PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

A cognitive dynamics framework for practical blockchain applications

Naseem Alsadi, Stephen Gadsden, John Yawney

Naseem Alsadi, Stephen A. Gadsden, John Yawney, "A cognitive dynamics framework for practical blockchain applications," Proc. SPIE 12542, Disruptive Technologies in Information Sciences VII, 1254206 (15 June 2023); doi: 10.1117/12.2664067

SPIE.

Event: SPIE Defense + Commercial Sensing, 2023, Orlando, Florida, United States

A Cognitive Dynamics Framework for Practical Blockchain Applications

Naseem Alsadi*[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

Blockchain technology has gained notoriety as the foundation for cryptocurrencies like Bitcoin. However, its possibilities go well beyond that, enabling the deployment of new applications that were not previously feasible as well as enormous improvements to already existing technological applications. Several factors impacting the consensus mechanism must fall within a specific range for a blockchain network to be efficient, sustainable and secure. The long-term sustainability of current networks, like Bitcoin, is in jeopardy due to their relatively uncompromising reconfiguration, which tends to be inflexible, and somewhat independent of environmental circumstances. To provide a systematic methodology for integrating a sustainable and secure adaptive framework, we propose the amalgamation of cognitive dynamic systems theory with blockchain technology, specifically regarding variant network difficulty. A respective architecture was designed with the employment of Long-Short Term Memory (LSTM) to control the difficulty of a network with Proof-of-Work Consensus.

Keywords: Blockchain, Cognitive Dynamics Systems, Machine Learning

1. INTRODUCTION

Blockchain technology has become more popular as the underlying technology for cryptocurrencies like Bitcoin. Yet this technology has far more promise than that. With blockchain technology, data can be shared and maintained without the use of intermediaries, making transactions safer, more effective, and more efficient [1].

Several features affecting the consensus process must fall within a certain range in order to guarantee the effectiveness, viability, and security of a blockchain network. To guarantee effective and long-lasting operations, the network's block size, block duration, and network difficulty, for example, must be precisely adjusted. However, a lot of the existing blockchain networks, including Bitcoin, are very rigid in their configuration, which results in stiffness and independence from environmental factors. Maintaining maximum effectiveness and security is difficult due to the existing networks' rigidity and lack of adaptation. Yet, a methodical approach for incorporating a durable and secure adaptive framework might be offered by amalgamating cognitive dynamic systems theory with blockchain technology.

Blockchain is a cutting-edge technology that is quickly growing and is fundamentally a mechanism for the decentralization of modern technological systems. Blockchain can eliminate the need for any centralization within various systems, including smart systems, although it is most notable when used to cryptocurrency. Decentralization can enhance a system's efficiency and security, among other things.

Blocks of data, or records, make up the distributed ledger known as blockchain. These blocks, which keep account of system transactions, are dispersed among several network nodes. A cryptographic hash of the block that came before it on the blockchain is contained in each block inside the network. The peer-to-peer network architecture supports the decentralization of the network and the equitable distribution of privileges across network nodes. In comparison, The client-server network model, for example, requires network clients to request services and resources from a centralized server.

*alsadin@mcmaster.ca

Disruptive Technologies in Information Sciences VII, edited by Misty Blowers, James Holt, Bryant T. Wysocki, Proc. of SPIE Vol. 12542, 1254206
 · 0277-786X · doi: 10.1117/12.2664067

