Design Methodology For Using Blockchain In Swarm Robotics

Sathishkumar Ranganathan
Universiti Malaysia Sabah,
ranganathan_sathishkumar_dk20@iluv.ums.edu.my

Muralindran Mariappan
Universiti Malaysia Sabah, Kota Kinabalu, Sabah, Malaysia
murali@ums.edu.my

Karthigayan Muthukaruppan PG
INTSYS SDN BHD Selangor, Malayasia, karthi@pgintsys.com

2021 IEEE 19th Student Conference on Research and Development (SCOReD) | 978-1-6654-0193-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/SCOReD53546.2021.9652778

***Abstract*— Swarm robotics is an evolving realm that aims to achieve a common goal in coordinated way. But the current communication and control mechanism between the robots is not secure, efficient, capable, and it is more centralized. Blockchain, a decentralized, transparent, and immutable P2P communication technology, is the right fit to pair with swarm robotics. This paper discusses the current challenges in paring blockchain with swarm robotics and the applied methodology for the amalgamation of these futuristic technologies.**

Keywords— Swarm robotics, blockchain, secured communication, consensus.

I. INTRODUCTION

In the present connected world, Industrial 4.0 transforms the technology landscape towards well connected, smarter, decentralized and more autonomous cyber-physical systems such as IIoT, AI, Data Analytics, Blockchain, Cloud, Robotics, etc. Among these, Swarm Robotics is one of the prominent technologies with potential to accomplish any complex tasks with improved accuracy and efficiency. For example, working in remote places, hazardous or dangerous environments, smart manufacturing jobs, search and rescue operations, large area surveillance, etc. etc. However, there are some challenges like reliable and secured data communication, decentralized decision making, fault tolerance, etc. are becoming more real and complex.

To address these challenges, researches have suggested Blockchain based solutions for swarm robotics [3-5, 7]. Being a distributed ledger of untrusted parties using P2P network, blockchain technology is suitable for implementing data security and decentralized decision making in swarm robotics [1, 2, 11]. However, these solutions are still lagging in important aspects like suitable consensus algorithm to validate the actual task execution and its outcome in swarm robotics network [8, 9, 11, 12]. This paper will analyze the challenges and gaps of the current solutions and outline the suitable blockchain based solution for swarm robotics.

Rest of this document is organized in sections as follows. Section 2 discuss the challenges in the current blockchain based solutions, defines the problem statement, list out the objectives and scope of this paper. Section 3 outlines the methodology of the proposed solution. Finally, Section 4 discusses the key improvements of this proposed solution.

II. CURRENT CHALLENGES

Many studies suggested using of state-machine replication or broadcast control models [37] and high-order bilateral consensus [38] for swarm robotics. While these are controlling the physical attributes of the robots, they are not considering the issues like communication security, Byzantine fault-tolerance, or Sybil attack. To overcome these gaps, studies suggested using of Blockchain based distributed consensus in swarm robotics. As the core of blockchain, consensus algorithm helps to achieve unanimity between untrusted parties in the network. This agreement is achieved to select one or more nodes that are responsible for validating and recording the transactions, generating the data blocks, and broadcast the newly generated blocks to the blockchain network. Thus, efficiency of the consensus algorithm impacts security and performance of the entire blockchain system. Most common consensus algorithms used are Proof of Work (PoW) [6], Proof of Stake (PoS) [8, 13], Delegated Proof of Stake (DPoS) [14, 15] and Practical Byzantine Fault Tolerance (PBFT) [16, 17, 30]. There are also about 30 new consensus algorithms derived based on these 4 algorithms like Ripple Protocol Consensus Algorithm (RPCA) [18], Proof of Authority (PoA) [3], Tendermint [19], Stellar [20], Proof of Bandwidth (PoB) [21], Proof of Reliability (PoR) [22], Proof of Luck (PoL) [25], and many more. These algorithms are primarily designed based on computing power of the node required to solve a complex mathematical puzzle, stake owned by the individual node or voting process among the nodes in the P2P network, etc.

By comparing pros and cons of various consensus algorithms as per the studies [1, 6, 8, 9, 11, 13], and various other works on derived consensus algorithms like Proof-of-Burn PoB [23], Proof of Activity PoA [24], Stellar Consensus Protocol SCP [26], Raft [31, 32], RPCA [33], Tendermint [34], The 2-hop consensus [35], PoSV [36], it is evident that, in one way or the other, these algorithms are falling short to support the performance and security requirements of swarm robotics networks.

