IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Securing cyber physical systems using feather blockchain consensus model

Mr. Shital Agrawal [1]
Research Scholar [1]
[1]Shri JJT University

Dr. Shailesh Kumar [2]
Associate Professor [2]
[2]Shri JJT University

Abstract: Cyber physical systems (CPS) are associated at remote spots, because of which their computational and capacity abilities are restricted. These gadgets are sent in modern conditions where everyday openness, actual observation and persistent administration is unimaginable. Because of these entrance impediments, the conveyed gadgets can be undermined by undesirable foes, who can infuse spying, satirizing and other hub level deficiencies. To lessen the likelihood of these assaults, this text proposes a feature proof-of-trace (FPoT) agreement system, that can be coordinated with new and existing CPS organizations. The agreement model uses follow data from 'k' irregular adjoining hubs during block creation. Since all checks are done on the CPS centre point hub, the follow data is added to the square with practically no confirmation on hub side. This decreases computational intricacy while adding the square to the blockchain. The convention utilizes blockchain for information check and detectability on the center point side, which guarantees that all correspondences inside the organization are gotten, and flawed hubs are followed back with high exactness. It was likewise seen that the quill blockchain organization has 15% better speed when contrasted and standard agreement models, 25% better throughput, 16% better energy proficiency, and 8% better bundle conveyance proportion when contrasted and cutting-edge models under a similar organization condition.

Keywords: CPS, blockchain, energy, security, proof-of-trace

1. Introduction

Further developing security for Industrial CPS networks is a multidomain task, which includes protection safeguarding, validation, access control, demonstrating of key trade instruments, sealed framework plan, and so forth To play out this errand, a wide assortment of safety models are proposed by scientists previously. These security frameworks incorporate, information encryption frameworks, public key foundation (PKI) frameworks, hashing models for information approval, rule-based models for versatile access control, and so on These conventions are sent at various CPS layers, which incorporates, edge layer, stage layer, and undertaking layer. Every one of these layers are additionally isolated into different subcomponents as seen from figure 1, wherein sensors, actuators, validation gadget, information stockpiling gadget, application developer's connection point, and so forth are seen.

Utilizing this model, it tends to be seen that different CPS parts including clinical, power, vehicle, planned operations, consideration organizations, and so on are developed of sensors for perusing part information, and actuators for controlling these parts. Information from these gadgets is given to a CPS passage, from where it comes to at stage level. The stage level information is given to different investigation, and representation models, wherein stream-based handling utilized. At long last, the examined and pictured stream information is given to big business arrangements, where different warehousing, high request investigation, and work process handling activities are performed.