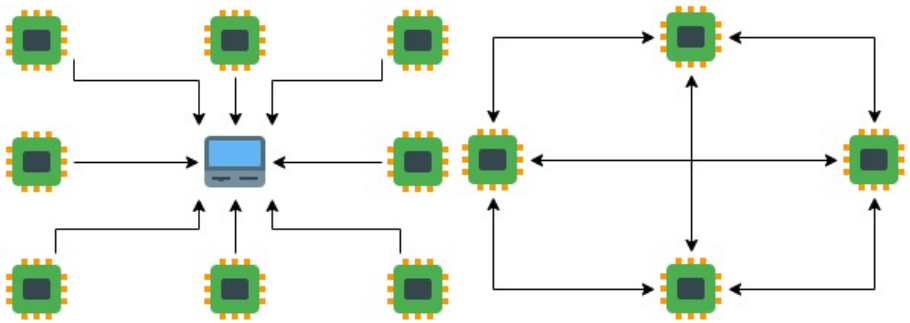

Figure 1: a) Centralized Network b) Decentralized Network [2]

Blockchain technology's consensus protocol method is essential for ensuring that all nodes in the network agree on the ledger's current state. The Proof of Work (PoW) consensus algorithm is the most widely utilized in blockchain networks. It makes use of computing power to verify transactions and build new blocks. The network's nodes compete to figure out a mathematical conundrum, and the first node to do so gets to add the next block to the chain. Because to the prohibitively high cost of changing a block's data, this method makes sure that the network is safe.

Another crucial component of blockchain technology is difficulty, which defines how difficult the mathematical puzzle that nodes in the network must solve in order to produce new blocks. To maintain a steady flow of new blocks and the security of the network, the difficulty level is frequently changed. Blocks are formed too rapidly when the complexity is set too low, which might cause security problems. On the other hand, if the difficulty is too high, blocks are generated too slowly and transaction confirmation times are prolonged.

The importance of both the consensus protocol mechanism and difficulty in blockchain technology cannot be overstated. The consensus protocol mechanism ensures that all nodes within the network agree on the same state of the ledger, thereby ensuring its security and immutability. The difficulty level ensures that the network remains secure by adjusting the complexity of the mathematical puzzle required to create new blocks. By adjusting the difficulty level, the network can maintain a consistent rate of block creation, which ensures that transaction confirmation times remain low.

The consensus protocol mechanism and difficulty are essential components of blockchain technology. These aspects ensure the network's security, immutability, and efficiency. As blockchain technology continues to evolve, it is essential to ensure that these components are optimized to meet the needs of the network and the applications built on top of it. This will help ensure that blockchain technology remains a secure and efficient way to facilitate peer-to-peer transactions without the need for intermediaries.

An interdisciplinary area called cognitive dynamic systems theory brings together ideas from engineering, psychology, and neuroscience to improve our comprehension of complex systems. The idea focuses on the significance of feedback loops and adaptability in systems, emphasizing how these components may enhance performance and allow systems to react to shifting environmental conditions.

The notion that systems are dynamic and always changing is one of the core tenants of cognitive dynamic systems theory. This means that for systems to continue working efficiently, they must be able to adapt to changes in their environment. Systems can track their performance and modify their behaviour to operate at their best even in the face of changing circumstances by implementing feedback loops.

The use of the four main components of cognition—perception and actuation, memory, attention, and intelligence—is highly valued in cognitive dynamic systems. In a system with several heterogeneous subcomponents, the emergent capacity of dynamic and autonomous change can be fostered when all system components function in unison.

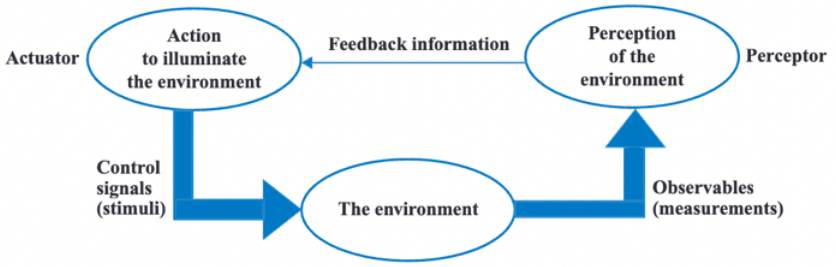

Figure 2: Perception-Action Cycle [3]

