Energy Reports 10 (2023) 1565–1574

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Research paper

A scalable, efficient, and secured consensus mechanism for Vehicle-to-Vehicle energy trading blockchain

Yingsen Wang [a], Yixiao Li [c], Yao Suo [a], Yan Qiang [a,*], Juanjuan Zhao [a], Keqin Li [b]

[a] Taiyuan University of Technology, Taiyuan, China
[b] State University of New York, New Paltz, NY, USA
[c] Shandong University, Jinan, Shandong, China

ARTICLE INFO

Article history:
Received 5 August 2022
Received in revised form 22 January 2023
Accepted 18 July 2023
Available online xxxx

Keywords:
Blockchain
Consensus
Electric vehicles
Energy trading
Internet of Electric Vehicles
Vehicle-to-Vehicle

ABSTRACT

Vehicle-to-Vehicle (V2V) energy trading has emerged as a promising scheme to relieve the load imposed on the grid without intermediaries. The blockchain has always been regarded as the most potential solution for addressing the security and privacy issues of the Internet of Electric Vehicles (IoEV). The consensus mechanism is the core of the blockchain, it determines the security, efficiency, and scalability of the system. However, consensus mechanisms currently employed in V2V energy trading are traditional algorithms, which are unsuitable for the IoEV due to their high computational power and communication overhead. Therefore, we are motivated to propose a Block Alliance Consensus (BAC) mechanism based on Hashgraph. BAC can maintain the high throughput of the Hashgraph, and it solves the problem that the Hashgraph cannot support the dynamic addition and deletion of nodes if it is directly applied to V2V energy trading. We utilize the sharding technique, and each shard generates a consortium blockchain in accordance with the characteristic of the IoEV. The centralized component is retained to ensure macroeconomic control by state and local governments. We design a cryptography-based leader election combined with a reputation incentive mechanism to fairly elect centralized leader committee and motivate honest electric vehicles (EVs). We implement the BAC consensus and V2V energy trading blockchain (ETB) on the Hyperledger Fabric. The performance and practicality of BAC and the V2V ETB are verified through experiments.

1. Introduction

Existing energy trading systems have started to go beyond their limitations due to the surge in electricity and the promotion of new energy power generation in recent years (Siano et al., 2019). As a promising alternative, EVs have emerged as an effective way to satisfy energy demands, eliminate hazardous emissions, and maximize revenue (Xia et al., 2020; Sharma, 2018). Though the decentralized V2V trading model could solve problems in the traditional structure, it brings new challenges such as security and privacy-preserving (Wang, 2022). The advent of blockchain attracts enormous attention to P2P energy trading and offers new avenues to curb the penetration and disruption of cyber attacks (Sun et al., 2020). Blockchain is a decentralized, distributed, and immutable ledger made up of an irrevocable sequence of blocks (Gao et al., 2018; Xie et al., 2020). It allows mutually distrustful vehicles to keep transparent transaction records. Attackers in blockchain must possess a majority of the network's mining power to conduct a successful attack (Salimitari et al., 2017; Zhao et al., 2019). Although the blockchain originated from digital currencies (Wood et al., 2014; Li and Gong, 2022), it is now being used in many other non-monetary scenarios. Blockchain is attracting enormous attention to P2P energy trading and promoting trusted smart grid developments toward decentralization.

As the core of blockchain technology, the consensus mechanism determines the security and efficiency of the blockchain (Kang et al., 2019). However, consensus mechanisms designed for the V2V blockchain are still rare (Abishu et al., 2021). Besides, to the best of our knowledge, most studies about P2P energy trading have adopted traditional consensus such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). Due to their high computational power and communication overhead, they are not suitable for Internet of Things (IoT) such as the energy trading in IoEV. Therefore, we are encouraged to develop a secured and efficient BAC mechanism utilizing Hashgraph (known as the revolutionary technology of

* Corresponding author.
E-mail addresses: wangyingsen0065@link.tyut.edu.cn (Y. Wang), 202034669@mail.sdu.edu.cn (Y. Li), suoyao0607@link.tyut.edu.cn (Y. Suo), qiangyan@tyut.edu.cn (Y. Qiang), zhaojuanjuan@tyut.edu.cn (J. Zhao), lik@newpaltz.edu (K. Li).
URL: http://www.cs.newpaltz.edu/~lik/ (K. Li).

https://doi.org/10.1016/j.egyr.2023.07.035

List of Key Acronyms

EVs	Electric Vehicles
IoEV	Internet of Electric Vehicles
P2P	Peer-to-Peer
V2V	Vehicle-to-Vehicle
V2G	Vehicle-to-Grid
DC-DC	Direct Current to Direct Current
ETB	Energy Trading Blockchain
BAC	Block Alliance Consensus
BFT	Byzantine Fault Tolerance
ABFT	Asynchronous Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
PoW	Proof-of-Work
PoS	Proof-of-Stake
CPoS	Competition-based Proof of Stake
IoT	Internet of Things
WPT	Wireless Power Transfer
CA	Certificate Authority
SC	Smart Contract
ID	Identification
VRF	Verifiable Random Function
P	Primary
CP	Candidate Primary
CS	Consensus Node
DAG	Direct Acyclic Graph

consensus) while making up for Hashgraph's deficiencies in performance and practical applicability. The time complexity of BAC is $O(N)$ and scalable compared with the traditional BFT $O(N^2)$. Compared with the Hashgraph, the BAC mechanism supports the dynamic addition and deletion of EVs while maintaining the security and high throughput of Hashgraph, and can resist Sybil Attacks in networks with large-scale EVs. Furthermore, a cryptography-based leader node election combined with a reputation incentive is proposed to motivate honest EVs and defend against malicious nodes. Reducing carbon emissions and relieving pressure on the power grid are the advantages of EVs over conventional vehicles. These advantages are the reason and motivation for people to adopt EVs instead of conventional vehicles. Our research focuses on how to ensure cyber security and improve the efficiency of energy trading in the context of connected vehicles when the adoption of EVs is known.

2. Related works

Several researchers have proposed innovative schemes for V2V and vehicle-to-grid (V2G) energy trading. Ucer et al. (2019) proposed a flexible bidirectional direct current to direct current (DC-DC) energy transfer as an alternative to current V2G charging. Alvaro et al. (2014) presented a V2V market for decreasing the energy cost in smart grids. Wang et al. (2019b) presented a charging strategy for EVs in a smart community with renewables using a game-theoretical framework. Saad et al. (2011) presented a non-cooperative games-based and double auctions-based decision-making process for the power market with EVs. Xu and Wong (2011) developed a coordinated charging control algorithm to minimize the cost of charging for the aggregator and reduce power loss. A P2P energy trading between two sets of EVs was proposed in Alvaro-Hermana et al. (2016) to lessen the effect of the charging procedure during business hours. Most of these energy sharing methods adopt an energy aggregator or DC-DC converter, reducing the energy transfer efficiency between EVs. Wireless power transfer (WPT) technology has been developed to tackle this issue. Sousa et al. (2018) proposed a method connecting two EVs directly via WPT instead of an energy aggregator. Bi et al. (2016) and Triviño et al. (2021) proposed a review of the WPT technology for V2V energy trading. Machura et al. (2020), Baharom et al. (2020) and Mou et al. (2018) proposed V2V charging scheme based on WPT. WPT has become a popular technology for EV energy transfer due to its advancements (Mou et al., 2018; Li and Mi, 2014; Das et al., 2018).

