An Adaptive Approach to Blockchain in Smart System Applications

Naseem Alsadi*[a], Alessandro Giuliano [a], Stephen A. Gadsden[a], John Yawney[b]
[a]Intelligent and Cognitive Engineering Laboratory, McMaster University, 1280 Main St W, Hamilton, ON L8S 4L8 ; [b]Adastra Corporation, 8500 Leslie St #600, Thornhill, ON L3T 7M8

ABSTRACT

As the technological landscape continues rapidly evolving, blockchain technology has been widely integrated and employed in various areas of application. Blockchain, at its core, offers a decentralized method for system security and communication. This is in contrast with classical security systems, which necessitate a central node for data processing and communication, therefore augmenting vulnerability to a single point of failure and attack. Incorporating adaptive sub-systems into various blockchain technology features might greatly enhance their functionality without jeopardizing the chain's immutability. Several publications have focused on the analysis of network node data in an effort to offer an adaptive version of the consensus mechanism used in the blockchain process. This paper presents a novel adaptive consensus mechanism that regulates the Proof-of-Work mining difficulty based on the perceived anomalous level of network nodes.

Keywords: Blockchain, Proof-of-Work, Machine Learning

1. INTRODUCTION

Highly distributed connected systems, such as the Internet of Things (IoT) and smart systems, have found widespread adoption in a variety of applications. The Internet of Things (IoT) and smart systems provide a technique for connecting diverse heterogeneous devices via the internet, allowing for the effective distribution, gathering, and processing of system-related data. While system interconnection has improved communication and the efficacy of integrated technologies, it has also raised system vulnerability. Researchers have suggested different security protocols and frameworks for IoT ecosystems for this purpose. The majority of these communication and security frameworks, however, are centralized. While centralized frameworks are the most common with regard to IoT, they do not complement the distributed nature of IoT environments.

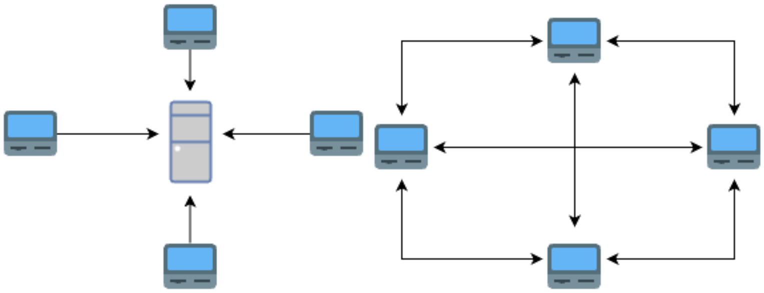

Figure 1: a) Centralized Network b) Decentralized Network

Blockchain technology is a distributed ledger system that allows numerous parties to keep a secure and immutable record of system data. A blockchain's fundamental components are blocks, which hold system data and other core information about the block and chain, and a consensus process for validating new blocks and appending them to the chain [1], [2]. The combination of blockchain and smart systems allows for a more robust overall security framework. Smart systems are, by definition, highly dispersed. However, relying on a centralized cloud increases system vulnerabilities. Fundamentally, blockchain deployment in smart system applications will aim to decentralize the entire system network and supplement the distributed nature of smart systems.

*alsadin@mcmaster.ca

Big Data V: Learning, Analytics, and Applications, edited by Panos P. Markopoulos,
Bing Ouyang, Vagelis Papalexakis, Proc. of SPIE Vol. 12522, 1252209
© 2023 SPIE · 0277-786X · doi: 10.1117/12.2662231

With the aim of further ensuring the security of a smart system, various aspects of blockchain architecture can be made adaptive. This will therein allow the blockchain to adapt to changing environmental factors which is a major challenge for smart system applications which will deal with constantly varying external environments. There are numerous ways to integrate adaptive behaviour within the blockchain architecture with numerous publications touching on this. [3]– [18]

In this paper, we propose an adaptive consensus mechanism that adjusts the mining process's difficulty based on the anonymity level in network node data. Our approach aims to enhance the security and efficiency of blockchain networks without compromising the inherent benefits of decentralization.

2. PROPOSED METHOD

We propose an adaptive consensus mechanism that adjusts the mining process's difficulty based on the anonymity level in network node data. To do such we store network node data in the chain and update it at predefined intervals which are baked into the protocol.

