This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

BBNP: A Blockchain-based Novel Paradigm for Fair and Secure Smart Grid Communications

Haiyong Bao, Binbin Ren, Beibei Li, *Member, IEEE,* and Qinglei Kong, *Student Member, IEEE*

***Abstract*—As the future energy infrastructure, smart grid aims to overcome the disadvantages of traditional power grid, e.g., low efficiency and unstable service. However, the frequent collection and analysis of the user's electricity data may bring various security and privacy threats. Besides, the traditional centralized data storage model in the smart grid is prone to the single point of failure. To address these challenges, in this paper, for fair and secure smart grid communication, a blockchain-based novel paradigm, named BBNP, is proposed. Specifically, based on pseudo-random function and auxiliary information generation and sharing technology, a lightweight data aggregation protocol is designed firstly to protect the user's data privacy and ensure communication confidentiality. Then, a novel efficient authentication mechanism is proposed to generate and share session keys in a non-interactive way, which is leveraged for MAC authentication to achieve data integrity of the transmitted data. After that, based on subjective logic reputation model, a blockchain node consensus mechanism is studied to efficiently store smart grid big data and effectively solve single point failure problem. By constructing the long-term reputation model for consensus nodes and integrating batch verification technology, the problems of consensus nodes fair selection and scalability of large-scale nodes are solved simultaneously. Finally, performance evaluation indicates that BBNP outperforms the state-of-the-art similar schemes in computing complexity, communication cost, system availability, and fairness of block generation.**

***Index Terms*—Smart grid, Blockchain, Data aggregation, Reputation.**

I. Introduction

SMART grid, as the next generation of the power grid, has attracted wide attention in recent years [1] [2] [3]. The user's data are collected by smart meters and delivered to the control center (CC) for real-time monitoring and comprehensive analysis. However, the user's data, $e.g.$, collected every 15 minutes, is highly relevant to the user's lifestyle. Thus, it is of vital importance to preserve the user's privacy [4] [5]. In addition to the user's privacy, data integrity is also critical in the smart grid. Besides, the traditional smart grid mainly adopts centralized architecture, thus it has the inherent defect of the single point of failure.

To solve privacy preservation, data integrity, and the single point of failure issues, researchers have proposed various schemes. Among them, data aggregation is utilized to protect the single user's data from being violated [2], [6]–[10]. Lu *et al.* presented a privacy-preserving multidimensional data aggregation scheme [2] by integrating a super increasing sequence and the homomorphic Pallier cryptosystem [11]. Guo *et al.* formulated a lightweight data aggregation scheme based on the symmetric homomorphism scheme [6]. Khan *et al.* utilized Boneh-Goh-Nissam (BGN) cryptosystem to achieve privacy preservation [7]. Badra *et al.* proposed a lightweight data aggregation scheme [8] based on symmetric homomorphic encryption and Elliptic Curve Differ-Hellman (ECDH) key exchange techniques. Liu *et al.* proposed a practical data aggregation scheme without a trusted third party, in which the trusted users constructs a virtual aggregation area to preserve the user's privacy [9]. Ni *et al.* presented a secure data aggregation scheme [10], which is constructed by homomorphic encryption, trapdoor hash function, and homomorphic authenticators.

In addition, a line of research studies have also been carried out on data integrity in smart grid [6], [7], [12]–[14]. Guo *et al.* proposed a data integrity scheme [6] from Password Authenticated Key Exchange (PAKE) [15] based certification agreement. Khan *et al.* utilized the Boneh-Goh-Nissam (BGN) cryptosystem and Elliptic Curve Digital Signature Algorithm (ECDSA) authentication to resist Fault Data Injection (FDI) and data reply attack [7]. Fan *et al.* realized data integrity utilizing Boneh-Lynn-Shacham short signature and SHA-256 [14]. Hur *et al.* effectively guaranteed data integrity through the identification-based sequential signature scheme [12]. Kong *et al.* proposed a conditional group blind signature and homomorphic encryption marker mechanism to verify data integrity [13].

In the above schemes, the user's data are stored in a centralized manner, which is prone to the single point failure. Due to its decentralization and non-tampering features [16], the emerging blockchain technology provides a new opportunity to address the above problems. Currently, some researchers have integrated the blockchain into the smart grid [17]–[19]. Fan *et al.* proposed a data aggregation scheme based on the blockchain, which stores the user's data in the blockchain [17]. Guan *et al.* presented a blockchain assisted data aggregation scheme for smart grid, which divides users into different

H. Bao is with Software Engineering Institute, East China Normal University, Shanghai 200062, China.

H. Bao and B. Ren are with School of Computer Science and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China.

B. Li is with College of Cyber Science and Engineering, Sichuan University, Chengdu 610065, China.

Q. Kong is with School of Science and Engineering, Chinese University of Hong Kong, Shenzhen 518172, China.

This work was partially supported by the National Natural Science Foundation of China (No. 62072404, No. 62002248, and No. 62072403), the National Key Research and Development Program of China (No. 2020YFB1805400), the China Postdoctoral Science Foundation (No. 2019TQ0217 and No. 2020M673277), and the Provincial Key Research and Development Program of Sichuan (No.20ZDYF3145).

Corresponding author: Binbin Ren (renbbzjhz@163.com).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

groups and records the user's data in the private blockchain [19]. Chen *et al.* designed double blockchain based data aggregation, which utilizes Practical Byzantine Fault Tolerant consensus mechanism (PBFT) to verify and store the user's data [18].

However, the consensus mechanism selected in some schemes lacks fairness and randomness [17], [18]. Fan *et al.* selected Delegated Proof of Stake (DPoS) consensus mechanism to store the user's data in the blockchain, which is not random and fair enough [17]. Chen *et al.* adopted PBFT consensus mechanism to achieve consensus, which tolerates the Byzantine nodes. Observing that all nodes have the same probability of being selected as primary node, PBFT lacks randomness and fairness [18].

Therefore, privacy preservation, data integrity, high utility, and fairness are of great significance. Motivated by this observation, we propose a blockchain-based novel paradigm for fair and secure smart grid communications (BBNP) by integrating blockchain, modular-addition-encryption, complete data verification mechanism, consensus mechanism based on subjective logic reputation model, and batch verification technique. Specifically, the main contributions of this paper are summarized as follows.

- Firstly, we propose a novel and efficient identity authentication scheme, which flexibly generates and shares the session keys in a non-interactive way, and organically integrates secure authentication MAC to ensure the integrity of data communications. Besides, based on modular-addition-encryption, the user's data are securely encrypted and aggregated, which effectively protects the user's privacy.
- Secondly, we design a secret information sharing technology that satisfies specific algebraic relationships, utilizing the pseudo-random-function and auxiliary information generation technology to group the users non-linearly and efficiently. It also achieves data confidentiality for the smart grid communications.
- Finally, we integrate the blockchain into the smart grid. Utilizing the blockchain to store the user's data effectively solves the single point of failure problem. Meanwhile, we improve the traditional PBFT, which is based on the proposed subjective logic reputation model, random threshold technique, and signature batch verification. This design effectively alleviate the scalability issue of PBFT and significantly improves the fairness of smart grid communication.

The remainder of this paper is organized as follows. We first specify the problem formalization, including system model, attack model, and design goal in Section II, and briefly review some preliminaries in Section III. Then, our novel data aggregation scheme is presented in Section IV. Subsequently, the security analysis and performance evaluation are demonstrated in Section V and Section VI, respectively. Finally, our conclusions are drawn in Section VII.

II. Problem Formalization

In this section, we formalize the system model, attack model, and identify the design goal.