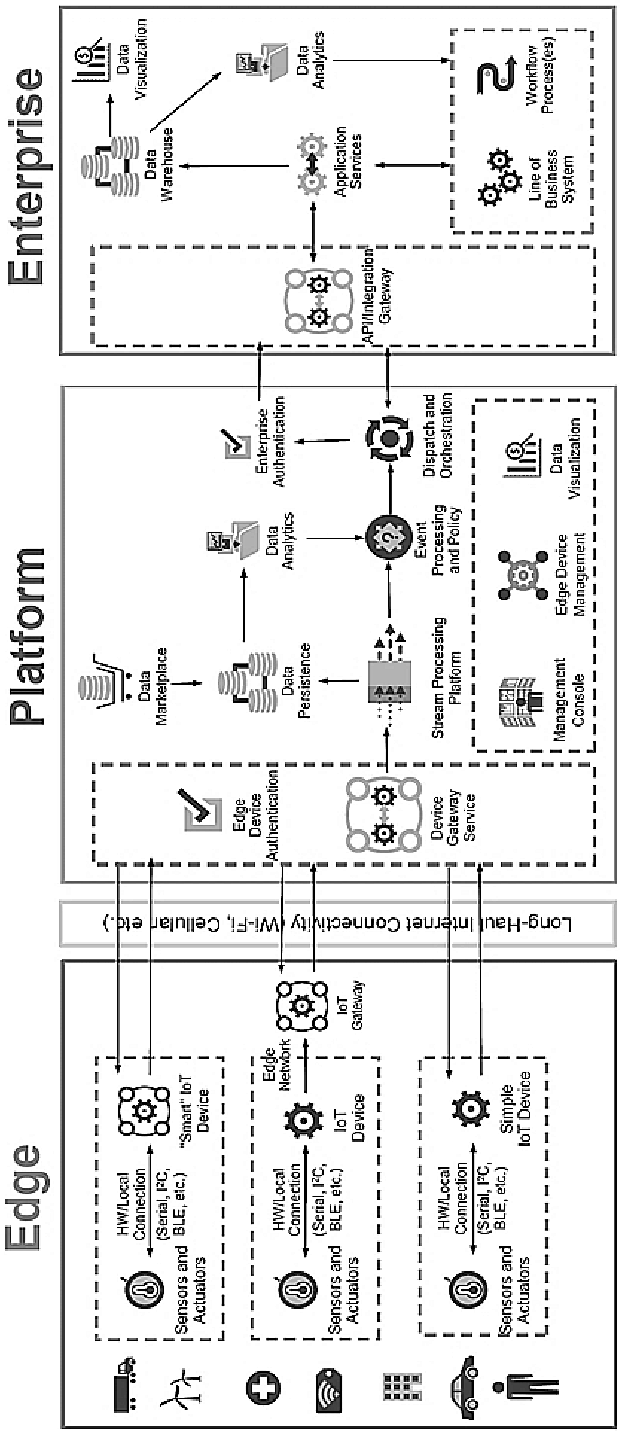

Figure 1. A typical CPS security model

At every one of these layers, require different client confirmation, access control, information security, and trust-based information update convention models. To give these abilities, a wide assortment of framework models are created by scientists and digital examiners. From the audit, it is seen that blockchain based models outflank different models as far as generally speaking security, because of their straightforwardness, changelessness, discernibility, and disseminated processing abilities. According to a CPS viewpoint, information approval before incitation is one of the main parts of framework plan. Since in Industrial conditions, miniscule information detecting and approval blunders can cause huge framework disappointments. To stay away from this, solid executions of agreement models are required, in light of the fact that, agreement models further develop information approval capacities by confirming information accuracy from an enormous number of verifier hubs. Spurred by this, the hidden work proposes an original quill verification of-follow (FPoT) agreement blockchain for further developed detectability and information approval. To plan this FPoT model, a wide assortment of agreement and security models were surveyed. Conversation about these models, alongside their subtleties, benefits, downsides, and future examination bearings can be alluded from the following part of this text. This is trailed by conversation of exploration procedure applied to execute the FPoT agreement model. This conversation is trailed by prologue to agreement, and its utilization case for blockchain, which goes before plan of the FPoT model. Afterward, this text examines parametric outcome examination of the proposed model, and its correlation with different best in class agreement conventions as applied to a similar organization. At last, this text closes for certain fascinating perceptions about the proposed model, and prescribes different techniques to further develop its presentation.

2. Literature review

A wide assortment of agreement models are created by analysts throughout the long term. For example, the models in [1, 2, 3] use asset cutting, appointed verification of stake by means of downsizing hubs, and pontoon agreement models. These models depend on using specific verifier hub boundaries to appraise assuming that the given square should be checked or not. Every one of these models have innate restrictions of slow speed, and high energy utilization because of intricacy of agreement estimations. To assess their exhibition, and inside further develop it, the work in [4, 5] can be alluded. Here, different blockchain agreement models alongside suggested advancement techniques can be noticed. It is referenced that focal agreement estimations have preferable productivity over appropriated ones, which is the principle inspiration of this text. A strategy that utilizes this agreement approach can be seen from [6], wherein various tokens confirmation of stake (MPoS) is utilized to further develop generally framework effectiveness. Comparable models are seen in [7, 8, 9, 10, 11], where scientists have investigated Byzantine Consensus, programming watch augmentations

(SGX) for further developing agreement execution, Wi-Fi-Dependent Consensus, credit instruments in agreement and sharding based agreement. This multitude of models are material to explicit situations, and hence have restricted constant immaterialness. To eliminate this disadvantage, the work in [12] proposes a General Secure Consensus Scheme (GCGS) which depends on hub believability. The model is seen to outflank proof of-work (PoW), evidence of-stake (PoS) [13], proof of-trust (PoT) [15], and chart based [15] models as far as QoS and security execution.

