2022 IEEE the 14th International Conference on Wireless Communications and Signal Processing

GaS-PBFT: A Game-based Node Selection Consensus Mechanism for Internet of Things

Yiheng Jiang*,Yuwei Le*†, Jiaheng Wang*†, Xiaohu You*†‡
*National Mobile Communications Research Laboratories, Southeast University, Nanjing 210096, China
†Purple Mountain Laboratories, Nanjing 211100, China
Email: {cyluo, ywle, jhwang, xhyu}@seu.edu.cn

2022 14th International Conference on Wireless Communications and Signal Processing (WCSP) | 978-1-6654-5085-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/WCSP55476.2022.10039397

***Abstract*—Future communication systems are trending to embrace an open and collaborative ecology for a rising number of edge services and applications, enabling the evolutions of multiple wireless ecosystems such as the Internet of things (IoT). The collaborations among multi-party IoT users, devices, and infrastructure require further designs in terms of security, trust, and efficiency. Blockchain is considered a promising solution to facilitate trusted multi-party collaborations, enhance security, and protect privacy in the IoT. However, the research on IoT-friendly blockchains is still facing a number of challenges due to the heterogeneity and limited capabilities of IoT devices. In this paper, we propose a hierarchical blockchain consensus combining practical Byzantine fault tolerance and a game-based node selection mechanism (GaS-PBFT). GaS-PBFT enables a logical two-layer consensus network structure, groups heterogeneous IoT participants into multiple collaborating consensus groups, and imposes an efficient and fair game on each group for selecting block generators of the IoT blockchains. Finally, we conduct comprehensive simulations to show the performance of the proposed GaS-PBFT consensus in terms of consensus latency, transaction speed, node capacity, and security.**

***Index Terms*—Internet of things, blockchain, consensus mechanism**

I. Introduction

Research on the beyond fifth-generation (B5G) and the sixth-generation (6G) communication systems is gaining steam recently [1]–[4]. Future communication systems are envisioned to provide global coverage, support full applications and ensure strong security, especially at the network edge [5], [6]. Researchers have also envisioned an evolution of the Internet of things (IoT) that could bring a more open, efficient, collaborative, and secure industrial ecology for ubiquitous wireless services and applications [7]. An increasing number of studies have been searching for implementations with emerging technologies such as blockchain. Blockchain is an immutable distributed ledger technology proposed with Bitcoin [8]. It admits a number of traits such as openness, transparency, tamper-proof, multi-maintenance, etc., making it a promising security solution and trusted collaboration enabler for the industry [9].

As the core mechanism of blockchain, the consensus mechanism guarantees data consistency among multiple blockchain participants [10]. A number of schemes [11]–[14] have been proposed to integrate blockchains with the IoT, aiming to facilitate cross-network collaborations, enhance the security of IoT devices and protect device privacy. Some studies classified heterogeneous IoT devices into multiple task groups. Devices with abundant resources maintain the blockchain consensus, while others help disseminate or verify blockchain messages [11], [12]. Moreover, some works also took reputation or credit evaluation into consideration by modifying the classic proof of work to endow those high-rated nodes with more opportunities to generate new blocks [13], [14].

However, designing an IoT-friendly blockchain consensus is still facing a number of challenges. For one thing, the IoT networks are usually regionally governed and have an increasing demand for cross-region sharing and collaboration. Most existing works focused on the conceptual integration of blockchain consensus and the IoT but overlooked these impending needs. For another, many studies, though considering the limitations in the IoT and adopting the BFT-based blockchain consensus, are still far from practical applications. For example, the communication overhead in most BFT-based consensus grows quadratically with the number of participants, which would quickly consume and saturate the capabilities of those resource-constraint IoT devices.

In this paper, we incorporate the practical Byzantine fault tolerance (PBFT) [15] consensus and a node selection game to solve the challenges. The contributions of our work can be concluded as follows. 1) We design a two layered IoT consensus network with the PBFT consensus in the upper-layer and a game-based node selection (GaS) consensus in the lower-layer. In the lower-layer, we set up a *consensus group* scheme to virtually group massive IoT participants into multiple subnetworks where leader nodes are elected to execute the upper-layer consensus. By this means, we connect the PBFT and the GaS and form the GaS-PBFT consensus mechanism. 2) We design the IoT-friendly, energy-efficient GaS consensus mechanism with a four-stage *block epoch* scheme and a game for selecting lower-layer leaders. The GaS runs parallel to the upper-layer PBFT and the node selection game is organized every block epoch to maintain the decentralization and democracy of the consensus. 3) We demonstrate the performance of our proposed consensus mechanism via extensive simulations of the consensus latency, transaction speed, node capacity, and security.

