SV-PBFT: An Efficient and Stable Blockchain PBFT Improved Consensus Algorithm for Vehicle-to-Vehicle Energy Transactions

Yao Suo[1], Yingsen Wang[1], Shichao Luo[1], Qianqian Yang[2], Juanjuan Zhao[1,2*]

[1] College of Information and Computer, Taiyuan University of Technology, China
[2] College of Information, Jinzhong College of Information, China
suoyao0607@link.tyut.edu.cn, 552383989@qq.com, q997012329@vip.qq.com, evie_yang@qq.com, zhaojuanjuan@tyut.edu.cn

Abstract

Aiming at the problems of difficult charging, long waiting time and energy loss of IoEV (Internet of electric vehicles) during peak charging period, we design a V2V (vehicle to vehicle) energy trading model to simulate the energy trading process. Considering the problems of malicious node attacks and privacy protection, we combine the V2V energy transaction model with a federated chain and explore a distributed ledger to record the V2V energy transaction process. In addition, we design a credibility mechanism to initialize nodes according to their comprehensive strength and select master nodes based on their behavioral performance of participating in consensus, which ensures the reliability of the consensus. Based on this, we propose a more efficient and promising consensus algorithm SV-PBFT (shapley value-PBFT), which simplifies the consensus process, reduces the communication overhead, and improves the consensus efficiency. The SV-PBFT consensus algorithm is used to replace the traditional consensus algorithm in V2V energy trading. The proposed SV-PBFT algorithm is validated by extensive simulation experiments, and numerical results are provided to confirm the good performance of SV-PBFT in V2V energy trading models.

Keywords: Blockchain, Consensus algorithm, Vehicle to Vehicle, Reputation mechanism

1 Introduction

1.1 Motivation

EVs (electric vehicles) [1] are a promising solution to combat climate change and reduce harmful emissions. In recent years, EVs are expected to be one of the most critical transportation modes and renewable energy users in intelligent transportation networks in future due to low carbon emissions, moderate costs, and environmental safety.

Energy demand has been growing rapidly due to the increasing number of electric vehicles and smart devices embedded in their systems. In recent years, V2G (Vehicle-to-Grid) [2] technology has been introduced to solve the demand response management problem of IoEVs. This is an emerging technology that combines renewable energy systems with EVs [3]. However, it cannot meet the demand for energy trading in social hotspots far from the main grid. And there is a high energy loss and long waiting time due to the presence of a large number of detour charging of EVs during peak charging hours and a large number of EVs with excessive energy. V2V energy sharing, on the other hand, is a more convenient and flexible way to charge EVs and helps to reduce their energy consumption [4]. The design and implementation of a V2V energy sharing network will greatly reduce mileage anxiety of EVs while requiring minimal infrastructure investment. By actively guiding pure EV owners to charge in the low valley, they can obtain the reduced charging cost due to the low valley price difference and effectively reduce their daily car costs. And by actively guiding pure EV owners to charge in the low valley, they will receive a reduction in charging costs due to the low valley price difference, effectively reducing daily charging costs.

The IoEV environment is considered unreliable and the trust of energy sellers, buyers and intermediaries is questionable (centralized trading can lead to monopolistic practices, for example, price gouging). The centralized V2V model can lead to security threats such as single point of attack and privacy leakage from external and internal sources by nodes to secure their own interests. To address the above issues, A. Dorri et al. [5-7] have applied Blockchain to energy transactions as a way to ensure secure energy delivery services. Blockchain is a distributed ledger that allows untrusted vehicles to maintain a distributed and transparent record of transactions. Blockchain [8] itself is decentralized, open and autonomous. C. Han et al. [9-11] illustrate blockchain applications in data security, financial education, and food traceability, respectively. Consortium chain [12] is a type of blockchain, mostly used for the collaboration between organizations and institutions, which can significantly reduce the cost of collaboration between enterprises and is therefore suitable for IoT applications. Consensus mechanism is the core of blockchain and is used to maintain trust between untrustworthy nodes [13]. The efficiency of blockchain systems depends heavily on the design of the consensus mechanism, which strongly influences the transaction processing rate, scalability, reliability, and security of the system [14]. Although consensus mechanisms such as proof-of-work (PoW), proof-of-stake (PoS), proof-of-authority (PoA), practical Byzantine fault tolerance (PBFT), and proof-of-reputation (PoR) have been proposed. However, there are

*Corresponding Author: Juanjuan Zhao; E-mail: zhaojuanjuan@tyut.edu.cn
DOI: 10.53106/160792642022112306003

still few consensus mechanisms specifically designed to improve the efficiency of V2V energy transactions for EVs.

Current consensus mechanisms are not effective for V2V energy transactions, and the main characteristics of IoT devices are the limitation of computational resources and memory, as well as the strict requirements for energy efficiency, which limit the computational difficulty of consensus algorithms. Currently, electric vehicles are embedded with smart devices to run real-time security applications, road infotainment, and utilize limited resources to allocate resources in complex communication environment. Therefore, we are motivated to design effective consensus mechanisms for V2V energy transactions to solve the above-mentioned problems in the V2V energy transaction process.

1.2 Main Contributions

The main contributions of this paper are as follows:

(1) This paper designs a blockchain-based V2V energy transaction model that uses a distributed ledger to record the V2V energy transaction process to ensure the security and tamper-evident of the transaction records.

(2) A reputation mechanism is designed to initialize points to nodes based on their overall strength. The master nodes are selected based on the behavioral performance of participating in consensus. And three types of nodes, including consensus nodes, preparatory nodes and blacklisted nodes are set, together with reward and punishment rules and node conversion rules, so as to reduce the probability of master nodes doing evil, reduce the frequency of view replacement and improve the efficiency of the algorithm.

(3) To address the problems of low throughput, high latency, and high communication overhead, we propose the SV-PBFT consensus algorithm, which speeds up the consensus process by changing the five stages of the PBFT algorithm consensus process into three stages.

(4) We provide a large number of numerical results to evaluate the performance of the proposed algorithm. It is verified through simulation experiments that SV-PBFT has good performance on V2V energy trading.

