Advances and Applications in Mathematical Sciences
Volume 21, Issue 5, March 2022, Pages 2707-2720
© 2021 Mili Publications, India

A SURVEY ON BLOCKCHAIN SMART NETWORK BASED ON CONSENSUS ALGORITHM

SUBHITA MENON[1,*], DIVYA ANAND[1] and KAVITA[2]

[1]School of Computer Science
and Engineering, Lovely Professional
University, Phagwara, India 144411

[2]School of Computer Science
and Engineering, Chandigarh University
Chandigarh, India 140413
E-mail: divyaanand.y@gmail.com
kavita@ieee.org

Abstract

The fast growth of Blockchain technologies over the last decade has grabbed the attention of both the business community and scientific research community. It is regarded as a technical innovation that has the potential to disrupt a variety of application fields affecting many aspects of our life. The need of a comprehensive literature study on the sustainability of consensus mechanisms motivated this survey and provided a detailed view by emphasizing on scalability, throughput, computation overhead and latency. Consequently, we present a detailed survey of the growing uses of Blockchain networks in a wide range of network domains, with a focus on how consensus mechanisms influence these applications. We address many open difficulties in Blockchain consensus algorithm design with future research directions.

1. Introduction

We are seeing an increase in the Blockchain based Internet of Things (IoT) applications in our homes, offices, neighborhoods and cities. The adoption of Blockchain based IoT technology is ready for major impact on our day-to-day lives, including power, productivity and intelligent transport cities. As more autonomous implementations of potentially large-scale IoT

2020 Mathematics Subject Classification: 68T42.
Keywords: Block Mining; Consensus Algorithm; Incentive Mechanisms; P2P Networks.

*Corresponding author; E-mail: subhita.20260@lpu.co.in; subhitamenon1@gmail.com

Received September 17, 2021; Accepted November 30, 2021

systems occur, ensuring the protection, confidentiality and availability of data, devices, and networks becomes increasingly essential (Kumar et al., [19]). IoT network consist of sensors and devices for the communication among devices with each other in a distributed environment. This includes a process by which the validity of any transmitted data can be accepted by an agreement between different nodes present in IoT network, this needs a consensus approaches which allow diverse nodes to make a collaborative choice to reach a common opinion without the intervention of a central controller (Sethi et al., [30]). Consensus approaches generally involve a lot of computing and communication power (Kaur et al., [17]).

A Blockchain network's objective is to guarantee that all the nodes of the networks agree on a single, tamper-proof transaction ledger (Mense et al., [20]). New transaction will be added in the network once all node approves the new block by running the consensus algorithm (Samy et al., [28]). In recent studies, it has been anticipated that Multiple Blockchains are going to offer different characteristics to build the future. Here, Blockchain network may be enterprise, home network or the internet (Xie et al., [34]). Blockchain network can be categorized in public, consortium and private Blockchain. In the consensus algorithm, the type of Blockchain determines the membership power. The Blockchain type should be selected according to the idea behind the business application. Blockchain achieves data integrity by employing sophisticated secure hash algorithms, which prevent data manipulation, as well as the recording of incorrect information (Reyna et al., [24]). It is the sequence of unaltered block on the distributed and immutable ledger. Figure 1. represent the Blockchain architecture, internal mechanism, and process.

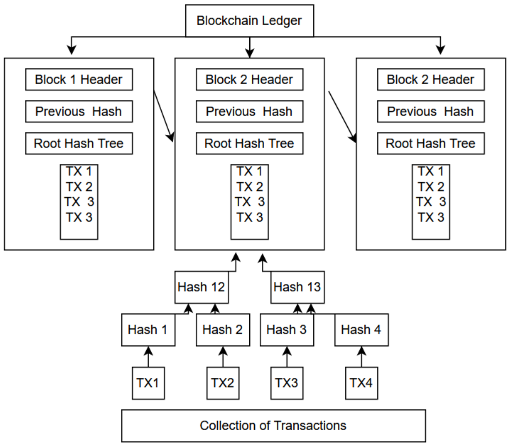

Figure 1. Structure of Blockchain Network.

Sections 2 discuss existing study on the application area of Blockchain technologies and user safety. Section 3 provided the various consensus approaches. Result discussion and comparative analysis of Blockchain with various QoS parameter is provided in Section 4. We put forward conclusions and some of the open research issues in Section 5.