Compromises between time prerequisite and memory necessity should likewise be thought of while planning agreement models. The work in [16] half breed of PoW, and Proof-of-Memory (PoM) models for upgrading deferral and memory execution of blockchain models. The model's application is restricted as far as number of upheld hubs, and number of upheld networks, which is because of its limit as far as streamlining block confirmation delay. To work on this presentation, Byzantine-Based Blockchain Consensus [17], Mixed Byzantine Fault Tolerance (MBFT) [18], blockchain relevance structure [19], blockchain-based believed information the executives plot [20], Zyzzyva agreement [21], and Proof of Block and Trade (PoBT) [22] can be alluded. These models help with further developing agreement execution by specifically offloading confirmation calculations among verifiers and cloud hubs. Models like Vague Sets based Delegated Proof of Stake [25], blockchain–IoT-based food detectability framework [24], and rest booking agreement [25]are expansions to existing agreement models, yet target working on computational productivity by lessening redundancies in existing confirmation procedures. In light of this audit, the proposed model is intended to have semi-brought together methodology, which helps with further developing QoS execution, while keeping up with high assault strength, and adaptation to non-critical failure capacities. Plan of the proposed model is done by means of a progression of smart advances, which can be seen from the following segment of this text.

3. Proposed novel feather proof-of-trace (FPoT) consensus blockchain for improved traceability

Adding further developed detectability to existing blockchain models will permit scientific specialists and organization originators to traceback information changes, course changes, network design changes, and some other kind of substance change which may influence (or upset) ordinary organization working. To play out this undertaking, an original FPoT agreement model plan is portrayed in this part. Every one of these models are depicted in discrete sub-segments, which will permit per-users to duplicate them (to some degree or entire), for their CPS organizations. This multitude of sub models use a particular square design, which can be seen from table 1, wherein inner square parts are portrayed.

Prev. Main Hash	Prev. Entity Hash	Source IP	Dest. IP
Entity ID	Entity Data	Timestamp	Main Nonce
Entity Nonce	Main Data	Verifier nodes	Meta Data

Table 1. Internal block structure used for the FPoT based blockchain

Every one of these parts fill a particular need during FPoT agreement, which can be depicted as follows,

- Prev. Principal Hash, will be hash of the past block put away in the blockchain

- Prev. Substance Hash, will be hash of the past element (information, course, area, and so on) block information put away with the hubs.

- Source IP, Destination IP, stores IP addresses for source and objective hubs.

- Element ID, Identifier of the substance which is being put away on the blockchain

- Element information, information of element put away on the blockchain

- Timestamp, is the time moment at which this information was put away.

- Fundamental Nonce, will be nonce number for the principle blockchain

- Substance nonce, will be nonce number for the element being put away

• Principal Data, stores the fundamental information which is being put away on the blockchain

• Verifier hubs, comprises of a rundown of hubs which are utilized for block confirmation.

• Meta information, stores any meta information which is required for putting away element information or fundamental information