We organize the rest of this article as follows. Section II briefly describes our hierarchical IoT consensus network.

‡ Yiheng Jiang and Yuwei Le are co-first authors and contribute equally to this paper.

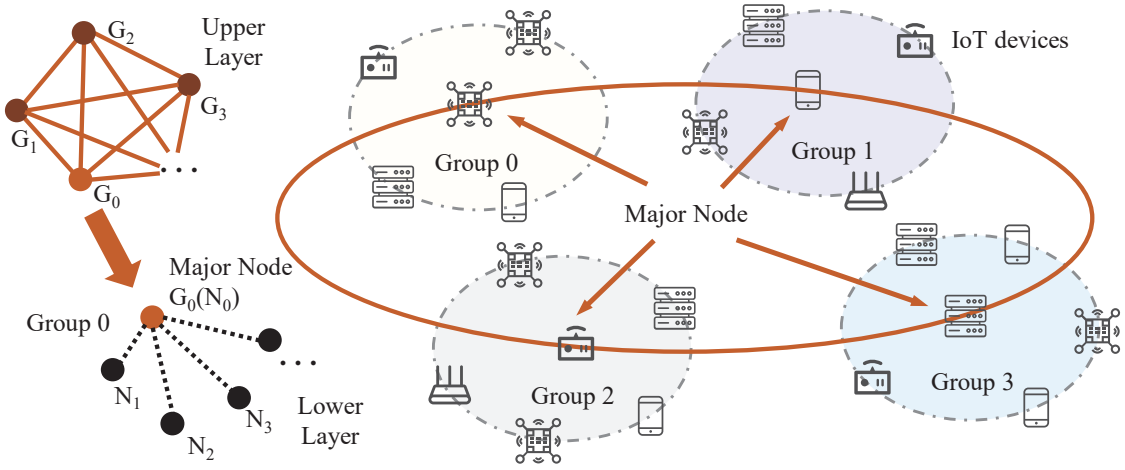

Fig. 1. The proposed two-layer IoT consensus network.

Section III presents the detailed designs of the two-layer consensus along with our game-based node selection mechanism. Section IV conducts several numerical experiments on the proposed GaS-PBFT consensus, followed by concluding remarks of Section V.

II. Hierarchical IoT Consensus Network

The proposed two-layer IoT consensus network is shown in Fig.1. The network is composed of several *consensus groups* of nodes and each group represents a subnetwork of a number of heterogeneous IoT devices. Every group has a major node, and the major nodes form the upper-layer consensus network. Different from Nakamoto-type consensus mechanisms, the major node selection is driven by an efficient game-based node selection (GaS) consensus mechanism (that we will introduce in Section III) rather than energy-wasting mining or time-consuming voting. Thus, both the upper-layer and lower-layer consensus mechanisms are maintained by only a minority of IoT participants, and communication resources during the consensus can be saved.

In our proposed network, the upper-layer runs the main PBFT consensus that maintains the blockchain. It involves a group of major nodes that are chosen from groups in the lower-layer via the GaS consensus. The chosen major nodes are responsible for packing transactions, maintaining the upper-layer consensus, and ensuring controllable latency and reliable security.

The two-layer consensus network is devised to balance network workload, shorten consensus latency and improve transaction efficiency. Specifically, it embraces the following features.

- **Low consensus latency**: Due to the design of consensus groups in our network, the upper-layer PBFT consensus does not need all nodes' participation. Therefore, the communication delay and bandwidth overhead can be significantly reduced.
- **Large network capacity**: Although the computation and communication complexity of the PBFT grows quadratically with the number of participating nodes in our network, new network participants are first assigned to the lower-layer and thus would not degrade the performance of the upper-layer PBFT consensus.
- **High transaction speed**: The major node of each subnetwork is responsible for packing the transactions generated in its belonging subnetwork and executing the consensus mechanism in the upper-layer. Since all the transaction validations are done by major nodes, the fixed number of consensus participants and message routing can lead to more efficient message propagation and lift the achievable transaction speed.
- **Flexible and scalable network**: Based on our design, the network can be flexibly configured to cover more geographic areas and accommodate more heterogeneous devices without costing extensive computation, storage, and communication resources.