A. System model

Based on the typical scenario of the smart grid communications, the entire system architecture is shown in Fig. 1, which mainly includes the following five participants.

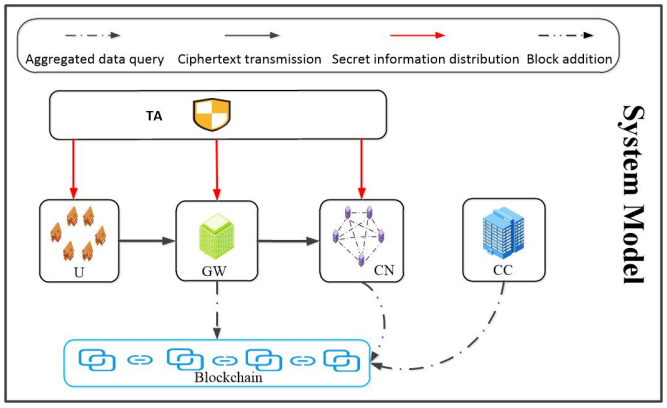


Fig. 1: System model under consideration

Trusted Authority (TA), who is responsible for managing and distributing the secret information of all entities in the system, and is a powerful and trusted third party.

Control Center (CC), who is responsible for integrating, processing, and analyzing the periodic time-series data from the users to provide reliable and intelligent services.

Gateway (GW), who connects the CC and users, is responsible for aggregating data submitted by users and forwarding communications.

Users (U), which includes N smart users, *i.e.*, $U = \{U_1, \cdots, U_N\}$, who are responsible for collecting real-time data and transmitting to the GW after encryption.

Consensus Nodes (CN), which includes M consensus nodes, *i.e.*, $CN = \{CN_1, \cdots, CN_M\}$, who are mainly responsible for generating new blocks and storing the user's data in the blockchain.

B. Attack model

In our attack model, there may exist a malicious external adversary $\mathcal{A}$, who could compromise the security and practicability of the smart grid. Besides, we consider that all the participants follow the protocol faithfully ("honest"). The possible attacks are as follows.

- $\mathcal{A}$ may reveal the user's privacy by eavesdropping, intercepting, and maliciously analyzing the user's communication packages.
- $\mathcal{A}$ may destroy the user's data integrity, and transmit the malicious data, which will cause the CC to make wrong decisions, and affect the availability of the smart grid.
- $\mathcal{A}$ may attack the centralized storage of the user's data, and cause the single point of failure, which will seriously affect the security and practicality of the smart grid.
- $\mathcal{A}$ may attack the operation of the consensus mechanism, and undermine its fairness. More seriously, it will result in long-term failure for reaching the consensus, which will severely affect the availability of the smart grid.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

Note that we focus on preventing the external attacks from causing security and privacy threats, and reducing the availability of smart grid. Other attacks, for example, the internal attack, are beyond the scope of this study, and will be discussed in future work.

C. Design goal

Considering the above system model and attack model, our design goal is to propose a blockchain-based novel paradigm for fair and secure smart grid communications. Specifically, the following design goals should be satisfied.

- ***Privacy preservation.*** Even if the malicious attacker $\mathcal{A}$ could steal the transmitted communications, the user's privacy cannot be disclosed. Meanwhile, although $\mathcal{A}$ could intrude into servers of the GW, and deploy some undetectable malwares, it still has no way to reveal the user's privacy either.
- ***Data integrity.*** The valid communications cannot be destroyed during the transmission. If $\mathcal{A}$ launches the attacks on the data integrity of communications (such as modification, forgery, injection, *etc.*), the malicious behaviors should be detected.
- ***Communication confidentiality.*** The encrypted information is transmitted between different entities in the smart grid. Although $\mathcal{A}$ could steal the information, it cannot recover the original data, which ensures communication confidentiality.
- ***High utility.*** The proposed system is based on the blockchain, which has strong robustness and stability. Taking good advantage of its characteristics of secure data storage, the system should effectively solve the traditional problem of single point failure.
- ***Fairness.*** In our consensus mechanism, the primary node is responsible for verifying the aggregated data and generating new blocks. Due to the complex operations of the nodes and the existence of Byzantine nodes, the efficiency and security of the consensus mechanism are easy to be seriously affected. Therefore, the fairness of the consensus mechanism should be ensured.

III. Preliminary

In this section, we briefly introduce the basic knowledge of the blockchain, subjective logic reputation model, practical byzantine fault tolerant, bilinear pairing, and Boneh-Lynn-Shacham short signature.

A. Blockchain

The blockchain is considered as a peer-to-peer (P2P) distributed database that creates blocks and links in chronological order [20], which is designed to provide decentralized and distributed solutions for a wide range Internet of Things (IoT). Specifically, in the blockchain network, all participants will act as distributed nodes to jointly maintain transaction information. However, some existing blockchain consensus mechanisms lack fairness, which leads to the same probability of all nodes becoming primary nodes. Our consensus mechanism introduces the reputation mechanism to improve fairness.

B. Subjective Logic Reputation Model

Currently, there are various reputation evaluation models. According to the different evaluation theories, reputation models are roughly divided into two types, *i.e.*, precise theory based and imprecise theory based, as shown in Fig. 2.

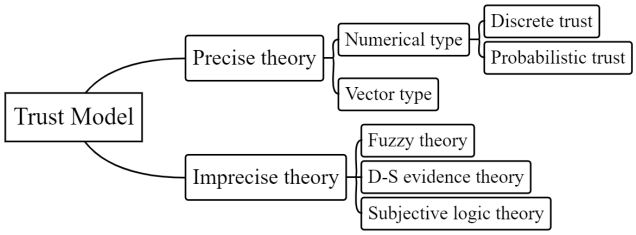


Fig. 2: Classification of trust assessment models

The model based on precision theory is divided into numerical and vector types. Numerical evaluation models perform trust evaluation based on the given transaction results, which can be divided into discrete and probabilistic trust values [21]. The vector evaluation model [22] [23] mainly calculates the reputation based on multidimensional vectors. There are three main types of models based on imprecise theory, *i.e.*, fuzzy theory, D-S evidence theory [24], and subjective logic theory [25] [26]. Specifically, our reputation model is based on subjective logic theory. Jøsang *et al.* utilized subjective logic theory to model the trust relationship [25]. They introduced the probability of the evidence space and the concept space, which can better depict the subjective tendency in real life.

The concept space consists of a triple $w_j^i = (b_j^i, d_j^i, u_j^i)$, where w_j^i represents the subjective opinion of entity i on j, and b_j^i, d_j^i, u_j^i represent the trust, distrust, and uncertainty of j, respectively. w_j^i satisfies the relationship of $b_j^i + d_j^i + u_j^i = 1$, and $b_j^i, d_j^i, u_j^i \in [0, 1]$. And, the evidence space consists of a set of correct events r and incorrect events s. b_j^i, d_j^i, u_j^i are defined as $b_j^i = \frac{r}{r+s+C}$, $d_j^i = \frac{s}{r+s+C}$, and $u_j^i = \frac{C}{r+s+C}$, respectively, where C is the uncertainty factor. Besides, the mathematical expectation E_j^i is defined as $E_j^i = b_j^i + a_j^i u_j^i$, where a_j^i represents the prior probability of i to j. In our model, we define E_j^i as the trust value of i to j.