2. Related Study

Ricquebour et al. demonstrate the required components for Smart Home. The basic requirement of the infrastructure to transport data from heterogeneous smart objects. Next requirement is software architecture to use the data and for same a service- oriented technique is used to handle data and provide more personalized services through the use of heterogeneous sensors (Ricquebourg et al., [25]). I. Bisio et al. studied that for active ageing, rehabilitation and geriatric monitoring Internet of Things (IoT) is really helpful, particularly for in-home treatments, and it has considered Movement Recognition (MR) and Activity Recognition (AR) for this purpose AR senses whether a patient is standing, walking, still, climbing or descending stairs, or moving, while MR recognizes complex movements that are often needed (Bisio et al., [5]). The obtained results allow for the inference that MR and AR functions can be implemented on smartphones with effective result. Another interesting conclusion about MR is that in some cases it might be important to differentiate between ArmCircleFront and ArmCircleBack or

ShoulderRolls- Front and ShoulderRolls Back.

D. J. Cook et al. investigated machine learning algorithms and sensor data to see whether the influence of MCI and PD could be sensed and identified. Findings suggest that smart homes, wearable devices, and pervasive computing technology may be useful for tracking activity and analysing data to identify variations between stable older adults and those with Parkinson's disease or MCI. The innovations can also help with care validation by offering an ecologically valid environment where people can be tracked when going about their everyday lives in their own homes (Cook et al., [7]). P. N. Dawadi et al. introduces CAAB's approach to model a person's activity behavior using smart home sensor. CAAB collects sensor data, models activity results, it also extracts appropriate statistical features and predicts clinical scores using supervised machine learning. This is a long-term technique in which a person's own repetitive actions and changes in behavior are used to assess their functional abilities (Dawadi et al., [8]).

Chen et al. introduced smart contract to help secure privacy and create networks more believable and trustworthy the approach ensures security and privacy while exchanging the information. To monitor the exchange of information, the authors constructed a Blockchain and virtual information using a counter-based algorithm. These counters resulted in trusted information on the social networks (Chen et al., [6]). The approach tends to prove exponentially helpful but in case if the communicators are insecure in the starting stages then this approach is not favorable. Atzei et al. conducted one of its firsts survey on Ethereum smart contracts with respect to attacks and also highlighted the taxonomy of Ethereum smart contract vulnerabilities. They also surveyed other popular vulnerable contracts like Rubixi, DAO, and King of the Ether throne and Govern Mental (Atzei et al., [3]).

Ashar Ahmad et al. examined the performance of PBFT, PoW, PoET, PoS and Clique consensus algorithms for Blockchain based audit system. They evaluated the performance of such consensus algorithms using data from a real-world audit system. According to the findings other algorithm gives high throughput but low latency so Cliquw, PoET and PoSare the most suitable and useful for audit systems (Ahmad et al., [1]). Jayabalan et al. discusses distributed consensus and the many methods that can be used to build a

Blockchain network. Attaining consensus can be challenging for a variety of reasons, including active node crash, malicious node presence, network issues, latency and the fact that not all pairs are connected (Jayabalan et al., [15]).

Walid K A Hasan et al. studied the expansion of Blockchain in IoT with prime focus on privacy and security. It has discussed the benefits and drawbacks of using Blockchain in IoT. Blockchain is a relatively new mechanism for health-care system and smart homes etc. (Walid et al., [31]). Furthermore, because of the global COVID 19 issue, there is a greater demand for enhancing Smart Healthcare applications. Marc Jayson et al. presents a solution for enhancing the security of a home network. It incorporates private Blockchain technology as well as RSSI-based trilateration for localization. This study looked at advantages of Private Blockchainover Public Blockchain and tested the localization algorithm against several wireless technologies to improve its precision. It also determines which of the three communication technologies among WiFi, BL and ZigBee produces the most accurate RSSI generation. WiFi remained the most consistent, according to the findings. As a result, the architecture is more suited for RSSI measurements by merging private Blockchains over public and WiFi (Baucas et al., [4]).