III. Game-based Node Selection (GaS) Consensus

A. GaS Consensus Overview

We design the GaS consensus to decide major nodes in lower-layer networks via a game-based mechanism. Major nodes selected by the GaS consensus will participate in the upper-layer network as PBFT consensus maintainers. The selection is conducted every *block epoch* in each consensus group to preserve decentralization and democracy among network participants. Specifically, in the lower-layer network, we set up multiple consensus groups that are formed by a number of IoT devices. A block epoch refers to a contiguous sequence of blocks, during which each participating consensus group elects a new leader, i.e., major node, according to the

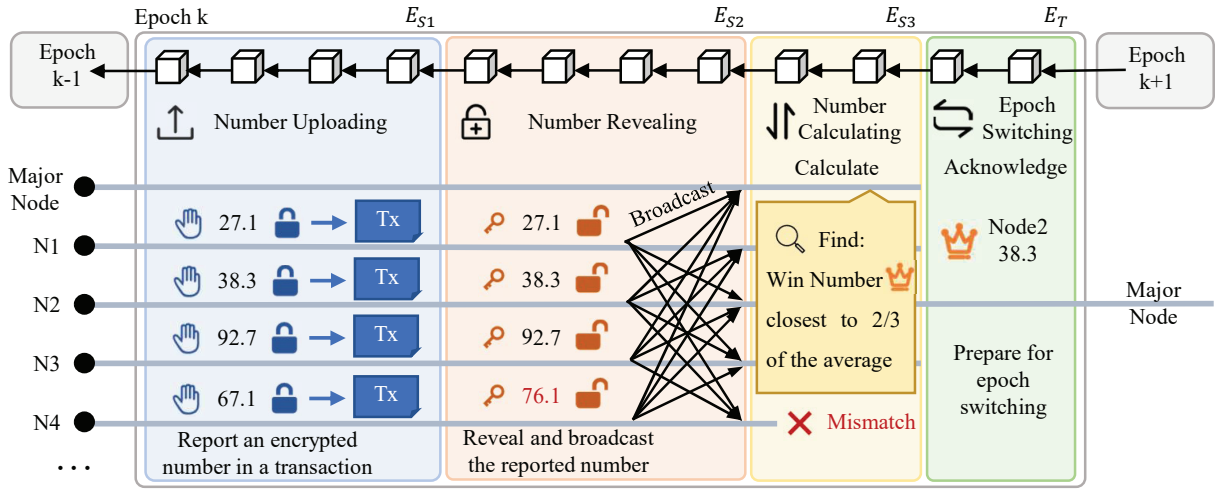

Fig. 2. The working process of the GaS consensus. (In the number calculating stage, the win number 38.3 is the closest number to 2/3 of the average of all valid numbers.)

game-based selection mechanism introduced in Section III-B.[1]

B. Game-based Selection Mechanism and Block Epoch Design

We introduce a fair game, namely "guess 2/3 of the average", to form the game-based selection mechanism.[2] Nodes participate in the GaS consensus by uploading a number between 0 and 100 and wait for the winner to be announced. The winner is the node that uploads a number closest to 2/3 of the average of all the valid uploaded numbers.

However, it is challenging to apply this game with the blockchain. It is possible for blockchain users to track others' uploaded numbers and create an unfair campaign. Therefore, we design a four-stage block epoch to counter this issue, as shown in Fig. 2. A block epoch E consists of T consecutive blocks and is divided into four stages: 1) number uploading stage (block 1 to E_{s1}), 2) number revealing stage (block E_{s1} to E_{s2}), 3) number calculating stage (block E_{s2} to E_{s3}), 4) epoch switching stage (block E_{s3} to E_T). The following steps describe the workflow of an epoch, but notice that the first block in the blockchain, i.e., genesis block, is not subject to these steps and is created along with the blockchain initialization.