C. Practical Byzantine Fault Tolerant

The Practical Byzantine Fault Tolerant (PBFT) consensus mechanism is proposed by Miguel Castro and Barbara Liskov [27], which can tolerate Byzantine nodes. Assume the system has f number of Byzantine nodes, and $2f + 1$ normal nodes, thus the total number of nodes is $3f + 1$. In PBFT, nodes are divided into primary nodes and replica nodes. The primary node is mainly responsible for verifying transactions and generating candidate blocks. The replica node is mainly responsible for verifying the blocks. As shown in Fig. 3, we take four nodes as an example, and the process of PBFT is divided into five stages, *i.e.*, **Request**, **Pre-prepare**, **Prepare**, **Commit**, and **Reply**. Moreover, it should be noted that we apply the batch verification technique to address the scalability issue of PBFT.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

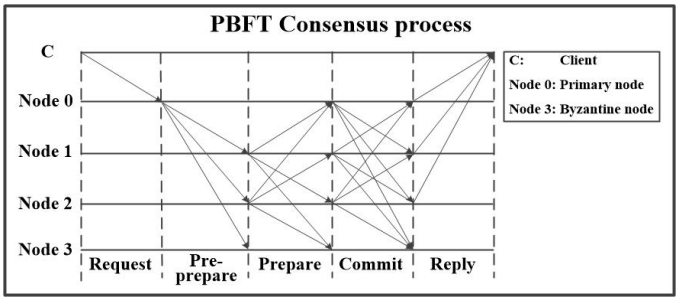


Fig. 3: The process of PBFT consensus protocol

D. *Bilinear Pairing*

Let G and G_T be cyclic groups of order p, where p is a big prime number. There is a non-degenerate, efficient, and computable bilinear mapping [28] [29] $e : G \times G \rightarrow G_T$ with the following properties.

1) **Bilinearity.** $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $g_1, g_2 \in G, a, b \in Z_p^*$.
2) **Non-degeneracy.** For all $g_1, g_2 \in G$, $e(g_1, g_2) \neq 1$.
3) **Computability.** The bilinear pair function $e(g_1, g_2)$ is computable with an efficient algorithm for all $g_1, g_2 \in G$.

E. *Boneh-Lynn-Shacham Short Signature*

Boneh-Lynn-Shacham (BLS) short signature [30] is a typical bilinear pairing scheme. Let the bilinear pairing be $e : G \times G \rightarrow G_T$, and the hash function be $H : \{0,1\}^* \rightarrow G$. The BLS is divided into three stages, *i.e.*, **Key generation**, **Signature**, and **Verification**.

1) **Key generation.** Pick a random $x \overset{R}{\leftarrow} Z_p$, and compute $v \leftarrow g^x$. The public key is $v \in G$. The private key is x.
2) **Signature.** Given a private key $x \in Z_p$, and a message $M \in \{0,1\}^*$, compute $h \leftarrow H(M)$ and $\sigma \leftarrow h^x$, where σ is the signature.
3) **Verification.** Given a public key v, a message M, and a signature σ, compute $e(\sigma, g)$ and $e(H(M), v) = e(h, v)$. If $e(\sigma, g) = e(h^x, g) = e(H(M), g^x) = e(h, v)$, σ is correct and valid.

IV. Proposed Scheme

In this section, we propose BBNP scheme as shown in Fig. 4. According to the complete data life cycle, the proposed scheme can be divided into the following four phases, *i.e.*, **System initialization**, **Data reporting**, **Secure data aggregation**, and **Secure data storage**.

A. *System Initialization*

The TA performs the following steps to initialize the system.

1) Given a secure parameter Ψ, run the system initialization function $\mathcal{F}(\Psi)$, and output the system parameters (G, G_T, g, p, e), where p is a secure big prime number, G, G_T are cyclic groups of order p, g is the generator of the group G, and $e : G \times G \rightarrow G_T$ is the bilinear mapping.

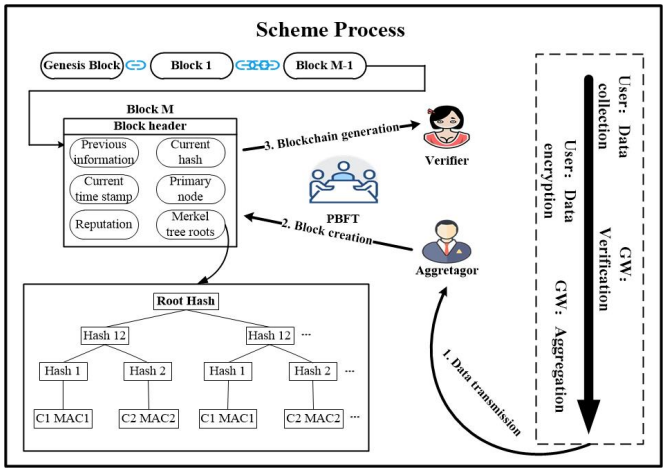


Fig. 4: The process of proposed scheme

2) Perform the following procedures to assign the secret information of all users $U = \{U_1, \cdots, U_N\}$, GW, and consensus nodes $CN = \{CN_1, \cdots, CN_M\}$.
   a) Randomly select N number of $s_i \in Z_p$, and calculate $S_i = g^{s_i}$, where $i = 1, 2, \cdots, N$. s_i and S_i are the private and public keys of U_i (with identity information ID_i), respectively.
   b) Calculate $s_g \in Z_p$ to satisfy $s_g + \sum_{i=1}^{N} s_i = 0$, and $S_g = g^{s_g}$. s_g and S_g are the private and public keys of the GW (with identity information ID_g), respectively.
   c) Randomly select M number of $\alpha_j \in Z_p$, and $c_j \in Z_p$, respectively, and calculate $G_j = g^{\alpha_j}$, where $j = 1, 2, \cdots, M$. α_j and G_j are the private and public keys of CN_j, respectively, and c_j is public random value of CN_j.
   d) Randomly select one secure hash function $H : \{0,1\}^* \rightarrow G$.
   e) Select the secure authentication function $MAC_k = HMAC(k, m)$, where k is the secret key and m is the data.
   f) Publish the system parameters $(G, G_T, g, p, e, S_g, ID_g, H, MAC_k)$, $< ID_i, S_i >$, and $< c_j, G_j >$, where $i = 1, 2, \cdots, N$, and $j = 1, 2, \cdots, M$.
3) According to the performance and status of CN_j, set the initial reputation value $T_j \in [0, 1]$, for $j = 1, 2, \cdots, M$, and the reputation threshold $T = \frac{\sum_{j=1}^{M} T_j}{M}$.

It should be noted that after each round of the consensus, T_j, for $j = 1, 2, \cdots, M$, and T will be updated, the details of which will be illustrated in Subsection IV-D.

B. *Data Reporting*

U_i performs the following procedures at the data reporting time point t_τ to report the current perception data m_i to the GW, where $i = 1, 2, \cdots, N$.

1) Compute the session key shared with the GW in a non-interactive way as $k_{i,g} = H(S_g^{s_i} || ID_i || ID_g || t_\tau) = H(g^{s_g s_i} || ID_i || ID_g || t_\tau)$.
2) Calculate the ciphertext as follows.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

a) According to the topology of the node network and the characteristics of neighbor nodes, some users are randomly selected as the cluster users of U_i by calculating secure pseudo-random-function (PRF) values. The PRF satisfies the following characteristics. If $U_s \in U$ chooses $U_t \in U$, U_t must choose U_s. Define h as the maximum number of users in the cluster, and $idx_i[j]$ represents the index of h cluster users selected by U_i, where $j = 1, 2, \cdots, h$. If $PRF(r_1) \leq \frac{e}{N-1}$, U_s chooses U_t as the cluster member, where $e = E(h)$, $E(\cdot)$ represents the mathematical expectation, and r_1 is the dynamic public information. The probability that U_s chooses U_t is $\frac{e}{N-1}$.

b) Calculate the auxiliary information $AUI_{i,j} = (i-j)/|i-j| \cdot PRF(r_2)$, where $j = 1, 2, \cdots, h$, r_2 is the dynamic public information, and $r_2 \neq r_1$. It is obvious that $AUI_{i,j} = -AUI_{j,i}$.

c) Calculate $C_i = m_i + k_{i,g} + \sum_{j=1}^{h} AUI_{i,idx_i[j]} + s_i$.

d) Calculate $MAC_k^{i,g} = HMAC(k, m) = HMAC(k_{i,g}, < C_i, t_\tau >)$.

e) Send $< C_i, MAC_k^{i,g} >$ to the GW.

