A PROPOSED E-POV CONSENSUS TO ATTAIN RESILIENCE OF POWER GRID FRAMEWORK FROM CYBER ATTACKS

Rashi Saxena
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Hyderabad, Telangana, India- 500075
rashisaxena.cse@klh.edu.in

P. Lalitha Surya Kumari
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Hyderabad, Telangana, India- 500075
vlalithanagesh@gmail.com

Article history:
Received 16.03.2024, Accepted 04.06.2024

Abstract

In recently, the blockchain has grown in prominence, but studies have concentrated on its underlying consensus mechanisms. The majority of the present consensus mechanism study focuses on public blockchains but is based on advanced distributed algorithms or consensus algorithms which are currently in use. On the consortium blockchain, many different application scenarios have been created, however few researchers focus on bespoke consistency algorithms. Furthermore, while building consensus procedures, security and performance must be traded off. Proof of Vote (PoV) is the name given to the efficient voting-based consensus algorithm disclosed in this paper.With the fundamental concept of creating distinct security identities for network nodes, PoV distinguishes among voting & bookkeeping rights. EPoV is an effective voting-based consensus algorithm that we propose in our paper. We change the gaps in PoV to Extend PoV, as required by the power grid system model. The comprehensive and in-depth final result aims to expand on current knowledge of PoV's possible applications and open up new research directions

Key words

Extended Proof of Vote, Consensus Algorithms, Security, Block Chain, Smart grid, Cyber Security

1 Introduction

1.1 Smart Grid System Model

Power & energy system infrastructure with operation are constantly improved by incorporating new power generation designs and cutting-edge protection and control technologies. As a consequence, multiple protective strategies & control methods were needed to guarantee the reliability of smart energy systems. Because energy and power supply affect practically each part of our lives in certain manner, incorporating new digital methods in the power system has grown crucial in past few decades. Structures including smart buildings, Smart Grids (SGs), smart houses, smart appliances, & tech devices incorporate technological tools. Improvements in data transfer via communications systems, as well as different methods for improving communications infrastructure safety via intelligent systems, have contributed to the present study focus in this subject [6] [14].

1.2 Block Chain Design Model

The blockchain was created as a novel method of data storage for the network of cryptocurrencies like Bitcoin [7]. This could keep all past statistical info, account statements, as well as other pertinent data by adopting a self-referencing blockchain system for storing information. A tremendous quantity of information is stored in a peer-to-peer distributed network [16] and is cryptographically bundled into several data blocks. Every data block in the chain structure contains the critical identification data (Hash) of the previous blocks, connecting the blocks chronologically to produce a globally dispersed log record [3]. If hackers wish to change a particular data item within a block, they need recalculate the blocks as well as all subsequent block info. The consensus mechanism, which renders data manipulation for attackers computationally almost impossible, is one of the blockchain's key innovations. Blockchain application fosters spontaneous self-development in a decentralised system by utilising a consensus process, peer-to-peer transmission, distributed storage, & cryptography [10].

The three major blockchain classifications are public, private, and consortium blockchains [4]. Due to its openness, untraceability, and limited controllability, the public blockchain is subject to a number of prohibitions in many nations. The consortium blockchain provides the advantage of achieving "partial decentralisation" across some established structures, hence keeping the consortium effective & fair. It is a hybrid of the private & public blockchain systems. Depending on the engagement of significant international banking heavyweights in the R3 CEV blockchain project [9], banking firms seem to be drawn to the use cases of consortium blockchains. The transparency and unreliability of information on the Internet allow for identity theft. Therefore, traditional Internet transaction data needs to be verified as accurate by a third-party reputable agency [8]. Online trading poses a security risk because if a third-party platform fails, the assurance it offers cannot be relied upon. Because it is built on cryptography rather than trust, the blockchain is a key capability for effectively conveying & safely preserving transaction information.