Current research efforts on ETB have been adopting traditional consensus algorithms. For example, Sun et al. (2020) utilized the PBFT-based Delegated PoS (PDPoS) in IoEV and Garg et al. (2019) utilized PBFT for V2G energy trading. Su et al. (2018) proposed a reputation-based BFT to efficiently reach consensus in the permissioned energy blockchain. Based on the Byzantine consensus architecture, Sheikh et al. (2019) concentrated on the energy transaction process between EVs and the distribution network. Feng et al. (2018) proposed a scalable, dynamic multi-agent hierarchical PBFT method (SDMA-PBFT) that decreases the communication overhead from $O(N^2)$ to $O(nk * log(nk))$. Wang et al. (2019a) suggested voting rewards and punishments, a credit evaluation mechanism, and PBFT-based consistency protocol. YuboSong and Zhang (2020) presented a competition-based proof of stake (CPoS) consensus method that may swiftly eliminate forks while maintaining decentralization. Yang et al. (2020) proposed a PBFT-based algorithm for multi-energy interactive entities. Cai et al. (2020) presented a DPBFT appropriate for energy blockchain dynamic reputation.

Although the above research solves the problem of low participation of nodes, the issue of high transaction delay and low throughput has not been completely solved. Existing consensus mechanisms still have a big gap in achieving the security and efficiency of the ETB. Most studies implement the consensus mechanism as a small part of the research, and most adopt the traditional or an improved PBFT as their consensus mechanism. They are incapable of meeting the requirements of large-scale energy transactions. As a result, the current energy trading platform urgently needs improving the performance of the consensus mechanism.

Traditional consensus mechanisms in blockchain originated from digital currencies or BFT, which are inapplicable to energy trading due to their heavy computational load and enormous communication complexity. Although improved versions based on these traditional consensus mechanisms have been proposed in recent years, their performance still needs to be improved for energy trading, much less for V2V scenarios where EVs change in real time. Our proposed BAC consensus mechanism departs from the constraints of traditional consensus and utilizes a Direct Acyclic Graph (DAG)-based Hashgraph. BAC significantly improves the throughput of the system by concurrently generating blocks. The number of nodes in Hashgraph is predefined, while IoEV allows real-time geographic location variations for EVs. Considering this property of V2V energy trading, we use the sharding technique, and each shard constitutes a consortium blockchain environment within each shard. The sharding technique happens to enhance the scalability of V2V ETB, making the BAC consensus better scalable (see Table 1).

3. System model

Fig. 1 shows the trading procedure of our V2V ETB system model. We group EVs into different shards according to their location, direction, and velocity. Each shard consists of energy sellers and buyers, block publishers and validators. We utilize the Hyperledger Fabric, a consortium blockchain platform with

Table 1
Comparison with different consensus mechanisms for P2P energy trading.

Mechanisms	Decentralization	Permissions	Scalability	Throughput	Latency	Computing	Communication overhead
PoW	High	Public	Low	Low	High	High	High
PoS	High	Public	Low	Low	Medium	Low	Low
DPoS	High	Public	Low	Medium	Medium	Low	Low
PBFT	Low	Private	Low	Low	High	Low	High
DAG	Medium	Consortium	Medium	High	Low	Low	Low
Hashgraph	Medium	Private	Medium	Very High	Low	Low	Low
BAC	Medium	Consortium	High	Very High	Low	Low	Low

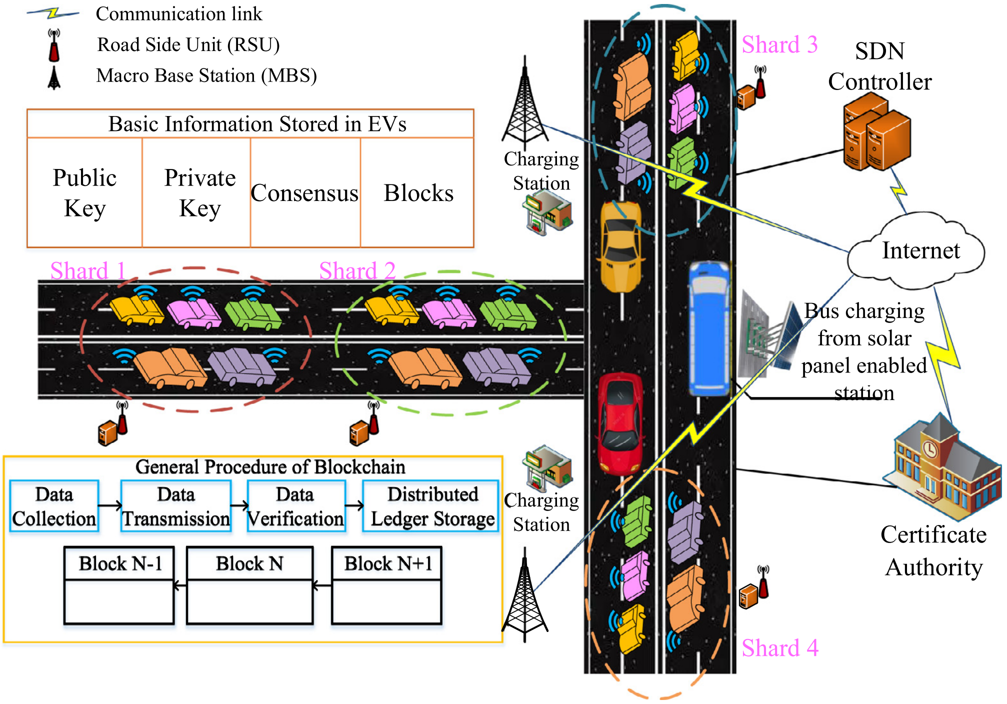


Fig. 1. System model for V2V energy trading blockchain.

a certificate authority (CA) and smart contract (SC) to ensure the security and transparency of the ETB. Let $i \in S = \{1, 2, \ldots, X\}$ be an energy seller, and $j \in B = \{1, 2, \ldots, Y\}$ be an energy buyer. A seller S_i or buyer B_j participates in the ETB with its authenticated identification (ID) obtained form the CA and a pair of encryption keys (PK_{S_i}, SK_{S_i}), (PK_{B_j}, SK_{B_j}), respectively. The asymmetric encryption technology (Aitzhan and Svetinovic, 2016) is utilized to ensure the security and validity of the message between senders and receivers:

$$D_{PK\,a}(Sig_{SK\,a}(H(m))) = H(m) \tag{1}$$

where $Sig_{SK\,a}()$ denotes a message sender a's digital signature using its private key, $D_{PK\,a}()$ denotes that message receivers could decrypt the message's hash value using a's public key, and $H(m)$ denotes the hash value of the message m.