The two principal elements in cognitive dynamic systems are perception and actuation. The system can perceive its surroundings through perception, but it can also change it through actuation. Sensing devices, whether internal or external to the system, are used to enable these interactions and give the system information about the status of the environment at any given time. Data obtained by the system's perceptual unit will eventually help the system make a choice, which may then use actuation devices to change the physical state of its surrounding environment. Another crucial element of cognitive dynamic systems is memory. Memory allows for the preservation of prior events and information from both internal and external environments, which makes it easier to derive insights from past experiences. Perceptual memory, executive memory, and working memory are the three main subtypes of the system's memory. The information that a preceptor learns from their surroundings is stored in their perceptual memory, and the information in this memory is continually changing over time in reaction to environmental changes. Executive memory is the practical knowledge that an actuator gains through the experiences gained from actions taken in a particular environment. In order to prioritize the system's limited processing resources, attention is a crucial subsystem. Attention is a method that protects both the perceptual-processing power of the preceptor and the decision-making capabilities of the actuator from information overload through the prioritization of how these computing resources are deployed. The ability of a cognitive dynamic system to continually adjust itself through an adaptive process is what is referred to as intelligence. This is accomplished by requiring the preceptor to respond to recent environmental changes in order to motivate the actuator to act and behave in innovative ways. In other words, intelligence allows the system to pick up information from its surroundings and modify its behaviour. The integration of adaptive techniques within the blockchain architecture has been explored in the literature [4]–[16]. In this brief paper, the suggested integration of blockchain technology with cognitive dynamic systems theory focuses on varying network difficulty. With this strategy, a blockchain network can adjust its necessary parameters in response to shifting environmental factors. It would be able to maximize network performance, increase energy efficiency, and improve reliability by doing such.

2. COGNITIVE BLOCKCHAIN

Perception and actuation, memory, attention, and intelligence are the four main facets of CDS. These capabilities may be used to incorporate adaptive difficulty in blockchain networks, enhancing the network's stability and security. The capacity of a system to detect and react to changes in the environment is referred to as perception and actuation. This is possible in the blockchain environment by tracking the hash rate of miners and altering the difficulty level as necessary. The system can react to fluctuations in the hash rate and make sure that blocks are generated at a mostly consistent pace by continuously monitoring the network. Keep in mind that there are different network components that might be detected and cause a change in the network. Network's average block mining time may be greatly impacted by a rapid inflow of new miners or a major shift in the processing capacity of the current miners. An adaptive difficulty algorithm may be able quickly to adjust the level of difficulty in certain situations to keep the block mining time within the desired range. Depending on a number of variables including user adoption, network congestion, and transaction fees, the demand for transaction processing on a blockchain network might change significantly over time. An adaptive difficulty algorithm might assist in adjusting the difficulty level in cases when there are abrupt increases or decreases in network utilization to guarantee that the block mining time is minimized. While the majority of blockchain networks employ a set goal block time (such as 10 minutes for Bitcoin), certain networks may utilize a flexible target block time that varies according to network

circumstances. In these circumstances, an adaptive difficulty algorithm might assist in adjusting the difficulty level to correspond with the goal block time, ensuring that the network functions well.

Memory is the capacity of a system to retain and retrieve data. This may be accomplished using blockchain technology by keeping track of changes to the difficulty level and the related hash rates. With the use of this knowledge, the difficulty level may be adjusted in response to anticipated variations in the hash rate. The system can respond to network changes more swiftly and precisely by leveraging past data to guide decision-making. This is a major improvement in comparison to contemporary difficulty adjustment techniques which are often criticized for being too reactive.

The capacity of a system to prioritize and focus on key information is referred to as attention. This is possible in the context of blockchain by establishing thresholds for the hash rate and difficulty level modifications. In order to maintain network stability and security, the system might prioritize adjusting the difficulty level when the hash rate exceeds a specified threshold.

