УДК 004.75 https://doi.org/10.30837/IYF.PCEIP.2024.108

ANALYSIS AND COMPARISON OF THE PALA CONSENSUS PROTOCOL

Кравченко А.А.
Науковий керівник: д.т.н, проф. Олійников Р.В.
Харківський національний університет радіоелектроніки, каф. БІКС,
м. Харків, Україна
e-mail: anastasiia.kravchenko@nure.ua

The PaLa protocol is known for its simplicity and effectiveness in achieving Byzantine Fault Tolerance (BFT). This thesis discusses the main properties of the PaLa – partially synchronous blockchain protocol, its advantages and disadvantages, and key aspects of its structure. We also compare PaLa with other algorithms, such as Tendermint, Hotstuff, and Casper FFG, which have fewer limitations due to their more complex structure. Based on the considered limitations, the following modifications are presented, which allow to extend them: Pipelet protocol, Committee rotation algorithm, and Streamlet protocol.

The PaLa protocol was proposed as a new consensus protocol based on simplicity and efficiency, aiming to streamline the consensus process while maintaining security standards. It is considered one of the simplest and most efficient classical BFT consensus protocols, focusing on removing unnecessary complexities present in previous protocols to enhance performance. PaLa is inspired by the pipelined-BFT paradigm and a generalization called "doubly-pipelined PaLa", which is oriented towards settings that require high performance [1].

PaLa stands out as a simple partially synchronous blockchain protocol inspired by the pipelined-BFT paradigm. Unlike its predecessors, PaLa focuses on removing unnecessary complexities to streamline the consensus process. By leveraging a partially synchronous network model and tolerating up to ⅓ corruptions, PaLa aims to achieve fast transaction confirmations while maintaining security. The PaLa protocol has several advantages over other blockchain consensus protocols making it an outstanding solution in this field.

Key features of PaLa:

– Efficiency: PaLa minimizes the number of messages required to reach a consensus and increases transaction speed without compromising security;

– Simplicity: by eliminating the inefficiencies present in traditional protocols, PaLa provides a simple and elegant solution for Byzantine fault tolerance;

– Security: While speed is a priority, PaLa incorporates robust security measures to protect against malicious activity and guarantee transaction integrity;

– Network Model Adaptability: PaLa is based on partially synchronous network assumptions and can tolerate up to ⅓ corruptions, making it adaptable to various network settings while maintaining efficiency. The protocol's ability to achieve consensus with just O(n) messages showcases its adaptability and scalability in different blockchain environments [3].

Perhaps, the key features sufficiently describe the advantages of using this protocol, so we should move on to the disadvantages and limitations, which are also here. Although PaLa is recognized as the simplest and most efficient classic BFT consensus protocol, it does not introduce many new innovations compared to other protocols such as Tendermint, FBFT, Casper FFG, and Hotstuff. In addition, there are scalability issues: for a network with more nodes, maintaining speed becomes more difficult, which affects performance. In addition, the focus on simplicity, speed, and increased throughput can lead to various security issues. The protocol's responsiveness to real-world network delays, denoted as δ, is essential for achieving fast transaction finality. Adapting to network conditions and minimizing delays is crucial for enhancing transaction speed within the PaLa protocol. The risks associated with generating a large number of orphan blocks should not be overlooked: maintaining a balance between block production rate and network latency is crucial to prevent high rates of empty blocks that can affect transaction completion and overall network efficiency.

As noted, one of the advantages of using PaLa is speed, so for a clearer understanding, let's compare it with other protocols used:

– Tendermint: Tendermint is known for its high throughput and fast finality, making it a scalable solution for blockchain networks. It achieves consensus through a practical Byzantine Fault Tolerance (PBFT) algorithm, offering robustness in handling a large number of transactions [2]. It also has an optimal solution to improve the efficiency of work in such conditions is to perform load balancing or use rpc nodes, not just individual network validators. This allows to increase the speed and avoid cases of node overload [5];

– Hotstuff: Hotstuff is another protocol that focuses on scalability and efficiency by utilizing a leader-based approach for consensus. It offers fast confirmation times and high throughput, addressing scalability challenges effectively [2];

– Casper FFG: Casper FFG introduces a hybrid Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanism to enhance scalability and security. By combining these two approaches, Casper FFG aims to achieve a balance between transaction speed and network scalability [2].

It becomes apparent that in comparison to these protocols, PaLa may face limitations in scalability due to its partially synchronous nature and the challenges associated with handling network delays as the network grows.

1. Pipelet protocol

Pipelet protocol: the Pipelet protocol was introduced as a practical streamlined consensus protocol to improve scalability. Pipelet protocol: the Pipelet protocol was introduced as a practical streamlined consensus protocol to improve scalability, including extending the longest chain and finalizing the middle of three consecutive normal notarised blocks, using familiar rules [4].

Pipellet aims to combine the advantages of simplicity, performance and practicality found in other protocols such as Streamlet and PaLa, and offers a conceptually different approach that reduces the message costs required to finalize a block.

2. Committee rotation algorithm

A committee rotation algorithm is proposed to enhance the scalability and security of PaLa. The algorithm aims to dynamically rotate consensus nodes in dynamic networks using verifiable random functions (VRFs) to reduce communication requirements in stable network conditions [4].

3. Streamlet protocol

The Streamlet protocol provides a simple and natural paradigm for building consensus protocols, inspired by core technologies discovered in the past Streamlet and PaLa messages grow exponentially with the number of nodes. To address scalability concerns, detailed specifications on assumptions, consistency and effectiveness under partial synchronization are provided [4].

Recent studies have evaluated the performance and scalability of prominent consensus protocols like PBFT, Tendermint, HotStuff, Streamlet, and PaLa under identical conditions. These evaluations highlight limitations in communication complexity for larger networks and emphasize the need for practical solutions like Pipelet to address scalability challenges effectively.

In conclusion, this paper has discussed the general properties of the PaLa algorithm, its advantages and disadvantages in comparison with some other popular algorithms. This protocol is quite simple and robust, but it may have some scaling issues due to its structure. However, several modifications almost solve these problems while maintaining the basic structure of the protocol, the best of which, in the author's personal opinion, is Pipelet due to its practical applicability.

Список використаних джерел

1. KARIHALOO, Vivek, et al. Pipelet: Practical Streamlined Blockchain Protocol. *arXiv preprint arXiv:2401.07162*, 2024.

2. Qi G., Lu P. Consensus Protocols 101. *https://docs.thundercore.com/consensus-protocols-101.pdf.*

3. Kim C. Blockchain Project Thundercore Releases Code for 'Pala' Consensus Protocol. *CoinDesk: Bitcoin, Ethereum, Crypto News and Price Data*. URL: https://www.coindesk.com/markets/2019/05/15/blockchain-project-thundercore-releases-code-for-pala-consensus-protocol/

4. CHAN, TH Hubert; PASS, Rafael; SHI, Elaine. Pala: A simple partially synchronous blockchain. *Cryptology ePrint Archive*, 2018.

5. Дубіна В.В., Олійников Р.В. Аналіз властивостей децентралізованого протоколу консенсусу із підвищеною пропускною здатністю. Проблеми інформатизації: десята міжнародна науково-технічна конференція. Харківський національний університет радіоелектроніки - Черкаси – Баку – Бельсько-Бяла – Харків – 2022.