Faculty of Electrical Engineering
WARSAW UNIVERSITY OF TECHNOLOGY

SITEE2025

# A Survey of Consensus Algorithms in Distributed Ledger Technology for Internet of Things

Paweł Podgórski
*Faculty of Electrical Engineering*
*Warsaw University of Technology*

***Abstract*—This comprehensive survey examines consensus algorithms utilized in Distributed Ledger Technology (DLT) for Internet of Things (IoT) environments. The paper provides a comparative analysis of consensus protocols including Proof of Work, Proof of Stake, Proof of Authority, Proof of Elapsed Time, Proof of Space, Proof of Activity, Practical Byzantine Fault Tolerance algorithm and Directed Acyclic Graph based approaches such as Adaptive Proof of Work, and Temporal Proof.***

## I. Distributed Ledger Technology

Distributed ledger technology (DLT) is system that enable secure, transparent, immutable, and distributed data storage. DLT uses peer-to-peer (P2P) network [1]. The first DLT implementation was blockchain, which structure is shown on Figure 1.

Based on blockchain, other technologies classified as DLT have also emerged, such as Tangle, Hashgraph, Holochain and Tempo [2]. IOTA Tangle 2.0 uses directed acyclic graph (DAG) instead of blockchain. Each node of the graph contains a message, that is equivalent to a transaction in blockchain technology.

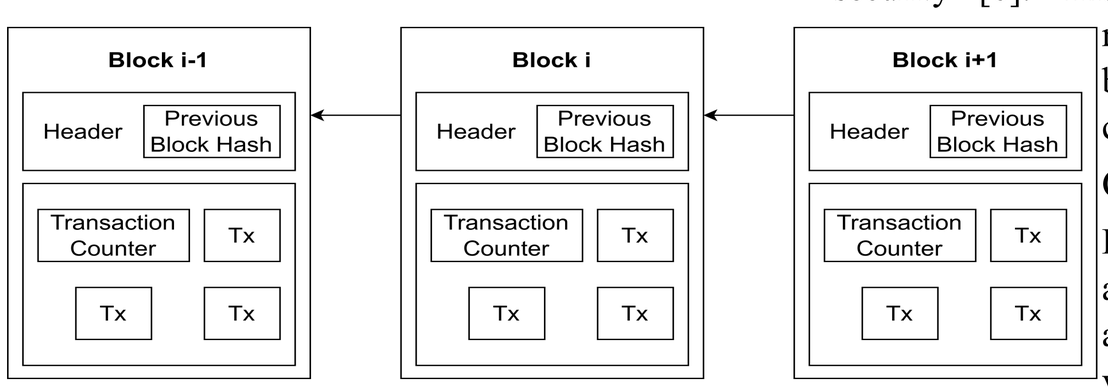


Figure 1. Structure of blockchain

To add a new message to the graph, participant must first verify two other messages [3]. Structure of IOTA Tangle graph is shown on Figure 2. DLT comparison is shown on Table 1.

## II. Consensus Algorithms

In decentralized networks, to maintain security, it is necessary to solve the Byzantine Generals Problem. It is challenge that illustrates how distributed systems must achieve reliable consensus when some participants may be unreliable or malicious, similar to military generals coordinating an attack while some might be traitors [4]. In most of the DLTs, this problem is resolved through a consensus algorithm[5].

### A. Proof of Work

The first reliable consensus algorithm was Proof of Work. In this algorithm, block creation occurs after correctly finding a number which, when added to the block, creates a hash with an appropriate number of zeros at the beginning. In this algorithm, there exists a danger and possibility of fraud in the case of a participant who possesses a significant portion of the total computational power of participants [5].

### B. Proof of Stake

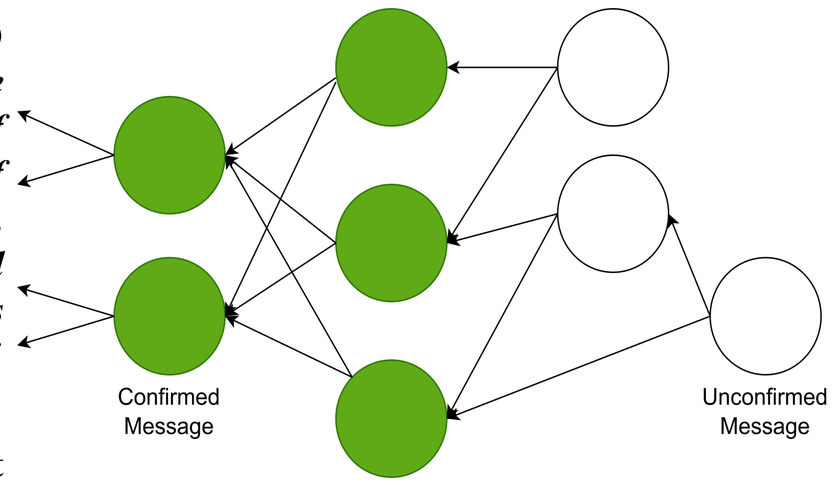


Figure 2. Structure of DAG on example of IOTA Tangle 2.0

Another popular consensus algorithm, resistant to such threats, is Proof of Stake (PoS). The right to accept transactions is granted based on the stake and resources of network participants who declare that they will lose their contribution, if they approve an invalid transaction. It is impossible to simultaneously achieve scalability, decentralization, and network security [6]. The author is currently conducting research on consensus algorithm based on PoS, where trust is contribution [7].