A system's capacity for learning and situational adaptation is referred to as intelligence. To do this in the context of blockchain, machine learning algorithms are used to examine previous data and forecast potential network changes in the future. The system's accuracy and efficiency in altering the difficulty level may be improved by continuing to learn and adapt. Additionally, by employing intelligent algorithms, the system is able to recognize and react to network irregularities, such as a rapid rise or fall in hash rate or even changing node conditions.

To showcase the utilization of an adaptive blockchain using a cognitive framework we employ a simple blockchain simulation with a proof of work consensus mechanism and a Long-Short Term Memory (LSTM) model. The architecture senses key characteristics of the blockchain network:

1. **Hash Time:** The time it takes to complete the hashing process and successfully mine a block.
2. **Hash Rate:** The number of hashes the miner can complete per second.
3. **Average Network Hash Rate:** The average hash rate across all miners in the network.
4. **Difficulty:** Indicates how challenging it is to locate a hash that will be lower than the network's set objective.

For the first analysis, we assume that the miner's hash rate remains constant, and no new miners join the network, therefore maintaining the average hash rate in the network.

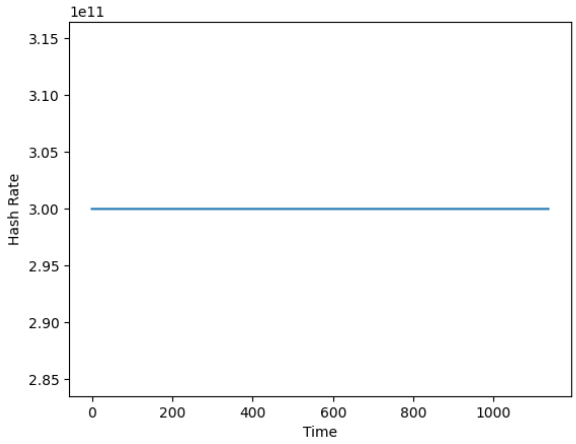

Figure 3: Constant Average Network Hash Rate

The average network hash rate is held at a value of 300 GH/s. Figure 3 shows that the respective hash rate is held at this value over the entire period of the simulation. This is not an unlikely scenario given a more private Blockchain network;

however, practically speaking, there will be slight variances in the average network hash rate as a result of miners joining and leaving the network.

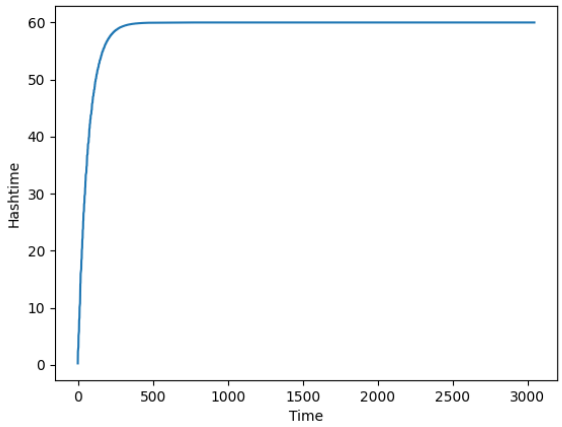

Figure 4: Hash Time with a Constant Average Network Hash Rate

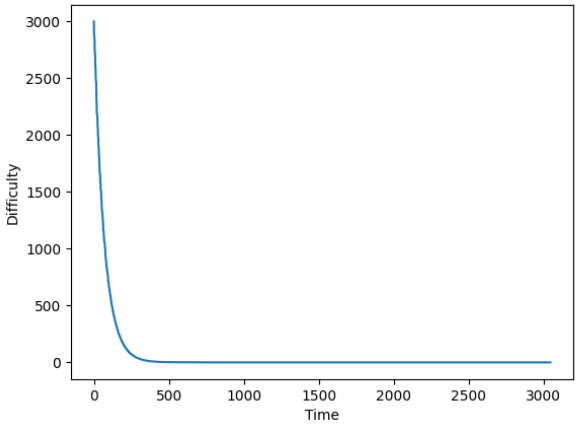

Figure 5: Difficulty with a Constant Average Network Hash Rate

Figures 4 and 5 show the simulation process when dealing with a constant average network hash rate. It is clear that the controller is capable of modifying the difficulty of the network to reach the predefined hash time setpoint value in a relatively short period of time. In a practical application, the average hash rate of the network will not remain constant as a result of various factors, including novel miners joining the network. Therefore, we analyze two key situations, namely, when the hash rate increases instantaneously at a given time step, and when the hash rate decreases instantaneously at a given time step.