The verifiable random function (VRF) (Micali et al., 1999) is utilized to select the primary node randomly based on EVs' reputation value. The VRF is divided into two parts: proof generation and verification. The generation process is expressed as:

$$P = VRF_{proof}(SK, m) \tag{2a}$$

$$Q = VRF_{P2H}(P) \tag{2b}$$

where m is the original input message of an EV, P is the proof generated by the EV's SK and m, and $P2H$ is a function of converting the proof to a unique hash value. Other EVs use the EV's PK to verify whether the proof P is generated from the original message m: $VRF_{verify}(PK, M, P)$. EVs in our ETB are divided into three categories: Primary (P), Candidate Primary (CP), and Consensus (CS). EVs' location coordinates in two-dimensional space are expressed as (y_i, z_i), and (y_j, z_j), $\forall i \in S, \forall j \in B$. Then the Euclidean distance between energy supplier i and requester j in each shard is expressed as:

$$d_{i,j} = \sqrt{(y_j - y_i)^2 + (z_j - z_i)^2}, i \in S, j \in B \tag{3}$$

4. Proposed block alliance consensus mechanism

We first combine BFT with chain structure to reduce the time complexity of BAC from the traditional $O(N^2)$ to $O(N)$ without consuming tremendous arithmetic power (Wang et al., 2022b,a). Fig. 2 shows the principle of BAC consensus model (Wang et al., 2022a). The EV P in a shard packages energy transaction requests from requesters into a $block(i)$ where i denotes the height of a block, and calculates the $block(i)$'s hash value. The P and CP store the whole block; most CS only need storing the whole block (both block header and body). We optimize the BAC with threshold signatures (Shoup, 2000). The n EVs generate their own private keys and then they can take a (k, n) threshold signature for a message. The i_{th} EV_i contributes its partial signature $\varrho_i \leftarrow sign_i(m)$ on message m utilizing its private key. Only after the signature "fragments" from k separate nodes are gathered together can be aggregated into a complete signature: $\iota \leftarrow combine(m, \{\varrho_i\}_{i \in I})$, where $|I| = k$, $k = n/2$ in BAC.

Block-request: A CP verifies the $block(i) = (header(i), data(i))$, an unvalidated block that requests to be connected at height i in

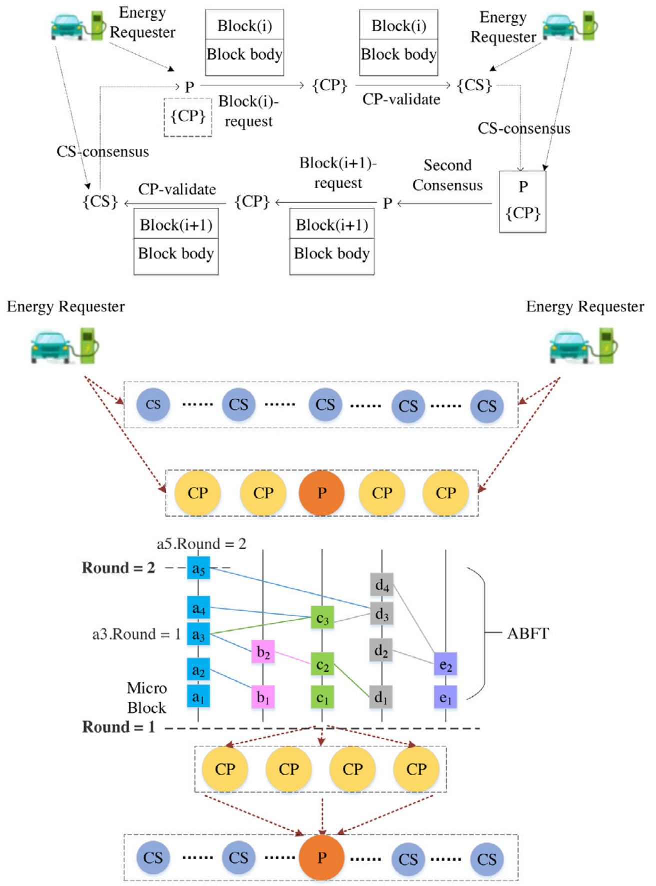


Fig. 2. BAC consensus model.

Algorithm 1: Block Consistency

```
Input: $T$: a set of transactions; $t$: $t \in T$; $H()$: the hash
       function; $P = \{\mathrm{P}, \mathrm{CP}_1, \mathrm{CP}_2, \ldots, \mathrm{CP}_\mathrm{p}\}$;
       $C = \{\mathrm{CS}_1, \mathrm{CS}_2, \ldots, \mathrm{CS}_\mathrm{s}\}$
Output: $out$
$P, C \leftarrow T$;
while $\underline{\text{P calculates } H(I) = H(block(i-1))_\mathrm{P}}$ do
    $block(i) \rightarrow P$;
    calculate $H(II) = H(block(i-1))_{\mathrm{CP}}$;
    if $\underline{H(II) \neq H(I)}$ then
        $\langle$CP-validate$\rangle$: $\mathrm{CP}(c)_{reject} \rightarrow C$
    end
    if $\underline{H(II) == H(I)}$ then
        $\langle$CP-validate$\rangle$: $\mathrm{CP}(c)_{accept} \rightarrow C$
    end
end
while $\underline{P \leftarrow \langle \mathrm{CS}-consensus \rangle}$ do
    obey "majority" rule;
    if $\underline{|C(c)_{accept}|} > \underline{|C(c)_{reject}|}$ then
        packages the next new $block(i+1)$
    end
    while $\underline{P \leftarrow block(i+1)}$ do
        verify $H(block(i))$ in $block(i+1)$;
        if $\underline{|CP(c)_{accept}|} > \underline{|CP(c)_{reject}|}$ then
            publish $block(i)$ into blockchain
        end
    end
    out = success
end
return out
```

the V2V blockchain. The $BLOCK(i)$ is a validated block at height i. CP calculate the hash $H(II)$ of $BLOCK(i-1)$ which CP have already received and validated, and compare the $H(II)$ and the $Prev\_Hash$.

Block-commit: The first round of consensus is completed in this stage. The P and CP collect the vote message with threshold signature from CS and obey the "majority" rule: the $block(i)$ can be published in the ETB as long as more than 50% of CS message are received.

Block-on-chain: The BAC avoids pairwise communication between CS thus reduces the time complexity. However, it results in only a subset of nodes (P and CP) are aware of whether the $block(i)$ is verified by the whole network. Thus in the second round of BAC, the P broadcasts the $block(i+1)$ which contains the $block(i)$'s hash value in $block(i+1)$'s header.

Algorithm 1 illustrates the details of the BAC basis process (Wang et al., 2022b). (→: broadcasting authenticated messages; ←: receiving authenticated messages) The complexity of the traditional BFT is high because each node performs much repeated work—each node needs to broadcast its own vote and gather the votes of others. Such a situation is unnecessary for BAC because the threshold signature prevents vote fraud and tampering, so only the EV primary is in charge of gathering votes and broadcasting the results to each node. Suppose there are c CP nodes and n CS nodes in a shard, where c is a fixed constant value and $c \ll n$. The rounds of communication are c and cn in the Block-request and CP-validate stage, respectively. The CS-consensus communication's rounds are $n(c+1)$. So the total rounds of communication are:

$$T = 2[c + cn + (c+1)n] = C_1 n + C_2 \tag{4}$$

where $C_1 = 4c + 2$, $C_2 = 2c$. So the time complexity of the BAC is $O(n)$.

The optimized BAC adopts the Hashgraph structure based on DAG to improve the transaction rate. BAC generates micro blocks in the form of DAG and creates an official (master) chain by the primary in a chain structure. We define a block in the Asynchronous Byzantine Fault Tolerance (ABFT) stage as a micro block that consists of four parts: energy transaction information of EVs, timestamps, and a hash connected to its two parent micro blocks. EVs reach consensus on micro blocks in the form of virtual voting. This procedure is virtual because each EV broadcasts the micro block to a number of neighboring EVs rather than broadcasting its own authentication (vote) result for the micro block to all other EVs. Thus other EVs cannot determine whether the block is authenticated right away after receiving it, but they can do so throughout the subsequent process due to the structure of the hash pointer in the micro-block: each micro block needs to link two parent blocks, one of which is the previous micro block of itself, and the other is the micro block of any other node. If a micro block y could be traced back to some ancestor block x, the block y can see x. The block y could strongly see block x if the path passes through most EV nodes. If a micro block strongly sees most of the previous EVs, the micro block is in a new round, denoted as R. All EVs are in the same round $R = 1$ in their initial states. As shown in Fig. 2, the micro a_5 is in a new round $R + 1$ as it could strongly sees a_1, b_1, c_1, and d_1.