### C. Proof of Authority

Proof of Authority was designed as an optimized version of the PoS algorithm. A small group of validators is selected based on identity or staked reputation [8]. To become a validator, a user is required to have their identity verified, and there should be no grounds for distrusting the user [9].

### D. Proof of Elapsed Time

Proof of Elapsed Time is an algorithm that uses special hardware and execution environment to ensure that a device will not cheat. Each participant receives a random waiting time, and the one who finishes waiting first creates a block. The algorithm is energy-efficient and fair through randomness [10].

### E. Adaptive Proof of Work

The algorithm used in IOTA Tangle network is called Adaptive Proof of Work. The message (transaction) verification process involves calculating a hash function, similar to the Proof of Work consensus algorithm. The difficulty of this verification is proportional to the number of transactions initiated by the verifying actor during a defined period of time [3].

### F. Temporal proof

In Tempo, the consensus component of DLT is only activated when at least one participant questions validity of a request (transaction). This questioning can apply to any request that is already part of the ledger.

## III. Conclusions

This survey systematically evaluated both Distributed Ledger Technologies and their underlying consensus algorithms in the context of IoT, using key metrics such as efficiency, scalability, latency, throughput, and security. By outlining the capabilities and compromises of existing solutions, this work offers an overview to support informed decisions when selecting or adapting DLTs for IoT applications.

## References

[1] K. Kaur and R. Jaswal, “Exploring the potential of blockchain technology in enhancing security of smart systems,” in 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023, pp. 551–555.

[2] S. Gaba, H. Khan, K. J. Almalki, A. Jabbari, I. Budhiraja, V. Kumar, A. Singh, K. K. Singh, S. S. Askar, and M. Abouhawwash, “Holochain: An agent-centric distributed hash table security in smart iot applications,” IEEE Access, vol. 11, pp. 81 205–81 223, 2023.

[3] N. Sealey, A. Aijaz, and B. Holden, “Iota tangle 2.0: Toward a scalable, decentralized, smart, and autonomous iot ecosystem,” in 2022 International Conference on Smart Applications, Communications and Networking (SmartNets), 2022, pp. 01–08.

[4] L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Trans. Program. Lang. Syst., vol. 4, no. 3, p. 382–401, Jul. 1982. [Online]. Available: https://doi.org/10.1145/357172.357176

[5] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” in 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2017, pp. 2567–2572.

[6] M. Bez, G. Fornari, and T. Vardanega, “The scalability challenge of ethereum: An initial quantitative analysis,” in 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), 2019, pp. 167–176

[7] P. Podgórski, “Repozytorium pos-iot,” https://github.com/pjpawel/pos-iot.

[8] P. Zhang, D. C. Schmidt, J. White, and A. Dubey, “Chapter seven - consensus mechanisms and information security technologies,” in Role of Blockchain Technology in IoT Applications, ser. Advances in Computers, S. Kim, G. C. Deka, and P. Zhang, Eds. Elsevier, 2019, vol. 115, pp. 181–209.

[9] Changelly, “What is proof of authority (poa)?” 2019, accessed: 2025-03-20. [Online]. Available: https://changelly.com/blog/what-is-proof-of-authority-poa/

[10] D. Stefanescu, L. Montalvillo, P. Gal´an-Garc´ıa, J. Unzilla, and A. Urbieta, “A systematic literature review of lightweight blockchain for iot,” IEEE Access, vol. 10, pp. 123 138–123 159, 2022.

| DLT name | Structure | Approach | Secutiry | Energy consumtion | Latency | Scalability | Storage allocation |
|---|---|---|---|---|---|---|---|
| Blockchain | Chain of blocks | Data-centric | High | Depends on consensus alg. | High | Low | High |
| Tangle | DAG | Data-centric | Medium | Low | Low | High | High |
| Hashgraph | DAG | Data-centric | Medium | Low | Depends on Gossip Delay | High | Low |
| Holochain | DHT with hash chain | Agent-centric | Medium | Low | Application-dependent | High | High |
| Tempo | DAG | Data-centric | High | Low | Depends on Gossip Delay | High | Low |

Table 1. DLT Comparison