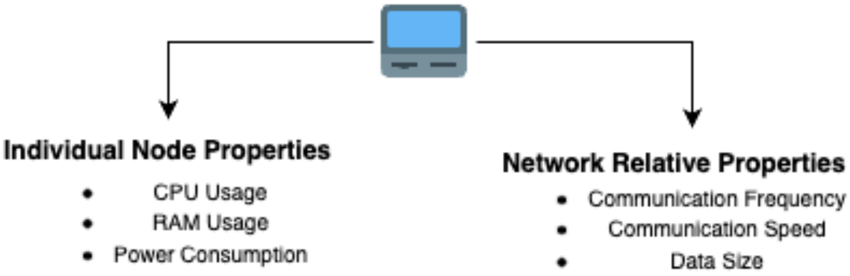

Figure 2: Two Variant Types of Node Characteristics

We utilize two variant types of device characteristics, namely individual properties and network-level properties, which are properties of the nodes which can be verified independent of that node’s testimony. The objective of doing such is to remove trust from the network.

We assume that device properties can disclose important information regarding node behaviour. To support this assumption, there has been a lot of research conducted on the identification of anomalous behaviour using various examples of device attributes [6]-[10]. Employing a variety of machine learning models to detect anomalous behaviour using node power usage is one example of such research [11]. RAM and CPU usage can also be utilized to detect anomalous behaviour [12].

To detect anomalous behaviour, we employ the Local Outlier Factor (LOF) method which takes advantage of the fact that data points have a significantly different local density than their neighbours. When using LOF, a data point's local density is compared to the densities of its k-nearest neighbours. The LOF approach does not rely on any presumptions regarding the distribution of the underlying data and is applicable to both univariate and multivariate data. Additionally, it can handle data of any size and shape, and it is resistant to data noise. Figure 4 shows an example of anomalous node activity being captured by the LOF model.

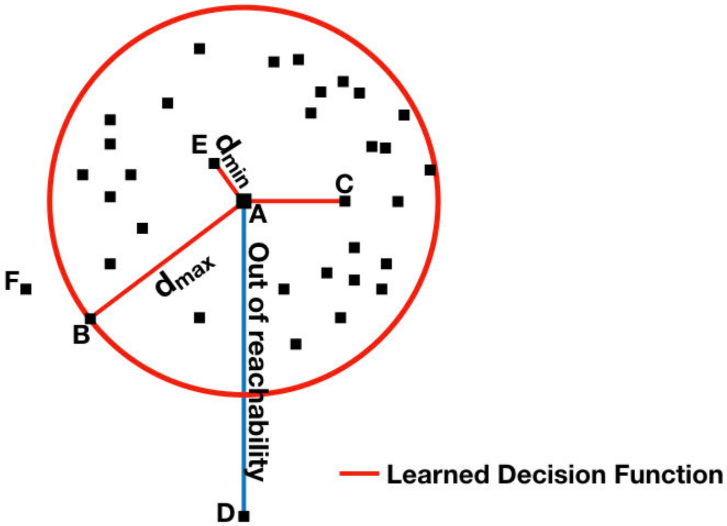

Figure 3: When Using a Local Outlier Factor Instead of Comparing Each Point to Its Global Neighbors, Each Point Is Compared to Its Local Neighbors [19]

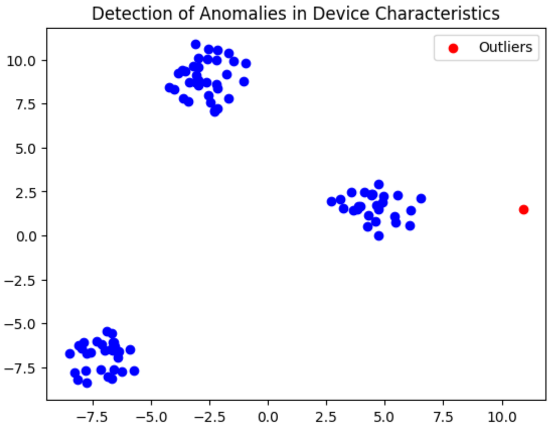

Figure 4: Detection of Anomalies Using Local Outlier Factor

Based on the perceived level of anomalous behaviour, our adaptive consensus system changes the mining difficulty to maintain a balance between security and efficiency. When the amount of anomalous behaviour is high, the mining difficulty is increased to give additional protection to the network against a specific node. When anonymity is low, the mining difficulty is reduced to increase network efficiency.

To display the effectiveness of the proposed method we present a series of results from a simulation employing the proposed architecture. In the first simulation scenario, we utilize a set of nodes which do not display abnormal behaviour and operate within all normal standards.