As shown in Fig. 2, the micro block b_5 strongly sees c_1: the b_5 can see c_1 through 3 paths passing four EVs B, C, D, and E in total, satisfying the condition of more than 2/3 (here the "majority" satisfies BFT Castro et al., 1999) of the total number of EVs. A witness is the first micro block created in round R. If a micro block y strongly sees the majority of witnesses, its vote for a witness x

is valid. Then if the number of votes on the x exceeds 2/3, the x can be marked as a famous witness; that is, the micro block x cannot be changed.

The ABFT stage is entirely decentralized, but it is unrealistic for the IoEV scenario because, given the current social system, getting a secure and reliable IoEV system made up entirely of EV users is impossible. As a result, the leader should exist, meaning the ETB will be heavily dependent on it. If the primary is malicious or is the victim of a cyber attack, the blockchain system will lose activity or security. To address this issue, we suggest a random election system for the primary (P and CP), but the process is not entirely random; the more an EV's reputation value, the greater the likelihood of being chosen as the primary. To determine an exact reputation value, we utilize a reputation management strategy based on subjective logic (Abishu et al., 2021). The evidence space and opinion space between EV sellers and buyers could be expressed as $\{\Phi_{i,j}, \eta_{i,j}, \varphi_{i,j}\}$ and $\{b_{i,j}, d_{i,j}, u_{i,j}\}$, respectively. The mapping of the opinion space to the evidence space could be expressed as:

$$b_{i,j} = \frac{\Phi_{i,j}}{\Phi_{i,j} + \eta_{i,j} + \varphi_{i,j}}, b_{i,j} \in [0, 1] \tag{5a}$$

$$d_{i,j} = \frac{\eta_{i,j}}{\Phi_{i,j} + \eta_{i,j} + \varphi_{i,j}}, d_{i,j} \in [0, 1] \tag{5b}$$

$$u_{i,j} = \frac{\varphi_{i,j}}{\Phi_{i,j} + \eta_{i,j} + \varphi_{i,j}}, u_{i,j} \in [0, 1] \tag{5c}$$

$$b_{i,j} + d_{i,j} + u_{i,j} = 1 \tag{6}$$

where $\Phi_{i,j}$, $\eta_{i,j}$, and $\varphi_{i,j}$ denote the number of honest behaviors, dishonest behaviors, and doubtful behaviors, respectively. Thus $b_{i,j}$, $d_{i,j}$, and $u_{i,j}$ denote the probabilities of "belief", "distrust", and "uncertainty", respectively. Finally, the reputation value of an EV could be calculated:

$$\rho_l = b_{i,j} + \varepsilon u_{i,j} \tag{7}$$

where ε is a preset constant that expresses the degree to which unknown behaviors impact the trust value.

Let ρ_i denote the EV_i's reputation, and $R = \sum_i \rho_i$ denote the reputation of all EVs. The probability that EV_i selected as a P or CP is proportional to ρ_i/R. A randomly chosen *seed* that is known to the public provides the randomization in primary elections. The verifiable random function (VRF) (Micali et al., 1999) is utilized. Any input string x will be returned by VRF into two results: a hash and a proof π allowing EVs to validate that the hash corresponds to x, without knowing the private sk.

The primary election is shown in Algorithm 2. A *role* parameter is required in BAC to distinguish between the various roles an EV may be chosen for. The expected number of EVs chosen for P or CP is specified by a threshold τ in BAC and an EV_i is elected with probability $p = \frac{\tau}{R}$. The λ parameter denotes how many times an EV is chosen (an EV with high reputation may be elected more than once). The binomial distribution describes the likelihood that precisely k out of the ρ_i will be elected:

$$B(k; \rho_i, p) = C_{\rho_i}^{k} p^k (1-p)^{\rho_i - k} \tag{8}$$

where $\sum_{k=0}^{\rho_i} B(k; \rho_i, p) = 1$. To determine how many of an EV's ρ_i units are elected, the election algorithm of BAC divides the interval [0, 1) into consecutive intervals and it could be expressed as:

$$I^{\lambda} = \left[\sum_{k=0}^{\lambda} B(k; \rho_i, p), \sum_{k=0}^{\lambda+1} B(k; \rho_i, p)\right) \tag{9}$$

where $\lambda \in \{0, 1, \ldots, \rho_i\}$. If $hash/2^{hashlen}$ ($hashlen$ is the bit-length of hash) falls in the interval I^{λ}, then the EV_i has exactly λ selected units, i.e., the EV_i is elected λ times. To better understand, the interval can be compared to a line segment of length 1. The segment is separated into numerous sections based on the EV's reputation value. An EV has a better chance of getting chosen if it possesses more reputation value since more copies are mapped to the line segment.

Algorithm 2: Primary Election

```
Input: $sk$, $seed$, $\tau$, $role$, $\rho_i$, $R$
Output: $\langle hash, \pi, \lambda \rangle$
$\langle hash, \pi \rangle \leftarrow VRF_{sk}(seed||role)$;
$p \leftarrow \frac{\tau}{R}$;
$\lambda \leftarrow 0$
while $\frac{hash}{2^{hashlen}} \notin \left[\sum_{k=0}^{\lambda} B(k; \rho_i, p), \sum_{k=0}^{\lambda+1} B(k; \rho_i, p)\right)$ do
    $\lambda$ ++;
    out $\leftarrow \langle hash, \pi, \lambda \rangle$
end
return out
```

5. Performance evaluation

We write a Python program and combine it with a blockchain simulator VIBES, on a computer with Windows Ultimate 64- bit, Intel i7-8550 CPU @ 1.80 GHz and 8.0 GB 2133 MHz LPDDR3, Java JDK Version 11.0.10, Scala Version 2.13.5, and Akka Version 2.6.14, to demonstrate the superior performance of our BAC. We also implement our ETB in the Hyperledger Fabric running 64-bit Ubuntu 16.04.6 LTS with 1.6-GHz Intel Core i5 Quad-CPU and 6G RAM, utilizing the Caliper for further performance evaluation. Our experiment considers a V2V blockchain network with four separate shards. Each shard has a diameter ranging from 0 to 3 km. Each EV travels at 45 to 60 miles per hour and charges at 22 kWh. The RSUs transmit at a 300 m radius. There are two key parameters related to the V2V blockchain system. The energy block size is 1.0 MB, with a propagation latency of 0.6s. The energy micro block size is 0.5 MB, with a propagation latency of 0.5s. There are seven other parameters: number of EVs, number of neighbors an EV owns, transaction size, neighbors discovery interval, micro block propagation delay, network bandwidth, and the transaction fee. The values of these parameters depend on the specific experimental environment.

