21, rue d'Artois, F-75008 PARIS
http: //www.cigre.org

CIGRE US National Committee
2021 Grid of the Future Symposium

Conceptual Design of a Consensus Mechanism for Renewable Energy Markets on Blockchain

A. ARAB[1], A. KHODAEI[1], M. CHOOBINEH[2], H. ZHENG[3], A. VUKOJEVIC[3]
University of Denver[1], Independent Researcher[2], Commonwealth Edison Company[3]
USA

SUMMARY

Blockchain is a powerful enabling technology for the decarbonization, decentralization, and digitization (3D's) of energy systems. The 3D's are some of the driving forces of transition into a new energy economy that has a higher level of efficiency, sustainability, and equity. However, there is still a set of limitations in existing blockchain technology that preclude a full-scope, wide-scale adoption of this technology in power and energy systems. This paper intends to address one of the pressing implementation challenges by proposing a novel consensus mechanism, namely *Proof-of-Reserve* (*PoR*). The goal is to facilitate an efficient peer-to-peer consumer-prosumer transactions on a blockchain platform as a transaction infrastructure for renewable energy markets.

KEYWORDS

Blockchain, consensus mechanism, decarbonization, energy market, power systems.

ali.arab@du.edu

1. INTRODUCTION

Decarbonization, decentralization, and digitalization are the pillars of the new energy economy. Blockchain technology has shown a promising potential to facilitate the transition to this new paradigm by providing a secure, peer-to-peer (P2P) transaction infrastructure. It can potentially significantly impact the existing operational models in power systems, including networked grids, demand-side management, the Internet of Things (IoT), electric vehicles (EVs), and cybersecurity, among others [1].

As a digital distributed ledger, blockchain can support a broad range of data—from financial transactions to power system signals—that are stored in a package called a *block*. These blocks are connected in chronological order and identified by a cryptographic characteristic called a *hash*. Besides the current hash, the previous block hash is also included in the block, that links them and creates a chain of blocks, hence the name *blockchain*. In general, each block in the blockchain contains a *block header* and a list of all transactions. The block header includes the *Merkle Root* of all transactions inside the block, the previous block hash, a *time stamp*, and a *nonce* (an arbitrary piece of data used for consensus). A specific process called *consensus mechanism* is required to make the blockchain fault-tolerant and prevent the injection of falsified data into the chain.

Through the consensus mechanism, all nodes in the chain agree on the correctness of the latest block added to the chain. This task is delegated to *miner nodes* in the blockchain, and the action itself is called *mining*. In other words, mining is the instance of validating and adding the new blocks to the chain. For this purpose, a mathematical problem should be solved that needs a considerable amount of computational power. In fact, this process has been designed to prevent hackers from injecting falsified data into the chain. The most common consensus algorithms are Proof-of-Work (PoW), Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof-of-Authority (PoA), and Proof of Elapsed Time (PoET) [2-6]. For example, in PoW as one of the most popular consensus methods, a miner node collects pending transactions, finds their corresponding Merkle Root, and together with some other data, collectively hashes a value that is less than a preset value. This preset value is a 32-byte number with some zeros usually at the beginning of the block hash, which makes the PoW adequately difficult to solve. To change the hash value, a nonce is embedded in the block header. Therefore, solving this problem is a probabilistic process that needs significant computational power. If the number of zeros is equal to n, then PoW needs, on average, 2^n attempts before the problem is solved, where the probability of finding such nonce for a given target value T is equal to $T/2^{256}$ [7].

Although several consensus mechanisms have been developed to improve the system throughput, more efforts are needed to create a mechanism that offers better energy savings, a higher level of tolerance for threshold adversary, as well as improved scalability, security, and privacy [8]. Currently, PoW, one of the most frequently used consensus algorithms, provides a relatively fair and secure method to reach a consensus. However, this algorithm suffers from high energy consumption and is still vulnerable to the 51% attacks. Authors in [9] characterized PoS as an algorithm that was designed to mitigate the limitations of PoW by replacing mining action with forging. This algorithm ensures lower energy consumption and processing time at the expense of a lower decentralization in the network. As in the PoS algorithm, nodes with higher tokens at stake have a higher voting power, which clearly renders the blockchain network vulnerable to monopolization. To solve this issue, Delegated Proof-of-Stake (DPoS) was introduced. In DPoS, every wallet with coins can vote for some delegates who then are responsible for validating the transactions and creating the blocks [10]. In this method, even users with small stakes can be selected as delegates. While this algorithm helps achieve a higher