Design of the proposed model is depicted in figure 2 as follows,

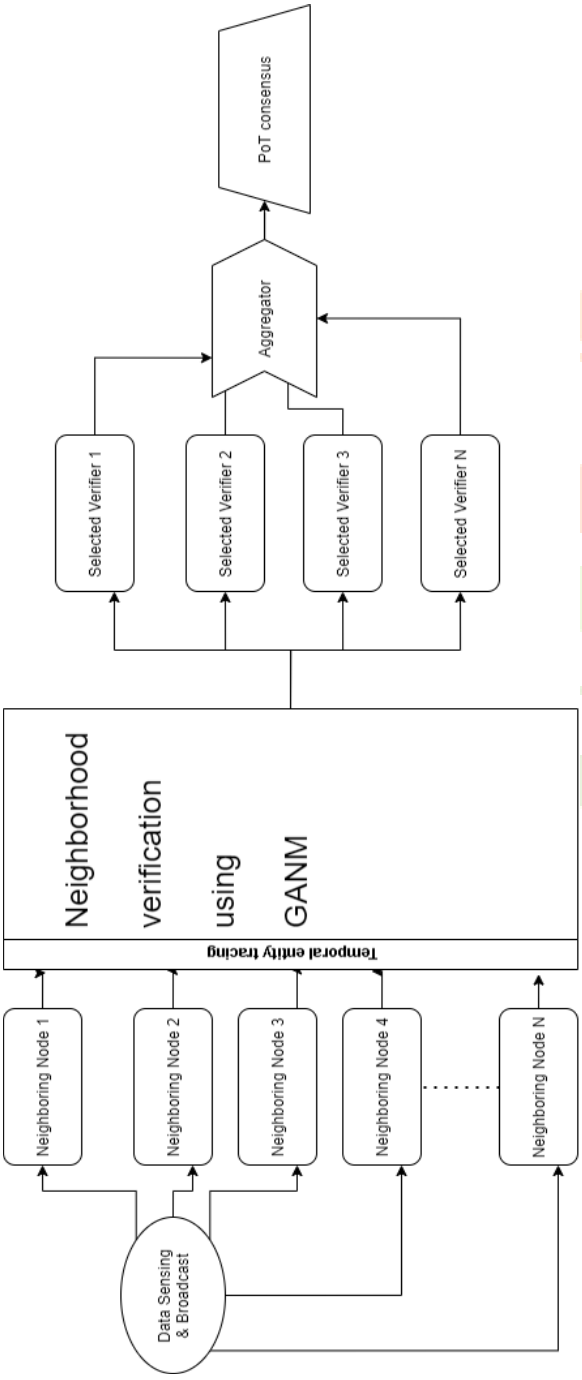

Figure 2. Overall architecture of the proposed model

The GANM block gives a rundown of verifier hubs that can be utilized for high velocity, low power, and high throughput confirmation. To play out this errand, every one of the chose verifier hubs are gone through a low intricacy information really looking at motor. Aftereffects of this motor are amassed utilizing an aggregator model to confirm whether the given square should be added to the blockchain or should be disposed of. Design of the whole interaction can be seen from figure 3, wherein generally process, beginning from block confirmation solicitation to definite check reaction should be visible. The total layer gives its results to the PoT agreement model, which permits the framework to have better recognizability. Total layer inputs all the chose verifier hubs, and following the provided steps to perform last confirmation,

- Neighborhood blockchains of all verifier hubs is unscrambled, and all squares are decoded
- Blocks with same Source IP-Destination IP-Entity-ID sets are assembled, and bunch groups are shaped
- For each gathering bunch, the accompanying system is performed,
    - ○ Evaluate group variance (G_V) of entity data using equation 1,

$$G_V = \sqrt{\frac{\sum_{i=1}^{N_C}(ED_i - \sum_{j=1}^{N_C}\frac{ED_j}{N_C})^2}{N_C - 1}} \ldots (1)$$

Where, ED, N_C represent entity data, and number of nodes in the given cluster respectively.

- Evaluate the value of G_V for all groups having same source IP address, and then evaluate value of group source variance threshold using equation 2,

$$G_{TH_S} = WoV_{src} * \sum_{i=1}^{N_S} G_{V_i} * \frac{G_{LF}}{N_S} \ldots (2)$$

Where, $G_{TH_S}, G_V, and\ N_S$ represent Group source variance threshold, Group variance, and number of Groups having same source IP.