The nodes in the PoW mine to calculate a random number that meets the difficulty requirement. The system adjusts the mining difficulty in real-time to ensure a certain outgoing fast speed. The block-generating speed determines the block-generating interval, which needs to be kept stable to ensure the system's security. In Bitcoin, the block-generating interval is 10 min. Mining will cause a considerable waste of resources, and the consensus-reaching period is long, which is unsuitable for IoT applications. PoW, PoS, and other consensus mechanisms cannot be divorced from the existence of tokens. The system's normal operation requires the reward mechanism of coins, and the system coin holders' maintenance guarantees the system's security. When the blockchain system is applied to IoT applications, the value of the assets it carries may far exceed the value of the coins issued by the system. It will only be reliable if the holders of the coins guarantee the security and stability of the system. The message-passing-based consistency algorithm PBFT goes through three steps to achieve consistency, with the possibility of failure at any stage. The PBFT system may normally operate without tokens, and each node's consensus comprises industry players or regulators. Security and stability are also ensured by the parties involved in the industry. However, PBFT requires fixed nodes and cannot be used in cases where the number of nodes is unknown. The communication

Table 2
The latency of different consensus mechanisms.

Mechanism	Latency				
	200 (EVs)	250 (EVs)	300 (EVs)	400 (EVs)	500 (EVs)
BAC	20 ± 2.98	20 ± 3.11	19 ± 2.87	20 ± 2.79	21 ± 3.47
Hashgraph	10 ± 2.88	10 ± 2.06	11 ± 2.32	9 ± 2.83	11 ± 2.69
PBFT	83 ± 2.92	85 ± 4.76	85 ± 5.08	89 ± 3.84	88 ± 4.54
PoW	41 ± 1.89	40 ± 2.38	41 ± 3.22	40 ± 2.93	40 ± 2.87

[1] Values are presented as the Confidence Interval.
[2] The Confidence Level is 95%.

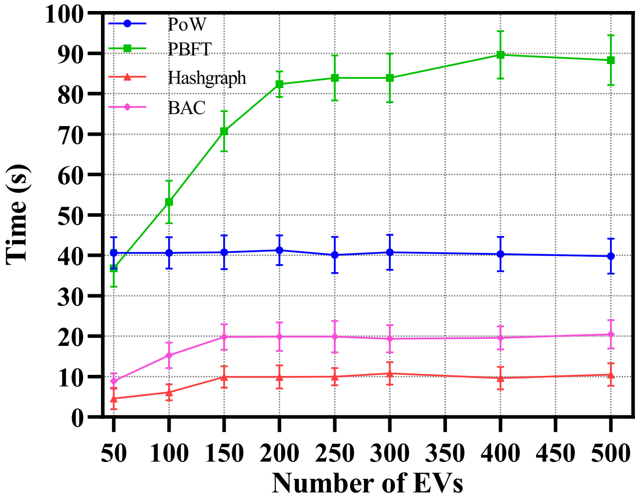


Fig. 3. Latency for a block published, with 50 to 500 EV users.

complexity of PBFT is $O(N^2)$ and can support only a small number of nodes. The computation of the leader node is fixed, which is very easy to be known and attacked by malicious nodes.

Block time is a crucial measure, often known as the interval between blocks. It may be used to evaluate the available system's condition. After the previous block, a new one can be spotted right away. Because nodes may need more time to send transactions, synchronize their transaction pools, or update the blockchain, short block times might result in odd behavior. The block period can therefore account for anomalous behavior. Scalability is one of the most pressing problems facing blockchains similar to bitcoin. Transactions per second (tps) are the primary parameter for evaluating scalability. One of its limitations is that this statistic needs more data about transaction size or usefulness. Adding a block size restriction is required to examine the impact of various input parameters on the scalability. This makes it possible to simulate BAC and other consensuses more precisely. All produced blocks adhere to the block size restriction depending on whether the simulation is a Blockchain simulation like Bitcoin. The simulator assumes an infinitely large block size and an infinitely high number of transactions per block if the block size limit is set to zero. Visualizations showing how many transactions are included in blocks and how many are pending would be highly instructive. Additionally, this is beneficial for determining accuracy.

Fig. 3 demonstrates the time to publish a block to blockchain in different consensus mechanisms, with the number of EVs varying from 50 to 500. Table 2 is only used as a reference. Most important is the height and trend of the data in the resultant graph. The duration of the simulation is set to 4 h. 50 experiments for each method have been replicated under the condition of the same number of EVs. Then we calculate the average of these 50 data points of each method and compare them. As for the confidence interval, here we take several sets of data for calculation. Hashgraph gains the best performance since it is completely decentralized - all the ETB participates generate blocks concurrently. And Hashgraph does not need to spend time deciding the block publisher and verifying the block's legitimacy. The performance of our BAC model is slightly inferior to Hashgraph in the interval of 50 to 500 EVs since BAC requires the leader EV with high reputation score to generate and publish blocks. And the legitimacy of the $block(i)$ depends on whether the subsequent $block(i+1)$ can enter the chain. The performance of PoW is relatively stable because it has a difficulty adjustment mechanism like Bitcoin in our experiments. However, PoW requires huge computing power. And to prevent blockchain forks, it needs a long enough time (appropriate difficulty) to generate a block. PBFT has the worst performance since its time complexity is $O(N^2)$ and communication complexity is too high. The ETB system cannot operate normally if the number of EVs exceeds 100. As can be observed, traditional consensus mechanisms are unsuitable for P2P energy trading.

Fig. 4 demonstrates the scalability of BAC and Hashgraph, scaling the number of EVs from 500 to 5000. The latency of BAC is about 4 times higher than that shown in Fig. 3. However, the scaling performance remains relatively flat all the way to 5000 users, indicating that BAC scales effectively. The latency of Hashgraph is about 9 times higher than Fig. 3. When the number of EVs exceeds 1500, BAC outperforms Hashgraph since the majority of EVs implement distributed storage. Each EV in Hashgraph must perform the gossip and "gossip about the gossip" protocol, resulting in two bottlenecks: CPU time and bandwidth. Compared to PoW and PBFT, BAC achieves latency improvement at any number of EVs. As shown in Fig. 3 in the original paper, up to 500 nodes, BAC and Hashgraph perform much better than the other two consensus mechanisms. When the number of EVs exceeds 500, we do not continue to show the performance of PBFT and PoW. The performance of PBFT only decreases as the number of nodes increases or stays at a high level. The performance of PoW stays the same, but the system needs to adjust the difficulty factor continuously. As the number of nodes increases, the difficulty factor will become larger and larger, and the arithmetic power required by the nodes to solve the puzzle will also become more extensive. Therefore PoW cannot be directly applied to the resource-constrained vehicular network.

Hashgraph is able to achieve enterprise-level throughput that is not affected by the number of nodes within a certain range, while BAC needs to spend some time and communication costs for the election of leader and committees, as well as the consensus of members within the committees, which also includes the time to propagate blocks. However, as the number of nodes increases (more than 1500), the advantages of BAC's sharding technique combined with our design of the original BAC can be manifested. Compared with the bandwidth and communication consumed by the gossip and gossip about gossip protocols in Hashgraph, the communication consumed by the consensus of committee members and ordinary EVs in BAC seems insignificant. Furthermore, standard nodes struggle to provide the broadband brought by hundreds of thousands of TPS alone. Nowadays, a

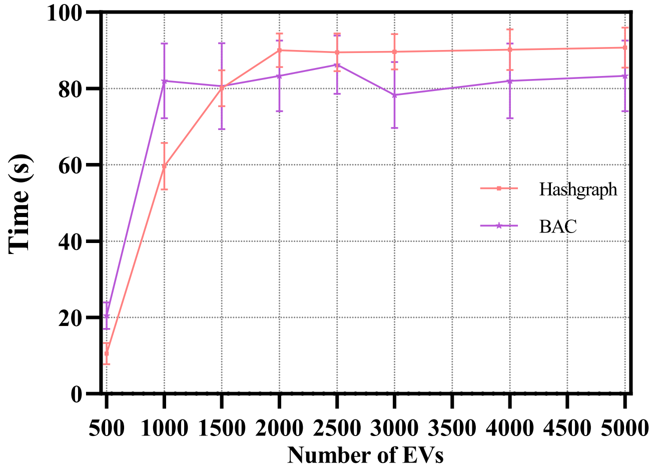


Fig. 4. Latency for a block published, with 500 to 5000 EV users.