level of decentralization and scalability, it still suffers from the issue that people with higher stakes have more voting power, and hence more influence on the network. Proof-of-Activity is a mechanism that integrates the PoW and PoS algorithms to add another level of security to the network [11]. In this algorithm, the probability of choosing a node as a miner depends on their tokens at stake (similar to PoS). The probability that a miner could create a block and receive the reward depends on their computational power, as is the case in PoW. Thus, security in this method still comes at the expense of higher energy input needed to solve the PoW problem. Proof-of-Capacity (PoC) uses the participants' available hard disk capacity as a meter to allocate the mining rights instead of computational power or the tokens at stake [12]. This algorithm also has a "monopoly issue" since the participants can outsource the file storage to an external capacity. PoET solves the computational power or staking issues by running a lottery-based election model. Each validator requests a wait time in this algorithm, and the shortest wait time wins the lottery. This validator is called a *leader* who can mine the block [13]. PoET uses the trusted enclave in Intel's Software Guard Extensions (SGX), which makes this consensus algorithm dependent on a third party (Intel), which is in clear contrast with the promise of blockchain technology. Further, an attacker can always win the lottery if they can break a piece of trusted hardware in this network [12]. Revealing the identity of the miners and validators is another issue in some blockchain platforms. For instance, the PBFT (used in Hyperledger Fabric) and Tendermint consensus mechanisms need to have the user's information to select a primary/proposer in each round; however, they can only handle not more than one-third of malicious nodes [14].

A review of the existing work reveals three main issues in existing consensus algorithms: (a) high computational power needs, (b) creation of a monopoly in the network, and (c) disclosing user's information. These problems are major obstacles to the adoption of blockchain technology in the power sector. The computational power consumed by algorithms such as PoW imposes a significant burden on power systems. This issue is so significant that recent research work indicate that the total power consumption used by these algorithms is comparable to the total power demand in Denmark or Switzerland [1], [15]. This extra burden on power demand can significantly stress the entire grid operations. The second issue can endanger the efficiency of the power markets by creating a monopoly because of using the existing consensus mechanisms. This could cause not only a few groups of nodes to always win the mining reward, but also, in a worst-case scenario, they could manipulate the system by earning more than 50% of the mining power. This is obviously not an appropriate design choice in the power grids since it causes considerable security and underperformance issues. Finally, the third issue makes the existing consensus mechanisms inefficient in power system applications, as compromising users' privacy and data protection is not a choice in power grids. All these discussions imply that a custom-built design of consensus mechanism is required for power system applications.

A number of recent research work have focused on developing a set of consensus mechanisms that address cost and energy concerns. For instance, authors in [16] proposed an alternative consensus model, namely Proof-of-Energy (PoE). The PoE operates similarly to a PoS, where energy consumption is considered as the stake. This is intended to increase prosumer self-consumption levels, and therefore reduce power losses. Authors in [17] adopted a consensus algorithm to determine potential rewards for the prosumers who use less energy during peak hours. Utility companies can establish a reward policy by adjusting the rewards for the PoW. To fill this existing gap, in this paper we propose a novel consensus mechanism specifically designed to facilitate peer-to-peer solar energy trading in power systems. The remainder of this paper is organized, as follows. Section 2 provides an overview of P2P energy trading. Section 3 presents the novel consensus mechanism. Concluding remarks are made in Section 4.

2. P2P ENERGY TRADING ON BLOCKCHAIN

To develop a blockchain-based power trading platform, there must be a distributed market clearing process to determine the optimal price and quantity for power supply by prosumers. A mechanism where prosumers and consumers can initiate their transactions on a blockchain platform needs to be designed to facilitate this process. Therefore, a transaction structure where each transaction can be performed and broadcasted to the blockchain network must be developed. At this stage, a consensus mechanism needs to be designed for the network to complete the transaction and form a block. We propose a novel consensus algorithm, namely Proof-of-Reserve, to address this issue. In the proposed PoR consensus mechanism design, once a block is created, the transaction will be finalized and stored in the digital distributed ledger.