A. Problem statement

Based on the above analysis, following problem statement has been derived.

1) Current solutions do not have efficient consensus algorithm to address the data validation, security, and efficiency requirements of swarm robotics network.

2) Inability to identify and isolate the malicious or malfunctioning robots in the swarm network.

B. Objective

Following are objectives of this proposal to address the current gaps in using the blockchain technology with swarm robotics network as follows:

1) To formulate an efficient consensus algorithm that meets the data validation, security, and efficiency requirements of the swarm robotics network.

a) Analyse the present blockchain implementation models to identify the gaps in using blockchain technology with swarm robotics.

b) Design and model a new consensus algorithm using blockchain that suits swarm robotics network.

c) Do simulate and verify using the new algorithm using swarm robotics simulator environment.

2) To implement a suitable security protocol to enhance the work safety.

a) Create a blockchain network using the new consensus algorithm.

b) Add simulated robots to the above blockchain network.

c) Assign robots with parallel / sequential tasks to simulate a swarm robotic network.

d) Validate and verify the new algorithm against the identified challenges and fine tuning the algorithm

e) Compare the results of the new algorithm with targeted efficiency and security requirements.

3) To develop a framework to identify and isolate the malicious or malfunctioning robots in the swarm robotics network.

a) Develop a framework encapsulating the above consensus algorithm.

b) Add simulated robots to the above blockchain network.

c) Assign one of the robots with malicious behavior in the swarm robotic network.

d) Validate the framework to identify and isolate malicious robots in the network.

C. *Scope of study*

This research is aimed to eliminate unwanted complexities that are currently associated to various layers of the blockchain architecture and outline the feasible solution to enhance the performance and security aspects of the Consensus Layer, Incentive Layer and Network and Security Layer, thus providing a significant output that addresses the gaps and improves the overall security, reliable data communication and performance. This conforms with the current trends and future technology in Manufacturing, Medical, Finance, Security, or surveillance (Civil and Military), etc. sectors.

III. METHODOLOGY

Current studies have generally proven that, because of the distributed data storage and decentralized decision making [1], blockchain technology is the right platform to store the shared data across connected devices using cryptography techniques and hash functions [1-4]. This paper is aimed to outline the possibility of creating an efficient consensus algorithm for blockchain system that suits the needs of swarm robotics network. This section briefly discusses about blockchain architecture, basics of swarm robotics, describing the experiment setup, and finally, integration of swarm robotics with suitable blockchain system.

A. *Introduction to Blockchain*

Blockchain is an important development in the distributed ledger technology. Today, blockchain is well known to the technology world. This was brought to light by Bitcoin, a digital currency exchange system [1]. This technology plays an immense role in bridging the gap in trust between mutually dependent untrusted parties. The application area this technology is ever expanding like digital currency, smarter financial markets [10] and connecting worldwide logistics chain, etc. Centralized systems are more prone to single point of failure. As blockchain is based on distributed ledger technology, it eliminates the risks related to centralized data storage like accidental data loss or modifications and secured the transactions by making the data immutable.

B. *Blockchain architecture*

Blockchain applications are built for network connected computing devices with data storage capacity. The chain structure is initiated with genesis block, a block with no predecessors followed by data blocks. Any data block in a chain will have header and body sections in it. Each data block will have an index number, block creation timestamp, hash of the previous block, a proof, and list of transactions. As shown in Fig. 1, an interlinked chain of blocks will be created by adding the hash of the previous block into the new block. This interlinked structure makes chain of blocks immutable.

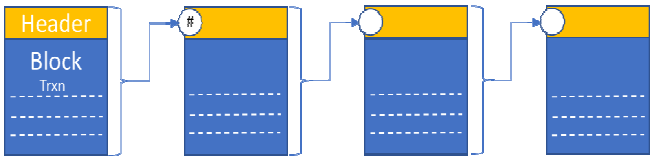

Fig. 1. Blockchain data model

As shown in Fig. 2 as per model [27], blockchain architecture will have different layers that are responsible for handling storage, communication, consensus, incentive, and business function execution. In a typical blockchain system, each connected device is a node of P2P network. Each node will locally store all agreed transactions of the network with a unique cryptographic signature [28]. It is very apparent that the current design and working principles of various layers of the blockchain technology is not a straight fit in adapting these solutions to swarm robotics [8, 29].