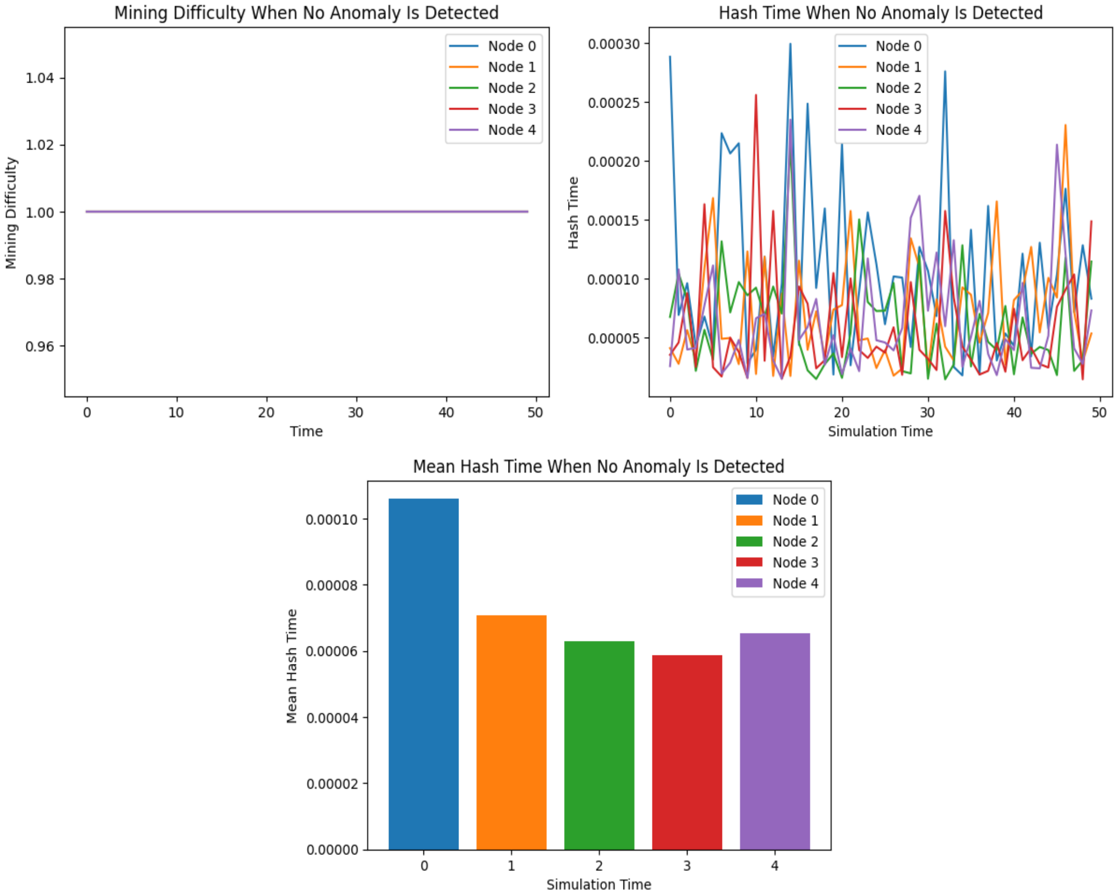

Figure 5: Mining Difficulty, Hash Time and Mean Network Hash Time When Anomalous Behaviour Is Not Detected

The results of this simulation scenario are shown in Figure 5. We can see that the mining difficulty is not changed, and mining time remains similar for all nodes in the network. This simulation is crucial for understanding how the architecture will operate in typical environmental circumstances when faced with no anomalous node activity.

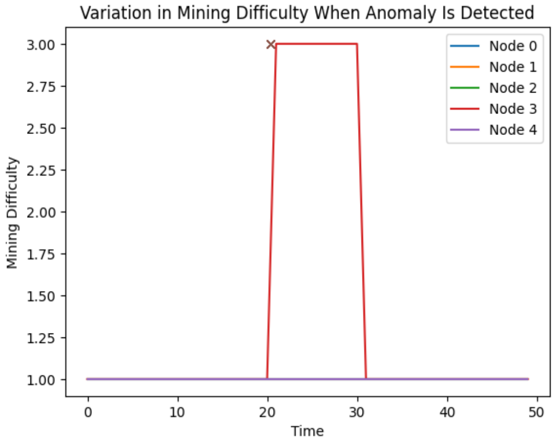

Figure 6: Increase in Mining Difficulty When a Single Node is Registered as Anomalous

In this simulation scenario, a single node is registered as anomalous, and the subsequent mining difficulty is adjusted according to the level of perceived anomalous activity.