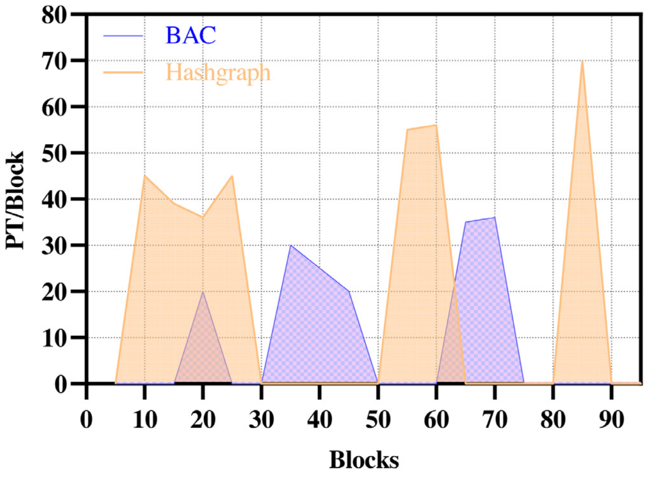


Fig. 5. Pending transactions in BAC and hashgraph.

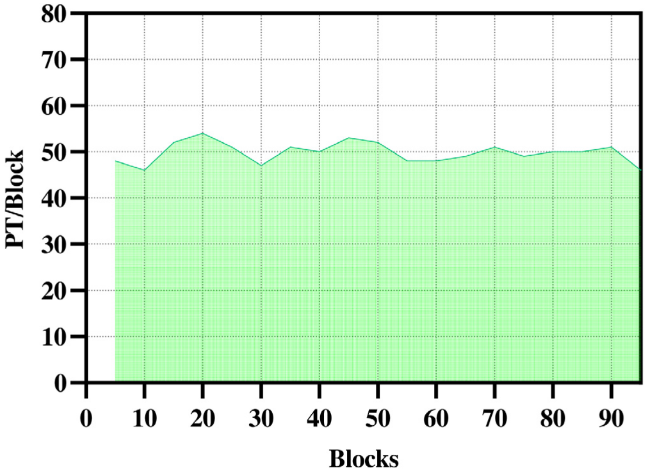


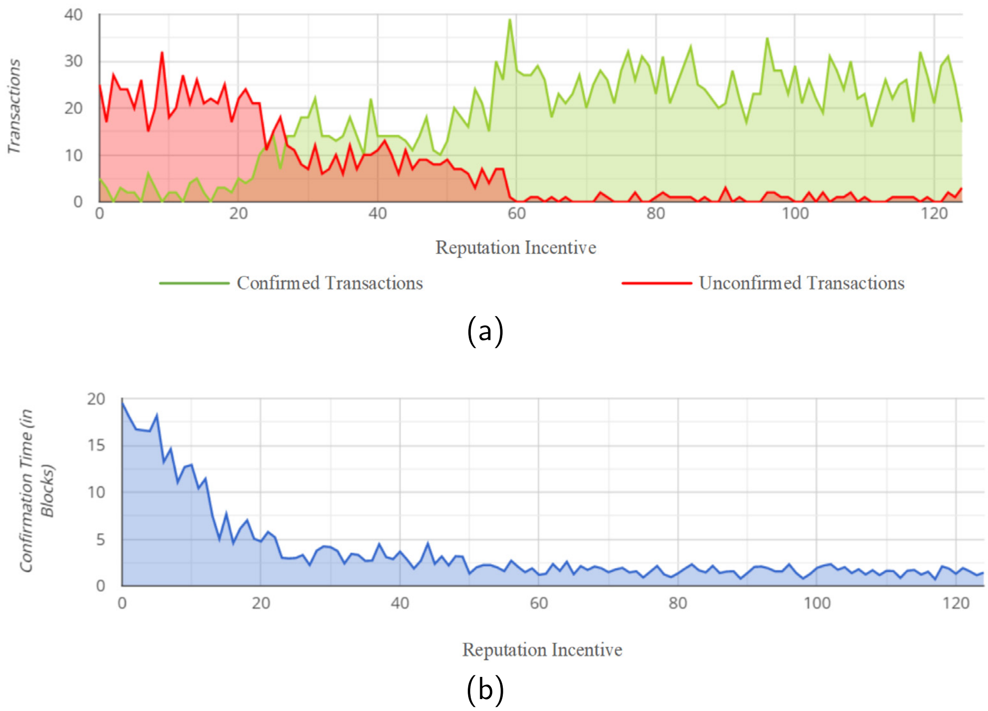
Fig. 6. Pending transactions in PoW.

single-core CPU can only verify the signatures of a few thousand transactions per second in a normal machine configuration, while the highest transaction rate of Enterprise Operation System (EOS) super nodes is only around 4000 transactions per second. In other words, even if Hashgraph has hundreds of thousands of transactions per second, only bank-grade or enterprise-grade hardware can support its operation. Moreover, it is a significant overhead for an ordinary EV node to process the data in the ledger, maintain the gossip graph, and the virtual voting mechanism.

While the number of EVs participating in Hashgraph inside a shard is static, the number of EVs within a shard is dynamic. The amount of transactions in the Hashgraph is scalable, but not the number of EVs. The BAC uses cryptographic random elections, and only those selected trusted EVs are allowed to take part in the consensus at the Hashgraph stage. These EVs are the primary generators and verifiers of blocks, and their number is predetermined. The quantity of EVs outside the committee within a given shard of the V2V blockchain, however, is constantly changing and may move between various shards. All miners in the initial step of most blockchain sharding systems provide proofs of work, allowing miners to validate their identities and fend against the Sybil Attack. If the outcomes of any miners' computations meet certain global difficulty requirements, they could become shard nodes. These shards conduct many rounds of PBFT consensus after the shard is built to package and publish fresh blocks to the blockchain network. From a cryptography standpoint, the BAC uses secondary sharding rather than conventional techniques. The status of the EVs determines how the first shard is organized (similar to network sharding). The second shard involves the selection of the committee from a cryptographic point of view to avoid the enormous computing power required by PoW, and to decrease the amount of communication overhead, microblock asynchronous BFT of the hashgraph is used in place of regular PBFT.

Pending transactions (PTs) of BAC and Hashgraph are shown in Fig. 5. PTs of PoW are shown in Fig. 6. PTs are those that are awaiting confirmation from EVs before being packaged into a block. The transaction request issued by an EV requester j is delayed until it has a sufficient credit balance if its current credit is insufficient. If the network is congested during peak trading hours, trading requests that have not yet been packaged during this period are also called pending transactions. Then we calculate the number of pending transactions of Hashgraph as 1725, BAC as 825. In terms of transaction processing capability, our BAC is 52% better than Hashgraph. The Hashgraph does not support the variable change of EVs, so Hashgraph cannot be adopted in V2V ETB. There currently needs to be a way to consider the throughput of Hashgraph in the consortium and public blockchains, so it cannot be applied to IoT with a large number of nodes. Despite its high throughput, Hashgraph cannot be applied in real-world IoT scenarios. PoW can support dynamic addition and deletion of nodes and can be applied in public blockchains. However, PoW cannot be applied to resource-constrained IoT either due to its substantial computational requirements and low throughput.