C. *Swarm Robotics*

Swarm robotics is an approach to manage small to large number of robots with capability to operate autonomously to perform tasks in a cooperative manner with collective effort. These robots in the swarm can perform variety of tasks with no or minimum physical modification to it. But, each individual robot in the swarm may have some limitations (sensing, processing, etc.) in terms of achieving the overall mission objective. Hence, any individual robot may not have the knowledge of all the activities happening with other participants of the swarm network. So, for the successful accomplishment of predefined network objective, any individual robotic depends on the information sharing among the participants in the network.

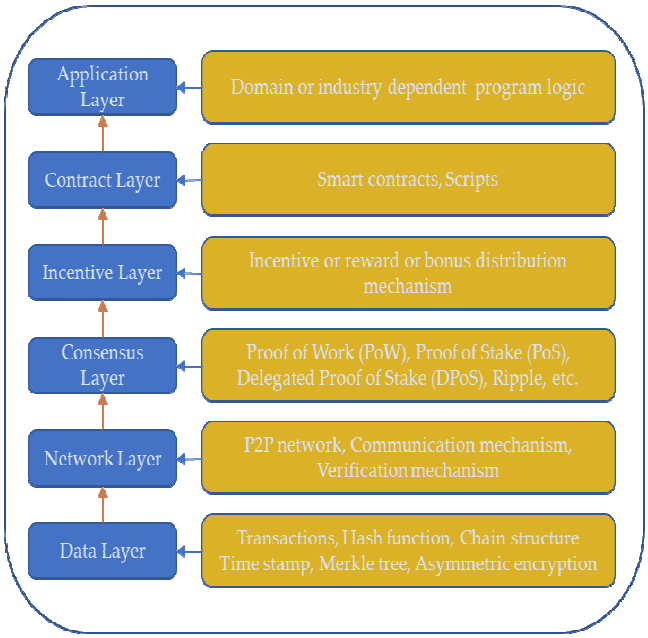

Fig. 2. Blockchain infrastructure model [11, 8]

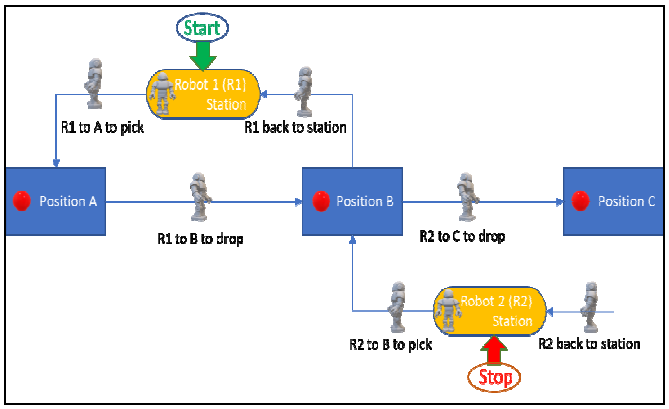

Fig. 3. Swarm robotics experiment setup without byzantine robot

D. *Experimental Setup*

Fig. 3 depicts a simple swarm robotic setup with an objective of shifting a ping pong ball from position A to B and then to C. 2 robots are used in this setup. The flow of events shown in Fig. 4 explains the details of the tasks performed by robots in a predefined sequence. Both these robots are pre-configured to perform their tasks. In this setup, the robots are working in silos and are isolated from sharing

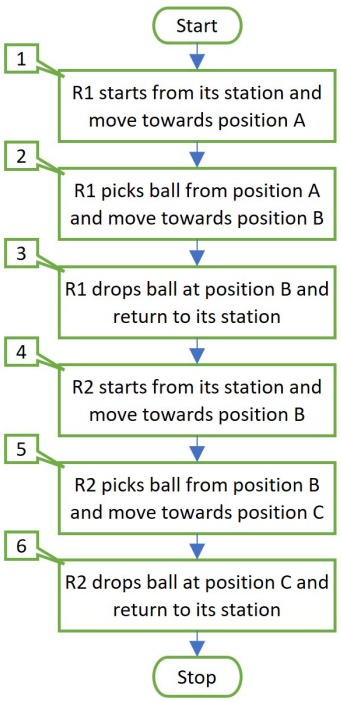

Fig. 4. Flow of events for Fig. 3

information between them. Some of the impending challenges in this setup is to ensure the safety of any individual robot, identifying faulty behaviours or byzantine robots, assuring authenticity of the information exchanged, achieving common consensus, and control or eliminate data loss, etc. The dynamic environment and volatile nature of robots in the network makes it difficult to trace the individual robot's behavior in the swarm. This leads to the need for an efficient approach in cooperative decision making and robust security solution in the swam network.