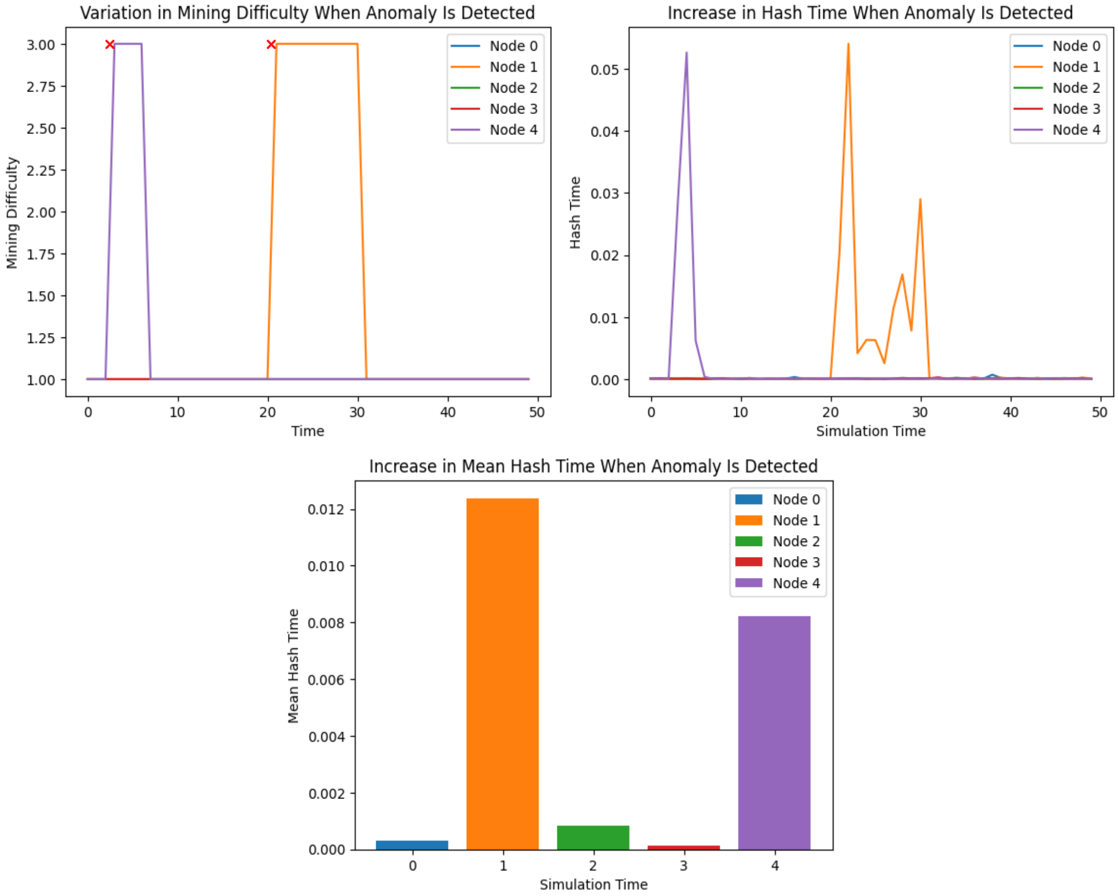

Figure 7: Mining Difficulty, Hash Time and Mean Network Hash Time When Anomalous Behaviour Is Detected

In the final simulation scenario, shown in Figure 7, we utilize two anomalous nodes which are detected at variant times. We can see that the respective mining difficulty is adjusted for the period of time they were acting anomalously. Due to this, there is a large increase in hash time for only those respective nodes.

3. CONCLUSION

In this paper, we proposed a novel adaptive consensus mechanism that adjusts the mining difficulty for specific nodes based on the level of anomalous behaviour in network node data. Our approach aims to enhance the security and efficiency of blockchain networks without compromising the inherent benefits of decentralization. Our experimental results demonstrate the effectiveness of our method in swiftly responding to anomalous node behaviour and increasing the difficulty of communication for the respective node.

REFERENCES

[1] X. Deng, K. Li, Z. Wang, J. Li, and Z. Luo, “A Survey of Blockchain Consensus Algorithms,” in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, Jul. 2022, pp. 188–192. doi: 10.1109/ICBCTIS55569.2022.00050.

[2] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, “Bitcoin and Blockchain: Security and Privacy,” *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, Oct. 2020, doi: 10.1109/JIOT.2020.3004273.

