the computational capabilities of controllers in smart meters are much lower. The Scrypt function is based on SHA-256, however, it is much more demanding in terms of resources and RAM including [24] to complicate the selection of the hash function by brute force, and therefore, the use of SHA-256 itself is the most justified. At the same time using the system in Russia in accordance with legal regulations, it is necessary to build a system based on the Stribog hash function and digital signature GOST R 34.10-2012.

## IV. Conclusion

DLT can be used in distributed power engineering to ensure the integrity and availability of information on smart energy meter readings. A review of sources on the application of distributed ledger technologies in the power industry showed that, although graph ledger technology is more convenient for building a ledger, existing projects use chain ledger technology. At the same time, the Ethereum chain ledger is usually used. Most of the projects have not reached the stage of wide practical application, and those that have reached often impose excessive demands on the power and cost of equipment. In this regard, the development of technology that does not impose high requirements on the computing power and memory counters seems to be relevant. Further development of the system can be carried out in the following ways:

1. Development of technology for secure transmission of data from the counter to a trusted node, which writes the records to the ledger. Data protection is based on the use of low-resource cryptography.

2. Development of a meter model, the resources of which are sufficient for calculating the electronic signature on the measurement results

3. Development of a distributed ledger model for storing meter readings based on graph ledger technology.

## Acknowledgment

The research is supported by RFBR grants #19-07-00972 and #17-07-00351. Research work of Konstantin Mironov is supported by the Russian President scholarship for young scientists and doctoral students #SP-1484.2019.5.

## References

[1] Program “Digital Economy of the Russian Federation” accepted by the decision of the Government of Russian Federation of 28.07.2017 #632-r

[2] Montemayor, L., Boersma, T. and van Dorp, T. (2018). Comprehensive Guide to Companies involved in Blockchain & Energy. Solarplaza. Date Views 29.01.2019 https://ipci.io/wp-content/uploads/2017/12/Energy-Blockchain-Report.compressed.pdf

[3] Federal Law “On energy saving and energy efficiency improvements and on amendments to certain Legislative Acts of Russian Federation” of 23.11.2009 #261-FL

[4] IOTA (MIOTA) - Whitepaper Date Views 29.01.2019 https://ipci.io/wp-content/uploads/2017/12/Energy-Blockchain-Report.compressed.pdf https://whitepaperdatabase.com/iota-miota-whitepaper/

[5] Edeland C., Mörk T., 2018. Blockchain Technology in the Energy Transition: An Exploratory Study on How Electric Utilities Can Approach Blockchain Technology. Date Views 29.01.2019 https://kth.diva-portal.org/smash/get/diva2:1235832/FULLTEXT01.pdf

[6] Exergy electric power technical whitepaper. Date Views 29.01.2019 https://exergy.energy/wp-content/uploads/2017/12/Exergy-Whitepaper-v8.pdf

[7] Grid+ White paper. Date Views 29.01.2019 https://gridplus.io/assets/Gridwhitepaper.pdf

[8] PowerLedger Whitepaper.Date Views 29.01.2019 https://cdn2.hubspot.net/hubfs/4519667/Documents%20/Power%20Ledger%20Whitepaper.pdf

[9] Greeneum Whitepaper. Date Views 29.01.2019 https://www.greeneum.net/whitepaper

[10] Wepower White Paper. Date Views 29.01.2019 https://icorating.com/upload/whitepaper/CDt62AS6IjlVUY8CNdHk0aYJycsT7ez8Yp5HgKod.pdf

[11] Electrify ICO Whitepaper. Date Views 29.01.2019 https://electrify.asia/whitepaper/

[12] The Energy Web Chain: AcceleratingtheEnergyTransitionwithanOpen-Source, Decentralized Blockchain Platform. Date Views 30.01.2019 https://energyweb.org/wp-content/uploads/2018/10/EWF-Paper-TheEnergyWebChain-v1-201810-FINAL.pdf

[13] SolarCoin A blockchain-based solar energy incentive. Date Views 30.01.2019 https://solarcoin.org/wp-content/uploads/SolarCoin_Policy_Paper_EN-1.pdf

[14] Qiwi is going to implement blockchain into the energy sector of the Crimea.Date Views 31.01.2019 https://forklog.com/qiwi-eyes-annexed-crimea/

[15] Potential of the Blockchain Technology in Energy Trading. Date Views 30.01.2019 https://ponton.de/downloads/mm/Potential-of-the-Blockchain-Technology-in-Energy-Trading_Merz_2016.en.pdf

[16] Androulaki E. et al., 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference. – ACM, 2018. – С. 30.

[17] Tendermint Documentation Date Views 29.01.2019https://media.readthedocs.org/pdf/tendermint/v0.21.0/tendermint.pdf

[18] BigchainDB 2.0 The Blockchain Database May 2018 Paper version 1.0 Date Views 29.01.2019 https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

[19] Ethereum (ETH) prices and statistics Date Views 25.01.2019 https://bitinfocharts.com/ru/ethereum/

[20] M. Feldhofer and C. Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In First International Workshop on Information Security—IS 2006, volume 4277 of Lecture Notes in Computer Science, pages 372–381. Springer-Verlag, 2006

[21] Poschmann A. Lightweight Cryptography - Cryptographic Engineering for a Pervasive World, 2009. Ph.D. Thesis, RuhrUniversityBochum,

[22] Zhukov A. Y. Lightweight cryptography, 2015. Part 2 Voprosy kiberbezopasnosti, 2(10) (in Russian).

[23] Manifavas C., Hatzivasilis G., Fysarakis K., Rantos K. Lightweight Cryptography for Embedded Systems - A Comparative Analysis, SETOP’2013

[24] GuidoBertoni, JoanDaemen, MichaëlPeeters, GillesVanAssche. TheKeccakreference, Version 3.0, January 14, 2011. – С. 1-69.