In Fig. 5, after the sequence of activities this process is expected to stop at R2 station. But Robot 3 (R3), which could be a malfunctioning, or an unexpected intruder (byzantine), enters this process and trying to shift the object from position C to D. This activity is not part of original objective. Such undefined or unexpected behavior by unauthorized participant in the swarm is the biggest security threat to the defined objectives or even to the authentic robots of the swarm. This is where the distributed, transparency and immutable nature of blockchain technology can be leveraged to address the challenges faced in swarm robotics.

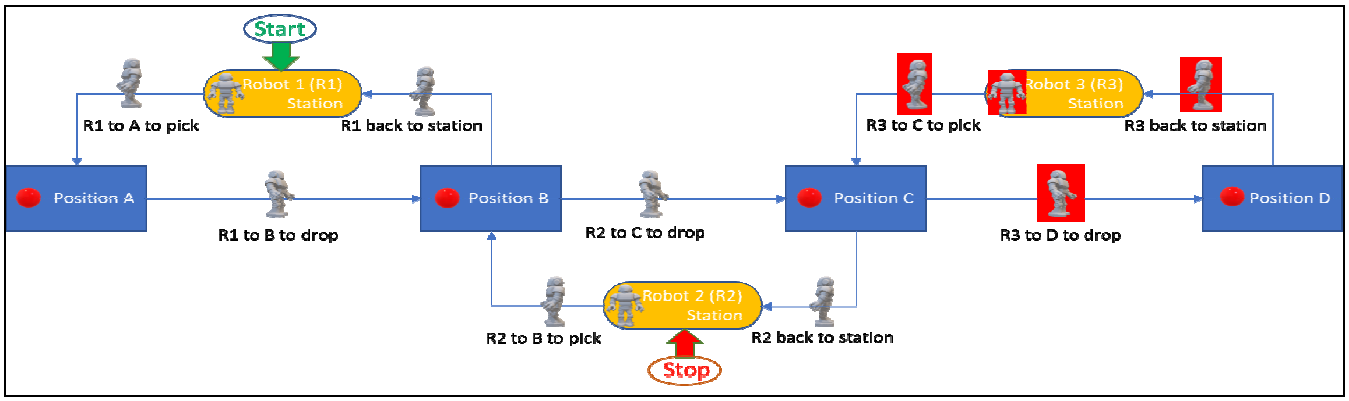

Fig. 5. Swarm robotics experiment setup with byzantine robot

E. *Swarm Robotics with Blockchain*

The setup shown in Fig. 7 is the same swarm robotic setup explained in Fig. 5 but integrated with a private blockchain network. Collective decisions making is one of the important capabilities any swarm robotic network should have. To achieve this, participants of the network need to share and aggregate their information using a distributed consensus protocol. In this integrated setup, all the legitimate robots of the swarm are considered nodes of the network, uniquely identifiable and participants of decentralised decision making. The flow chart in Fig. 6 lists down the activities in achieving the objectives of this experiment shown in Fig. 7. Steps 7 to 12 will be repeated until achieving the pre-defined objectives of the network defined in step 1. The process is expected to end there. But, when R3, an undefined participant, is trying to shift the ball from Position C to D, consensus will not be reached at step 4 and condition will be false at step 5. Approval to execute this task will not be issued by the network to R3. Instead an alert will be sent out to notify this security breach to the predefined communication channel at step 6.

IV. Discussion

This paper is aimed to eliminate unwanted complexities that are currently associated to various layers of the blockchain architecture and outline the feasible solution to enhance the performance and security aspects of these core layers that is very much suitable to swarm robotics.

A. *Consensus Layer*

Achieving consensus is the primary role of any blockchain system. So, the working principles of this layer will be designed to consider the aspects and semantics of swarm robotics, and to enhance the security and performance of the overall system.

B. *Incentive Layer*

From swarm robotics perspective, no digital currency transactions or bonus benefits sharing or stakes exchange between the network members is required. So, this layer can be very slim and suitable enough to support the appropriate logical and security needs of the swarm network. This way the overall security and performance can be improved.