2 Related Work

2.1 V2V Energy Transfer

Several studies have been carried out to propose new solutions for V2V and V2G energy sharing. A. M. Koufakis et al. [15] proposed an online V2V energy exchange strategy based on price control. A. M. Koufakis et al. [16] proposed an optimal EVs charging scheduling scheme with V2G and V2V energy transfer options. M. E. Kabir et al. [17] developed an integer linear program (ILP) to maximize the number of EVs served by determining the optimal trajectory for each truck. S. K. Vempalli et al. [18] proposed a novel V2V charging technique that allowed charge transfer between two off-grid EVs and discussed its operation mode.

In addition, blockchain technology is used in energy trading to ensure the security and privacy of transactions conducted by untrusted nodes. R. Khalid et al. [19] presented a blockchain-based hybrid P2P energy trading market solution to reduce the cost of energy consumption, reduce harmful emissions (because renewable energy sources (RESs) are used to generate electricity at customer premises) and improve the resilience of smart grids. V. Hassija et al. [20] proposed a lightweight blockchain-based protocol called directed acyclic graph-based V2G network (DV2G). A. Barnawi et al. [21] proposed a blockchain-based demand response management for efficient energy trading between electric vehicles and charging stations. S. Aggarwal et al. [22] Deploying a secure V2G network in a smart grid (SG), we propose an energy trading scheme with blockchain between three communicating parties (i.e., EVs, CSs, and utility centers).

Koufakis, Kabir, Vempalli et al. [15-18] innovated EVs energy trading in terms of route planning, energy price adjustment, and new charging technologies for EVs, but the overall system is still centralized, which may bring problems such as the monopoly in practical application, so the introduction of blockchain can be considered to achieve decentralization effect. Khalid, Hassija, Barnawi, Aggarwal et al. [19-22] combined the designed system with blockchain, which improved the security of the system while increasing the efficiency, but little research was done on the consensus algorithm.

2.2 Consensus Mechanism

PoW [23] is mainly used to determine who will be out of the block by calculating the difficulty value. The workload of POW refers to solving the equation, whoever solves it first has the right to be out of the block. PoS (Proof of Stake) [24] can solve the problem of a large number of resources being wasted in PoW. Similar to the shareholder mechanism in real life, the more shares are owned, the easier it is to obtain bookkeeping rights. PoR (Proof of Retrievability) [25] can effectively resist centralization by selecting honest nodes, havng good fault tolerance performance, resisting double spend attacks, and sybil attacks. PBFT [26] was a state machine copy replication algorithm, i.e., the service is modeled as a state machine, but as the size of the network increases, the communication complexity and cost also increases.

In the IoEV, G. Sun et al. [27] combined the PBFT algorithm with the DPOS algorithm to design a more efficient and promising consensus algorithm, called DPOSP, which significantly reduces resource consumption and improves consensus efficiency. S. Garg et al. [28] applied the PBFT algorithm to energy transactions to address various security and privacy challenges with minimal communication and computational overhead for resource-constrained hardware devices. Y. Wang et al. [29] introduced the PoR consensus algorithm in energy transactions. R. Khalid et al. [30] developed V2V and V2G energy trading environments for EVs and CSs (charging posts) using a federated blockchain with proof-of-authority (PoA) consensus mechanism and smart contracts for efficient energy trading. M. Ali et al. [31] proposed an efficient and secure energy trading scheme in IoEV energy trading using directed acyclic graph (DAG) based IOTA. Z. Su et al. [32] a reputation based delegated Byzantine fault tolerance (DBFT) consensus algorithm is proposed to efficiently achieve the consensus in the permissioned blockchain.

Except for Z. Su et al. [32], Sun, Garg, Wang et al. [27-31] used consensus algorithms to improve system efficiency, but simply combined blockchain consensus algorithms such as Pow, PoR, PBFT, POA, etc., or combined both of them without further improvement of existing consensus algorithms for their own design systems, and did not introduce reputation mechanisms. The existing research has explored less on Shapley value in reputation value mechanism, considering the article [33] investigated a typical IoT network scenario, analyzed the characteristics of real constrained IoT devices in terms of both computational power and data rate, and confirmed that PBFT consensus algorithm has a better performance in IoT system.

Therefore, we combine the Shapley value-based reputation mechanism with PBFT to design an improved consensus algorithm SV-PBFT applied to the scenario of electric vehicle energy trading, and a V2V energy trading model.

3 System Model

3.1 Architecture and Entities

Blockchain is of great advantages for V2V applications because it is decentralized, distributed and credible. In the energy market, it is very expensive to establish and maintain a public blockchain between electric vehicles with limited resources and energy, and it is too expensive to reach a consensus on all involving electric vehicles. In addition, the Consortium chain is still a centralized network, which is controlled by an organization that cannot guarantee the reliability of transaction data if used directly. Therefore, we use a portion of nodes selected by the designed reputation mechanism to participate in consensus as a way to reduce consensus overhead. Distributed consensus can reduce the possibility of collusion to tamper with data because authoritative nodes that can be trusted and betrayed are easily detected. Therefore, this paper constructs a V2V energy trading system based on a coalition chain, which ensures the security of transaction data and the privacy of EVs users, while reducing the maintenance cost and consensus delay of the blockchain. Its model is shown in Figure 1, which mainly includes the following entities:

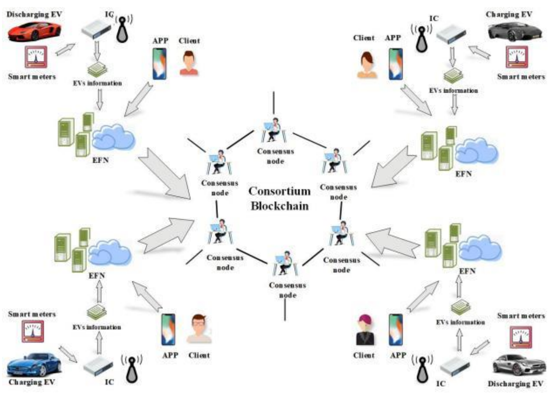

Figure 1. V2V energy trading model

(1) EFN (Energy Fog Node): The fog computing resource is abstracted as EFN, which collects energy transaction information directly through hardware such as sensors for updating and maintaining reputation values. Energy buyers and sellers can send requests to EFN to ensure the balance of cost and profit between buyers and sellers in energy transactions through ENF. EFN also participates in consensus as a node in the federated chain and elects a master node to package the transactions after successful consensus. The legitimate transaction records are stored in the blockchain in a distributed manner to ensure the openness, transparency and traceability of transactions. Considering the practical situation, EFNs should be located in social hotspots, such as supermarkets, shopping malls and hospitals, to facilitate the collection of information.

