**Artem Popov, Sergii Stirenko, Heorhii Loutskii.**

# DECENTRALIZED LEDGER TECHNOLOGY MEETS INTERNET OF THINGS. SECURITY AND FAULT-TOLERANCE ENHANCEMENT

This paper focuses on increasing of performance and fault-tolerance of blockchain core and infrastructure that can be reached by design of lightweight protocol for IoT. Literature review has been made regarding to using of DLT in distributed systems design that have enhanced fault-tolerance and performance.

**Key words**: blockchain, IoT, consensus algorithms, distributed applications.

Fig.: 0. Tabl.: 1. Bibl.: 17.

**Introduction.** Security may be one of the greatest barriers for IoT adoption. The widespread use of such systems as Smart Home, Smart City and Smart Fabric has the exponential growth from year to year. However, vendors of IoT devices pay too little attention to security in their solutions. The Open Web Application Security Project (OWASP) made comprehensive survey [1] where the main vulnerabilities of IoT devices are highlighted. In this report, lack of updating mechanism is considered to be a significant threat.

In 2018, a comprehensive analytic paper [2] was performed. In their work, the authors investigated attack surfaces to IoT devices. The security model shows how vulnerable IoT infrastructure is. The authors noticed that security solution should be built as a composite system where each component could enhance security of another.

In this paper we show how DLT brings to IoT a significant security enhancement. Binding of Blockchain with classic approaches to detect and prevent attacks provides fault-tolerance, constantly determining the faults and intrusion system.

**Background.** From the research in blockchain core perspective, there are many studies in cryptography and different blockchain architectures. The novel core part of blockchain – consensus algorithms has dynamic growth of new principles in performance and security.

**Consensus protocols.** Tschorsch and Scheuermann [3] made a comprehensive review of blockchain core, architecture and infrastructure layers of blockchain technology in bitcoin. As Nakamoto's bitcoin is the first applicable realization of blockchain, there is the sense to use his work and reviews as the basic for future research. Despite double spending risks, centric miners (groups) and high cost of computation and transaction fee, bitcoin is considered impossible to hack. Even if a group of fraudsters capture about fifty percent of entire network, it will have a huge cost because of expensive equipment. There is no any income from such types of

attack, and capturing the mining payload for fraud is senseless. Following this research, bitcoin reached resilience, so called *2f + 1* resilience. It means that if the number of honest nodes in network is more than twofold number of malicious nodes, the system is safe. In other words, if fraudsters capture less than one third of the whole computational power, network is resilient.

Some parts of the blockchain core presented in Marko Vukolic's review [4] deserve our attention. Firstly, it is the consensus algorithm named Byzantine Fault Tolerance (BFT) which is based on the famous Byzantine Generals problem [5]. As Proof-of-Work consensus algorithm consumes a lot of energy (miners computing useless crypto-puzzle) and has a low performance (bitcoin provides only 7 transaction per second) and scalability, in [4] various modifications of BFT algorithms are presented. These modifications promise reaching the *O(n)* complexity of such consensus protocols.

In his article, Yin Yang [6] proposed a novel linear BFT algorithm. The author promises complexity of LinBFT as $O(N)$, while Practical BFT has a complexity $O(N^2)$. However, there is need in a leader for every consensus round, so it increases a risk of denial-of-service attack. Consequently, there is still no any applicable realization of this approach.

An alternative version was proposed in the article [7] – CheapBFT. The authors decreased the number of replicas during consensus round. It became possible due to using special hardware, a hidden counter inside processor units. However, using special hardware means that software that should be installed on it should come from the trusted parties. Participants of such blockchain networks should trust the developers of software, but it is contrary to the main principle of public blockchain: no one can be trusted.