C. Secure Data Aggregation

At the time point t_τ, the GW performs the following procedures to aggregate the user's data.

1) Compute the session key shared with U_i in a non-interactive way as $k_{g,i} = H(S_i^{s_g} || ID_i || ID_g || t_\tau) = H(g^{s_g s_i} || ID_i || ID_g || t_\tau)$, where $i = 1, 2, \cdots, N$.
2) Calculate $MAC_k^{g,i} = HMAC(k, m) = HMAC(k_{g,i}, < C_i, t_\tau >)$. If it equals to $MAC_k^{i,g}$, the communications are integrated.
3) Aggregate the ciphertexts of all users as $C_g = \sum_{i=1}^{N} C_i = \sum_{i=1}^{N} (m_i + k_{i,g} + (\sum_{j=1}^{h} AUI_{i,idx_i[j]}) + s_i) = \sum_{j=1}^{N} (m_i + k_{i,g} + s_i)$. Since $AUI_{i,j} = -AUI_{j,i}$, $\sum_{i=1}^{N} \sum_{j=1}^{h} AUI_{i,idx_i[j]} = 0$.
4) Calculate $C_g - \sum_{i=1}^{N} k_{g,i} + s_g = \sum_{i=1}^{N} (m_i + k_{i,g} + s_i) - \sum_{i=1}^{N} k_{g,i} + s_g = \sum_{i=1}^{N} m_i + s_g + \sum_{i=1}^{N} s_i = \sum_{i=1}^{N} m_i = sum_{t_\tau}$, where sum_{t_τ} is the aggregated data of U_i at t_τ, and $i = 1, 2, \cdots, N$.
5) Calculate $\sigma_{GW}^{(1)} = H(sum_{t_\tau})^{s_g}$, where $\sigma_{GW}^{(1)}$ is the signature of sum_{t_τ}.
6) Send $< sum_{t_\tau}, \sigma_{GW}^{(1)} >$ to CN_x, where CN_x is the primary node of the next round consensus. It is worth noting that the detailed means to determin CN_x will be introduced in Subsection IV-D.

D. Secure Data Storage

After the primary node CN_x receives sum_{t_τ} from the GW, CN_j utilizes the PBFT to store sum_{t_τ} in the blockchain, where $j = 1, 2, \cdots, M$. It is worth noting that the primary node CN_x is selected collectively by all CN according to their individual reputation values, which will be updated after each round of consensus. The whole process can be divided into three phase, *i.e.*, **Primary node selection**, **Block generation and verification**, and **Node reputation update**. The symbols used in this section along with their meaning are shown in TABLE I.

TABLE I: Key notations

Symbol	Definition
X	Random number
G_j	Public key of CN_j
Γ_j	Reputation of CN_j
α_j	Private key of CN_j
σ	Signature utilizing BLS
T_j	Initial reputation of CN_j
$H : \{0,1\}^* \rightarrow G$	Secure hash function

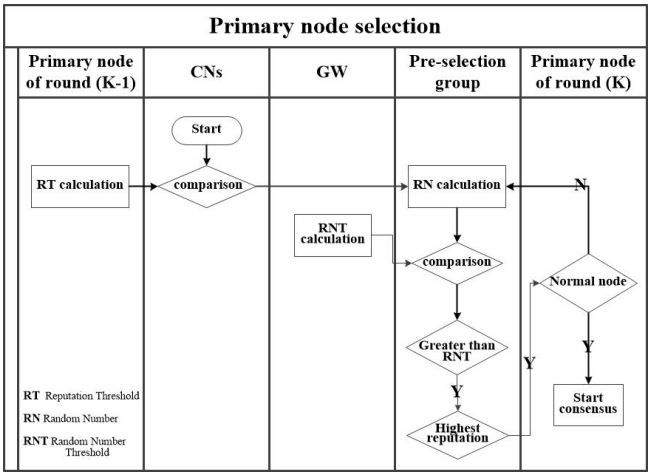


Fig. 5: Primary node selection

*1) **Primary Node Selection**:* The primary node is selected before each round of consensus. More specifically, first, the nodes that meet the reputation threshold are selected to form the pre-selected group. Then, to prevent the primary node from being known in advance by the attacker, the nodes that meet the random number threshold are selected from the pre-selected group. Finally, among the nodes that meet the above conditions, the node with the highest reputation value is selected as the primary node. The selection mechanism mainly includes three stages, *i.e.*, **Form the pre-selection group**, **Sort nodes in the group**, and **Determine the primary node**, as shown in Fig. 5.

1) **Form the Pre-selection Group**

a) If it is the first round of consensus, such nodes CN_j with $T_j \geq T$, are selected to form the pre-selection group, where T_j is the initial reputation of CN_j, for $j = 1, 2, \cdots, M$, and T is the reputation threshold.

b) If it is not the first round of consensus, such nodes CN_j with $\Gamma_j \geq T$, are selected to form the pre-selection group, where Γ_j is the reputation of CN_j, for $j = 1, 2, \cdots, M$.

c) After the above procedures, without loss of generality, suppose that the pre-selection group contains Q number of nodes, *i.e.*, CN_q, where $q = 1, 2, \cdots, Q$.

2) **Sort Nodes in the Group**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

a) Each node CN_q, for $q = 1, 2, \cdots, Q$, in the pre-selection group performs the following steps to generate the signature of the self-chosen random number.
   i) Select the random number X_q.
   ii) Sign X_q as $\sigma_q = H(X_q)^{\alpha_q}$, where α_q is the private key of CN_q.
   iii) Send $< X_q, \sigma_q >$ to the GW and the other nodes CN_p in the pre-selection group, where $p = 1, 2, \cdots, Q$, and $p \neq q$.

b) Other nodes CN_p and the GW calculate $e(\sigma_q, g)$ and $e(H(X_q), G_q)$, where G_q is the public key of CN_q. If $e(\sigma_q, g) = e(H(X_q), g)^{\alpha_q} = e(H(X_q), G_q)$, it indicates that σ_q is legal and valid.

c) The GW performs the following steps to generate the system threshold.
   i) Select the random number X_{GW} as the threshold Θ.
   ii) Sign X_{GW} as $\sigma_{GW}^{(2)} = H(X_{GW})^{s_g}$, where s_g is the private key of the GW.
   iii) Without loss of generality, the nodes CN_q with $X_q \geq \Theta$ form the group P.
   iv) Send $< \Theta, \sigma_{GW}^{(2)}, P >$ to each node CN_q in the pre-selection group, where $q = 1, 2, \cdots, Q$.

d) After CN_q receives $< \Theta, \sigma_{GW}^{(2)}, P >$ from the GW, CN_q calculates $e(\sigma_{GW}^{(2)}, g)$ and $e(H(X_{GW}), S_g)$ to verify $\sigma_{GW}^{(2)}$, where $q = 1, 2, \cdots, Q$, and S_g is the public key of the GW. If $e(\sigma_{GW}^{(2)}, g) = e(H(X_{GW}), g)^{s_g} = e(H(X_{GW}), S_g)$, $\sigma_{GW}^{(2)}$ is legal and valid.