- Repeat this process for all groups, and then evaluate the final validation threshold using equation 3,

$$V_{TH} = \sum_{i=1}^{N_{UIP}} \frac{G_{TH_{S_i}}}{N_{UIP}} \ldots (3)$$

Where, $V_{TH}, N_{U_{IP}}$ represents validation threshold, and number of unique source IPs obtained from all the verifiers.

- Evaluate variance for the given source IP from which block addition request was initiated using its entity data values in equation 1.
- Accept the block addition request if this variance is lower than V_{TH}, else discard this block.
- If the block is verified, then increase value of WoV for the given source using equation 4, else reduce its value using equation 5,

$$WoV_{new} = WoV_{old} + \frac{1}{G_{LF}} \dots (4)$$

$$WoV_{new} = WoV_{old} * G_{LF} \dots (5)$$

- Due to this drastic variation in weight of variance factor for each node, a reward and penalty mechanism is modelled. This mechanism allows the nodes to maintain high value of WoV for effective verification.

Due to this adaptive process, after each verification the value for weight of variance is updated, thereby improving quality of verification. Moreover, due to use of temporary blockchains, and then merging them with main blockchain, the system’s traceability is improved, thereby making it resilient against any kind of data-level or entity-level attacks. The performance analysis of the proposed model is done via observation of end-to-end delay, energy efficiency, throughput, packet delivery ratio, and jitter parameters. This evaluation can be observed from the next section of this text.

4. Results and statistical comparison

Because of fuse of quill stochastic displaying, the proposed FPoT model should have lower postponement, and better energy productivity. This is going with alleviation of different assaults and blames because of joining of blockchain. To confirm this conduct, the proposed model was contrasted and [1], [15], and [25], which grandstand comparative agreement comportment.For the basic organization setup, blockchain correspondences were started. These interchanges were changed somewhere in the range of 20 and 200 linearly, and execution boundaries were assessed. To test network security, number of aggressors were fluctuated from 1% to 10% to cover different assaults. During the assault stage, mean qualities for energy utilization (E), packet delivery ratio (PDR), delay (D), throughput (T), and delay jitter (JD) were assessed. Flawed hubs were likewise infused into the organization, and comparable mean execution esteems were assessed. Every one of these assessments can be seen from the accompanying sub-areas, wherein crude execution of various agreement conventions, execution of these conventions enduring an onslaught, and execution of these conventions under shortcoming conditions should be visible.

As far as crude QoS execution the proposed model is seen to beat agreement models portrayed in [1], [15], and [25]. Number of blockchain demands for correspondence (NC) are shifted somewhere in the range of 10 and 100, and normal QoS esteems for every boundary. Due to averaging, issues like arbitrary hub situation, irregular correspondence, and parcel drops are displayed to average out, and drop their impacts on definite organization execution. Following this cycle, the qualities for start to finish delay for various agreement models are assessed and arranged in table 3 as follows,

NC	D (ms) [1]	D (ms) [15]	D (ms) [25]	D (ms) Proposed
20	0.97	1.10	1.20	0.87
30	1.05	1.20	1.33	0.94
40	1.19	1.30	1.42	1.02
50	1.23	1.36	1.47	1.05
60	1.25	1.40	1.54	1.10
70	1.34	1.51	1.64	1.17
80	1.43	1.60	1.79	1.31
90	1.50	1.88	2.21	1.67
100	1.94	2.65	2.99	2.19
110	2.91	3.28	3.55	2.54
120	3.11	3.48	3.79	2.74

130	3.27	3.76	4.19	3.05
140	3.64	4.38	4.82	3.48
150	4.38	4.93	5.36	3.87
180	4.65	5.30	5.93	4.32
200	5.07	6.33	6.86	4.62

Table 3. Mean end-to-end delay for different consensus models

The proposed FPoT agreement model has 10% better execution when contrasted and [1], 25% better execution when contrasted and [15], and practically 45% lower postpone when contrasted and [25]. This is because of the low intricacy displaying utilized by the proposed strategy, which permits the framework model to lessen number of superfluous hub level calculations, accordingly diminishing deferral of agreement. Comparable perceptions are ruined energy execution, and arranged in table 4 as follows,