Byzantine Fault Tolerance (BFT)-based consensus uses a voting-based mechanism to improve efficiency at the cost of safety. Since of access issues, there are less nodes, allowing the ultimate choice to be based on the voting outcomes of the bulk of nodes. Instances of widespread BFT consensus are PBFT and BFT-SMART [5], [2]. The introduction of centralized nodes into the distributed system in BFT-based blockchain results in an improvement in throughput. With the fundamental concept of creating distinct security identities for network nodes, PoV (Proof of Vote) [11], [12] separates the voting rights and bookkeeping rights. Unlike a third-party mediator or uncontrollable public awareness, the results of vote among core consortium members decide block creation & authentication. When there are more than 100 nodes, PoV only has total traffic complexity of O(3N), which is a significant improvement over BFT-based consensus.

Blockchain is an irreversible distributed ledger that enables the storage of information without the involvement of a third party. Blockchain technology has piqued the interest of many researchers, notably in its use in smart grid cyber security. Despite considerable attempts to employ blockchain in the smart grid for data security, a comprehensive study of blockchain in the smart grid for cyber security from both an application & technical standpoint is lacking. 51% attack tolerance, near-impossible manipulation, and no finality are all influenced by security performance. 33.33% attack tolerance, changeable, finality enabled [20]. Overcoming this difficulty, we are going to focus on a novel technique and preforming superior results.

1.3 Focus and Gap

According to our previous research, a PoV consensus block chain could be a realistic option for increasing the data safety of the current power strategy. In addition, a previous study found a 51% attack vulnerability in the block chain and smart grid. Finally, the system's efficacy has been analyzed based on the possibility of attacks, and it has been determined to be successful. Thus, we claimed that using metres as nodes in a distributed net that encodes metre data as blocks could enhance the rigidity & security of the power grid. The use of PoV in the proposed distributed Block-chain for power grid networks increases the level of security and resistance to cyber-attacks. Additional future work targeted at safeguarding against cyberattacks while finding a balance between privacy protection and regulation will improve the performance of our Block-chain system with PoV agreement. So, we are focused on the Extended PoV approach, in order to satisfy or improve the privacy and confidentiality of people's information.

1.4 Objective

To propose an Extended Proof-Of-Vote Consensus to attain resilience and consistency of the framework. Our work is the combination of Proof-Of-Work and Proof-Of-Vote. In our research, we use PoW to strengthen security & satisfy or enhance the confidentiality and safety of people's information. When adopting our recommended approaches, the produced blockchains and votes that are gathered and counted are secure and safe. We highlight various conditions that must be met in order to update the consensus process of a PoW blockchain in a safe, profitable, and easy manner. The proposal should strengthen the security of our consensus by minimizing existing attack avenues and blocking new ones. Depending on the cryptographic underpinning of blockchain systems, PoW ensures its security & confidentiality by utilising the secure and dependable setting of the commissioner nodes. This paper presents a comprehensive consensus mechanism that utilizes voting processes with consortium blockchains. The existing consensus technique sacrifices performance to ensure security because security and availability are so important. Under safety-assured settings, our approach can offer better block chain efficiency with minimal transaction identification delays.

Our proposed method is structured as follows: Section 2 covers writings that are connected to one another. Part 3 explains our proposed technique, including the tools and methodology we applied. The conclusion and discussion are included in Section 4. The paper concludes at Section 5.

2 Related Works

In this section, we look at existing studies, authors, and proposed blockchain models, as well as their pros and cons.

According to Line et al. [13] presented the security architecture as a block chain in smart grid application. This system does have a few drawbacks. Some components of the layered stack are not industry standard. This lack of standardisation affects cross-protocol levels like the service layer as well as the performance monitoring layer, which might have an influence on security token issuance & maintenance.

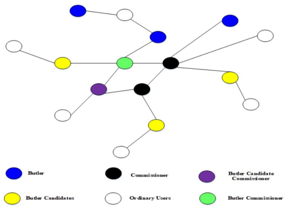

Figure 1. Four roles in PoV

Anusha Vangala et al [18], proposed a fresh smart grid-based blockchain-envisioned authenticated key agreement technique for a setting of smart farming. Comparing the proposed SCBAS-SF to various authentication systems, a detailed comparison reveals that it offers higher security at a lower communication cost and comparable computation cost. Block-chain technology has been viewed as a viable approach for addressing the aforementioned cyber security challenges in smart grids [16-19].