C. *Network and Security Layer*

By removing unrelated complex logics from consensus and incentive layers, heavy data exchanges between the robots in the swarm will reduce to the greater extend. Thus, the network latency can be reduced, and the security and performance of the overall system can be improved.

V. Conclusion

While Swarm robotics system is one of the evolving and prominent technologies, equally, blockchain technology is well known and accepted platform for its decentralised, fault tolerance and P2P network features. Even though there are

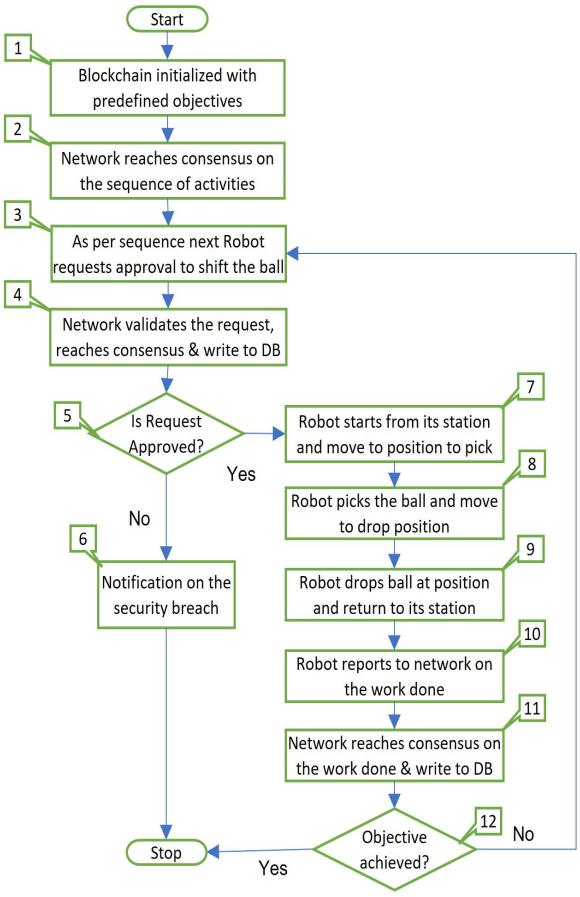

Fig. 6. Flow of events for Fig. 7

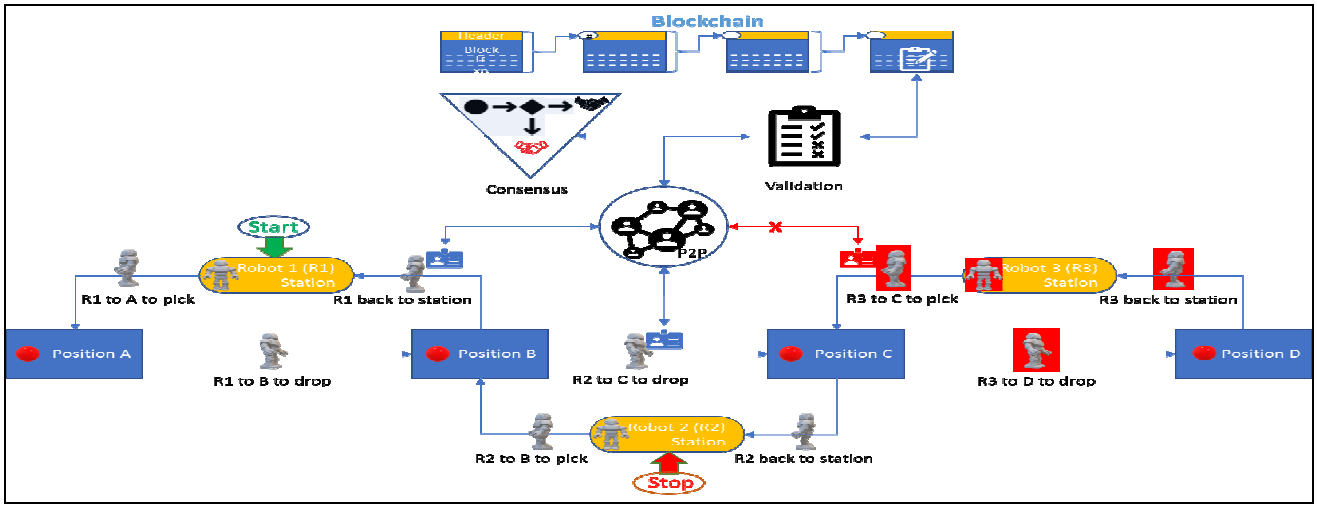

Fig. 7. Swarm robotics experiment setup with blockchain integration

TABLE I. COMPARISION OF VARIOUS SWARM IMPLEMENTATIONS

Index to measure	Non Blockchain implementation	Existing Blockchain implementation	Proposed Blockchain implementation
Mining (Block creation)	No recording or recording their activities in centralized DB. No mining processes.	Based on complex mathematical logic that requires high computing power in participating devices (node) or, stake owned by individual nodes that creates monopoly in the network.	Based on consensus between nodes as per the predefined machine objectives. Reduced complexity in the network.
Activity Validation	Happening in a centralized way. No validation of individual node activities.	Financial or point based rewards are primary factor for validating transactions as part of block creation (mining)	Eliminate reward-based network as it is not suitable for swarm robotics. All participating nodes will have equal rights in validating transactions.
Security	Based on centralized model. No commonly agreed distributed implementation.	Have no or low security checks or extremely high complex logics used to identify faulty behaviors or byzantine nodes.	Based on multi-factor authentication and distributed network authorization. Eliminate the risk of giving network control to faulty or byzantine robots.

many studies suggesting the usage of blockchain technology in swarm robotics, there are still gaps and challenges in practical application of these 2 great technologies together. As listed in the above table 1, this paper has done a comprehensive analysis on current challenges in using Non-Blockchain and Blockchain based technologies in its current form for swarm robotics and explore the opportunities for improvements. As part of this analysis, the architecture overview and core characteristics of blockchain technology has been studied. Particularly, the focus is to analyse the suitability of using the typical consensus algorithms of today's blockchain applications for swarm robotics systems. A basic swarm robotic setup has been used to explain the current challenges and use of blockchain with swarm robotics with possible improvements. Finally, in the discussion section, potential areas of improvements in performance and security aspects of blockchain for swarm robotics has been discussed.