Muhammad Adnan Khan et al. discussed that intrusion detection is still a difficult task in smart homes, particularly in terms of predication and evaluation. This paper proposed a simple yet successful technique for detecting and predicting intruder's. A Blockchain based Deep Extreme Learning Machine (DELM) architecture was presented with promising results that can be extended using other datasets and different designs (Khan et al., [18]) M. Giannoutak is et al. study the smart home ecosystem which are prone to cyber attacks. It offers a Blockchain framework to assist the cyber security mechanisms of smart home installations, with an emphasis on the immutability of the users and devices. The designed methodology picks the accurate Smart Contract for the gateway integrity of Smart Homes also immutable and dynamic management of blocked malicious IPs (Giannoutakis et al., [12]).

3. Blockchain Consensus Algorithms

The Consensus Algorithms are the foundation of every Blockchain network that allows the distributed nodes to reach on a collaborative decision for adding a node in the chain. A variety of consensus approaches have been designed and developed in recent years for various application areas. This section will provide the detail on most used consensus algorithms.

3.1 Proof of work

Proof of work is one of the expensive computational approach. In this approach, a cryptographic hash function, SHA-256 is solved by various nodes in a Blockchain. A unique, fixed size hash of 256 bits is created by SHA-256. The role of miner is crucial in the process of mining where it needs to find the next block by solving hash. The miner will recognize it as a legitimate block, if the output is less than the desired value, move on to the next step for new block. This method is mathematically difficult and time expensive because it can only be accomplished by brute force, and miners must attempt arbitrarily different nonce numbers in order to reach the goal value. While Proof of Work has shown to be a useful solution for crypto currencies over time, it does not appear to be feasible for IoT networks due to its high computational and bandwidth needs (Yazdinejad et al. [37], Wang et al. [33], Gemeliarana, I. et al. [11]).

3.2 Proof of stake

This is the most popular consensus approach used by cryptocurrencies after proof of work. It is having similar property of proof of work, but excludes the process in which nodes compete to solve next block. A node is picked to mine the next block depending on its proportional stake in the network. In this process, all coins are available from the first day and there is no mining incentive production and only a transaction fee is awarded to the miners. Although Proof of Stake removes the computational requirements of proof of work. This method relies on the nodes with the most stakes, making the Blockchain relatively centralized. However for resource-constrained IoT networks, it has made computing a lot easier as compare to proof of work requirements (Platt et al., [21], Saleh et al. [26]).

3.3 Practical byzantine fault tolerance

A practical Byzantine Fault Tolerance consensus algorithm is developed to address a number of difficulties with existing Byzantine Fault Tolerance algorithms. PBFT attempts to give a useful resource replication of the Byzantine state machine that can operate even if malicious nodes are able to operate in the system. The PBFT provide efficient results with limited nodes in distributed network, due to the significant communication overhead which grows exponentially with each additional node in the network (Fekih et al. [10], Rakitin et al. [23]).

3.4 Delegated byzantine fault tolerance

NEO introduced Byzantine Fault Tolerance also recognized as “Ethereum of China”. This technique does not require the participation of all nodes to add the block in the network which makes it more scalable. There’s no anonymity on the Blockchain, as delegates need to work under real identities which needs to be get elected. The system involves regulated Blockchains, including a certain degree of centralization. Its average block formation latency is 15 s, which is not sufficient for an IoT network (Jeon et al., [16], Yang et al. [36]).

3.5 Ripple

Ripple consensus algorithm uses the sub network which is collectively trusted among the whole network. This protocol is executed in rounds to ensure the accurateness of network for every single second. Each node at the beginning announces a candidate list publicly by considering the valid transaction before the round of consensus. The number of votes listed is compared with a threshold value and accepting/discarding the value transaction is based on same. A final round to agree on the transaction is carried out needs 80% of the nodes to agree on a transaction (Schwartz et al. [29], Amores et al. [2]).

3.6 Raft

Raft is a consensus-building mechanism based on voting and designed to make the Paxos algorithm more applicable in real-world systems. The two phases of Raft includes the election of leaders and the replication of logs. It’s the responsibility of the leader to order the transactions. When an existing leader fails, a randomised timeout is used for each server during the leader selection step. When a leader is picked, the stage of log replication is triggered. The leader takes customer log entries and broadcasts transactions in this stage to complete the transaction log version. Its efficiency, on the other hand, is determined by the leading node, which has complete control over the system. As a result, if the leader node is deliberately infected, the entire device will be destroyed. It is not very suitable for IoT networks due to lower security and limited throughput [Javaid et al. [14], Dib et al., [9]).