(2) EV (Electric vehicle): It is a new type of pollution-free and low-noise electric energy vehicle with pluggable two-way charging interface, which meets the environment-friendly concept of energy saving. At the same time, EV is both an energy consumer and an energy supplier in the energy trading system.

(3) SM (Smart Meters): Electric vehicles are equipped with smart meters to calculate and record the amount of electrical energy transactions in real time, providing a strong data basis for both parties to pay for the transactions.

(4) IC: IC is the information collector, responsible for collecting the configuration information of the car detected by the sensors. The configuration information includes vehicle brand, energy transaction information, mileage, etc.

3.2 Consortium Blockchain

Based on the reputation mechanism, some EFNs are selected as consensus nodes to participate in consensus, so as to jointly maintain the energy blockchain, unify the management of the distributed ledger, and complete transaction auditing and data sharing. The three main components of the consortium blockchain are as follows.

(1) Transactions: The current transaction contains the hash of the previous transaction. Multiple transactions will be associated with each other as the evidence. Once the transactions are broadcast to the federated chain network and a certain number of transactions are reached, consensus nodes will perform consensus. Then a certain number of transactions are recorded in the public ledger and packed into a block, and multiple blocks are connected together in chronological order to form a blockchain. To ensure the authenticity and accuracy of the transaction information, it is encrypted and digitally signed. To simulate fast payments, we use a crypto currency called Energy Coin (E-coin) as a digital energy transaction asset.

(2) Data blocks: Due to the limited storage resources and computing power of EV, all initial data are audited, stored and shared by the authoritative EFN. EV only needs to store a list of indexes indicating where metadata are stored, thus reducing the complexity and overhead of the system. The block consists of two parts: the block header and the block body. The block header includes: summary information of the transaction, M. Hash encryption of M, H(M). Timestamp, t. Signature information of the transaction, D(M). Number of the transaction information, m.

(3) Consensus algorithm: To achieve the blockchain synchronization, it must rely on distributed consensus algorithm. Unlike the PoW in the Bitcoin system, this paper further improves the PBFT consensus algorithm by combining the reputation mechanism to form a new consensus algorithm called SV-PBFT in order to improve consensus efficiency and support fast transactions and payments. Details of the reputation mechanism and SV-PBFT are provided in Sections 4 and 5, respectively.

(4) SC (Smart Contract): the SC defines the energy transaction logic that runs whenever the buyer and the seller send new transactions to buy and sell energy, respectively. The SC will perform logic operation according to its code and guarantee the implementation of the terms and conditions agreed to by all parties.

4 Reputation Mechanism

Shapley value [34] was proposed to solve the problem of multiple insiders conflicting over the distribution of benefits in the process of cooperation, which belongs to the field of cooperative games. One of the best features of applying Shapley value is to distribute the benefits according to the marginal contribution of the members to the coalition.

Shapley value has four unique advantages [35]: 1. Symmetry: ensures that the order or markers of stakeholders do not affect the outcome of benefit distribution. 2. Validity: ensures that the total value of the stakeholder alliance is guaranteed to be the sum of the Shapley values. 3. Redundancy: ensures that if a member does not contribute to any of the cooperative coalitions in which he participates, he should not benefit from all of them. 4. Additivity: ensures that if there are multiple collaborations, the benefits of each kind of collaboration are distributed in a way that is independent of the outcome of the other collaborations.

Therefore, this paper introduces reputation mechanism with the shapley value as its core to participate in the selection of blockchain master nodes, which ensures fairness in the system.

4.1 Initialize Point

There is a certain gap between the comprehensive strength of the nodes in the consortium blockchain, and usually the stronger the comprehensive strength of the nodes, the greater the performance and functional advantages the nodes have, and the better the node stability. We suppose that the nodes are represented as *N*, *N*={1,2 ..., n } representation. The number of consensus errors is E, denoted by {1, 2 ..., e}, and $Scord_i$ represents the comprehensive score of the node, and the higher the $Scord_i$, the higher the probability that the node is selected as the master node. *i* denotes the member, *lg* is the convergence function to avoid the points gap between the nodes due to the large difference in transaction amount, number of transactions and average time interval, which leads to monopoly. Multiplying by 100 is to ensure that the $Scord_i$ is a multiple of 100, which facilitates the integral adjustment. The initialized integral formula is as follows.

$$Scord_i = 100 \times \lg(\mathrm{Sum}'_i) + 100 \times \lg(\mathrm{T}'_i) + 100 \times \lg(\mathrm{N}'_i) - \mathrm{e}_i \times 100. \quad \textbf{(1)}$$

Sum_i represents the monthly transaction amount of the node, Sum_{min} represents the node that participates in the consensus with the least monthly transaction amount, Sum'_i is calculated by the following formula：

$$Sum'_i = \frac{\mathrm{Sum_i} - \mathrm{Sum_{min}}}{\mathrm{Sum_{min}}}. \quad \textbf{(2)}$$

T_i represents the average time interval between the customer's order and the successful transaction in that month, T_{min} represents the node that participates in the consensus with the shortest time interval, and T'_i is calculated as follows:

$$T'_i = \frac{\mathrm{T_{min}}}{\mathrm{T_i} - \mathrm{T_{min}}}. \quad \textbf{(3)}$$

N_i represents the number of monthly transactions of the node, N_{min} represents the node that participates in the consensus with the minimum monthly transactions, N'_i is calculated as follows:

$$N'_i = \frac{\mathrm{N_i} - \mathrm{N_{min}}}{\mathrm{N_{min}}}. \quad \textbf{(4)}$$

By the size of $Scord_i$, *N/2* nodes are selected as consensus nodes from high to low, the remaining *N/2* nodes are preparatory nodes, and the current number of blacklisted nodes is 0. The points are reinitialized every month to ensure fairness.