When the hash rate increases instantaneously at a given moment, because of numerous miners joining at the same time, for instance. Figure 6 showcases the step increase in the average network hash rate.

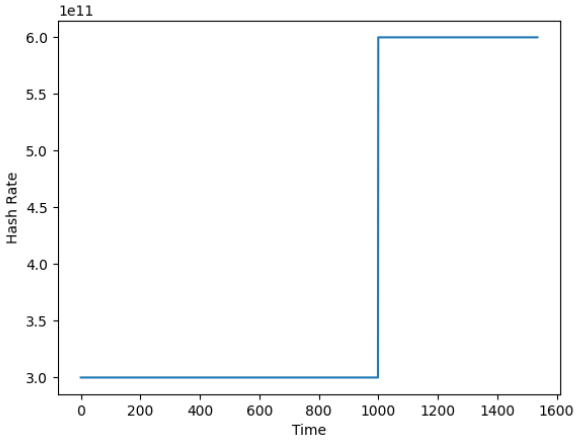

Figure 6: Step Increase in Average Network Hash Rate

The step increase displayed in Figure 6 happens after 1000 seconds in the simulation. The average network hash rate begins at 300 GH/s and increases to 600 GH/s. This increase is incredibly large and is unlikely to occur in a practical Blockchain over a short period of time. However, it is utilized to ensure the LSTM model can recover in the worst-case scenarios.

In this simulation, in Figure 7, the average network hash rate is doubled at an arbitrary time step, simulating a large step increase. As a result, we can see that the hash time dramatically decreases.

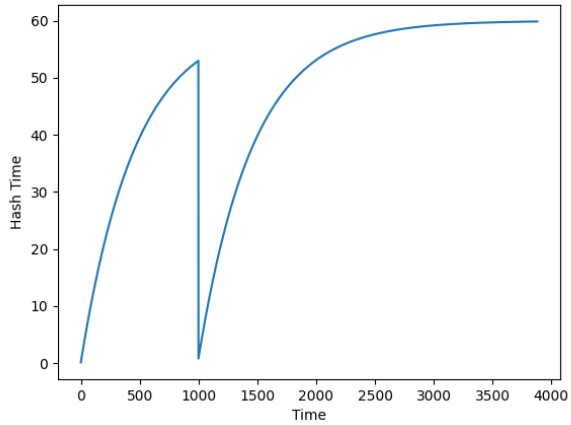

Figure 7: Hash Time with a Step Increase in Average Network Hash Rate

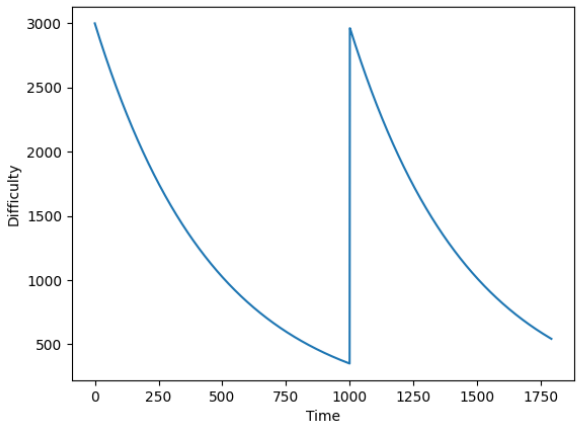

Figure 8: Difficulty with a Step Increase in Average Network Hash Rate

This can be detrimental to the network if difficulty is not modified with respect to this dynamic change. The LSTM model responds to this variance by adjusting the difficulty of the network to increase the hash time respectively. The controller is able to recover from the sudden increase in hash rate and bring the network to a predefined set point at a steady state.