3.7 Proof of Authentication

The PoA protocol, allows validators to have a monetary interest in the Blockchain which solves the problem of excessive energy consumption and dependency in the PoW consensus method. It achieved substantial performance gains with respect to messages exchange over the traditional BFT algorithms. A commonly used approach called mining rotation scheme is the backbone of PoA consensus and primarily necessary for the equal distribution between authorities for the formation of block, but it has some Scalability issues (Puthal et al. [22]).

3.8 DPoS

This is an elective consensus mechanism in which ‘voting’ is used by any node with a stake in the current network. DPoS takes a representative democratic approach, in contrast to the direct democratic approach adopted by PoS. Stakeholders elect the ‘witnesses’ to produce and verify a block. DPoS key weakness is when some participants will try to increase the probability of becoming validate itself even by manipulating others to vote (Salimitari et al. [27], Yang et al. [35]).

4. Results and Discussion

As discussed in previous sections, various kinds of Blockchain consensus algorithm and its application area emerged in various sectors. The key advantages of a public Blockchain is transparency and non-modifiability. However, due to its permission less feature, the key issue with the public Blockchain is its confidentiality and efficiency (Wang et al., [32]) Many individuals and regions are not able to implement Blockchain technology in their fields due to its resource consumption and Network Latency. Blockchain is a new technology that has yet to be fully adopted by major corporations. As shown in figure 2, this new study looked at literature from 2008 to 2021 to identify relevant issues of incorporating IoT systems with Blockchain Technology.

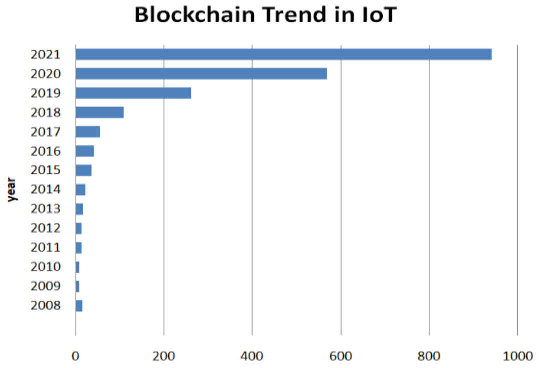

Figure 2. Blockchain Adoption.

The graph in Figure 2 shows that the two definitions have experienced mainly upward development in the year 2018 and 2019. Due to emerging issues of integration, compatibility, and scalabilities, 2017 of the study saw comparatively slower growth but again the study is in progress for the integration and adoption part of Blockchain.

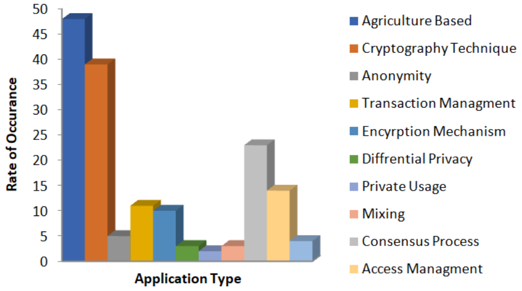

Figure 3. Blockchain Application Area.

In several application fields, Blockchain is a wonderful and effective complement for both data security and processing. Figure 3 depicts the health industry's significance in a variety of ways and health is a crucial sector. However, various health-related subfields are dealing with concerns such as incorrect treatment of individual patients' drug supply shortages, medicine counterfeiting and personal health records. Standardization and validation of every commodity in the supply chain ensures that any company provides a high-quality product to the market. Blockchain can be used to authenticate computers, increase IoT storage capacity, reduce data manipulation, and secure cloud servers because many regions do not have enough internet connectivity, people are more comfortable with paper-based processes than digital ones in the supply chain. Sensors and other devices find it difficult to communicate with the primary protocol because of a poor internet connectivity. Researchers have discuss the benefits of merging Blockchain technology with artificial intelligence in the field of water management. The introduction of Blockchain in the education sector has facilitated the provision of records and other assets in a global network. So far, Blockchain has only been used in voting to store voting data and only useful for small-scale voting. Smart contracts developed by the electoral administrator are used for voting purposes. Smart contracts perform the voting results automatically and also prevent the voting data from being tampered. The main issue is figuring out how to adapt Blockchain technology to meet the needs of individual applications. Each application has its own set of needs, which demands a new or customized Blockchain implementation in the Era. Table 1 will compare the consensus Algorithms which we have discussed so far with various aspects: decentralization, throughput, latency, scalability, adversary tolerance, storage and network overhead. High, Medium and low are represented by H, M and L respectively in table 1.