NC	**E (mJ)** **[1]**	**E (mJ)** **[15]**	**E (mJ)** **[25]**	**E (mJ)** **Proposed**
10	1.81	3.35	3.11	2.33
15	2.81	4.12	3.62	2.65
20	2.85	4.29	3.79	2.78
25	3.07	4.52	3.99	2.95
30	3.15	4.81	4.27	3.14
35	3.47	5.12	4.49	3.30
40	3.58	5.32	4.67	3.42
45	3.73	5.53	4.85	3.56
50	3.88	5.75	5.04	3.71
55	4.04	5.93	5.26	3.88
60	4.13	6.36	5.69	4.19
65	4.59	7.01	6.12	4.47
70	5.04	7.10	6.13	4.47
75	4.72	6.98	6.13	4.39
90	4.89	7.24	5.41	3.58
100	5.06	8.16	6.08	4.25

Table 4. Mean energy used for different consensus models

As noticed, the proposed FPoT agreement model has 9% better execution when contrasted and [1], 40% better execution when contrasted and [15], and practically 20% lower energy utilization when contrasted and [25]. This is because of the low intricacy displaying utilized by the proposed strategy, which permits the framework model to decrease number of pointless hub level calculations, accordingly lessening energy utilization required for agreement. This helps with further developing lifetime of the organization subsequently further developing relevance of the proposed model for low energy CPS organizations. Comparative perceptions are ruined throughput execution, and organized in table 5 as follows,

NC	**T (kbps)** **[1]**	**T (kbps)** **[15]**	**T (kbps)** **[25]**	**T (kbps)** **Proposed**
10	336.39	352.94	408.62	412.11
15	343.13	357.05	412.54	415.70
20	344.22	358.59	414.68	418.10
25	345.95	361.49	418.24	421.86
30	349.87	365.09	422.16	425.79
35	352.85	368.16	425.72	429.38
40	355.82	371.24	429.47	432.97

45	358.81	374.32	433.03	436.56
50	361.78	377.40	436.59	440.15
55	364.76	380.48	440.15	443.75
60	367.74	383.55	443.72	447.34
65	370.72	386.63	447.28	450.93
70	373.69	389.88	450.84	454.52
75	376.68	392.96	454.40	458.11
90	379.65	396.04	457.97	461.70
100	382.63	403.86	461.53	468.71

Table 5.Mean throughput for different consensus models

As noticed, the proposed FPoT agreement model has 20% better execution when contrasted and [1], 15% better execution when contrasted and [15], and practically 8% higher throughput when contrasted and [25]. This is because of the low intricacy demonstrating utilized by the proposed strategy, which permits the framework model to decrease number of superfluous hub level calculations, subsequently lessening delay during agreement. This helps with further developing information pace of the organization, consequently further developing relevance of the proposed model for fast and high transfer speed CPS organizations. Comparable perceptions are ruined PDR execution, and arranged in table 6 as follows,

NC	PDR (%) [1]	PDR (%) [15]	PDR (%) [25]	PDR (%) Proposed
10	73.63	73.73	74.62	79.97
15	75.12	74.58	75.35	80.68
20	75.36	74.88	75.72	81.15
25	75.73	75.50	76.38	81.86
30	76.61	76.26	77.12	82.62
35	77.25	76.90	77.77	83.32
40	77.89	77.54	78.42	84.02
45	78.55	78.18	79.07	84.71
50	79.20	78.83	79.72	85.41
55	79.86	79.48	80.37	86.12
60	80.50	80.12	81.03	86.81
65	81.16	80.78	81.68	87.50
70	81.81	81.42	82.34	88.21
75	82.47	82.06	82.98	88.91
90	83.11	82.72	83.64	89.60
100	83.77	83.36	84.29	90.32

Table 6. Mean packet delivery ratio for different consensus models

As noticed, the proposed FPoT agreement model has 8% better execution when contrasted and [1], 9% better execution when contrasted and [15], and practically 8% higher PDR when contrasted and [25]. This is because of the low intricacy demonstrating utilized by the proposed technique, which permits the framework model to lessen number of pointless hub level calculations, along these lines decreasing number of superfluous bundles conveyed during check. In this manner, the proposed model has better generally QoS when contrasted and standard agreement models.