The limiting values are not considered in our experiments. The number of EVs within the shard cannot grow indefinitely. There is no need to consider the limit value. First, the maximum number of EVs within the shard in our experimental environment reaches 5000. In the current IoEV, 5000 cars are enough to be implemented. Secondly, we use the sharding technique. Cryptography is combined within the shard to elect a central leadership committee randomly. The leadership committee carries out the core consensus part of the energy trading. Moreover, the distributed data distribution is done by these central nodes (e.g., some sizeable central servers). Even if the number of EVs within the slice keeps increasing, it will have little impact on the communication overhead of the IoEV. The communication complexity of the classical BFT mechanism is $O(N^2)$, and that of the BAC mechanism is $O(N)$. Theoretically, the communication



(a)

(b)

Fig. 7. Pending transactions. (a) Confirmed and unconfirmed transactions with the increase of reputation score. (b) Confirmation time with the increase of credit score.

complexity for several EVs of 70 in BFT is the same as that of 4900 in BAC. The BAC consensus mechanism dramatically improves the scalability of the system. Third, the BAC consensus mechanism applies to the current social form, which retains the centralized component. The applicable blockchain environment for BAC is the consortium blockchain. Five thousand electric cars are sufficient to constitute the consortium blockchain system in practical applications. If it exceeds this value, BAC must develop in the public chain's direction. Furthermore, the EVs exceed a specific value, meaning that user participation has reached a sufficient level. In this case, what V2V ETB needs more is universal participation. Each user may need to maintain a local blockchain, the infinite scalability we are currently working on.

Our proposed BAC consensus mechanism does not consider limit values since the simulated number of 5000 (at most) EV nodes is sufficient to demonstrate the excellence of the BAC approach. The experiments include PoW, the origin consensus mechanism of blockchain; PBFT, the classical BFT-based consensus mechanism; and Hashgraph, a new consensus mechanism based on DAG. Currently, V2V architecture is not widely used, so 5000 nodes are sufficient to support the pilot work of theoretical applications in the early stage of practical applications. We only compare the performance of BAC and Hashgraph after 500 nodes. We do not continue to compare the performance of PoW and PBFT because the performance gap between PoW, PBFT, and BAC, Hashgraph is already evident within 500 EV nodes. The performance gap between BAC and Hashgraph is insignificant. BAC is slightly inferior to Hashgraph within 500 nodes, but this impacts the V2V ETB system little. Hashgraph cannot be directly applied to V2V ETB because the number of nodes is fixed before joining Hashgraph. This makes Hashgraph cannot be applied to V2V ETB, where the number of nodes changes frequently.

There are two types of incentives in BAC. The ETB system awards EVs' reputation based on the effectiveness of the block's ultimate condition. The othre is the reward for CP or P broadcasting the required blocks to other EVs. As illustrated in Fig. 7, an EV utilizes its credits to attach a fee to a transaction, convincing the P and CP to include the transaction in the next block to be published.

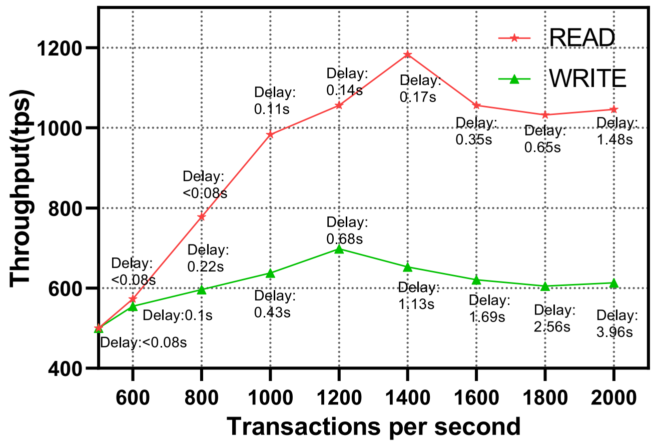


Fig. 8. Performance of READ and WRITE from/to the ETB.

The Hyperledger Fabric and Caliper are utilized to test ETB's performance. Fig. 8 illustrates our V2V ETB performance under a different number of workloads from 500 tps to 2000 tps. As can be seen in the figure, the throughput of READ can reach the highest to 1183 tps at 1400 tps workload, whereas WRITE reaches 698tps at 1200 tps workload with less than 0.7-second latency.

6. Conclusion

In this paper, we propose a blockchain-based V2V energy trading model. In contrast to most studies on blockchain-based energy trading, this paper suggests a novel BAC consensus mechanism instead of directly adopting the traditional consensus mechanisms such as PoW and PBFT. Our BAC allows the system to continue to work correctly when software errors or Byzantine EVs are present. Moreover, our proposed BAC mechanism solves the problems that Hashgraph cannot sovle in practical applications. We use the sharding technique to shard the IoEV based on the geographic location of the EVs. In addition to being consistent with V2V Energy Trading's properties, this significantly improves the system's throughput and scalability. We keep the centralized component to improve the practical utility of the V2V ETB. The centralized component includes government agencies or technical departments and EV users to motivate them to maintain the energy trading system fairly and efficiently. Cryptography is employed to elect the central leadership committee in a random (unpredictable) but fair (the more points, the higher the odds) manner. Hashgraph-based consensus mechanisms are used instead of traditional consensus mechanisms among the nodes of the leadership committee to achieve high speed and generate blocks concurrently. The BAC mechanism greatly improves the throughput and reduces the latency of V2V ETB. Compared with Hashgraph, BAC makes up for the application shortcomings of Hashgraph. BAC is more scalable due to the random leader election and sharding. Our BAC method reduces latency by 20% and 78% compared to PoW and PBFT, respectively. The BAC reduces latency by 10% compared to Hashgraph when the number of EVs exceeds 1500. In terms of transaction processing capability, our BAC reduces 52% PTs than Hashgraph. As new energy storage devices, EVs can save the grid huge sums of money in peaking costs and reduce investments in energy storage. However, this distributed energy trading approach must take into account the mobility of EVs. Our proposed V2V ETB takes this into account and designs a detailed scheme and algorithm for this purpose. However, how the EVs and the centralized institutions handle cross-shard transactions are not well designed in this paper. The next step of our study will also design a detailed game theory based incentive mechanism.

CRediT authorship contribution statement

Yingsen Wang: Conceptualization, Methodology, Formal analysis, Writing – original draft. **Yixiao Li:** Data curation, Writing – original draft. **Yao Suo:** Visualization, Investigation. **Yan Qiang:** Funding acquisition, Resources, Supervision. **Juanjuan Zhao:** Resources, Supervision. **Keqin Li:** Conceptualization, Supervision, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

I have shared the data set at the Attach File step.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. U21A20469 No. 61872261 No. 61972274).

References

Abishu, H.N., Seid, A.M., Yacob, Y.H., Ayall, T., Sun, G., Liu, G., 2021. Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles. IEEE Trans. Veh. Technol. 71 (1), 946–960.

Aitzhan, N.Z., Svetinovic, D., 2016. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secure Comput. 15 (5), 840–852.

Alvaro, R., González, J., Gamallo, C., Fraile-Ardanuy, J., Knapen, D.L., 2014. Vehicle to vehicle energy exchange in smart grid applications. In: 2014 International Conference on Connected Vehicles and Expo. ICCVE, IEEE, pp. 178–184.

Alvaro-Hermana, R., Fraile-Ardanuy, J., Zufiria, P.J., Knapen, L., Janssens, D., 2016. Peer to peer energy trading with electric vehicles. IEEE Intell. Transp. Syst. Mag. 8 (3), 33–44.