Sengan et al. [1] demonstrated the integrity of false data cyber-attacks in the physical layers of smart grids. The work then concentrates on employing an Agent-based strategy to decentralise Data Integrity Safety in the network. Lastly, the productivity and efficiency of the created modelling strategies are empirically evaluated and contrasted to current framework supervised deep-learning models. The next section gives the detailed explanation of our proposed work.

3 Research Methodology

3.1 Techniques Used

Problem Definition The PoV consensus mechanism proposed by the consortium blockchain is expected to meet the following requirements:

Consistency: All nodes' copies of the blockchain data should be able to achieve a last consistent state and provide a single external service. In PoV, the end validation and tamper-resistance of transactions are realized with just one block, which has consensus termination.

Availability: The system's services should always be accessible owing to the consensus mechanism. The system should react to every operation request in a certain amount of time. PoV makes sure that, with the right parameter values, the consensus process can operate and generate blocks in a finite amount of time.

Partition Tolerance: When the system breaks down in any network partition, the distributed system should ensure the provision of services. With specific security presumptions, PoV can tolerate partitions to a certain extent.

Efficient: The throughput must be as high as feasible, measured as the overall amount of transactions $\sum_i |t_i x_i h_i|$ executed per unit time.

Proof of Vote (PoV) The PoV consensus algorithm is detailly explained in this section. Proof of Vote (PoV) consensus procedure provide superior effectiveness than present ones in terms of security, resource consumption, transaction throughput & transaction confirmation time. In the consensus PoV design, nodes are classified into four roles: commissioner, butler, butler candidate, & ordinary user. The functions in the PoV system are depicted in Figure 1.

Commissioner: A consortium committee is formed by a number of businesses or organization's from around the world, and the group works together to operate a consortium blockchain system. One of the consortium committee members, a commissioner may also serve in other capacities. To join the network, a new commissioner should be authorized under it's proposed consortium rule & recognized by a node on the consortium blockchain system. The butlers are subject to commissioner recommendations, votes, and evaluations. Additionally, they have a duty to forward and confirm blocks of data. All commissioners will receive broadcasts of newly created blocks in the blockchain network for verification. A block is deemed genuine and added to the blockchain when it receives a majority of votes. Voting outcomes reflect the consensus of all commissioners.

Butler: Block production is a specialty of butlers. There are a finite number of butler nodes. By designing the butler job, we separate the voting with bookkeeping rights. While butlers are in charge of generating blocks, or bookkeeping, voting is handled by commissioners. Butlers are similar to Bitcoin's miners, but they don't have to squander processing resources to claim the right to make blocks. Instead, they are chosen at random by the consensus rule to produce a block. A butler must gather network transfers, put them together into a block, and then sign the block. To choose the butler team, the commissioners cast votes for butler applicants. The butlers alternately create blocks in a random manner throughout their tenure, then when their terms expire, they agree to run for office again. At the same time, a node can serve as both a commissioner and a butler. Two steps are required to become a butler:

●Sign up as a candidate for butler. ●Gain the butler's election.

Butler Candidate: Because there are a finite number of butlers, commissioners can only choose butlers by ballot from candidates who are butlers. If the butler candidates don't win, they can hang around online while they wait for the next election. To become a butler candidate, follow these three steps:

● Make an user id in the consortium platform and submit an application for the post of butler ● Send a letter of recommendation dated and signed by at least one commissioner. The commissioner calls an asymmetric encryption function to produce the recommendation letter, which is produced similarly to the invitation code. To avoid forgery, the recommended letter is encrypted using the private key.

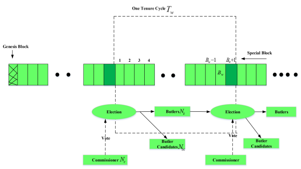

Figure 3. Consensus model of one tenure cycle

• Make the required deposit to apply to be a butler. For the purpose of recommending themselves to be butler candidates, commissioners can continue to serve in both of their dual responsibilities as commissioners and butler candidates.