3) **Determine the Primary Node**

a) Among the group P, the node with the highest reputation value of Γ (or T, for the first round consensus) is selected as the primary node CN_x.

b) CN_x is broadcasted to each consensus nodes.

*2) **Block Generation and Verification**:* According to the PBFT, CN_j completes block generation and data verification, where $j = 1, 2, \cdots, M$. The specific process is mainly divided into five stages, *i.e.*, **Request**, **Pre-prepare**, **Prepare**, **Commit**, and **Reply**.

1) **Request**
After the above procedures, the primary node CN_x calculates $e(\sigma_{GW}^{(1)}, g)$ and $e(H(sum_{t_\tau}), S_g)$ to verify $\sigma_{GW}^{(1)}$, where $\sigma_{GW}^{(1)}$ is the signature of sum_{t_τ}, sum_{t_τ} is the user's aggregate data, and S_g is the public key of the GW. If $e(\sigma_{GW}^{(1)}, g) = e(H(sum_{t_\tau}), g)^{s_g} = e(H(sum_{t_\tau}), S_g)$, $\sigma_{GW}^{(1)}$ is legal and valid.

2) **Pre-prepare**
The primary node CN_x constructs the block according to the information of the previous block, user's data sum_{t_τ}, *etc*. The block request information is $< blockquest, block, Bd, < sum_{t_\tau}, \sigma_{GW}^{(1)} >, \sigma_x >$, where $block$ is the block message including user's data sum_{t_τ}, the reputation value of CN_j, *etc*, $Bd = H(block)$, $\sigma_x = (Bd^{\alpha_x})^{c_x}$ is the signature of the $block$, α_x is the private key of CN_x, and c_x is the public random value of CN_x. Then, CN_x sends request information to other nodes CN_i, where $i = 1, 2, \cdots, M$, and $i \neq x$.

3) **Prepare**
After the other nodes CN_i receives the request information, CN_i performs the following procedures, where $i = 1, 2, \cdots, M$, and $i \neq x$.

a) Perform the following operations to verify $\sigma_{GW}^{(1)}$ and σ_x, where $\sigma_{GW}^{(1)}$ is the signature of sum_{t_τ}, and σ_x is the signature of the $block$.
   i) The correctness of $\sigma_{GW}^{(1)}$ verification is the same as that of CN_x verifies $\sigma_{GW}^{(1)}$.
   ii) Calculate $e(\sigma_x, g)$ and $e(Bd, G_x^{c_x})$ to verify σ_x. If $e(\sigma_x, g) = e(Bd, g)^{\alpha_x c_x} = e(Bd, G_x^{c_x})$, σ_x is legal and valid, where G_x is the public key of CN_x, and c_x is the public random value of CN_x.

b) Send the preparation information $< blockprepare, < Bd_i, \sigma_x >, \sigma_i >$ to each nodes, where $Bd_i = Bd$, $\sigma_i = (Bd_i^{\alpha_i})^{c_i}$ is the signature of CN_i, and c_i is the public random value of CN_i.

4) **Commit**
After CN_j receives the preparation information, CN_j performs the following procedures, where $j = 1, 2, \cdots, M$.

a) Calculate $e(\prod_{i=1}^{\mathcal{B}} \sigma_i, g)$ and $e(Bd, \prod_{i=1}^{\mathcal{B}} G_i^{c_i})$ to batch verify σ_i, where $\mathcal{B}$ is the number of block preparation information received by CN_j. If $e(\prod_{i=1}^{\mathcal{B}} \sigma_i, g) = e(Bd_i^{\sum_{i=1}^{\mathcal{B}} \alpha_i c_i}, g) = e(Bd_i, G_i^{\sum_{i=1}^{\mathcal{B}} c_i}) = e(Bd_i, \prod_{i=1}^{\mathcal{B}} G_i^{c_i})$, $\mathcal{B}$ number of σ_i are legal and valid, where G_i is the public key of CN_i, c_i is the public random value of CN_i, and $i = 1, 2, \cdots, M$.

b) If CN_j receives $2f + 1$ (including itself) legal preparation informations, it constructs a confirmation information $< blockcommit, \sigma_j >$, and broadcasts to other nodes, where $\sigma_j = (H(block)^{\alpha_j})^{c_j}$, α_j is the private key of CN_j, c_j is the public random value of CN_j, and $j = 1, 2, \cdots, M$.

5) **Reply**
If CN_j receives $2f + 1$ (including itself) legal confirmation information, the block is issued. Besides, CN_j responds to CN_x. It should be noted that the validation process is similar to that in Step **4)**.

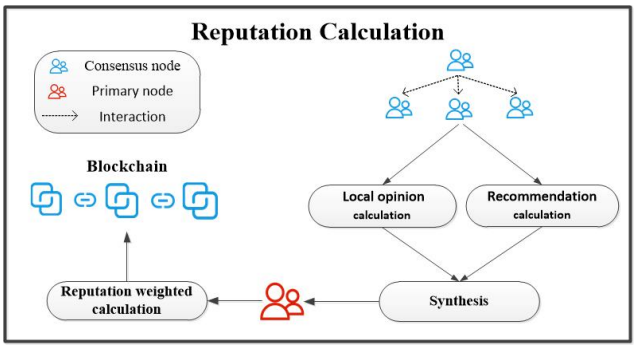


Fig. 6: The flow of node reputation calculation

TABLE II: Key notations

Symbol	Definition
$s_{i:j}$	Communication quality
$\{b_{i:j}, d_{i:j}, u_{i:j}\}$	Trust, distrust, and uncertainty of CN_i to CN_j
$\{b^r_{t:j}, d^r_{t:j}, u^r_{t:j}\}$	Recommended opinion of CN_t to CN_j
$\Gamma_j^{(\kappa)}$	Reputation value of CN_j in the (κ)-th round of consensus
α_{11}/α_{12}	Recent interaction with fast/slow response time in positive influence
α_{21}/α_{22}	Past interaction with fast/slow response time in positive influence
β_{11}/β_{21}	Recent/Past interaction with wrong signature sending in negative influence
β_{12}/β_{22}	Recent/Past interaction with untimely signature sending in negative influence

*3) **Node Reputation Update**:* Reputation is the cumulative evaluation of long-term behavior [31], and it has the characteristics of uncertainty, complexity, and dynamism.

Inspired by the subjective logic theory in [32], we propose our reputation model. Specifically, assume each node CN_j interacts with the other nodes CN_i in the pre-prepare, prepare, and commit phases of each round of PBFT consensus, where $i = 1, 2, \cdots, M$, $j = 1, 2, \cdots, M$, and $i \neq j$. From the interactive behavior, CN_i evaluates CN_j's reputation $T_{i:j}^{(\kappa)}$ in the (κ)-th round of consensus through the subjective logical reputation model. Then, the primary node CN_x synthesizes $T_{i:j}^{(\kappa)}$ and $\Gamma_i^{(\kappa-1)}$ to obtain the final reputation value of CN_j, where $\Gamma_i^{(\kappa-1)}$ is the reputation of CN_i in the $(\kappa-1)$-th round of consensus. The main process of reputation calculation and maintance can be divided into two stages, *i.e.*, **Subjective logical reputation calculation** and **Reputation weighted calculation**, as shown in Fig 6.