4.2 The Selection of the Master Node

All replicas in the PBFT consensus algorithm operate in a view rotation process, and the master node is determined by the view number as well as the set of node numbers. *V*: view number, |*R*|: number of nodes, *p*: master node number. The formula for the master node selection is as follows:

$$\mathrm{P} = \mathrm{V} \bmod |\mathrm{R}|. \quad \textbf{(5)}$$

In SV-PBFT, if member i has the largest $\&_i(v)$ value, which means that he contributes the most to the current benefits gained by the coalition and is more trustworthy. Therefore the node i should be selected as the master node. *S* represent different members forming different coalitions, *S* is a subset of *N* denoted by {1, 2 ..., s}, and s denotes the number of members contained in coalition S. The total points of the coalition *S* are *V(S)*, $\&_i(v)$: denotes the benefits that member i in the coalition should reap. *v(S)* is calculated as follows:

$$\mathrm{V(s)} = 2\sum_{i=1}^{n} \mathrm{Scord_i} - (\mathrm{n}-1) \times 100. \quad \textbf{(6)}$$

Then the benefit shared by member i from the overall benefit *V(N)* is:

$$\&_{\mathrm{i}}(\mathrm{V}) = 2\sum_{\mathrm{s \in N}} \frac{[(\mathrm{s}-1)!(\mathrm{n}-\mathrm{s})!]}{\mathrm{n}!} \times [\mathrm{V(S)} - \mathrm{V(S \backslash \{i\})}]. \quad \textbf{(7)}$$

Consensus nodes that are elected as master nodes have the right to package transactions.

4.3 Points Adjustment Rules and Node Conversion Rules

In the SV-PBFT algorithm, there are three states of nodes. We set a new Scordi adjustment rule to adjust the states among the nodes, and the nodes are converted to each other by the $\mathrm{Scord_i}$ as follows:

1. Addition rule: if the master node is elected from the consensus node for the first time, the points will be added 100 for each successful completion of consensus. If the master node is elected after being downgraded from the consensus node to the preparatory node and then converted to consensus

node, the points will be added 50 for each successful completion of consensus. The formaula is as follows:

$$\mathrm{Scord_i} = \begin{cases} Scord_i + 100,\ Consensus \\ Scord_i + 50,\ Preparatory\ \rightarrow Consensus\,. \end{cases} \quad \textbf{(8)}$$

2. Deduction rule: Once the master node makes an error, 1/3 of its points will be deducted directly, and the points will be zeroed directly if the number of errors reaches 3 times. If the master node is demoted from consensus node to preparatory node, and then elected from Preparatory node to consensus node, 1/2 of its points will be deducted for each error, and the points will be zeroed if the number of errors reaches 2 times.

$$\mathrm{Scord_i} = \begin{cases} Scord_i - \frac{Scord_i}{3},\ Consensus \\ Scord_i - \frac{Scord_i}{2},\ Preparatory\ \rightarrow Consensus\,. \end{cases} \quad \textbf{(9)}$$

3. Node conversion rules: A. If the $Scord_i$ of the consensus node is zero for the first time, it will be converted to a preparatory node. If the $Scord_i$ of the consensus node is zero for the second time, it is directly converted to a blacklisted node. B. When none of the preparatory nodes has ever been a consensus node, the node with the largest $Scord_i$ among the preparatory nodes is selected to be a consensus node. If there is a case that the preparatory nodes have the same number of points, they are selected in the order of ranking. If a preparatory node becomes a consensus node for the second time, its points are initialized according to Equation (1). C. Blacklisted nodes cannot be turned into consensus nodes and preparatory nodes, and cannot participate in the consensus process.

5 SV-PBFT Consensus Algorithm

5.1 SV-PBFT Consensus Algorithm

The specific process of PBFT consensus algorithm is shown in Figure 2. Compared with PBFT, considering that the consortium blockchain itself has a certain threshold and requires authentication at the time of entry, it can effectively avoid problems such as Sybil attacks, and at the same time we make the following improvements for the shortcomings of PBFT:

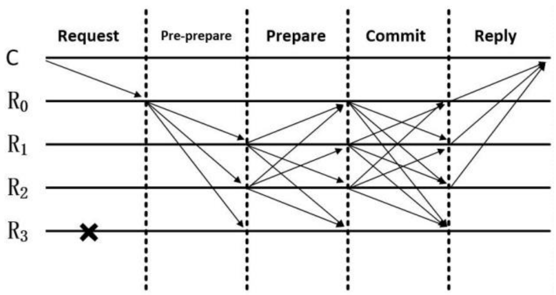

Figure 2. The process of PBFT consensus algorithm execution

1. The request and reply phases in the consistency protocol are omitted. The request and reply phases in the PBFT algorithm are interactions between the system nodes and the client, while the data blocks are generated directly by the master node in the consensus process after a successful consensus, without the participation of the client. This not only improves efficiency, but also prevents system crashes due to too many request messages.

2. We introduce a reputation mechanism with shapley value as its core, which divides the nodes into three types: consensus nodes, preparatory nodes and blacklisted nodes. We assume that the number of malicious nodes is f, the total number of nodes is N, the number of nodes involved in consensus is *N\2*, and the total number of preparatory and blacklisted nodes is *N\2*. In any case, *N\2>=3f+1* must be guaranteed, where the consensus section is responsible for completing the system consensus process, and the consensus is successful when more than *2f+1* consistent messages from legitimate nodes are received in the SV-Response phase.

3. We simplify the Confirm phase. In PBFT algorithm, the node in the Prepare phase has completed the consensus process, and the role of Commit phase is mainly to enable each node to grasp the state of the remaining nodes. In the traditional distributed system, the Commit phase provides the process of state confirmation for the system so that each node can know the consensus state of the remaining nodes and confirm that the system reaches agreement. In a federated chain system, each consensus block can be used as a checkpoint, and the system can be agreed through block synchronization after the completion of consensus in the Interaction phase. The commitment phase can be simplified because the nodes in the federated chain have higher reliability, the system environment is more stable. And the improved master node election method and the traceability of the federated chain guarantee the legitimacy of the block synchronization process.