Ordinary User: Ordinary users do not need permission to enter or exit the system at any time. While accepting assistance of the system, they can also observe the entire consensus process. Ordinary users are required to participate in the block forwarding process as well as have the right to submit transactions during the block generating process.

PoV offers a flexible node access mechanism and a representation mechanism that substantially minimize communication complexity, greatly enhancing scalability [19]. The blockchain's throughput is significantly constrained by the serial production of blocks because it still records data in a linked framework. Figure 2 shows relationship between the roles used in PoV.

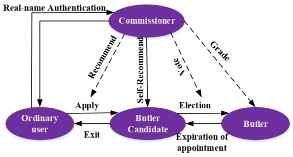

Figure 2. Conversion of four roles

3.2 Experimental setup

This section describes the experimental procedures employed in our proposed method. For our planned E-PoV effort, we use a consensus and voting process.

Consensus Process

We utilize the notation N_c for the number of commissioners, N_b for butlers, N_{bc} for butler candidates, and N_o for ordinary users. The total number of roles is N_{all} because each node may have several identities. This meets the condition $N_{\text{all}} \leq N_c + N_b + N_{bc} + N_o$, where N_b is a constant. Each butler is given a number between 0 and $N_b - 1$ for each tenure. Typically, there are more butler aspirants than butlers available $(N_{bc} < N_b)$. To guarantee that the process operates well, the butlers would be given numerous statistics if $N_{bc} < N_b$, that is, there are not enough contenders for the position of butler. For instance, when $N_b = 8$ and $N_{bc} = 6$, the system progressively allocates the butlers $\{B_1, B_2, B_3, B_4, B_5, B_6, B_1, B_2\}$ the numbers from 0 to 7. The butlers B_1 and B_2, who received the most votes, can each receive two butler numbers.

We suppose that the butler has a tenure of T_w during which time every tenure, $B_w + 1$ valid blocks are generated, the final among which is a special block holding information on the butlers' elections & associated data. For a block to be considered legitimate, it must amass at

A valid block is produced by a butler during a round of consensus. Every round of tenure has a total of $B_w + 1$ rounds of consensus, during which $B_w + 1$ valid blocks are created. At the end of every consensus round, the butler invokes a procedure to generate a random integer. The responsibility of creating a block in the next consensus round is therefore assigned to the butler whose number equals R. The $(R + 1)^{\text{th}}$ butler will re

The special block is the $(B_w + 1)^{\text{th}}$ block created during the tenure. In this round of consensus, the current butlers & butler hopefuls compete to become the next butlers of the upcoming tenure. The most popular N_b candidates will ultimately prevail in the election, with each commissioner providing a voting list. The results of the election and related data will be entered into this unique block. After this unique block was constructed, the current butlers formally retired, as well as the fresh butlers started working in the new tenure.

Voting Process The "proof of vote" concept is represented in the layout of two types of consensus mechanisms. The butler team is supported by the second and the block production by the first. By returning their signatures, the commissioners cast their votes.

Voting for block production: Butler i generates a block and sends it to every commissioner. If Butler i agrees to produce this block, a commissioner will encrypt the block header and return the signature to him. The block is considered legitimate if Butler i receives at least $\left\lfloor \frac{N_c}{2} \right\rfloor + 1$ signatures in the allotted per

Voting for the butler candidate: Butler j solicits votes from each commissioner. After collecting and tallying the ballots, Butler j creates a separate block containing the results of the election and any relevant documents. This block is then transferred to all commissioners for confirmation.

Voting for the butler candidate: Butler j solicits votes from each commissioner. After collecting and tallying the ballots, Butler j creates a separate block containing the results of the election and any relevant documents. This block is then transferred to all commissioners for confirmation. Every commissioner retains a database of the butler candi

Designated tickets: The commissioner selects a certain group of candidates while considering individual aspects, or selects a random group of candidates, increasing the butler's mobility.