1) **Number uploading stage**: A node n decides a number to upload. It chooses a number a and computes the hash value of a with the hash value of the previous block b_{prev} as:
$$Hash_n(a, b_{prev}).$$
Afterward, node n signs this hash value using its private key to form a transaction Tx which is then sent to the blockchain network.
2) **Number revealing stage**: Node n reveals its uploaded number by broadcasting it to the blockchain network.
3) **Number calculating stage**: Participants wait for the result. As for the major node of the consensus group, it needs to verify the validity of the data in the above two stages, calculate 2/3 of the average of all the valid numbers, and decide the winner.
4) **Epoch switching stage**: This stage reserves a certain amount of time for the results to be broadcast and notified to all the participants. Also, the change of network topology and establishment of new network connections can take place in this stage.

In every round of consensus, an IoT node only needs to compute the hash value once and create two transactions. In the block epoch design, we separate the number upload and reveal stages and use hash functions to safeguard the privacy of numbers during the consensus. The designed game-based selection mechanism is fair, energy-efficient, and IoT-friendly.

C. Security Mechanism

Based on the characteristics of the IoT devices, we set up two security mechanisms in the GaS consensus to resist attacks such as the Sybil attack and the 51% attack [17].

- **Radio frequency identification (RFID)**: RFID can be used as a unique identification of IoT devices [18]. It cannot be counterfeited, which guarantees the presence, uniqueness, and traceability of IoT participants.
- **Asset pledge**: The IoT devices should pledge a certain amount of assets in the transaction as a deposit when they upload the GaS number. This deposit can be used as a guarantee that nodes behave normally and honestly in the network. Otherwise, the misbehaved nodes would be punished by a loss of deposit.

[1]Note that the blocks are generated by the upper-layer PBFT consensus, and the block epoch used in the GaS consensus is to ensure a steady periodical alternation of the group of blockchain maintainers.

[2]"Guess 2/3 of the average" is a multiplayer game in which all participants first give a number from 0 to 100, and the one who gives the number closest to 2/3 of the average of all the given numbers will win the game and receive a prize. In this game, there is no sure-win strategy due to an existing Nash equilibrium point of 0 [16].

Table I: Simulation parameters.

Parameter	Definition
n	number of groups
v	transaction speed (TPS)
B	network bandwidth
r_m	ratio of the number of malicious devices to the total number of network nodes
s_{tx}	average size of a blockchain transaction
s_{head}	average size of a PBFT message header (e.g., the header of a *prepare* message)
s_{hash}	size of a hash digest
t_b	block time

D. Incentive Mechanism

The incentive mechanism is a critical driving factor to encourage blockchain nodes to participate in a variety of blockchain activities. In our proposed GaS consensus, the selected major nodes are rewarded for their contributions to maintaining the upper-layer PBFT consensus. Other nodes in lower-layer networks, if volunteering as validators or monitors of the GaS consensus, can be rewarded for reporting misbehaviors of major nodes such as not responding, selecting a wrong winner, or postponing the consensus operations deliberately. Once the reports are confirmed, these rewards would be taken from the deposits of the misbehaving major nodes.

IV. Numerical Results

A. Simulation Settings

In this section, comprehensive simulations are provided to show the performance of the GaS-PBFT consensus mechanism. We compare the performance of consensus latency, achievable transactions per second (TPS), node capacity,[3] and security of the GaS-PBFT consensus with that of the PBFT consensus by using the configuration in Table I. Unless otherwise specified, we set n as 4 groups, s_{tx} as 256 bytes, s_{hash} as 32 bytes, s_{head} as 256 bytes, and t_b as 2 seconds by default.

B. Evaluations

Fig. 3 shows the impact of the network bandwidth B, transaction speed v, and the number of groups n on the consensus latency. In Fig. 3(a), when fixing B as 1 Mbps and v as 50 TPS, one can see that the GaS-PBFT consensus latency is around 100 milliseconds (ms) which is much lower than that in Ethereum (14 seconds per block) and Bitcoin (10 minutes per block).[4] Moreover, Fig. 3(b) shows the impact on the latency by the number of consensus groups n with v fixed to 30 TPS. The increase in the number of groups would cause higher communication costs, leading to a growth in latency. In a nutshell, improving the network condition can significantly reduce the consensus latency, allowing for more participating consensus groups.