1) **Subjective Logical Reputation Calculation**
First, CN_i calculates local opinions based on the interaction with CN_j during the consensus process. Then, other nodes CN_t calculate CN_j's recommended opinions, where $t = 1, 2, \cdots, M$ and $t \neq i, j$. Finally, CN_i combines local opinions with recommended opinions to calculate the reputation evaluation of CN_j through logical operations. The main process can be divided into three stages, *i.e.*, **Local opinion calculation**, **Recommended opinion calculation**, and **Synthesis**. Table II shows the main symbols used.
   a) **Local Opinion Calculation**
   Considering the interactive behavior of CN_i and CN_j in the PBFT consensus process, we establish the multiple dimensions to depict the trust $b_{i:j}$, distrust $d_{i:j}$, and uncertainty $u_{i:j}$ of CN_j, respectively, where $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. Then, the local opinion of CN_i to CN_j is calculated according to the $b_{i:j}$, $d_{i:j}$, and $u_{i:j}$. The details of dimensions are as follows.
      i) **Influence of Interaction**
      For CN_j, reputation is performed through the accumulation of historical behaviors of interaction with CN_i, where $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. Note that the interaction between CN_j and CN_i mainly has two effects on the reputation value, *i.e.*, positive and negative. The quantification is expressed as ι and ς, satisfying $\iota + \varsigma = 1$, $\varsigma > \iota$, where ι is the positive influence, and ς is the negative influence.
      In order to make this factor more specific and consistent with the scenario of PBFT, we consider the following two sub-factors.
      A) **Positive Influence Type**
      Assume that CN_j sends $< blockprepare, Bd_j, \sigma_j >$ to CN_i, where $< blockprepare, Bd_j, \sigma_j >$ is the interactive information in the process of consensus. If σ_j is correct, it is a positive influence. For the positive influence, the faster response speed indicates better performance of nodes and more active participation in the consensus. Assume that the response of interaction is t, and the time limit for the active interaction is t_0. If $t \leq t_0$, it means that the response of the interaction is faster. Otherwise, the response is slower. The quantification is expressed as δ and ε, satisfying $\delta + \varepsilon = 1, \delta > \varepsilon$, where δ is the faster response of the interaction, and ε is the slower response of the interaction.
      B) **Negative Influence Type**
      In the PBFT consensus process, the negative influence is divided into two types, *i.e.*, sending the wrong signature and without sending the signature on time. Compared with sending the wrong signature σ_j, without sending σ_j on time has a lower impact on the evaluation of CN_j, where $j = 1, 2, \cdots, M$. The quantification is expressed as ϑ and μ, satisfying $\vartheta + \mu = 1, \vartheta > \mu$, where ϑ is depicted as sending wrong signature, and μ is depicted as without sening signature on time.
   ii) **Timeliness of Interaction**
   According to the dynamic nature of the trust, CN_j is not always credible, where $j = 1, 2, \cdots, M$. Therefore, the recent interaction has a greater impact on the evaluation of CN_j than the past interaction. Assume that the time scale of recent interactions and past interactions is defined by T_{recent}, *e.g.*, one day, and T_{now} is the current time. The quantification is expressed as ρ and χ, satisfying $\rho + \chi = 1, \rho > \chi$, where ρ is the recent interaction, and χ is the past interaction.

Therefore, according to the above dimensions, the trust $b_{i:j}$, distrust $d_{i:j}$, and uncertainty $u_{i:j}$ are depicted as $b_{i:j} = \frac{s_{i:j} \cdot \alpha_{i:j}}{\alpha_{i:j} + \beta_{i:j}}$, $d_{i:j} = \frac{s_{i:j} \cdot \beta_{i:j}}{\alpha_{i:j} + \beta_{i:j}}$, and $u_{i:j} = 1 - s_{i:j}$, where $\alpha_{i:j} = \iota[\rho(\delta\alpha_{11} + \varepsilon\alpha_{12}) + \chi(\delta\alpha_{21} + \varepsilon\alpha_{22})]$, $\beta_{i:j} = \varsigma[\rho(\vartheta\beta_{11} + \mu\beta_{12}) + \chi(\vartheta\beta_{21} + \mu\beta_{22})]$, $s_{i:j}$ is the quality of communication, which represents the probability that CN_i successfully receives the

interactive information of CN_j, and is affected by actual factors such as the network, $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. According to $b_{i:j}$, $d_{i:j}$, $u_{i:j}$, the local opinion of CN_i to CN_j is denoted as $T_{i:j}^{(\kappa)} = b_{i:j} + \Gamma_j^{(\kappa-1)} u_{i:j}$, where $\Gamma_j^{(\kappa-1)}$ represents the reputation value of CN_j in the $(\kappa-1)$-th round of consensus, $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. It should be noted that, as illustrated in Subsection III, a_j^i is the prior probability of the trust evaluation of CN_j, which represents the past experience, where $j = 1, 2, \cdots, M$.

b) **Recommended Opinion Calculation**
The recommended opinion is the synthesis of opinions on CN_j from CN_t, where $j = 1, 2, \cdots, M$, $t = 1, 2, \cdots, M$ and $t \neq i, j$. The specific process is as follows.

i) CN_t performs the following steps.

A) According to Subsection III, calculate $b_{t:j} = \frac{s_{i:j} \cdot \alpha_{t:j}}{\alpha_{t:j} + \beta_{t:j}}$, $d_{t:j} = \frac{s_{i:j} \cdot \beta_{t:j}}{\alpha_{t:j} + \beta_{t:j}}$, and $u_{t:j} = 1 - s_{t:j}$, respectively, where $j = 1, 2, \cdots, M$.

B) Calculate interaction frequency $IF_{t:j}$ as $IF_{t:j} = \frac{N_{t:j}}{\bar{N}_t}$ and the overall weight of reputation for local opinions $\tau_{t:j}$ as $\tau_{t:j} = \Gamma_t^{(\kappa-1)} \cdot IF_{t:j}$, where $j = 1, 2, \cdots, M$, $t = 1, 2, \cdots, M$, $t \neq i, j$, $N_{t:j} = \alpha_{t:j} + \beta_{t:j}$, $\bar{N}_t = \frac{1}{|S|} \sum_{s \in S} N_{t:s}$, $\Gamma_t^{(\kappa)}$ is the reputation value of CN_t in the (κ)-th round of consensus, S is the set of all nodes that interact with CN_t, and s is the node in S.

ii) CN_i calculates the recommended opinion as $b_{t:j}^r = \frac{\sum_t \tau_{t:j} b_{t:j}}{\sum_t \tau_{t:j}}$, $d_{t:j}^r = \frac{\sum_t \tau_{t:j} d_{t:j}}{\sum_t \tau_{t:j}}$, and $u_{t:j}^r = \frac{\sum_t \tau_{t:j} u_{t:j}}{\sum_t \tau_{t:j}}$, respectively, where $i = 1, 2, \cdots, M$ and $i \neq j$.

c) **Synthesis**
CN_i combines local opinion and recommended opinion through logical operations to calculate the trust, distrust, and uncertainty of of CN_j as $b_{i:j}^f = \frac{(b_{i:j} u_{t:j}^r + b_{t:j}^r u_{i:j})}{u_{i:j} + u_{t:j}^r - u_{i:j} u_{t:j}^r}$, $d_{i:j}^f = \frac{(d_{i:j} u_{t:j}^r + d_{t:j}^r u_{i:j})}{u_{i:j} + u_{t:j}^r - u_{i:j} u_{t:j}^r}$, and $u_{i:j}^f = \frac{(u_{t:j}^r u_{i:j})}{u_{i:j} + u_{t:j}^r - u_{i:j} u_{t:j}^r}$, respectively, where $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. The reputation value of CN_i to CN_j is defined as $T_{i:j}^{(f,\kappa)} = b_{i:j}^f + \Gamma_j^{(\kappa-1)} u_{i:j}^f$, where $\Gamma_j^{(\kappa-1)}$ represents the reputation value of the $(\kappa-1)$-th round of consensus on CN_j, $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$.