Table 1. Comparative Analysis between the Consensus Properties.

Consensus Algorithm	Decentralization	Throughput	Latency	Scalability	Storage Overhead	Network Overhead	Adversary tolerance
PoW[21-23]	H	L	H	H	H	L	<25% Computing Power
PoS[23,24]	H	L	M	H	H	L	<51% Stakes
DPoS[37-38]	M	H	M	H	N/A	M	<51% Validators
PBFT[26-27]	M	H	L	L	H	H	<33% Faulty Replicas
DBFT[28-30]	M	H	M	H	H	H	<33%Faulty Replicas
PoA[35-36]	M	L	M	H	H	L	<51%Online Stakes
Ripple[31-32]	H	H	M	H	H	M	<20%Faulty Replicas
RAFT[33,34]	M	H	L	H	H	N/A	<50 % Crash Fault

5. Conclusion

We have presented a complete overview of the current evolution of Blockchain technologies in this paper, with a particular focus on consensus protocol design approaches and related research. Some research activities have recently been carried out for the Comparison with the consensus algorithms used in the field of Blockchain which provide the new solution. Proof of Work has shown useful solution for crypto currencies over time, it does not appear to be feasible for IoT networks due to its high computational and bandwidth needs where Proof of Stake removes the computational requirements for Proof of Work but it relies on the nodes with the most stakes, which makes it more centralized. Now PBFT provide efficient results with limited nodes in distributed network, due to the significant communication overhead which grows exponentially with each additional node in the network. DBFT is not sufficient for an IoT network and RAFT is having lower security and limited throughput so by considering these parameters integrated model is required for future. In this article some missing areas are provided in the comparison so detailed quantitative and qualitative needs to be get discovered in the field also few experiments must be carried out to evaluate the Consensus algorithms' strengths and weaknesses with regards to the needs of big data.

References

[1] A. Ahmad, M. Saad, J. Kim, D. Nyang and D. Mohaisen, Performance Evaluation of Consensus Protocols in Blockchain-based Audit Systems, 2021 International Conference on Information Networking (ICOIN) (2021), 654-656.

[2] I. Amores-Sesar, C. Cachin and J. Mićić, Security Analysis of Ripple Consensus, (2020).

[3] N. Atzei, M. Bartoletti and T. Cimoli, A Survey of Attacks on Ethereum Smart Contracts (SoK) (2017), 164-186.

[4] M. J. Baucas, S. A. Gadsden and P. Spachos, IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization, IEEE Networking Letters 3(2) (2021), 52-55.

[5] I. Bisio, A. Delfino, F. Lavagetto and A. Sciarrone, Enabling IoT for In-Home Rehabilitation: Accelerometer Signals Classification Methods for Activity and Movement Recognition, IEEE Internet of Things Journal 4(1) (2017), 135-146.

[6] Y. Chen, Q. Li and H. Wang, Towards Trusted Social Networks with Blockchain Technology, (2018).

[7] D. J. Cook, M. Schmitter-Edgecombe and P. Dawadi, Analyzing activity behavior and movement in a naturalistic environment using smart home techniques, IEEE Journal of Biomedical and Health Informatics 19(6) (2015), 1882-1892.

[8] P. N. Dawadi, D. J. Cook and M. Schmitter-Edgecombe, Automated cognitive health assessment from smart home-based behavior data, IEEE Journal of Biomedical and Health Informatics https://doi.org/10.1109/JBHI.2015.2445754, 20(4) (2016), 1188-1194.

[9] O. Dib, B. Kei-Le, D. Antoine T. Eric and E. Ben Hamida, Consortium blockchains: Overview, applications and challenges, International Journal on Advances in Telecommunications 11(1-2) (2018).

[10] H. Fekih, S. Mtibaa and S. Bouamama, The dynamic reconfiguration approach for fault-tolerance web service composition based on multi-level VCSOP, Procedia Computer Science 159 (2019), 1527-1536.

[11] I. G. A. K. Gemeliarana and R. F. Sari, Evaluation of Proof of Work (POW) Blockchains Security Network on Selfish Mining, 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI) (2018), 126-130.