[3]Theoretically, our consensus allows unlimited nodes to access. Thus, the node capacity is defined as the maximum number of nodes that GaS can support while every node is sending transactions at a certain speed.

[4]https://www.blockchain.com/explorer, accessed Jul., 2022.

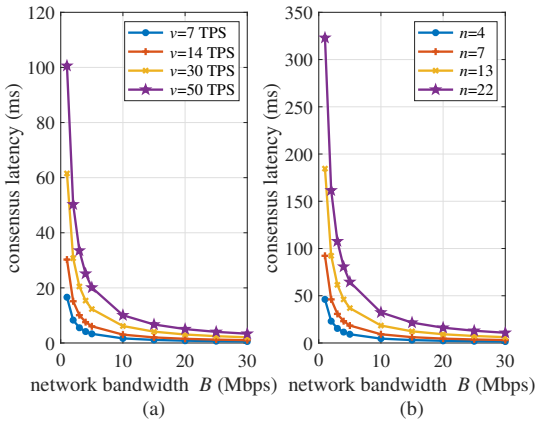

Fig. 3. The impact of the network bandwidth B, transaction speed v, and number of groups n settings on the consensus latency.

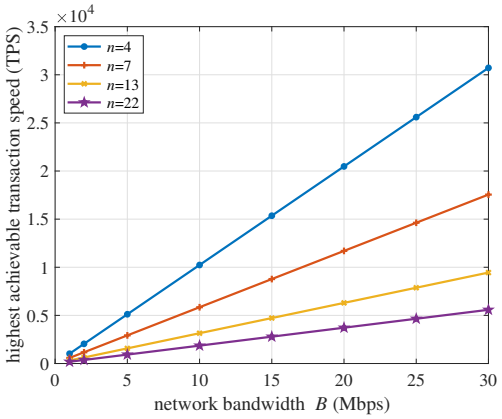

Fig. 4. The achievable transaction speed of the GaS consensus under varying network bandwidth B and number of groups n.

Fig. 4 demonstrates the achievable transaction speed of the GaS-PBFT network with different B and n. A higher bandwidth can lead to a higher achievable transaction speed, while more groups may result in a decrease. However, when n is set to 22 groups and B to 1 Mbps, the transaction speed of the GaS-PBFT consensus can still reach over 180 TPS which is significantly higher than that in Ethereum (14 TPS on average) and Bitcoin (7 TPS on average).

Fig. 5 compares the node capacity between GaS-PBFT and PBFT. The results show that our GaS-PBFT consensus has a significantly higher node capacity over the PBFT. The GaS-PBFT is capable of accommodating thousands of nodes while achieving a transaction speed of over 1000 TPS.

Furthermore, we simulate the security performance of the consensus under circumstances when the network crashes or in the presence of tampering. As the number of groups increases, the probability of successfully attacking GaS-PBFT network decreases. In GaS-PBFT networks, an attacker controlling more than 1/3 of the consensus groups can cause a network crash, but the network is able to recover itself without losing existing data. Fig. 6(a) illustrates the crash probability of the

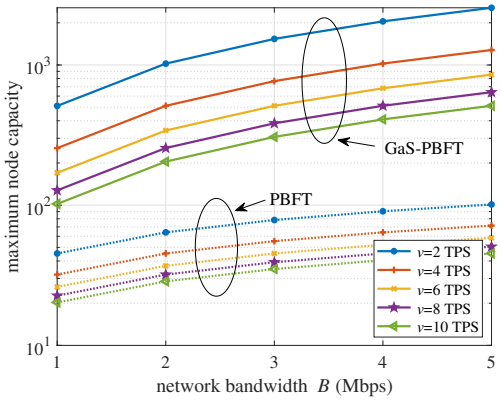

Fig. 5. The relationship between the node capacity and the network bandwidth B under different transaction speed v per node.