In the following simulation, the average network hash rate is suddenly decreased. This can happen when a large sum of miners go inactive or drop out of the network.

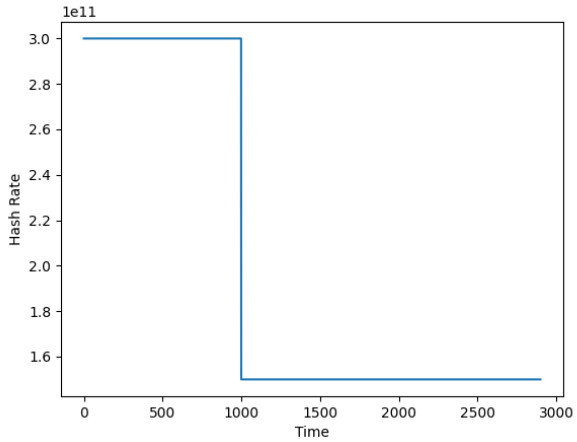

Figure 9: Step Decrease in Average Network Hash Rate

After 1000 seconds in the simulation, a step decrease in the average network hash rate is seen in Figure 9. Beginning at 300 GH/s and decreasing to 150 GH/s. This decline is enormous and unlikely to take place in a real Blockchain within a short amount of time. Again, it is used to guarantee that the LSTM model can recover in the worst-case conditions.

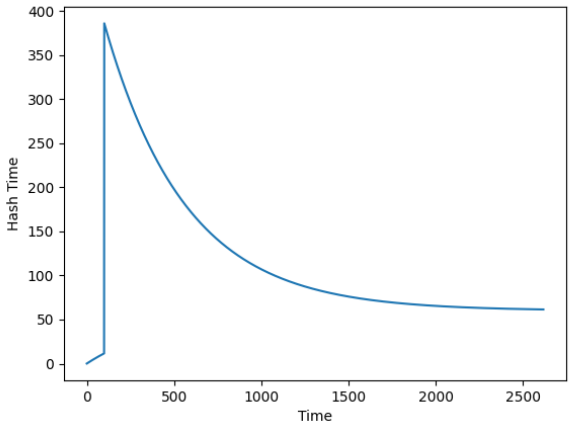

Figure 10: Hash Time with a Step Decrease in Average Network Hash Rate

The simulations presented in Figures 9 and 10 show the sudden decrease in the average network hash rate and the respective impact on the hash time. We can see that when the average network hash rate is halved, the hash time dramatically increases.

The LSTM model must make an adjustment to the difficulty immediately to allow miners to continue to mine a block in a reasonable time. Figure 10 shows how the LSTM model was able to adjust the network difficulty to, therefore, reduce hash time exponentially. The LSTM model was able to reach the predefined hash time and, in addition, dynamically adapt to sudden changes in the average network hash rate. The results clearly indicate that the performance of the model was excellent in the simulation.

To further reinforce the advantages introduced by a cognitive blockchain application, we expand on the implementation of a cognitive blockchain architecture within the fundamental methodology proposed by Alsadi et al. The proposed method detailed in [2] is based on a network of interconnected IoT devices, where data transmission between nodes is validated through the device characteristics, or fingerprint, of each node. The consensus algorithm uses collective network connectivity and computational power to validate data being appended to the chain.

Each node has individual and network-relative properties, with the set of device characteristics selected being dependent on the application space. Node responsibility is composed of four variant duties, namely challenger, challengee, witness, and validator. The challengee is the device that is attempting to transmit data, and the challenger ensures that the challengee is operating within regular node characteristics. The candidate pool is established using a pseudorandom number generator, and a novel method named stochastic consensus is used to select the witness and validator nodes.