1. SV-PBFT consensus algorithm has only three phases in the consistency protocol. R_0 is the master node, which is consensus nodes will verify the received interaction messages. And when there are *f+1* consistent interaction messages from different consensus nodes, the next stage can be carried out, otherwise the consensus process is aborted, the node with problems is replaced, and the consensus process is restarted.

2. SV-Commit: After completing the verification of interaction messages, all nodes including consensus nodes and preparatory nodes need to send confirmation messages to the master node. When the master node receives at least 2f+1 confirmation messages from different consensus nodes, the consensus is completed and the transaction information can be saved to the consortium blockchain.

There is a node timeout set in the system. If the master node fails in the above process, when the response timeout occurs, the node with the second largest $\&_i(v)$ value will be selected as the master node. If a consensus node that is not the master node fails, it will not affect the system as long as there are more than 2f+1 consensus nodes that can elected by shapley value as the core reputation mechanism. R_1, R_2, R_3 are consensus nodes, P_1 and P_2 are preparatory nodes. B_1 is the blacklisted node. *C* is the client identifier, *r* is the request result. Where *n* is to be in a certain range interval *[h,H]*. *v*: view number. $H(M_i)$ is the hash value of the summary information *M* of the transaction, *m* is the number of the transaction information, and *t* is the timestamp. R_i is the node that performs consensus this time. $D(M_i)$ is the signature of node R_i on the transaction information. The specific process of SV-PBFT consensus algorithm is shown in Figure 3 and the execution of this consensus algorithm is as follows Algorithm 1.

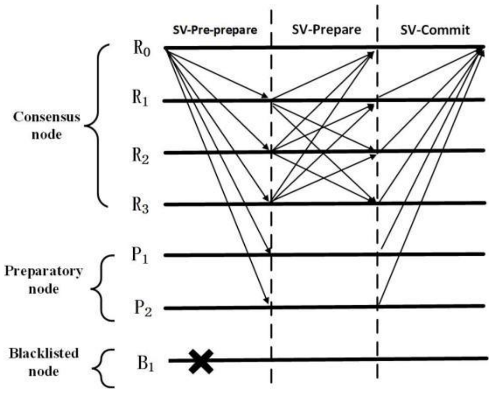

Figure 3. The process of SV-PBFT consensus algorithm execution

Algorithm 1. SV-PBFT

```
While master code = True do
    Broadcast (<<SV− PRE−PREPARE,v,n,t,H(Mi)>,m>);
    If   <SV−PRE−PREPARE,v,n,t,H(Mi)>,m>=True then{
            broadcast<SV−PREPARE,v,n,t,H(Mi),m,Ri>;
            receive<SV−PREPARE,v,n,t,H(Mi),m,Ri>;
    }
    else abort the consensus process and view change;
    if <<SV−PREPARE,v,n,t,H(Mi)>,m>=True && ∑result(i)≥(f+1) then{
            Send <SV−Commit,v,n,t,H(Mi),m,D(Mi),Ri> to master code;
            only master code receive <SV−PREPARE,v,n,t,H(Mi),m,Ri>;
    }
    else abort the consensus process and view change;
    If <SV−Commit,v,n,t,H(Mi),m,D(Mi),Ri>= True && ∑result(i) ≥ (2f+1) then{
            save transaction information;
    }
    else do nothing;
end
```

1. SV-Pre-prepare: The master node sends the message to other consensus nodes and preparatory nodes, where the consensus node needs to verify the message content. If the verification is passed, it will go to the next stage, otherwise it changes the view and replaces the master node.

2. SV-Prepare: After the consensus node completes the verification of the pre-prepared messages, it broadcasts the interaction messages to all consensus nodes. The consensus nodes will verify the received interaction messages. And when there are *f+1* consistent interaction messages from different consensus nodes, the next stage can be carried out, otherwise the consensus process is aborted, the node with problems is replaced, and the consensus process is restarted.

3. SV-Commit: After completing the verification of interaction messages, all nodes including consensus nodes and preparatory nodes need to send confirmation messages to the master node. When the master node receives at least 2f+1 confirmation messages from different consensus nodes, the consensus is completed and the transaction information can be saved to the consortium blockchain.

There is a node timeout set in the system. If the master node fails in the above process, when the response timeout occurs, the node with the second largest $\&_i(v)$ value will be selected as the master node. If a consensus node that is not the master node fails, it will not affect the system as long as there are more than 2f+1 consensus nodes that can operate normally.

5.2 Comparison of Communication Complexity

Assuming that the number of communications is C and the total number of current nodes is N, they can be seen from Figure. 2 The communication overhead of PBFT is mainly concentrated in three phases. In the Pre-Prepare phase, the master node sends messages to other consensus nodes, and the number of communications of the consensus network in this phase is *N-1*. In the Prepare phase, all nodes except the master node send messages to each other, and the number of communications in this phase is $(N-1)^2$. In Commit phase, all nodes verify the received Prepare messages. In this phase, the number of communications in the consensus network is N^2-N times. Therefore, the number of communications in a consensus process for the traditional PBFT consensus algorithm is the following formula.

$$C = 2N^2 - 2N. \tag{10}$$

We suppose that the number of blacklisted nodes is e. The number of communications of SV-PBFT in both SV-Pre-prepare and SV-Response phases is *N-1-e*. In the SV-Prepare phase, the total number of nodes involved in consensus is *N/2*, so the number of communications of the consensus network in that phase is *(N/2-1)2*. And then the number of communications of the SV-PBFT consensus algorithm in a consensus process is the following equation.

$$C = \frac{N^2}{4} + N - 1 - 2e. \quad \textbf{(11)}$$

Through the derivation of the formula, we analyze that the communication overhead of SV-PBFT consensus algorithm is lower than that of the traditional PBFT consensus algorithm.

6 Experiment Analysis

This section presents the algorithms PoW, PoR, PBFT and our proposed SV-PBFT for comparative evaluation in a simulation environment. A total of 70 nodes are set up for this experiment, and we will test and analyze four aspects of consensus latency, communication overhead, throughput and performance of energy transactions to compare the performance of the two algorithms. In this experiment, several virtual nodes with the same configuration are set up as experimental nodes in the internal LAN of the laboratory using FISCO BCOS [36], while PBFT Simulator [37] is used for the auxiliary simulation, and the specific configuration information of the experiment is shown in Table 1 and the simulation parameters are summarized in Table 2.