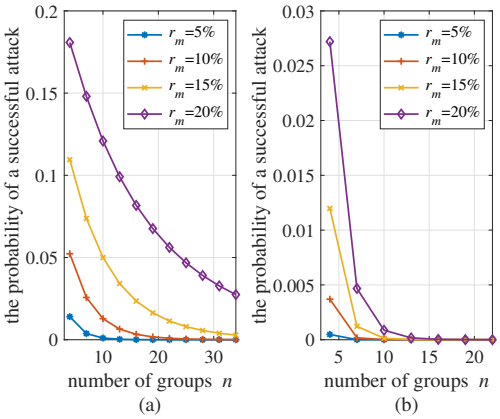

Fig. 6. The probability of a successful attack against the GaS-based network under different number of groups n and ratio of malicious devices r_m.

GaS-PBFT network when there exist a varying number of malicious devices. As one may notice, even if 10% of the devices in the network are malicious, the probability of causing a network failure is around 5% such that the network is still able to make a full recovery.

As shown in Fig. 6(b), when launching an attack on the GaS-PBFT network to tamper with the network data, the attackers only have a 3% chance of success even if they control 20% of all devices. In addition, if the number of groups n exceeds 7, the probability of a successful attack is even lower than 1%. The results show strong resilience against malicious devices and extreme security performance of our GaS-PBFT consensus.

V. Conclusion

This paper proposed an IoT-friendly consensus mechanism, GaS-PBFT, along with a hierarchical consensus network. We introduced a secure and efficient game into the maintainer elections of blockchains in the IoT. We also set up the four-stage block epochs to ensure the fairness of the game while guaranteeing the active participation of heterogeneous IoT devices. Finally, we construct simulations to verify the performance of GaS-PBFT. The results show that our proposed mechanism incorporates blockchain consensus into IoT environments with massive heterogeneous resource-constrained devices, while achieves short latency, large node capacity, high transaction speed, and strong security performance.

Acknowledgement

This work was supported in part by the National Key R&D Program of China under Grant 2022YFB2902204, the National Natural Science Foundation of China under Grants 61971130 and 61720106003, the Key Technologies R&D Program of Jiangsu (Prospective and Key Technologies for Industry) under Grants BE2022068 and BE2022068-3, the Natural Science Foundation on Frontier Leading Technology Basic Research Project of Jiangsu under Grant BK20212001, and the Huawei Cooperation Project under FA2019051081-2021-01.

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[2] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, "Blockchain enabled wireless communications: a new paradigm towards 6G," *Natl. Sci. Rev.*, vol. 8, no. 9, Apr. 2021. [Online]. Available: https://doi.org/10.1093/nsr/nwab069

[3] X. Ling, J. Wang, Y. Le, Z. Ding, and X. Gao, "Blockchain radio access network beyond 5G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 160–168, Dec. 2020.

[4] X. Ling, Y. Le, J. Wang, Z. Ding, and X. Gao, "Practical modeling and analysis of blockchain radio access network," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1021–1037, Feb. 2021.

[5] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang *et al.*, "Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, p. 110301, Nov. 2020.

[6] Y. Le, X. Ling, J. Wang, R. Guo, Y. Huang, C.-X. Wang, and X. You, "Resource sharing and trading of blockchain radio access networks: Architecture and prototype design," *IEEE Internet Things J.*, Dec. 2021.

[7] X. Ling, Y. Le, J. Wang, and Z. Ding, "Hash access: Trustworthy grant-free IoT access enabled by blockchain radio access networks," *IEEE Network*, vol. 34, no. 1, pp. 54–61, Jan. 2020.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Tech. Report*, Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2084–2123, Thirdquarter 2016.

[10] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for IoT networks," *IEEE Internet Things J.*, Sep. 2018.

[11] L. Lao, X. Dai, B. Xiao, and S. Guo, "G-PBFT: A location-based and scalable consensus protocol for IoT-Blockchain applications," in *Proc. IEEE 34th Int. Parallel Distrib. Process. Symp. (IPDPS'20)*, New Orleans, USA, May 2020, pp. 664–673.

[12] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, Mar. 2020.

[13] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Inf.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.

[14] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. K. Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," *Comput. & Secur.*, vol. 95, p. 101871, Oct. 2020.

[15] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[16] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT press, 1994.

[17] J. R. Douceur, "The Sybil attack," in *Proc. 1st Int. Wksp. Peer-to-Peer Syst. (IPTPS'02)*. Cambridge, US: Springer, Mar. 2002, pp. 251–260.

[18] K. Finkenzeller, *RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John Wiley & Sons, 2010.