The optimal interaction model between electrical nodes in the power system depends on how the system is governed. This issue becomes more critical when these interactions are carried out on a blockchain platform. To establish a fully distributed network, a game-theoretical mechanism design is needed to establish a Nash equilibrium between a group of prosumer and consumer nodes. A prosumer is considered a "leader" who determines the price, and a consumer is considered a "follower" who determines their optimal level of consumption. The sequence diagram in Figure 1 illustrates the end-to-end process in the proposed peer-to-peer energy trading model on a blockchain platform—from its initiation throughout the completion of a transaction. In this diagram, *C* denotes the consumer, and *P1-P4* denote four available prosumers in a pool of prosumers (chosen on an *ad hoc* basis for the sake of illustration). This diagram depicts a scenario where consumer *C* calls all four prosumers for the power it needs. Prosumers submit their bids, where among them, consumer *C* selects prosumer *P1* by sending an offer. Once the offer is accepted by prosumer *P1*, the transaction is initiated by consumer *C*, and the power will be supplied by prosumer *P1*. Next, the validation board is formed by remaining prosumers, and in a lottery where the odds of winning are based on power reserves, *P3* is selected to mine the block. Finally, the transaction is completed after prosumers receive and verify the data in the newly mined block, and all the nodes keep a ledger of the completed transaction.

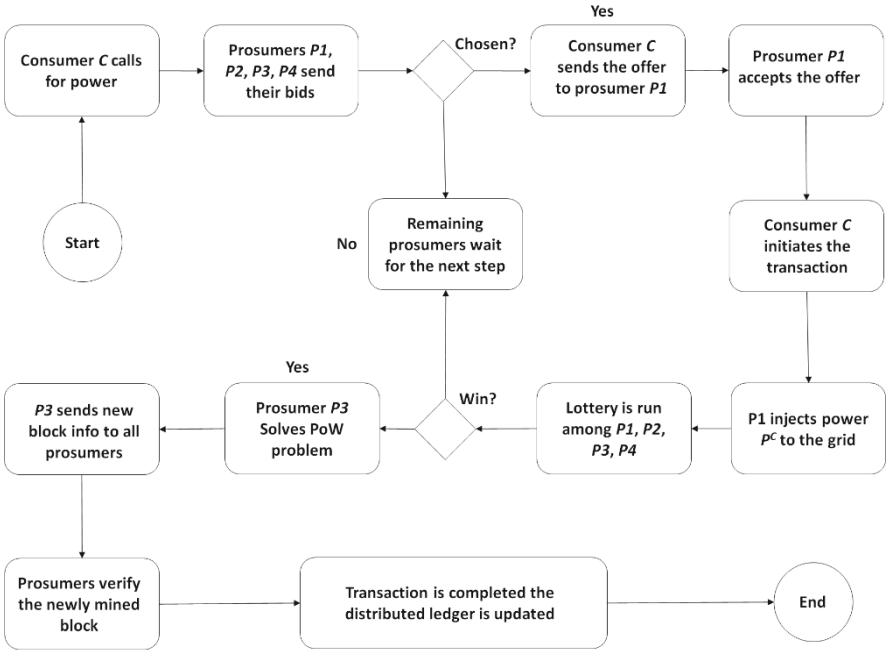

Figure 1. End-to-end process for peer-to-peer energy trading on blockchain

3. PROOF-OF-RESERVE MECHANISM

The consensus mechanism is developed based on the proposed PoR algorithm. This algorithm is a combination of PoS and PoW algorithms. On the one hand, it attempts to avoid the high computational power needed in the PoW algorithm while allowing as many nodes as possible to participate in the mining process. On the other hand, it maintains the voting procedure and higher scalability potential of the PoS algorithm. While the mining is still carried out in this mechanism, it is restricted to a certain number of candidate nodes. This algorithm involves cryptographic hashing where the new block is mined by solving a problem with a difficulty level that can be weighted based on the corresponding miner's power reserve. This power reserve can be calculated as follows:

$$R_i^{CM} \square P_i^{solar} - P_i^{C,pro} + C_i\, P_i^{B,\max} \qquad \forall i \in \mathrm{N} \tag{1}$$

where R_i^{CM} is the allocated reserve (in kW) for the consensus mechanism, P_i^{solar} is the real-time solar power generation by prosumer i (in kW), $P_i^{C,pro}$ is the power consumed by the prosumer i (kW), C_i is the price (in \$) for deep discharge of the battery installed at the prosumer i's location, $P_i^{B,max}$ is the maximum available battery capacity of prosumer i (in kW), and N is a set of prosumers. The detailed procedure of the PoR mechanism is defined, as follows:

- **Step1:** All candidate miners will announce the available power that they are willing to sell. We call this available power the *reserve*. If a prosumer does not intend to participate in the market, they will use their excess solar power to charge their on-site battery storage unit.
- **Step 2:** For each specific reserve level, a solar stake is allocated to each prosumer. For example, if a prosumer has n kW of reserve, they will obtain $[n/L]$ solar stakes, where L denotes each specified power level. Each solar stake can be earned by reaching a specific reserve.
- **Step 3:** All candidates will enter a lottery. The lottery is designed so that candidates with higher solar stakes have a higher chance of winning. A select number of candidates (validation board, k) will compete in the next round to solve a consensus problem and become a block miner. This process should first take place by verifying all transactions included in a prospective block. The difficulty of the consensus problem can be weighted according to the reserve that a prosumer holds. After the consensus problem is solved by one of the prosumers, the validation board will verify the mining process and publish their vote on whether a miner has won the lottery. If so, the winner will be rewarded with a token. Otherwise, that miner will be removed from the validation board and the competition will continue by the rest of the candidates.
- **Step 4:** This round of lottery will be closed, and new solar stakes will be calculated for the next round. This procedure will be repeated from Step 1 for each round.

The procedure described above will allow even prosumers with lower solar stakes to win the lottery and to mine the next block. Statistically speaking, this will virtually prevent the system from being monopolized, which, while theoretically possible, has an extremely low probability. This is due to the fact that a prosumer with higher reserves has a higher chance to mine the block and receive the reward. This mechanism seems fair as it provides a trade-off for prosumers. A rational prosumer intends to maximize their revenue by participating in the lottery with the highest reserve possible while they take into account the amount of electricity that is needed for mining. If a prosumer posts a reserve higher than the limit, they will need to buy the extra power from the market—which can significantly reduce the profit margin of the prosumer due to participating in both the market and the mining process. Obviously, the profit margin

depends on the reward value to be obtained by winning the lottery. Therefore, the blockchain platform administrator should face this subtle point of reward selection very carefully. Moreover, suppose a prosumer seeks to earn higher solar stakes in order to increase their chance of being selected for mining. In that case, they will be encouraged to install more PV panels which makes the grid cleaner, helps remediate grid congestions, and provides higher flexibility on the demand side. Therefore, while it is expected that some larger PV prosumers will have a higher chance of winning, this also may help to increase the efficiency of the entire network. It is worth noting that these large prosumers are only competing over creating a block and not making transactions. Therefore, the market clearing process and the PV trading may not be adversely affected, as all market participants are treated equally.

To illustrate the computational efficiency of the proposed consensus mechanism, we design a computational experiment with the combination of three different CPU configurations and two levels of difficulty to solve a consensus problem. We assumed the number of candidates in the validation board to be k=3, where candidates with 10, 9, and 8 solar stakes compete over solving a consensus problem in each combination of CPU configuration and difficulty level shown in Table 1. As shown, the same nonce values are obtained in all scenarios of a given difficulty level while computation time varies based on CPU configuration. For a given difficulty level, the time duration of the mining algorithm slightly increases by a reduction in computational power. However, the computation time is shown to be a function of the consensus problem's difficulty level, as expected. In addition, the results demonstrate that the nonce value increases significantly as the consensus problem's difficulty level increases. This is due to a higher number of iterations needed to meet the target value of a consensus mechanism with a higher difficulty level.