Table 1. The operating environment

Object	Configuration Information
CPU	Intel(R) Core(TM) i5-7300HQ
Operating System	Windows 10
System Memory	12GB DDR4
Hard Disk	1T SSD
Console Version	FISCO BCOS console（2.7.0）
Simulator	PBFT Simulator-master

Table 2. The simulation parameters

Parameters	Values
Number of Nodes	[10-70]
Number of EVs	[5-45]
V2V charging rate	18kw/h
Block size	0.1MB
The average transaction fee	0.000052E-coins
The average transaction size	0.000031MB
Base network latency between nodes	4ms
Block generation interval	1000*60*10ms
Maximum number of requests processed	1000
Number of clients	1
Node timeout setting	500ms
Network latency for system crashes	10000ms
Inter-node network bandwidth	300B

6.1 Communication Overhead

The communication overhead is the average number of communications required between the nodes of the system to complete one consistency protocol. To facilitate the observation, we set the number of energy transaction messages to 1 and the client nodes to 1, and compare only the communication overhead incurring during the consensus process. The experimental results of communication overhead are shown in Figure 4.

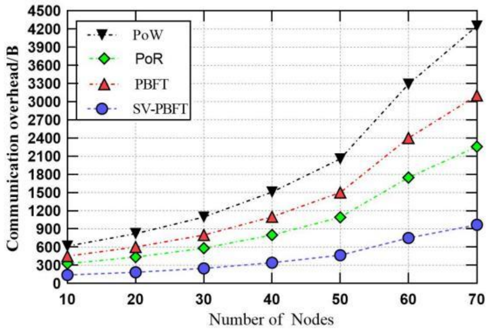

Figure 4. Results of the communication overhead comparison

Through simulation experiments, we find that the communication of SV-PBFT scheme is 93.81%, 68.71% and 21.37% lower than PoW, PBFT and PoR, respectively, and considering that SV-PBFT introduces a reputation mechanism to filter nodes, which greatly reduces the probability of view conversion, so in practical applications, the SV-PBFT algorithm will have better performance in communication overhead.

6.2 Consensus Delay

In blockchain systems, communication latency is the time required from the submission of a transaction request by a node to the completion of consensus in the system, and is an important parameter for evaluating the performance of consensus algorithms. Reducing the consensus latency can improve the system operation efficiency and practicality. In this experiment, the total number of nodes in the system is used as the experimental variable, and the number of nodes is incremented from 10 to 70. 20 transactions are conducted under different numbers of nodes, and the average value of consensus latency of these 20 transactions is taken as the final value of consensus latency under the current number of nodes, and the experimental results are shown in Figure 5.

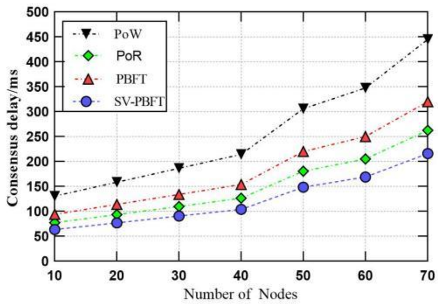

Figure 5. Results of the consensus delay comparison

The simulation results show that the communication of SV-PBFT scheme is 45.1%, 32.51% and 25.4% lower than

PoW, PBFT and PoR respectively. SV-PBFT has better performance in consensus delay.

6.3 Throughput

The throughput refers to the average amount of time that a single node can process per unit of time. 20 experiments are repeated under different node numbers, and the event amount of each experiment is set to 1000, and the final average of the experimental results is taken as the value of the throughput under different node numbers, and the experimental results are shown in Figure 6.

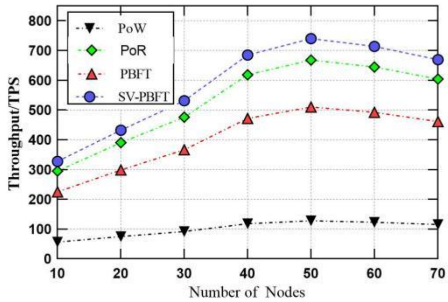

Figure 6. Results of the throughput comparison

A comparison of the experimental results shows that the SV-PBFT scheme has 401.3%, 45.09% and 10.12% higher throughput than PoW, PBFT and PoR, respectively. SV-PBFT has better performance in terms of throughput.

6.4 Performance of Energy Trading

We use SC to define the transaction logic, while using SM to report their consumed and produced energy respectively, while tracking energy transfers between buyers and sellers regarding the corresponding pre-established energy purchase agreements. Buyers and sellers send energy requests to the nearest EFN (Energy Fog Node), which are collected, collated and stored in the transaction pool. The elected master node calculates the total energy demand and broadcasts it to other nodes.

Also in this experiment, the number of EVs is used as an experimental variable, and the number is increased from 5 to 45. 20 transactions are conducted under different numbers of EVs, and the average of profit gain and purchase cost of these 20 transactions are taken, and the average profit gain of energy sellers and the average cost of energy buyers increase with the increase of EVs, as shown in Figure 7 and Figure 8.

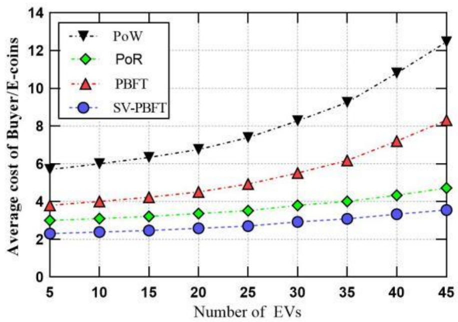

Figure 7. Comparative results of the average cost of energy buyers

A comparison of the experimental results shows that the SV-PBFT scheme reduces the required average cost by 71.51%, 57.28% and 24.63% compared to PoW, PBFT and PoR.

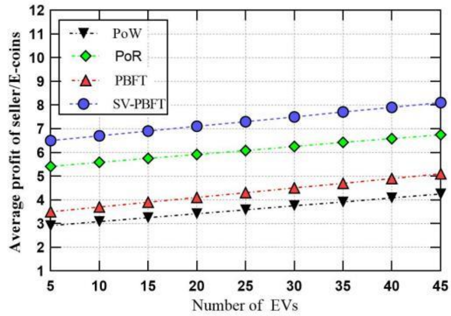

Figure 8. Comparative results of the average profit of energy sellers

A comparison of the experimental results shows that the SV-PBFT scheme increases the required average gain by 90.58%, 58.82% and 20.1% over PoW, PBFT and PoR, respectively.