3.3 Object of study

Extended Proof of Vote (EPoV) The current platforms have a number of limitations, including modu-

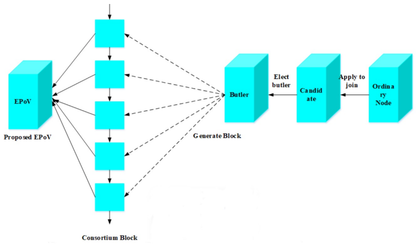

Figure 4. Proposed EPoV architecture

lar design, parallel computing, and privacy protection. In our analytical article, we use extended proof of vote to get beyond the privacy protection. Because of the great security features in Proof of Work, we integrate it with Proof of Vote. The generated blockchains and the votes that are gathered and counted are secure and safe when using our proposed methods. We outline some conditions in order to update a PoW blockchain's consensus mechanism in a safe, profitable, and smooth manner [15]. By reducing known attack vectors and blocking new ones, the plan should increase the security of our consensus. In essence, the system must be incentive-compatible, meaning that voters and commissioners should gain by adhering to the consensus rules while losing out if they do not. Depending on the cryptographic underpinning of blockchain systems, PoW ensures its safety & confidentiality by utilising the secure and reliable surroundings of the commissioner nodes. In this work, a full consensus model based on voting processes & consortium blockchains is provided. The existing consensus technique sacrifices performance to ensure security because security and availability are so important. Under safety-assured settings, our approach may offer high block chain efficiency & minimal transaction identification delays. We will examine the validity of POV in this section, which can be influenced by two factors: the incentive system and the voting process [17]. Figure 4 shows our proposed Extended Proof of Vote architecture. According to this diagram, ordinary nodes are attempting to join the candidate block before choosing to join the butler side. We create blocks on the butler side using our consortium algorithm. Votes generated by the commissioner are sent to the consortium blocks after the blocks have been generated, and the proposed EPoV method is then used to secure the votes in the consortium blocks. Our major goal is to secure or protect the votes and blocks that the commissioners and voters have produced and are registered in the proof of vote.

Security Lemma 1: Consider that there are N_c commissioners. Blocks are secure and legal as long as there are more than $\left\lfloor \frac{N_c}{2} \right\rfloor + 1$ effective commissioners.

Proof: Assume it is possible to successfully validate unlawful blocks. When there are more effectively commissioners than $\left\lfloor \frac{N_c}{2} \right\rfloor + 1$, the effective commissioners won't sign an illegal block because a butler has to obtain more than $\left\lfloor \frac{N_c}{2} \right\rfloor + 1$ signatures to generate a valid block. Consequently, the maximum number of signatures on an unlawful block is $N_c - \leq$

In order to accomplish desired results, implementing a new control system physically entails adjusting and utilizing a variety of physical characteristics within the system. This could entail modifying forces, energy, or other physical characteristics in order to affect the system's state or behavior. To improve the security and effectiveness of blockchain networks, a new control system that utilizes voting procedures and cryptographic principles (like those that support Proof of Work) is introduced within the framework of the Extended Proof of Vote (EPoV) architecture that is described in the analytical article. Physically speaking, this might entail:

Utilizing Computational Power: Computational power is needed for Proof of Work (PoW) to protect the blockchain network. The method makes use of computational resources to guarantee the security and integrity of the blockchain by fusing PoW with the EPoV voting mechanism.

Managing Energy Consumption: PoW systems frequently use large amounts of energy since mining requires a lot of processing power. Optimizing energy consumption while preserving security is critical from a physical point of view. It's possible that the new control system will include techniques to reduce energy use without sacrificing security.

Ensuring Data Integrity: Ensuring the integrity of votes and blocks is crucial in EPoV. Physically speaking, this can entail safeguards like encryption techniques or secure communication lines that guard against data manipulation or corruption.

Optimizing Resource Allocation: The goal of EPoV is to strike a compromise between security, privacy, and efficiency. Achieving these goals physically depends on allocating compute power, bandwidth, and other resources as optimally as possible.

Enhancing System Resilience: When designing a new control system, it is essential to take into account how resilient the system is to outside threats or disturbances. Physical steps like adding redundancy to hardware, spreading out network nodes, or putting failover mechanisms in place could be part of this.