In case of using non-public (private) blockchain network, there is a possibility to add trusted nodes. Hence, the performance of system will depend on network throughput, and consensus should be reached almost immediately. It will make possible to use such blockchain systems inside companies, or between companies and government, in the government itself, etc. Due to using the decentralized solution, there is solving the single point of failure issue as it is in server-client systems used nowadays. But the main property of blockchain – immutability of ledger in untrusted environment – will be lost due to its use in private network with access control. It makes sense to consider mixed or hybrid networks and application of mixed consensus algorithms, using special hardware, sharding (dividing the network into clusters for higher performance),

trusted elements, secure elements etc. Tien Tuan Anh Dinh reviewed in [8] a wide range of different consensus protocols and blockchain cores and compared them. Despite the fact that this analysis was made for only cryptocurrencies systems, it could be a good basis for further research in case of hybrid systems.

However, blockchain infrastructure, which is investigated and developed much earlier than the blockchain itself, still has issues with reliability and performance.

**Blockchain infrastructure.** Authors made theoretical and mathematically proved review in [9]. Using of De Bruijn topology provides benefits for peer-to-peer protocols such as significant reducing of routing tables. While the probability of succeed lookups is high in environment with constant node failures probability. There has been proved $O(\log N/\log\log N)$ complexity for lookup steps processing. In addition, De Bruijn topology solved conflicts issue – it is a good mechanism to handle key collisions. Authors presented results for right-shifting, left-shifting and excess-shifting (more than one bit) lookups.

Another study [10] presented overlay network based on De Bruijn graph that has self-stabilization feature. Authors proved $O(\log N)$ complexity for lookup steps processing on such model and constant node degree.

Comparing with [9], comprehensive review of existing models was made by authors in [11]. They proposed network model based on De Bruijn graph with right-shifting lookup and practically proved outperforming of the proposed solution in compare of existed solutions. As a result, a specific software was implemented for simulation and performance measurement.

How to enhance De Bruijn topology, presented in study [12]. Authors proposed to add excess code (*0/1/-1*) to De Bruijn graph and compared solution with hypercube, De Bruijn topology and classic solutions.

**Blockchain-based schemes.** In [13] the authors presented IoT devices authentication, avoiding the late man-of-the-middle attack approach. There are two stages: initialization and functioning. During the initialization stage, device is registering by sending transaction to blockchain that contains the following information: device ID, authentication method, authentication credentials, authentication list (rules for device, e.g. ports from/to, size of information etc.). All information except ID is encrypted. During the functioning stage, the device sends authentication request to gateway. Gateway gets information from blockchain by ID, decrypts it and replies if connection is successful. The

additional case: against later man-of-the-middle attack, the device sends ID and hash with nonce. Gateway gets information from the blockchain, computes hash and compares hashes.

In [14] the authors proposed the autonomous self-learning distributed system for detecting compromised IoT devices. This system provides two major features: the first one is a device-type identification that is based on network communication pattern of IoT device and provides abstract ID without dependency on a device type; the second one is an anomaly detection in traffic that generated by IoT device and autonomously trains model for each of the IoT device network behavior.

The conceptual blockchain-based compromised firmware detection and self-healing approach [15] is another solution that proposes to secure firmware of IoT devices and heal if they were compromised. There is using trusted node, which provide firmware, for validity participate in consensus with other firmware sources and hubs. IoT hub in the proposed scheme is used as storage of firmware for devices, which are connected to hub, and firmware versions for hub itself.

In [16] the authors proposed the concept of continuous firmware audit, also the scheme is presented for initial authentication and continuous authorization devices in IoT network with utilizing an additional hardware write-only module for continuously check firmware integrity. This paper shows how it is hard to make decision about device firmware integrity during the full lifecycle.

**The research objective.** The purpose of the study is to develop the protocol, namely, the improvement of the main characteristics: increasing the fault-tolerance and speed of interaction between nodes, resistance to attacks, reducing the requirements for computing resources, etc. Last research in fast and lightweight consensus protocols motivated us to develop distributed system with metastable consensus[17] protocols as a core.

The first needed distributed application is a firmware update. Secondly, the family of distributed applications that provide micro-payments is more suited for IoT devices. The success criterion is to improve fault-tolerance, performance, security and reduce computing consumptions, which will allow for the widespread use of such distributed systems in practical applications.

As it was considered above, using of excess De Bruijn topology can bring fault-tolerance and performance enhancement to peer-to-peer networks that are, namely, infrastructure of blockchain technology. Investigation of lookup trees for right-shifting, left-shifting and excess-shifting models as well as comparison with existed solutions is the intention of future research.