The simulation results illustrate that the SV-PBFT scheme can effectively support buyers and sellers to achieve the balance between cost and profit in energy trading.

6.5 Reliability of Consensus Nodes

The consensus node is the execution node of the consensus process, and the reliability of consensus nodes directly determines the achievement of system consensus. Since PBFT is more applicable to the restricted IoT than PoW and PoR, we compare SV-PBFT with PBFT. The experimental results are shown in Figure 9.

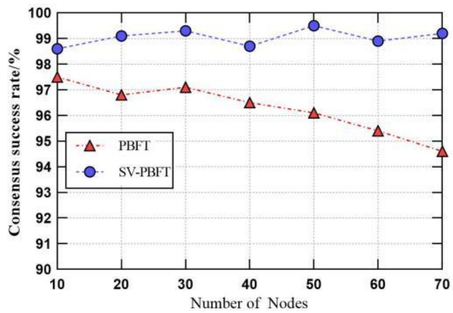

Figure 9. Comparative results of nodes reliability

7 Conclusion

In this paper, we design an improved PBFT based on shapley value reputation mechanism, called SV-PBFT algorithm. SV-PBFT algorithm simplifies the consensus process and improves the consensus efficiency compared to PBFT algorithm, divides nodes into three categories: consensus nodes, preparatory nodes and blacklisted nodes, ensures the reliability of consensus nodes to the maximum extent through reputation mechanism, and improves security. We design a blockchain-based V2V energy trading model around SV-PBFT on top of the decentralized, tamper-evident and open and transparent features of blockchain, and use a large number of data experiments to simulate the trading process and verify the usability of the scheme. The comparative experiments illustrate that the SV-PBFT algorithm has better performance in the V2V energy trading model than the traditional PoW, PoR and PBFT. Moreover, the SV-PBFT consensus algorithm is not only applicable to V2V energy transactions, but also to other coalition chain application scenarios that require efficient consensus. In the future, we will plan to further study the scalability of blockchain, increase the number of nodes that can participate in consensus, and further improve the efficiency of consensus algorithm refinement at the same time. On this basis, we will try to improve the SV-PBFT scheme by combining cryptography with machine learning techniques to improve the privacy and efficiency of the system.

Conflicts of Interest

The authors declare that they have no conflict of interest.

Acknowledgement

This work is supported by the National Natural Science Foundation of China grant number U21A20469, and the National Natural Science Foundation of China grant number 61972274.

References

[1] M Amjad, A Ahmad, M. H. Rehmani, T. Umer, A review of EVs charging: From the perspective of energy optimization, optimization approaches, and charging techniques, *Transportation Research Part D: Transport and Environment*, Vol. 62, pp. 386-417, July, 2018.

[2] Y. Ota, H. Taniguchi, T. Nakajima, K. Liyanage, J. Baba, A. Yokoyama, Autonomous distributed V2G (vehicle-to-grid) satisfying scheduled charging, *IEEE Transactions on Smart Grid*, Vol. 3, No. 1, pp. 559-564, March, 2012.

[3] G. R. Parsons, M. K. Hidrue, W. Kempton, M. P. Gardner, Willingness to pay for vehicle-to-grid (V2G) electric vehicles and their contract terms, *Energy Economics*, Vol. 42, pp. 313-324, March, 2014.

[4] M. Wang, M. Ismail, R. Zhang, X. Shen, E. Serpedin, K. Qaraqe, Spatio-temporal coordinated V2V energy swapping strategy for mobile PEVs, *IEEE Transactions on Smart Grid*, Vol. 9, No. 3, pp. 1566-1579, May, 2018.

[5] A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak, Z. Y. Dong, SPB: A secure private blockchain-based solution for distributed energy trading, *IEEE Communications Magazine*, Vol. 57, No. 7, pp. 120-126, July, 2019.

[6] P. Wongthongtham, D. Marrable, B. Abu-Salih, X. Liu, G. Morrison, Blockchain-enabled Peer-to-Peer energy trading, *Computers & Electrical Engineering*, Vol. 94, Article No. 107299, September, 2021.

[7] A. Esmat, M. de Vos, Y. Ghiassi-Farrokhfal, P. Palensky, D. Epema, A novel decentralized platform for peer-to-peer energy trading market with blockchain technology, *Applied Energy*, Vol. 282, Article No. 116123, January, 2021.

[8] J. Wang, C. Han, W. Yu, Y. Ren, R. S. Sherratt, Distributed Secure Storage Scheme Based on Sharding Blockchain, *CMC-Computers, Materials & Continua*, Vol. 70, No. 3, pp. 4485-4502, 2022.

[9] C. Han, G. J. Kim, O. Alfarraj, A. Tolba, Y. Ren, *ZT-BDS: A Secure Blockchain-based Zero-trust Data Storage Scheme in 6G Edge IoT*, *Journal of Internet Technology*, Vol. 23, No. 2 , pp. 289-295, March, 2022.

[10] Y. Chen, C. Bellavitis, Blockchain disruption and decentralized finance: The rise of decentralized business models, *Journal of Business Venturing Insights*, Vol. 13, Article No. e00151, June, 2020.

[11] J. F. Galvez, J. C. Mejuto, J. Simal-Gandara, Future challenges on the use of blockchain for food traceability analysis, *TrAC Trends in Analytical Chemistry*, Vol. 107, pp. 222-232, October, 2018.

[12] H. Wu, N. Su, C. Ma, P. Liao, D. Li, A privacy protection solution based on NLPCA for blockchain supply chain financial system, *International Journal of Financial Engineering*, Vol. 7, No. 3, Article No. 2050019, September, 2020.

[13] M. Salimitari, M. Chatterjee, A survey on consensus protocols in blockchain for iot networks, June, 2019. https://arxiv.org/abs/1809.05613

[14] Z. Zheng, J. Pan, L. Cai, Lightweight blockchain consensus protocols for vehicular social networks, *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 6, pp. 5736-5748, June, 2020.