2) **Reputation Weighted Calculation**
After the above operations, the primary node CN_x calculates the final reputation value of CN_j, where $j = 1, 2, \cdots, M$. The specific steps are as follows.

a) CN_i sends $T_{i:j}^{(f,\kappa)}$ to CN_x, where $T_{i:j}^{(f,\kappa)}$ is the reputation value of CN_i to CN_j in the (κ)-th round of consensus, $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$.

b) CN_x obtains the $M \times 2$ matrix, as

$$\begin{bmatrix} T_{1:j}^{(f,\kappa)}, & \Gamma_1^{(\kappa-1)} \\ T_{2:j}^{(f,\kappa)}, & \Gamma_2^{(\kappa-1)} \\ & \vdots \\ T_{M:j}^{(f,\kappa)}, & \Gamma_M^{(\kappa-1)} \end{bmatrix}, \quad (1)$$

where $T_{i:j}^{(f,\kappa)}$ represents the reputation value of CN_j on CN_i in the (κ)-th round of consensus, $T_{j:j}^{(f,\kappa)} = 0$, $\Gamma_M^{(\kappa-1)}$ is the reputation value of CN_j in the $(\kappa-1)$-th round of consensus, and $j = 1, 2, \cdots, M$.

c) CN_x updates the reputation of CN_j based on the $T_{i:j}^{(f,\kappa)}$ and $\Gamma_i^{(\kappa-1)}$, where $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, $i \neq j$, as

$$T_j^{(final,\kappa)} = \frac{\Gamma_1^{(\kappa-1)} T_{1:j}^{(f,\kappa)} + \cdots + \Gamma_M^{(\kappa-1)} T_{M:j}^{(f,\kappa)}}{\sum_{j=1}^{M} \Gamma_j^{(\kappa-1)}} \quad (2)$$

d) CN_x records $T_j^{(final,\kappa)}$ in the blockchain.

V. Security analysis

In this section, we will illustrate that the proposed BBNP scheme achieves all the security requirements defined in Section II.

A. *Privacy Preservation*

An adversary $\mathcal{A}$ may exist in the smart grid to eavesdrop on the communications. Suppose that $\mathcal{A}$ could eavesdrop on the report $< C_i, MAC_k^i >$ from U_i to the GW at time t_τ. The ciphertext C_i is based on the modular-addition-encryption, as $C_i = m_i + k_{i,g} + \sum_{j=1}^{h} AUI_{i,idx_i[j]} + s_i$. We will analyze that the plaintext m_i cannot be recovered.

1) Firstly, $k_{i,g}$ is the shared session key between U_i and the GW, as $k_{i,g} = H(S_g^{s_i} || ID_i || ID_g || t_\tau) = H(g^{s_g s_i} || ID_i || ID_g || t_\tau)$. Due to the discrete logarithm problem (DLP) on the group G, $\mathcal{A}$ is unable to obtain s_i, s_g. Therefore, $\mathcal{A}$ cannot calculate $S_g^{s_i}$.
2) Secondly, $S_g^{s_i}$, the identity information ID_i and ID_g, and t_τ are integrated into the hash function. According to the collision resistance of the hash function, $\mathcal{A}$ is unable to obtain the shared session key $k_{i,g}$.
3) Finally, for auxiliary information $AUI_{i,j} = (i-j)/|i-j| \cdot PRF(r_2)$, U_i randomly selects some users as its cluster users according to the pseudo-random-function (PRF). Because of the unpredictability of PRF, $\mathcal{A}$ cannot predict the clustered users of U_i, and calculate the auxiliary information either.

In summary, even if $\mathcal{A}$ could eavesdrop on the C_i at t_τ, m_i cannot be recovered, which effectively protects the privacy of users.

B. *Data Integrity*

The user's data may be attacked by $\mathcal{A}$ in the communication link. We will show that the communications in the smart grid cannot be altered.

1) Firstly, U_i and the GW calculate MAC_k, where the MAC_k is the message authentication technique utilizing the hash function with the secret key k.
2) Secondly, the safety of MAC_k mainly depends on the security of k and the hash function. Due to the DLP, $\mathcal{A}$ cannot obtain $k = k_{g,i} = k_{i,g}$. Besides, if $\mathcal{A}$ launches the birthday attack on the embedded hash function with output digest length n, it needs $\sqrt{2^n}$ input messages to find a hash collision, which is computationally infeasible. Therefore, $\mathcal{A}$ cannot forge and tamper with MAC_k, and the communications between U_i and the GW cannot be maliciously polluted.
3) Finally, for the same reason, the communications between the GW and the primary node CN_x cannot be polluted either.

Besides, U_i and the GW incorporate t_τ when calculating MAC_k. Because only the MAC_k corresponding to the current reporting t_τ can pass the verification, the proposed scheme can resist message replay attack.

C. *Communication Confidentiality*

$\mathcal{A}$ may attack the communications in the smart grid to destroy the confidentiality. Firstly, we consider the communications between U_i and the GW. After U_i collects the m_i, U_i calculates the key with the GW through the secret sharing technique as $S_g^{s_i} = g^{s_g s_i}$.

1) Due to the Computational Diffie-Hellman Problem (CDH), $\mathcal{A}$ cannot calculate $g^{s_g s_i}$.
2) The shared session key is calculated as $k_{i,g} = H(g^{s_g s_i} ||ID_i||ID_g||t_\tau)$. Therefore, $\mathcal{A}$ cannot obtain $k_{i,g}$. Since $C_i = m_i + k_{i,g} + \cdots + s_i$, $\mathcal{A}$ cannot decrypt C_i without knowing $k_{i,g}$ either.

Similarly, the communications between the GW and CN_x can not be decrypted illegally either. In summary, the proposed scheme can ensure communication confidentiality.

D. *High Utility*

In the proposed scheme, we deeply integrate the blockchain into the smart grid. Through the PBFT, CN_j stores the user's data in the blockchain, which effectively solves the single point failure. Specifically, in the following, we will prove that PBFT can tolerate $\lfloor \frac{n-1}{3} \rfloor$ Byzantine nodes are featured with two basic types of system property, *i.e.*, safety and liveness [27], where n is the total number of nodes.

Theorem. *For the PBFT, an asynchronous system $\mathscr{S}$ can tolerate $\lfloor (\mathscr{R}-\mathbf{1})/\mathbf{3} \rfloor$ fault replicas to provide the safety and liveness properties.*

Proof. We denote the set of replicas by $\mathscr{R}$, identify each replica using an integer in $\{0, \cdots, \mathscr{R}-1\}$, the set $\mathscr{C}$ contains n processes $\{\mathscr{P}_1, \mathscr{P}_2, \cdots, \mathscr{P}_n\}$, and f is the maximum number of replicas that may be faulty.