In order to accomplish the intended security, efficiency, and resilience goals specified in the EPoV design, adding a new control system generally entails adjusting and managing physical parameters within the system.

4 Result And Discussion

The success of the proposed approach is examined in the section on results and discussion. The proposed technique is carried out using the Python framework. The system configuration for the suggested solution consists of a display that does not enable pen or touch input, a 64-bit operating system, an x64-based processor, and 16.0 GB of RAM. The cumulative distribution function with chi-square transmission and the cumulative distribution function with non-central chi-square dispersion are examined using the possibility of mass function. The likelihood that a discrete random variable, X, equals a particular number is expressed as a function over the sample space of X called the probability mass function (PMF).

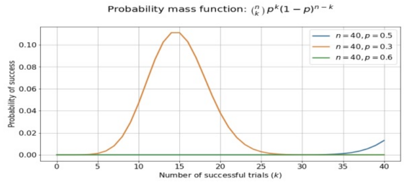

Figure 5. Probability Mass Function

The proposed approach's probability mass function is shown in Figure 5 along with the likelihood of success and the number of successful trials. The cumulative distribution curve is employed to explain the response variable's probability density function. It can be used to describe the potential for a discrete, continuous, or mixed parameter. The probability density function is added to determine the total probability for a random variable.

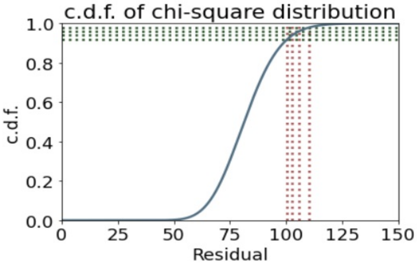

Figure 6. CDF of Chi-square distribution

Figure 5 represents the CDF of the chi-square distribution. The statistical technique known as the chi-square test is utilized to describe the connection among the categorical variables or columns in the database. It is used to demonstrate correlation without considering the order of the data. The chi-square test can be used in the following ways: Describe, in turn, the H0 and H1 suppositions. Determine the value of alpha (α) based on the domain you are functioning in. You should be prepared to tolerate a 0.5% risk or margin of error if α = 0.05. Check the information for Nans or other mistakes of this nature. Check the underlying assumptions of the test. After the test has been completed, determine whether to accept or reject the null hypothesis (H0). The Chi-square test procedure looks like this:

$$x^2 = \sum_i \frac{(O_i - E_i)^2}{E_i}$$

Where, x^2= chi-square, O_i = observed value, E_i= expected value. A research instrument for evaluating a number of data items is the Chi-square equation. It is indicated by x^2 and applied to information that have characteristics dispersed across various groups.

4.1 Potential applications of the results

Intriguing prospects for applications in physics and other natural sciences are presented by the Extended Proof of Vote (EPoV) architecture that proposed in this analytical study. Here are some possible uses for such a system:

Scientific Research Collaboration: In scientific research collaborations, EPoV could be used to safeguard and authenticate votes and blocks in consortium blockchains. Transparency and integrity in scientific research might be ensured by employing EPoV to securely preserve and verify study findings, experimental data, and even peer review procedures.

Data Integrity in Environmental Monitoring: EPoV could be used in environmental research domains to protect sensor-derived data that tracks several environmental characteristics like biodiversity, water quality, and air quality. EPoV has the potential to bolster confidence in environmental monitoring initiatives and facilitate evidence-based decision-making for environmental conservation and management by guaranteeing the validity and integrity of data held on consortium blockchains.

Secure Data Sharing in Astronomy: Researchers and observatories may benefit from the safe exchange and validation of astronomical data through the use of vEPoV. Collaboration and data integrity within the astronomy community might be ensured by storing observational data, computational models, and catalogs of celestial objects in consortium blockchains using EPoV.

Blockchain-based Particle Physics Experiments: EPoV has the potential to safeguard and validate data produced by particle physics experiments carried out at massive colliders . Through the use of consortium blockchains with EPoV, scientists could safely store and exchange experimental data, promoting cooperation and guaranteeing the accuracy of results in particle physics research.