[15] A. M. Koufakis, E. S. Rigas, N. Bassiliades, S. D. Ramchurn, Offline and online electric vehicle charging scheduling with V2V energy transfer, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 21, No. 5, pp. 2128-2138, May, 2020.

[16] A. M. Koufakis, E. S. Rigas, N. Bassiliades, S. D. Ramchurn, Towards an optimal EV charging scheduling scheme with V2G and V2V energy transfer, *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Sydney, NSW, Australia, 2016, pp. 302-307.

[17] M. E. Kabir, I. Sorkhoh, B. Moussa, C. Assi, Routing and scheduling of mobile EV chargers for vehicle to vehicle (V2V) energy transfer, *2020 IEEE Power & Energy Society General Meeting (PESGM)*, Montreal, QC, Canada, 2020, pp. 1-5.

[18] S. K. Vempalli, K. Deepa, G. Prabhkar, A novel V2V charging method addressing the last mile connectivity, *2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, Chennai, India, 2018, pp. 1-6.

[19] R. Khalid, N. Javaid, S. Javaid, M. Imran, N. Naseer, A blockchain-based decentralized energy management in a P2P trading system, *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, Dublin, Ireland, 2020, pp. 1-6.

[20] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, D. N. K. Jayakody, A blockchain-based framework for lightweight data sharing and energy trading in V2G network, *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 6, pp. 5799-5812, June, 2020.

[21] A. Barnawi, S. Aggarwal, N. Kumar, D. M. Alghazzawi, B. Alzahrani, M. Boulares, Path Planning for Energy Management of Smart Maritime Electric Vehicles: A Blockchain-Based Solution, *IEEE*

Transactions on Intelligent Transportation Systems, pp. 1-14, December, 2021.

[22] S. Aggarwal, N. Kumar, P. Gope, An Efficient Blockchain-based Authentication Scheme for Energy-Trading in V2G Networks, *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 10, pp. 6971-6980, October, 2021.

[23] J. Ouyang, Y. Deng, H. Tang, Blockchain Electronic Voting System for Preventing One Vote and Multiple Investment, *International Conference on Blockchain and Trustworthy Systems*, Guangzhou, China, 2019, pp. 752-757.

[24] P. Daian, R. Pass, E. Shi, Snow white: Robustly reconfigurable consensus and applications to provably secure proof of stake, *International Conference on Financial Cryptography and Data Security*, Frigate Bay, St. Kitts and Nevis, 2019, pp. 23-41.

[25] Q. Zhuang, Y. Liu, L. Chen, Z. Ai, Proof of reputation: A reputation-based consensus protocol for blockchain based systems, *Proceedings of the 2019 International Electronics Communication Conference*, Okinawa, Japan, 2019, pp. 131-138.

[26] M. Castro, B. Liskov, Practical byzantine fault tolerance, *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, Louisiana, USA, 1999, pp. 173-186.

[27] G. Sun, M. Dai, F. Zhang, H. Yu, X. Du, M. Guizani, M., Blockchain-enhanced high-confidence energy sharing in Internet of electric vehicles, *IEEE Internet of Things Journal*, Vol. 7, No. 9, pp. 7868-7882, September, 2020.

[28] S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, J. J. P. C. Rodrigues, An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment, *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, Shanghai, China, 2019, pp. 1-6.

[29] Y. Wang, Z. Su, N. Zhang, Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network, *IEEE Transactions on Industrial Informatics*, Vol. 15, No. 6, pp. 3620-3631, June, 2019.

[30] R. Khalid, M. W. Malik, T. A. Alghamdi, N. Javaid, A consortium blockchain based energy trading scheme for Electric Vehicles in smart cities, *Journal of Information Security and Applications*, Vol. 63, Article No. 102998, December, 2021.

[31] M. Ali, A. Anjum, A. Anjum, M. A. Khan, Efficient and Secure Energy Trading in Internet of Electric Vehicles Using IOTA Blockchain, *2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, Charlotte, NC, USA, 2020, pp. 87-91.

[32] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. C. Tian, N. Zhang, A secure charging scheme for electric vehicles with smart communities in energy blockchain, *IEEE Internet of Things Journal*, Vol. 6, No. 3, pp. 4601-4613, June, 2019.

[33] Y. Meshcheryakov, A. Melman, O. Evsutin, V. Morozov, Y. Koucheryavy, On performance of PBFT blockchain consensus algorithm for IoT-applications with constrained devices, *IEEE Access*, Vol. 9, pp. 80559-80570, June, 2021.

[34] E. Winter, The shapley value, in: R. Aumann, S. Hart (Eds.), *Handbook of game theory with economic applications*, Vol. 3, Elsevier B.V., 2002, pp. 2025-2054.

[35] J. Castro, D. Gómez, J. Tejada, Polynomial calculation of the Shapley value based on sampling, *Computers & Operations Research*, Vol. 36, No. 5, pp. 1726-1730, May, 2009.

[36] C. Mohan, State of public and private blockchains: Myths and reality, *Proceedings of the 2019 international conference on management of data*, Amsterdam, Netherlands, 2019, pp. 404-411.

[37] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi, A. Rindos, Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric), *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, Hong Kong, China, 2017, pp. 253-255.

Biographies

Yao Suo is studying for a master's degree at the College of Information and Computer at Taiyuan University of Technology. His research interests are decentralized systems and blockchain technology.

Yingsen Wang received the B.S. degree in Electronic Science and Technology from Taiyuan University of Technology, Taiyuan, China, in 2019, where he is currently pursuing the PhD degree with the College of Information and Computer. His research interests include decentralised systems and blockchain technology.

Shichao Luo graduated from the college of Information and Computer of Taiyuan University of Technology with a master's degree. His research area is medical image processing.

Qianqian Yang, born in Linfen, Shanxi, is a master, senior engineer, and lecturer at Jinzhong College of Information. Her main research interests are big data technology and artificial intelligence.

Juanjuan Zhao is a professor in the School of Computer Science and Technology at Taiyuan University of Technology, China. She received her PhD in computer application technology from TYUT in 2010. Her current research interests are medical image processing and the Deep Learning.