5. Conclusion

In view of the outcome investigation, it very well may be seen that the proposed FPoT agreement model has 10% better execution when contrasted and [1], 20% better execution when contrasted and [15], and practically 18% lower defer when contrasted and [25] under typical situation, assault situations, and flawed hub situations. This is because of the low intricacy demonstrating utilized by the proposed strategy, which permits the framework model to diminish number of pointless hub level calculations, accordingly decreasing deferral during agreement. This helps with further developing information pace of the organization, subsequently further developing relevance of the proposed model for high velocity and high transmission capacity CPS organizations. Additionally, the proposed FPoT agreement model has 30% better execution when contrasted and [1] under typical situation, assault situations, and flawed hub situations, 25% better execution when contrasted and [15], and practically 35% lower energy utilization when contrasted and [25] under ordinary situation, assault situations, and broken hub situations; and has 8% better execution when contrasted and [1], 6% better execution when contrasted and [15], and practically 39% higher throughput when contrasted and [25] under typical situation, assault situations, and defective hub situations. At last, the proposed FPoT agreement model has 20% better execution when contrasted and [1], 15% better execution when contrasted and [15], and practically 8% higher throughput when contrasted and [25] under typical situation, assault situations, and defective hub situations. Which grandstands a wide space of pertinence, with high assault flexibility, and high adaptation to internal failure abilities.

6. Future Work

Execution of the proposed model can be reached out by considering auxiliary QoS boundaries like steering load, computational proficiency, memory use on base station, energy decency, throughput reasonableness, and so on This will permit scientists to improve gauge of adjusted execution measurements, accordingly further aiding decreased deferral, low intricacy, and profoundly effective agreement convention plan. Transformation of sidechaining and AI models can likewise be tried for keeping up with balance between QoS to security execution.

7. References

[1] M. Hu, T. Shen, J. Men, Z. Yu and Y. Liu, "CRSM: An Effective Blockchain Consensus Resource Slicing Model for Real-Time Distributed Energy Trading," in IEEE Access, vol. 8, pp. 206876-206887, 2020, doi: 10.1109/ACCESS.2020.3037694.

[2] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong and M. Zhou, "Appointed 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.

[3] D. Huang, X. Mama and S. Zhang, "Execution Analysis of the Raft Consensus Algorithm for Private Blockchains," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 172-181, Jan. 2020, doi: 10.1109/TSMC.2019.2895471.

[4] Xiao, Yang and Zhang, Ning and Lou, Wenjing and Hou, Y.. (2019). A Survey of Distributed Consensus Protocols for Blockchain Networks.

[5] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[6] Y. Ache, "A New Consensus Protocol for Blockchain Interoperability Architecture," in IEEE Access, vol. 8, pp. 153719-153730, 2020, doi: 10.1109/ACCESS.2020.3017549.

[7] W. Hu, Y. Hu, W. Yao and H. Li, "A Blockchain-Based Byzantine Consensus Algorithm for Information Authentication of the Internet of Vehicles," in IEEE Access, vol. 7, pp. 139703-139711, 2019, doi: 10.1109/ACCESS.2019.2941507.

[8] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei and B. Chen, "When Blockchain Meets SGX: An Overview, Challenges, and Open Issues," in IEEE Access, vol. 8, pp. 170404-170420, 2020, doi: 10.1109/ACCESS.2020.3024254.

[9] C. E. Ngubo and M. Dohler, "Wi-Fi-Dependent Consensus Mechanism for Constrained Devices Using Blockchain Technology," in IEEE Access, vol. 8, pp. 143595-143606, 2020, doi: 10.1109/ACCESS.2020.3014287.