REFERENCES

[1] Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf.

[2] Strobel V, Castelló Ferrer E, Dorigo M. Managing byzantine robots via blockchain technology in a swarm robotics collective decision-making scenario. Paper presented at: Proceedings of the 17th International Conference on Autonomous Agents and Multi Agent Systems: 541–549 International Foundation for Autonomous Agents and Multiagent Systems; 2018; Stockholm,

[3] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, “An efficient blockchain-based approach for cooperative decision making in swarm robotics,” Internet Technology Letters, vol. 3, no. 1, p. e140, 2020

[4] Ferrer EC. The blockchain: a new framework for robotic swarm systems. Paper presented at: Proceedings of the Future Technologies Conference: 1037–1058 Springer; 2018; Vancouver, Canada.

[5] Lopes V, Alexandre LA, Pereira N. Controlling robots using artificial intelligence and a consortium blockchain. arXiv. 2019;arXiv:1903.00660.

[6] Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. Oleksandr Vashchuk, Roman Shuwar. Electronics and information technologies. 2018. Issue 9. P. 106–112.

[7] E. Castello Ferrer. 2016. The blockchain: A new framework for robotic swarm systems. pre-print (2016). arXiv:1608.00695v3

[8] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[9] Michael Neuder, Daniel J. Moroz, Rithvik Rao and David C. Parkes, “Selfish Behavior in the Tezos Proof-of-Stake Protocol”, 2019, arXiv:1912.02954v4 [cs.CR]

[10] G. Bansal, V. Hassija, V. Chamola, N. Kumar, and M. Guizani, “Smart stock exchange market: A secure predictive decentralised model,” 2019, pp. 9–13.

[11] Alladi, Tejasvi & Chamola, Vinay & Sahu, Nishad & Guizani, Mohsen. (2020). Applications of Blockchain in Unmanned Aerial Vehicles: A Review. Vehicular Communications. 10.1016/j.vehcom.2020.100249.

[12] Iuon-Chang Lin and Tzu-Chun Liao2. A Survey of Blockchain Security Issues and Challenges. International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 (DOI: 10.6633/IJNS.201709.19(5).01).

[13] Vasin, Pavel, “Blackcoin’s proof-of-stake protocol v2,” URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf 71 (2014).

[14] Dantheman, “DPOS Consensus Algorithm - The Missing White Paper,” [Online]. available: https://steemit.com/DPoS/@dantheman/DPoS-consensus-algorithm-this-missing-white-paper,2016.