**Conclusion.** Distinct features of DLT and, in particular, blockchain presented in Table 1 could give security enhancement to IoT networks such as Smart Home, Smart City etc. The presented solution describes only one possible brick in security wall. Applying DLT to other components of IOT networks security could strengthen overall resistance to various attacks and vulnerabilities.

*Table 1*

**Benefits of using DLT**

| Features | Benefits |
|---|---|
| Tamper-proof ledger | No way to spoof data from IoT devices or authentication credentials, hence prepare next step of attack |
| Smart Contracts | Gives a possibility of analytics based on data in ledger, proved by whole network |
| System is distributed | Avoiding single-point-of-failure |
| Immutability of ledger | No way to spoof data in network |
| Scalability | The solution for Smart Home scales to Smart Building and Smart City ecosystem |

As research enhancement, the paper obtained basic research of the possibility to apply excess code solution to existed peer-to-peer protocol based on De Bruijn topology. Next research steps should include implementation of distributed system with proposed solution. Performance tests along with experiments should be provided in environment with different percent of disconnected nodes as well as proposed solution should be tested under different types of attacks to consensus protocol and peer-to-peer network.

## References

1. [www.owasp.org OWASP IoT Top 10 (https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf)

2. [Abdul-Ghani, H. A., Konstantas, D., Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 3.

3. Tschorsch, F., Scheuermann, B. (2015). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. Humboldt University of Berlin.

4. Vukolic, M., (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. IBM Research, Zurich.

5. Lamport, L., Shostak, R., Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS) vol. 4, No.3, 382-401.

6. Yang, Y. (2018) LinBFT: Linear-Communication Byzantine Fault Tolerance for Public Blockchains.

7. Kapitza, R. et al. (2012). CheapBFT: Resource-efficient Byzantine Fault Tolerance. ACM 978-1-4503-1223-3/12/04.

8. Tien Tuan Anh Dinh et al. (2017). Untangling Blockchain: A Data Processing View of Blockchain Systems. National University of Singapore.

9. Gai, A.-T., Viennot, L. (2004). Broose: a practical distributed hashtable based on the de-Bruijn topology. IEEE Fourth International Conference on Peer-to-Peer Computing.

10. [Richa, A., Scheideler, C., Stevens, P. (2011). Self-stabilizing De Bruijn networks. Stabilization, Safety, and Security of Distributed Systems - 13th International Symposium, SSS 2011, Proceedings.

11. Amad, M., Aïssani, D., Meddahi, A., Benkerrou, M., Amghar, F. (2015). De Bruijn Graph based solution for lookup acceleration and optimization in P2P networks. Wireless Personal Communications 85: (3) ((2015) ), 1471–1486. doi:10.1007/s11277-015-2851-y.

12. Loutskii, H., Volokyta, A., Rehida, P., Honcharenko, O., Ivanishchev, B., Kaplunov, A. (2019). Increasing the fault tolerance of distributed systems for the Hyper de Bruijn topology with excess code. 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT).

13. Fayad, A., Hammi, B., Khatoun, R. (2018). An adaptive authentication and authorization scheme for IoT's gateways: a blockchain based approach. 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC).

14. Thien Duc Nguyen, Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., Sadeghi, A.-R. (2019). DÏoT: A Federated Self-learning Anomaly Detection System for IoT. 39th IEEE International Conference on Distributed Computing Systems (ICDCS).

15. Banerjee, M., Lee, J., Choo, K. R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, vol. 4, p. 149-160.

16. Banerjee, M., Lee, J., Chen, Q., Choo, K. R. (2018). Blockchain-Based Security Layer for Identification and Isolation of Malicious Things in IoT:

A Conceptual Design. 27th International Conference on Computer Communication and Networks (ICCCN).

17. Team Rocket (2018). Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies. t-rocket@protonmail.com.

## AUTHORS

**Artem Popov** – PhD student, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: popov.artem.mail@gmail.com

**Sergii Stirenko** (supervisor) – professor, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

**Heorhii Loutskii** (supervisor) – professor, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".