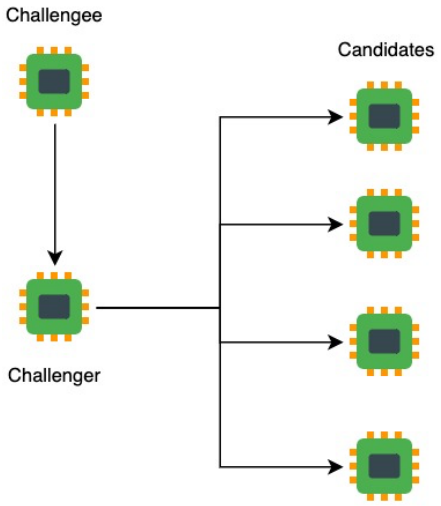

Figure 11: Proof-of-Integrity Process [2]

The fundamental purpose of employing a structure such as this is to ensure the non-anomalous behaviour of nodes in the cumulative network. The sensing of anomalous data is conducted with the employment of individual and network-relative properties. Using the exponential backoff limiting factor, when a device is flagged for anomalous behaviour, its communication frequency becomes limited, this is the core actuation of the architecture. Note this can be formulated as:

$$f = \frac{1}{b^c}, \tag{1}$$

where b is a base factor predefined in every network node and c is the number of times the suspected node has been flagged for anomalous behaviour. The device characteristics are stored in the chain and can subsequently be retrieved from it. The prioritization of resources in the network occurs when roles are assigned, and the subsequent responsibilities are realized by each node. The intelligence unit can be described by the chosen anomaly detection unit and the respective cumulative architecture. Note that even the most fundamental of computer operations, such as operational codes can reveal anomalous behaviour [17], [18]. In total, the employment of cognitive framework in this specific architecture allows for the organized implementation of adaptive behaviour in a blockchain architecture which senses anonymous behaviour and subsequently limits the communication frequency of the respective nodes in the network.

3. CONCLUSION

In this brief paper, we postulate the employment of a cognitive framework for the integration of adaptive behaviour in blockchain applications. We discuss an application using a Proof-of-Work consensus algorithm. The model senses key metrics in the network and uses an LSTM model to adjust the difficulty level of the network. The results indicate that model was capable of respectively adjusting the difficulty of the network to meet the respective network setpoints.

REFERENCES

[1] P. De Filippi, “The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies.” Rochester, NY, Sep. 14, 2016. Accessed: Nov. 06, 2022. [Online]. Available: https://papers.ssrn.com/abstract=2852689

[2] 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.

[3] S. Haykin, *Cognitive Dynamic Systems: Perception-action Cycle, Radar and Radio*. Cambridge University Press, 2012.

[4] E. Politou, F. Casino, E. Alepis, and C. Patsakis, “Blockchain Mutability: Challenges and Proposed Solutions,” *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 4, pp. 1972–1986, Oct. 2021, doi: 10.1109/TETC.2019.2949510.
[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] F. Saleh, “Blockchain without Waste: Proof-of-Stake,” *Rev. Financ. Stud.*, vol. 34, no. 3, pp. 1156–1190, Mar. 2021, doi: 10.1093/rfs/hhaa075.
[8] 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
[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] 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.
[14] 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.
[15] 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.
[16] 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.
[17] N. Alsadi, H. Karimipour, A. Dehghantanha, and G. Srivastava, “A Recurrent Attention Model for Cyber Attack Classification,” in *AI-Enabled Threat Detection and Security Analysis for Industrial IoT*, Springer, 2021, pp. 237–250.
[18] “A topic modeling-based approach to executable file malware detection.” https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12117/1211708/A-topic-modeling-based-approach-to-executable-file-malware-detection/10.1117/12.2619033.short?SSO=1 (accessed Apr. 12, 2023).