Optimizing Validator Selection for Enhanced Security in BFT Blockchains

Rachid Guedjali*[1], Jean-Philippe Georges , Sylvain Kubler , and Guilain Leduc

[1]Centre de Recherche en Automatique de Nancy – Université de Lorraine, Centre National de la Recherche Scientifique – Université de Lorraine, Campus Sciences, BP 70239, 54506 Vandoeuvre-les-Nancy Cedex, France

Résumé

Decentralized blockchain systems rely on consensus mechanisms to ensure both security and transaction processing integrity (10, 2). Validator selection within these systems plays a pivotal role in maintaining overall system integrity. This paper introduces an innovative algorithm tailored to optimize validator selection within blockchain networks, with a specific focus on the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. The algorithm dynamically adjusts the validator's pool, strategically integrating factors such as proximity, participation rates, and the inclusion of a trustworthy majority of validators (2).

Despite recent research initiatives exploring dynamic adjustments in validator pool sizes to enhance system resilience, existing methodologies often overlook the importance of node proximity or incur high resource consumption (7). To address these challenges, our algorithm dynamically varies validator nodes based on network distances and participation rates. Additionally, it incorporates randomness into the selection process to enhance unpredictability and overall network security (4, 8).

Related work in decentralized applications, cloud computing, and blockchain consensus mechanisms underscores the significance of randomness and node proximity in validator selection (9, 1, 6, 3).
The paper discusses the potential of using multi-agent systems (12), (11), (5) and analyzing the dynamics of their opinions to monitor the behavior of validator nodes and other entities in Blockchain systems based on BFT protocols. The objective is to develop a mathematical model based on a blockchain, where each node expresses an opinion that can be defined in relation to the state of the network, the state of the consensus protocol, or other factors. More specifically, the dynamics of opinions within the network could contribute to identifying the best validators, anticipating and avoiding the selection of nodes expressing negative opinions, which could be suspected of malicious behavior.

In conclusion, this research contributes to advancing the security and performance of decentralized blockchain systems by addressing critical challenges in validator selection and network monitoring, while drawing inspiration from the field of opinion dynamics. By leveraging innovative algorithms and considering key factors such as node proximity and randomness, our
approach aims to enhance the overall integrity and efficiency of blockchain networks operating on BFT protocols.

*Intervenant

Références

(1) M. Adler, R. Kumar, K. Ross, D. Rubenstein, T. Suel, and D.D. Yao. Optimal peer selection for p2p downloading and streaming. In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., volume 3, pages 1538–1549 vol. 3, March 2005.

(2) Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance. In Proceedings of
the Third Symposium on Operating Systems Design and Implementation, OSDI '99, page 173–186, USA, February 1999. USENIX Association.

(3) Xu Chen, Lei Jiao, Wenzhong Li, and Xiaoming Fu. Efficient multi-user computation offloading for mobile-edge cloud computing. IEEE/ACM Transactions on Networking, 24(5) :2795–2808, October 2016.

(4) Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand : Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, SOSP '17, page 51–68, New York, NY, USA, 2017. Association for Computing Machinery.

(5) Michel Grabisch and Agnieszka Rusinowska. A survey on nonstrategic models of opinion dynamics. Games, 11(4) :65, 2020.

(6) Tarandeep Kaur and Inderveer Chana. Energy efficiency techniques in cloud computing :
A survey and taxonomy. ACM Comput. Surv., 48(2), oct 2015.

(7) Guilain Leduc, Sylvain Kubler, and Jean-Philippe Georges. A centre-based validator selection approach for a scalable bft blockchain. In 22nd IFAC World Congress, IFAC 2023, 2023.

(8) Peilun Li, Guosai Wang, Xiaoqi Chen, Fan Long, and Wei Xu. Gosig : A scalable and
high-performance byzantine consensus for consortium blockchains. In Proceedings of the 11th ACM Symposium on Cloud Computing, SoCC '20, page 223–237, New York, NY, USA, 2020. Association for Computing Machinery.

(9) V. Lo, Dayi Zhou, Yuhong Liu, C. GauthierDickey, and Jun Li. Scalable supernode selection in peer-to-peer overlay networks. In Second International Workshop on Hot Topics in Peer-to-Peer Systems, pages 18–25, July 2005.

(10) Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. Decentralized Business
Review, 10 2008.

(11) Hossein Noorazar. Recent advances in opinion propagation dynamics : A 2020 survey.
The European Physical Journal Plus, 135 :1–20, 2020.

(12) Vineeth S Varma, Irinel-Constantin Morărescu, and Mehdi Ayouni. Analysis of opinion dynamics under binary exogenous and endogenous signals. Nonlinear Analysis : Hybrid Systems, 38 :100910, 2020.