[12] K. M. Giannoutakis, G. Spathoulas, C. K. Filelis-Papadopoulos, A. Collen, M. Anagnostopoulos, K. Votis and N. A. Nijdam, A Blockchain Solution for Enhancing Cybersecurity Defence of IoT, 2020 IEEE International Conference on Blockchain (Blockchain) (2020), 490-495.

[13] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi and U. Raza, Blockchain-enabled supply chain: analysis, challenges, and future directions, Multimedia Systems 27(4) (2021), 787-806.

[14] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan and R. Suman, Blockchain technology applications for Industry 4.0: A literature-based review, Blockchain: Research and

Applications 100027 (2021).

[15] J. Jayabalan and N, Jeyanthi, A Study on Distributed Consensus Protocols and Algorithms: The Backbone of Blockchain Networks, International Conference on Computer Communication and Informatics (ICCCI), (2021).

[16] S. Jeon, I. Doh and K. Chae, RMBC: Randomized mesh blockchain using DBFT consensus algorithm, International Conference on Information Networking (ICOIN) (2018), 712-717.

[17] S. Kaur, S. Chaturvedi, A. Sharma and J. Kar, A research survey on applications of consensus protocols in blockchain, Security and Communication Networks (2021), 1-22.

[18] M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser and A. Ali, A Machine Learning Approach for Blockchain-Based Smart Home Networks Security, IEEE Network 35(3) (2021), 223-229.

[19] S. Kumar, P. Tiwari and M. Zymbler, Internet of Things is a revolutionary approach for future technology enhancement: a review, Journal of Big Data 6(1) (2019), 111.

[20] A. Mense and M. Flatscher, Security Vulnerabilities in Ethereum Smart Contracts, Proceedings of the 20th International Conference on Information Integration and Web-Based Applications and Services (2018), 375-380.

[21] M. Platt and P. McBurney, Sybil attacks on identity-augmented Proof-of-Stake. Computer Networks 199 (2021), 108424.

[22] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos and G. Das, Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems, 2019 IEEE International Conference on Consumer Electronics (ICCE) (2019), 1-5.

[23] S. Rakitin, A. A. Visheratin and D. Nasonov, Byzantine fault-tolerant and semantic-driven consensus protocol, Procedia Computer Science 136 (2018), 25-34.

[24] A. Reyna, C. Martín, J. Chen, E. Soler and M. Diaz, On blockchain and its integration with IoT, Challenges and opportunities, Future Generation Computer Systems 88 (2018), 173-190.

[25] V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche and C. Loge, The Smart Home Concept: our immediate future, 1ST IEEE International Conference on E-Learning in Industrial Electronics (2006), 23-28.

[26] F. Saleh, Blockchain Without Waste: Proof-of-Stake, SSRN Electronic Journal, (2018).

[27] M. Salimitari, M. Chatterjee and Y. P. Fallah, A survey on consensus methods in blockchain for resource-constrained IoT networks, Internet of Things 11 (2020), 100212.

[28] H. Samy, A. Tammam, A. Fahmy and B. Hasan, Enhancing the performance of the blockchain consensus algorithm using multithreading technology, Ain Shams Engineering Journal 12(3) (2021), 2709-2716.

[29] D. Schwartz, N. Youngs and A. Britto, The ripple protocol consensus algorithm, Ripple Labs Inc White Paper 5 (2014).

[30] P. Sethi and S. R. Sarangi, Internet of Things: Architectures, Protocols, and

Applications, Journal of Electrical and Computer Engineering (2017), 1-25.

[31] Walid K Hasan, Albhalool M Abood, Mostafa Habal, A review of Blockchain-based on IoT application ieee explore, (2020).

[32] T. Wang, H. Hua, Z. Wei and J. Cao, Challenges of blockchain in new generation energy systems and future outlooks, International Journal of Electrical Power and Energy Systems 135 (2022), 107499.

[33] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen and D. I. Kim, A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks, IEEE Access 7 (2019), 22328-22370.

[34] G. Xie, Y. Liu, G. Xin and Q. Yang, Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency, Security and Communication Networks (2021), 1-15.

[35] 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. IEEE Access 7 (2019), 118541-118555.

[36] 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, IEEE Access 7 (2019), 118541-118555.

[37] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, H. Karimipour and S. R. Karizno, SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks, 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring) (2020), 1-5.