Baharom, R., Hakim, N., Rahman, N., 2020. Wireless vehicle to vehicle (v2v) power transmission using spmc. In: 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics. ISCAIE, IEEE, pp. 125–130.

Bi, Z., Kan, T., Mi, C.C., Zhang, Y., Zhao, Z., Keoleian, G.A., 2016. A review of wireless power transfer for electric vehicles: Prospects to enhance sustainable mobility. Appl. Energy 179, 413–425.

Cai, W., Jiang, W., Xie, K., Zhu, Y., Liu, Y., Shen, T., 2020. Dynamic reputation–based consensus mechanism: Real-time transactions for energy blockchain. Int. J. Distrib. Sens. Netw. 16 (3), 1550147720907335.

Castro, M., Liskov, B., et al., 1999. Practical byzantine fault tolerance. In: OsDI, 99. pp. 173–186.

Das, S., Pal, K., Goswami, P., Kerawalla, M., 2018. Wireless power transfer in electric vehicles. Int. J. Appl. Environ. Sci. 13 (7), 643–659.

Feng, L., Zhang, H., Chen, Y., Lou, L., 2018. Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain. Appl. Sci. 8 (10), 1919.

Gao, W., Hatcher, W.G., Yu, W., 2018. A survey of blockchain: Techniques, applications, and challenges. In: 2018 27th International Conference on Computer Communication and Networks. ICCCN, IEEE, pp. 1–11.

Garg, S., Kaur, K., Kaddoum, G., Gagnon, F., Rodrigues, J.J., 2019. An efficient blockchain-based hierarchical authentication mechanism for energy trading in v2 g environment. In: 2019 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, pp. 1–6.

Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D.I., Zhao, J., 2019. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Trans. Veh. Technol. 68 (3), 2906–2920.

Li, D., Gong, Y., 2022. The design of power grid data management system based on blockchain technology and construction of system security evaluation model. Energy Rep. 8, 466–479.

Li, S., Mi, C.C., 2014. Wireless power transfer for electric vehicle applications. IEEE J. Emerg. Select. Top. Power Electr. 3 (1), 4–17.

Machura, P., De Santis, V., Li, Q., 2020. Driving range of electric vehicles charged by wireless power transfer. IEEE Trans. Veh. Technol. 69 (6), 5968–5982.

Micali, S., Rabin, M., Vadhan, S., 1999. Verifiable random functions. In: 40th Annual Symposium on Foundations of Computer Science (Cat. No. 99CB37039). IEEE, pp. 120–130.

Mou, X., Zhao, R., Gladwin, D.T., 2018. Vehicle to vehicle charging (v2v) bases on wireless power transfer technology. In: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, pp. 4862–4867.

Saad, W., Han, Z., Poor, H.V., Başar, T., 2011. A noncooperative game for double auction-based energy trading between phevs and distribution grids. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 267–272.

Salimitari, M., Chatterjee, M., Yuksel, M., Pasiliao, E., 2017. Profit maximization for bitcoin pool mining: A prospect theoretic approach. In: 2017 IEEE 3rd International Conference on Collaboration and Internet Computing. CIC, IEEE, pp. 267–274.

Sharma, V., 2018. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (iov). IEEE Commun. Lett. 23 (2), 246–249.

Sheikh, A., Kamuni, V., Urooj, A., Wagh, S., Singh, N., Patel, D., 2019. Secured energy trading using byzantine-based blockchain consensus. IEEE Access 8, 8554–8571.

Shoup, V., 2000. Practical threshold signatures. In: International Conference on the Theory and Applications of Cryptographic Techniques. Springer, pp. 207–220.

Siano, P., De Marco, G., Rolán, A., Loia, V., 2019. A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. IEEE Syst. J. 13 (3), 3454–3466.

Sousa, T.J., Monteiro, V., Fernandes, J.A., Couto, C., Meléndez, A.A.N., Afonso, J.L., 2018. New perspectives for vehicle-to-vehicle (v2v) power transfer. In: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society. IEEE, pp. 5183–5188.

Su, Z., Wang, Y., Xu, Q., Fei, M., Tian, Y.-C., Zhang, N., 2018. A secure charging scheme for electric vehicles with smart communities in energy blockchain. IEEE Internet Things J. 6 (3), 4601–4613.

Sun, G., Dai, M., Zhang, F., Yu, H., Du, X., Guizani, M., 2020. Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles. IEEE Internet Things J. 7 (9), 7868–7882.

Triviño, A., González-González, J.M., Aguado, J.A., 2021. Wireless power transfer technologies applied to electric vehicles: A review. Energies 14 (6), 1547.

Ucer, E., Buckreus, R., Kisacikoglu, M.C., Bulut, E., Guven, M., Sozer, Y., Giubbolini, L., 2019. A flexible v2v charger as a new layer of vehicle-grid integration framework. In: 2019 IEEE Transportation Electrification Conference and Expo. ITEC, IEEE, pp. 1–7.

Wang, J., 2022. A novel electric vehicle charging chain design based on blockchain technology. Energy Rep. 8, 785–793.

Wang, Y., Cai, S., Lin, C., Chen, Z., Wang, T., Gao, Z., Zhou, C., 2019a. Study of blockchains's consensus mechanism based on credit. IEEE Access 7, 10224–10231.

Wang, Y., Li, Y., Zhao, J., Wang, G., Jiao, W., Qiang, Y., Li, K., 2022a. A fast and secured peer-to-peer energy trading using blockchain consensus. In: 2022 IEEE Industry Applications Society Annual Meeting. IAS, IEEE, pp. 1–8.

Wang, Y., Ma, Y., Qiang, Y., Zhao, J., Li, Y., Li, K., 2022b. Bac: A block alliance consensus mechanism for the mine consortium blockchain. Concurr. Comput.: Pract. Exper. 34 (27), e7344.

Wang, Y., Su, Z., Xu, Q., Yang, T., Zhang, N., 2019b. A novel charging scheme for electric vehicles with smart communities in vehicular networks. IEEE Trans. Veh. Technol. 68 (9), 8487–8501.

Wood, G., et al., 2014. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 151 (2014), 1–32.

Xia, S., Lin, F., Chen, Z., Tang, C., Ma, Y., Yu, X., 2020. A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles. IEEE Trans. Veh. Technol. 69 (7), 6856–6868.

Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H.-N., Imran, M., 2020. Blockchain for cloud exchange: A survey. Comput. Electr. Eng. 81, 106526.

Xu, J., Wong, V.W., 2011. An approximate dynamic programming approach for coordinated charging control at vehicle-to-grid aggregator. In: 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm). IEEE, pp. 279–284.

Yang, Y., Yang, W., Guo, Z., Zhu, J., 2020. Research on consensus algorithm of multi energy interaction agents based on pbft. In: 2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), 1. IEEE, pp. 416–421.

Yu-boSong, R.S., Zhang, Shi-qi, 2020. A blockchain consensus mechanism based on voting rights competition. J. Shandong Univ.(Nat. Sci.) 55 (3), 43. http://dx.doi.org/10.6040/j.issn.1671-9352.2.2019.142, http://lxbwk.njournal.sdu.edu.cn/EN/abstract/article_3240.shtml.

Zhao, W., Lv, J., Yao, X., Zhao, J., Jin, Z., Qiang, Y., Che, Z., Wei, C., 2019. Consortium blockchain-based microgrid market transaction research. Energies 12 (20), 3812.