Securing Genetic Data in Biology: Biology-related consortium blockchains storing genetic data may be protected and verified with EPoV. With the use of EPoV, genetic sequences, gene expression profiles, and genomic variants might be safely captured, improving data privacy and integrity for uses in personalized medicine and genetic research.

In conclusion, this article's proposed EPoV architecture presents a viable method for safeguarding votes and blocks in consortium blockchains, with possible applications across a range of physics and other natural scientific areas. By guaranteeing data confidentiality, transparency, and integrity, EPoV may help to advance scientific cooperation and study in these areas. The final section contains our document's conclusion.

5 Conclusion And Future Work

This article offers an innovative form of consortium-oriented consensus algorithm POV. In order to secure our built blockchain and the votes cast throughout the voting process, we additionally introduce Proof of Work alongside Proof of Vote. The PoV design, that is founded on the idea of voting by consortium members, is founded on the credibility difference among the consortium blockchain's core nodes as well as other nodes. The PoV paradigm defines four roles. The technique creates a voting system that guarantees that the consensus results are confirmed by a vast number of the commissioners but also offers the butler and butler candidate roles to guarantee consensus node rotation. Our future work will focus on detailed theoretical analysis and technical implementation, which will make it more suitable for real-world application scenarios.

References

M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac. Smart meter data privacy: A survey. *IEEE Communications Surveys & Tutorials*, 19(4):2820–2835, 2017.

A. Bessani, J. Sousa, and E. E. Alchieri. State machine replication for the masses with bft-smart. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 355–362, June 2014.

R. Bhattacharya, M. White, and N. Beloff. A blockchain based peer-to-peer framework for exchanging leftover foreign currency. In *2017 Computing Conference*, pages 1431–1435. IEEE, July 2017.

V. Buterin. On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, August 2015.

M. Castro and B. Liskov. Practical byzantine fault tolerance. In *OSDI*, February 1999.

D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275:1674–1683, 2018.

T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering*, 30(7):1366–1385, 2018.

R. Khalil and A. Gervais. Revive: Rebalancing off-blockchain payment networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 439–453, October 2017.

C. Khan, A. Lewis, E. Rutland, C. Wan, K. Rutter, and C. Thompson. A distributed-ledger consortium model for collaborative innovation. *Computer*, 50(9):29–37, 2017.

S. Kiyomoto, M. S. Rahman, and A. Basu. On blockchain-based anonymized dataset distribution platform. In *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*, pages 85–92. IEEE, June 2017.

K. Li, H. Li, H. Hou, K. Li, and Y. Chen. Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 466–473, December 2017.

K. Li, H. Li, H. Wang, H. An, P. Lu, P. Yi, and F. Zhu. Pov: an efficient voting-based consensus algorithm for consortium blockchains. *Frontiers in Blockchain*, 3:11, 2020.

M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer. Targeted attacks against industrial control systems: Is the power industry prepared? In *Proceedings of the 2nd Workshop on Smart Energy Grid Security*, pages 13–22, November 2014.

X. Liu and Z. Li. False data attack models, impact analyses and defense strategies in the electricity grid. *The Electricity Journal*, 30(4):35–42, 2017.

B. Mbarek, S. Chren, B. Rossi, and T. Pitner. An enhanced blockchain-based data management scheme for microgrids. In *Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020)*, pages 766–775. Springer International Publishing, 2020.

D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang. The blockchain as a decentralized security framework [future directions]. *IEEE Consumer Electronics Magazine*, 7(2):18–21, 2018.

S. Sengan, V. Subramaniyaswamy, V. Indragandhi, P. Velayutham, and L. Ravi. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. *Computers & Electrical Engineering*, 93:107211, 2021.

S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali. Smart grid cyber security: Challenges and solutions. In *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, pages 170–175, October 2015.

Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials*, 14(4):998–1010, 2012.

P. Zhuang, T. Zamir, and H. Liang. Blockchain for cybersecurity in smart grid: A comprehensive survey. *IEEE Transactions on Industrial Informatics*, 17(1):3–19, 2020.