[15] D. Larimer, “Delegated proof-of-stake (dpos),” Bitshare whitepaper, 2014.

[16] M. Castro, B. Liskov et al., “Practical byzantine fault tolerance,” in OSDI, vol. 99, no. 1999, 1999, pp. 173–186.

[17] Castro, M., & Liskov, B. (2002). Practical Byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), 20(4), 398-461.

[18] D. Schwartz, N. Youngs, A. Britto, “The Ripple Protocol Consensus Algorithm,” [Online]. available: https://ripple.com/files/ripple_consensus_whitepaper.pdf, 10 Apr. 2018.

[19] J. Kwon, “Tendermint: Consensus without mining,” Draft v. 0.6, fall, vol. 1, p. 11, 2014.

[20] D. Mazieres, “The stellar consensus protocol: A federated model for internet-level consensus,” Stellar Development Foundation, p. 32, 2015.

[21] M. Ghosh, M. Richardson, B. Ford, and R. Jansen, “A torpath to torcoin: Proof-of-bandwidth altcoins for compensating relays,” NAVAL RESEARCH LAB WASHINGTON DC, Tech. Rep., 2014.

[22] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, “Permacoin: Repurposing bitcoin work for data preservation,” in 2014 IEEE Symposium on Security and Privacy. IEEE, 2014, pp. 475–490.

[23] P4Titan. Slimcoin a peer-to-peer crypto-currency with proof-of-burn, May-2014. https://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_whitepaper.pdf.

[24] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. 2014. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract]y. SIGMETRICS Perform. Eval. Rev. 42, 3

(December 2014), 34–37. DOI:https://doi.org/10.1145/2695533.2695545.

[25] M. Milutinovic, W. He, H. Wu, et al., “Proof of Luck: An Efficient Blockchain Consensus Protocol,”// the 1st Workshop. ACM, 2016.

[26] D. Mazières, “The stellar consensus protocol: A federated model for internet-level consensus,” [Online]. available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.696.93&amp=&rep=rep1&amp=&type=pdf, 14 July 2015.

[27] Y. Yuan, F. Y. Wang, “Blockchain: The State of the Art and Future Trends,” Acta Automatica Sinica, vol. 42, no. 4, pp. 481−494, 2016.

[28] M. Walport, “Distributed Ledger Technology: beyond blockchain,” UK Government, 19 Jan. 2016.

[29] P. L. Zheng, Z. B. Zheng, X. P. Luo, X. P. Chen, X. Z. Liu, “A detailed and real-time performance monitoring framework for blockchain systems,” Proceedings of the 40th International Conference on Software Engineering in Practice. Gothenburg, Sweden: ACM, pp. 134-143, 2018.

[30] M. Castro, B. Liskov, “Practical byzantine fault tolerance and proactive recovery,” ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398-461, 2002.

[31] D. Ongaro, J. K. Ousterhout, “In search of an understandable consensus algorithm,” Proc. 2014 USENIX Annual Technical Conference, pp. 305-319, Mar. 2015.

[32] “Raft-based consensus for Ethereum/Quorum,” [Online]. available: https://github.com/jpmorganchase/quorum/blob/master/docs/raft.md.

[33] D. Schwartz, N. Youngs, A. Britto, “The Ripple Protocol Consensus Algorithm,” [Online]. available: https://ripple.com/files/ripple_consensus_whitepaper.pdf, 10 Apr. 2018.

[34] J. Kwon, “Tendermint: Consensus without mining,” [Online]. available: https://cdn.relayto.com/media/files/LPgoWO18TCeMIggJVakt_tenderrmint.pdf, 2014.

[35] T. Duong, L. Fan, H. S. Zhou, “2-hop blockchain: Combining Proof-of-Work and Proof-of-Stake Securely,” [Online]. available: https://eprint.iacr.org/2016/716.pdf, 15 Apr. 2017.

[36] L. Ren, “Proof of Stake Velocity: Building the Social Currency of the Digital Age,” [Online]. available: https://www.reddcoin.com/papers/PoSV.pdf, Apr. 2014.

[37] M.H. Mohamad Nor, Z.H. Ismail and M.A. Ahmad, "Broadcast control of multi-robot systems with norm-limited update vector", International Journal of Advanced Robotic Systems, July 2020.

[38] Liu, D, Zong, C, Wang, D, et al. Multi-robot formation control based on high-order bilateral consensus. Measure Control 2020; 53(5): 983–993.