Table 1. The consensus problem computation performance for different CPU configurations and difficulty levels

CPU Configuration	**Nonce / Computation Time (s)**	
	Difficulty level=27	**Difficulty level=29**
Core i7/ 3.00 GHz/ 8 GB RAM	85,139,183 / 275	1,418,926,383 / 4720
Core i5/ 3.00 GHz/ 4 GB RAM	85,139,183 / 281	1,418,926,383 / 4757
Core i3/ 3.00 GHz/ 2 GB RAM	85,139,183 / 293	1,418,926,383 / 4788

4. CONCLUSION

A conceptual design for a novel consensus mechanism for power systems, namely Proof-of-Reserve, was presented. The PoR mechanism can significantly reduce energy consumption, as only a fraction of prosumers can participate in the block mining process. The proposed design intends to prevent monopolization of the blockchain platform as opposed to the existing mechanisms such as PoS algorithms. A lottery-based system will determine the miners, and there is a possibility that any prosumer in the network can mine the next block. PoR establishes a competitive and fair environment among all participants and facilitates a transition towards a greener and more sustainable system. In our future work, an extended numerical analysis and mathematical formulation of a game-theoretical framework will be presented to quantitatively test the effectiveness of proposed model.

BIBLIOGRAPHY

[1] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, A. Peacock, "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities," Renewable and Sustainable Energy Reviews, vol. 100, pp. 143-174, 2019.

[2] C. Dwork, M. Naor, "Pricing via Processing or Combatting Junk Mail." Advances in Cryptology, vol. 740, pp. 139–147, 1993.

[3] S. King, S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake." Self-published Paper, 2012.

[4] M. Cortro and B. Liskov, "Practical Byzantine Fault Tolerance." Proc. 3rd Symp. Op. Sys. Design and Implementation, New Orleans, LA, 1999.

[5] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake." ACM SIGMETRICS Performance Evaluation Review, vol. 42, no. 3, pp. 34-37, 2014.

[6] G. Prisco. "Intel Develops Sawtooth Lake Distributed Ledger Technology for the Hyperledger Project." Bitcoin Magazine, 2016.

[7] N. Z. Aitzhan, D. Svetinovic, "Security and Privacy in Decenralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," IEEE Trans. on Dependable and Secure Computing, vol. 15, no. 5, pp. 840-852, Sep/Oct. 2018.

[8] L. Yang, "The Blockchain: State-of-the-Art and Research Challenges," Journal of Industrial Information Integration, vol. 15, pp. 80-90, Apr. 2019.

[9] A. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K. K. R. Choo, A. Y. Zomaya, "Blockchain for Smart Communities: Applications, Challenges and Opportunities," Journal of Network and Computer Applications, vol. 144, pp. 13-48, Jul. 2019.

[10] Z. Chen, Y. Zhu, "Personal Archive Service System using Blockchain Technology: Case Study, Promising and Challenging," IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, USA, Jun. 2017.

[11] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," in Proc. 9th Workshop Econ. Netw. Syst. Comput. (NetEcon'14), pp. 34–37, Jun. 2014.

[12] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Sok: Consensus in the Age of Blockchains," arXiv preprint arXiv:1711.03936, 2017.

[13] A. Baliga. "Understanding blockchain consensus models," Persistent Systems Ltd. Tech. Rep, [Online]. Available :https://www.persistent.com.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE 6th International Congress on Big Data, Honolulu, USA, Sep. 2017.

[15] S. Lee, Bitcoin's Energy Consumption Can Power an Entire Country- But EOS Trying to Fix That, *Forbes,* Apr. 2018. [Online]. Available at: https://www.forbes.com.

[16] P. Siano, G. De Marco, A. Rolán and V. Loia, "A Survey and Evaluation of the Potentials of Distributed Ledger Technology for Peer-to-Peer Transactive Energy Exchanges in Local Energy Markets," in IEEE Systems Journal, vol. 13, no. 3, pp. 3454-3466, Sep. 2019.

[17] K. Inayat, and S. O. Hwang. "Load Balancing in Decentralized Smart Grid Trade System Using Blockchain." Journal of Intelligent & Fuzzy Systems, vol. 35, Iss. 6, pp. 5901-5911. Jul. 2018.