[10] Y. Wang et al., "Investigation of Blockchains' Consensus Mechanism Based on Credit," in IEEE Access, vol. 7, pp. 10224-10231, 2019, doi: 10.1109/ACCESS.2019.2891065.

[11] S. Kim, "Two-Phase Cooperative Bargaining Game Approach for Shard-Based Blockchain Consensus Scheme," in IEEE Access, vol. 7, pp. 127772-127780, 2019, doi: 10.1109/ACCESS.2019.2939778.

[12] J. Wang, Y. Ding, N. N. Xiong, W. Yeh and J. Wang, "GSCS: General Secure Consensus Scheme for Decentralized Blockchain Systems," in IEEE Access, vol. 8, pp. 125826-125848, 2020, doi: 10.1109/ACCESS.2020.3007938.

[13] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Verification of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," in IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010.

[14] X. Zhu, Y. Li, L. Tooth and P. Chen, "An Improved Proof-of-Trust Consensus Algorithm for Credible Crowdsourcing Blockchain Services," in IEEE Access, vol. 8, pp. 102177-102187, 2020, doi: 10.1109/ACCESS.2020.2998803.

[15] K. Tsoulias, G. Palaiokrassas, G. Fragkos, A. Litke and T. A. Varvarigou, "A Graph Model Based Blockchain Implementation for Increasing Performance and Security in Decentralized Ledger Systems," in IEEE Access, vol. 8, pp. 130952-130965, 2020, doi: 10.1109/ACCESS.2020.3006383.

[16] M. J. Mihaljevic, "A Blockchain Consensus Protocol Based on Dedicated Time-Memory-Data Trade-Off," in IEEE Access, vol. 8, pp. 141258-141268, 2020, doi: 10.1109/ACCESS.2020.3013199.

[17] A. Sheik, V. Kamuni, A. Urooj, S. Wagh, N. Singh and D. Patel, "Got Energy Trading Using Byzantine-Based Blockchain Consensus," in IEEE Access, vol. 8, pp. 8554-8571, 2020, doi: 10.1109/ACCESS.2019.2963325.

[18] M. Du, Q. Chen and X. Mama, "MBFT: A New Consensus Algorithm for Consortium Blockchain," in IEEE Access, vol. 8, pp. 87665-87675, 2020, doi: 10.1109/ACCESS.2020.2993759.

[19] S. N. G. Gourisetti, M. Mylrea and H. Patangia, "Assessment and Demonstration of Blockchain Applicability Framework," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1142-1156, Nov. 2020, doi: 10.1109/TEM.2019.2928280.

[20] M. Zhaofeng, W. Xiaochang, D. K. Jain, H. Khan, G. Hongmin and W. Zhen, "A Blockchain-Based Trusted Data Management Scheme in Edge Computing," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2013-2021, March 2020, doi: 10.1109/TII.2019.2933482.

[21] N. Sohrabi and Z. Tari, "ZyConChain: A Scalable Blockchain for General Applications," in IEEE Access, vol. 8, pp. 158893-158910, 2020, doi: 10.1109/ACCESS.2020.3020319.

[22] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty and Y. Wang, "PoBT: A Lightweight Consensus Algorithm for Scalable CPS Business Blockchain," in IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2343-2355, March 2020, doi: 10.1109/JIOT.2019.2958077.

[23] G. Xu, Y. Liu and P. W. Khan, "Improvement of the DPoS Consensus Mechanism in Blockchain Based on Vague Sets," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4252-4259, June 2020, doi: 10.1109/TII.2019.2955719.

[24] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho and H. Y. Lam, "Blockchain-Driven CPS for Food Traceability With an Integrated Consensus Mechanism," in IEEE Access, vol. 7, pp. 129000-129017, 2019, doi: 10.1109/ACCESS.2019.2940227.

[25] Z. Mama, J. Fan, Y. Zhang and L. Liu, "Execution Analysis of Blockchain Consensus System With Interference Factors and Sleep Stage," in IEEE Access, vol. 8, pp. 119010-119019, 2020, doi: 10.1109/ACCESS.2020.3005919.