[3] S. Zhang and X. Ma, “A General Difficulty Control Algorithm for Proof-of-Work Based Blockchains,” in *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2020, pp. 3077–3081. doi: 10.1109/ICASSP40776.2020.9054286.

[4] N. Alsadi *et al.*, “An anomaly detecting blockchain strategy for secure IoT networks,” in *Disruptive Technologies in Information Sciences VI*, SPIE, May 2022, pp. 90–98. doi: 10.1117/12.2618301.

[5] S. Liaskos, B. Wang, and N. Alimohammadi, “Blockchain Networks as Adaptive Systems,” in *2019 IEEE/ACM 14th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, May 2019, pp. 139–145. doi: 10.1109/SEAMS.2019.00025.

[6] B. Sriman, S. Ganesh Kumar, and P. Shamili, “Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake,” in *Intelligent Computing and Applications*, S. S. Dash, S. Das, and B. K. Panigrahi, Eds., in Advances in Intelligent Systems and Computing. Singapore: Springer, 2021, pp. 395–406. doi: 10.1007/978-981-15-5566-4_34.

[7] S. Rai, K. Hood, M. Nesterenko, and G. Sharma, “Blockguard: Adaptive Blockchain Security.” arXiv, Jul. 30, 2019. Accessed: Sep. 20, 2022. [Online]. Available: http://arxiv.org/abs/1907.13232

[8] C. Qiu, X. Ren, Y. Cao, and T. Mai, “Deep Reinforcement Learning Empowered Adaptivity for Future Blockchain Networks,” *IEEE Open J. Comput. Soc.*, vol. 2, pp. 99–105, 2021, doi: 10.1109/OJCS.2020.3010987.

[9] “Difficulty control for blockchain-based consensus systems | SpringerLink.” https://link.springer.com/article/10.1007/S12083-015-0347-X (accessed Nov. 02, 2022).

[10] M. Fokaefs and M. Rasolroveicy, *Dynamic Reconfiguration of Consensus Protocol for IoT Data Registry on Blockchain*. 2020.

[11] X. Hu, Y. Zheng, Y. Su, and R. Guo, “IoT Adaptive Dynamic Blockchain Networking Method Based on Discrete Heartbeat Signals,” *Sensors*, vol. 20, no. 22, p. E6503, Nov. 2020, doi: 10.3390/s20226503.

[12] V. Amelin, N. Romanov, R. Vasilyev, R. Shvets, Y. Yanovich, and V. Zhygulin, “Machine Learning View on Blockchain Parameter Adjustment,” in *2021 3rd Blockchain and Internet of Things Conference*, Ho Chi Minh City Vietnam: ACM, Jul. 2021, pp. 38–43. doi: 10.1145/3475992.3475998.

[13] V. Amelin, N. Romanov, R. Vasilyev, R. Shvets, Y. Yanovich, and V. Zhygulin, “Machine Learning View on Blockchain Parameter Adjustment,” in *2021 3rd Blockchain and Internet of Things Conference*, Ho Chi Minh City Vietnam: ACM, Jul. 2021, pp. 38–43. doi: 10.1145/3475992.3475998.

[14] J.-P. Bahsoun, R. Guerraoui, and A. Shoker, “Making BFT Protocols Really Adaptive,” in *2015 IEEE International Parallel and Distributed Processing Symposium*, Hyderabad: IEEE, May 2015, pp. 904–913. doi: 10.1109/IPDPS.2015.21.

[15] G. Hovland and J. Kucera, “Nonlinear Feedback Control and Stability Analysis of a Proof-of-Work Blockchain,” vol. 38, no. 4, pp. 157–168, Oct. 2017, doi: 10.4173/mic.2017.4.1.

[16] “Research on PBFT consensus algorithm for grouping based on feature trust | Scientific Reports.” https://www.nature.com/articles/s41598-022-15282-8 (accessed Dec. 11, 2022).

[17] G. Leduc, S. Kubler, and J.-P. Georges, “Sabine: Self-Adaptive BlockchaIn coNsEnsus,” in *2022 9th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2022, pp. 234–240. doi: 10.1109/FiCloud57274.2022.00039.

[18] D. Meshkov, A. Chepurnoy, and M. Jansen, “Short Paper: Revisiting Difficulty Control for Blockchain Systems,” in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017, pp. 429–436. doi: 10.1007/978-3-319-67816-0_25.

[19] “Towards a Better Gold Standard | Proceedings of the 2018 on Audio/Visual Emotion Challenge and Workshop.” https://dl.acm.org/doi/10.1145/3266302.3266307 (accessed Apr. 12, 2023).