1) **Liveness**: In order to ensure the liveness of the $\mathscr{S}$, the processes in the $\mathscr{S}$ can be executed as $\mathscr{P}_1 \vdash \mathscr{P}_2 \vdash \cdots \vdash \mathscr{P}_n$. Since f is the number of fault replicas, the $\mathscr{S}$ satisfying the condition of $Q \leq \mathscr{R} - f$ can operate stably, where Q is the threshold to ensure that $\mathscr{S}$ communicates successfully.
2) **Safety**: Without loss of generality, take $\mathscr{P}_1$ as an example, and the state of $\mathscr{P}_1$ in $\{0, 1\}$ is $\{\mathscr{P}_1^0, \mathscr{P}_1^1\}$. According to the quorum intersection property [27], if the replicas support $\mathscr{P}_1^0$ and $\mathscr{P}_1^1$ satisfying $2Q - \mathscr{R} > 0$, the state of $\mathscr{P}_1$ can be reached. Since there are f fault replicas in $\mathscr{S}$, it is obvious that $2Q - \mathscr{R} > f$.
The derivation process is as follows.

$$\left.\begin{array}{l} Q \leq \mathscr{R} - f \\ 2Q - \mathscr{R} > f \end{array}\right\} \Longrightarrow f + \mathscr{R} < 2Q$$
$$\Longrightarrow f + \mathscr{R} < 2(\mathscr{R} - f) \quad (3)$$
$$\Longrightarrow f < \mathscr{R} - 2f$$
$$\Longrightarrow 3f < \mathscr{R}$$
$$\Longrightarrow \mathscr{R}_{min} = 3f + 1$$

Besides, $\mathcal{A}$ may attack the nodes to reach the wrong consensus. In order to successfully tamper the data, $\mathcal{A}$ is required to control at least $\lfloor (n-1)/3 \rfloor$ nodes. If the probability of successful attack is $1/2$, the probability of successful tampering is $1/2^{\frac{n-1}{3}}$, which is almost negligible. In summary, the proposed scheme greatly improves utility of the smart grid.

Meanwhile, it should be noted that we apply the batch verification technique to improve the scalability of the PBFT consensus mechanism. In the consensus process, CN_j requires two pairing calculations to verify the signature of CN_i, where $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. Here, assume the calculation time of the pairing operation is T_p. Then, it needs $4T_p(M-1)M$ for CN_j to verify the signature, and the time required for batch checking is $4T_pM$. Therefore, it is helpful to improve the scalability of PBFT.

E. *Fairness*

In the PBFT, the primary node is mainly responsible for verifying aggregated data and generating new blocks. Therefore, a fair primary node selection mechanism is important. We calculate $T_j^{(final,\kappa)}$ through the reputation model based on subjective logic, where $T_j^{(final,\kappa)}$ is the reputation value of CN_j in the (κ)-th round of consensus, as follow.

1) The methods to update the reputation values is based on multiple dimensions and long-term comprehensive behavior evaluation of the nodes [31]. We innovate three evaluation factors, *i.e*, positive influence type, negative influence type, and timeliness to maintain the reputation value.
2) Through the reputation model, we calculate the triple $w_{i:j} = (b_{i:j}, d_{i:j}, u_{i:j})$, where $b_{i:j} = s_{i:j}\frac{\alpha_{i:j}}{\alpha_{i:j}+\beta_{i:j}}$, $d_{i:j} = s_{i:j}\frac{\beta_{i:j}}{\alpha_{i:j}+\beta_{i:j}}$, $u_{i:j} = 1 - s_{i:j}$ are the value of the trust, distrust, and uncertainty, respectively, $j = 1, 2, \cdots, M$, $i = 1, 2, \cdots, M$, and $i \neq j$. Then the reputation value of CN_i to CN_j is $T_{i:j}^{(f,\kappa)} = b_{i:j}^f + \Gamma_j^{(\kappa-1)} u_{i:j}^f$, where $\Gamma_j^{(\kappa-1)}$ represents the reputation value of CN_j in the $(\kappa-1)$-th round of consensus.
3) The final reputation value of CN_j is calculated as $T_j^{(final,\kappa)} = \frac{\Gamma_1^{(\kappa-1)} T_{1:j}^{(f,\kappa)} + \cdots + \Gamma_M^{(\kappa-1)} T_{M:j}^{(f,\kappa)}}{\sum_{j=1}^{M} \Gamma_j^{(\kappa-1)}}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

4) According to $T_j^{(final,\kappa)}$ and the threshold Θ, the primary node is selected.

Firstly, the consensus negotiation process is similar to the real society. Secondly, the reputation value is based on the observation of the individual's historical behavior to get the expectation of the future behavior [31]. Finally, through 50 simulation experiments, it reveals that ten nodes with the toppest reputation value among 100 nodes have been selected as the primary node for more than 35 times, and the node with the highest reputation value will not always be selected. Therefore, the fairness of our consensus mechanism is improved by introducing the reputation mechanism and random number technology.

VI. Performance Evaluation

In this section, firstly, the performance of the proposed scheme is compared with other four similar and state-of-the-art data aggregation schemes [14], [17], [33], [34]. The features of these schemes are compared in TABLE III. Subsequently, the simulation experiments are conducted to verify the fairness of the primary node selection mechanism.

TABLE III: Feature comparison

	Ours	[14]	[17]	[34]	[33]
D	Yes	Yes	Yes	Yes	Yes
P	Yes	Yes	No	Yes	Yes
C	Yes	Yes	Yes	Yes	Yes
H	Yes	Yes	Yes	No	No
F	Yes	No	No	-	-

D: Data integrity **P**: Privacy preservation **C**: Communication confidentiality **H**: High utility **F**: Fairness

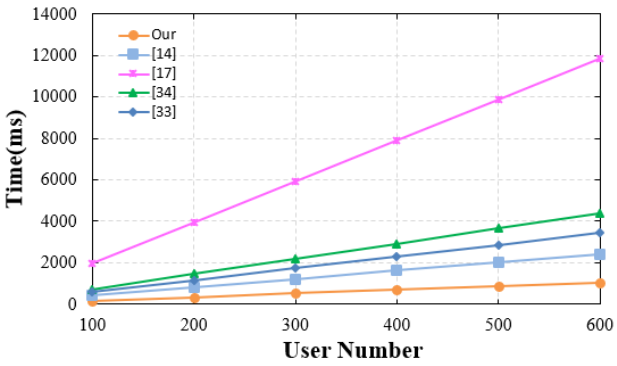
Note that, due to the introducing of blockchain and reputation mechanism, the proposed scheme is not exactly the same as the architecture of [14], [17], [33], [34]. Therefore, we mainly focus on the computational complexity and communication cost of data aggregation.

A. *Comparison of Computation Complexity*

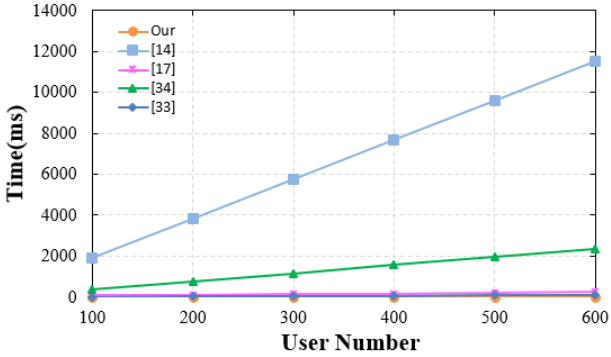
We perform the experiments with MIRACL [35] [36] and JPBC [37] running on a 3.0ghz processor Pentium IV system to study the computational complexity of data aggregation. To illustrate it clearly, we list the time cost of all the original operations in TABLE IV. Then, in TABLE V, the calculation time costs of the user and the aggregator of the four schemes are calculated and compared. Finally, we plot the comparisons of computation complexity in Fig. 7.

TABLE IV: The time cost of the original operations

Notations	Descriptions	Time Cost
C_a	Addition	$\approx 0.004ms$
C_e	Exponentiation	$\approx 1.7ms$
C_H	Hash	$\approx 0.0036ms$
C_{HM}	HMAC	$\approx 0.0075ms$



(a) Performance comparison of computation cost at user side



(b) Performance comparison of computation cost at aggregator side

Fig. 7: Comparisons of computation complexity

TABLE V: Comparisons of computation complexity

Scheme	User (MS)	Aggregator (MS)
Our	$3C_a + C_e + C_H + C_{HM}$	$2(n+1)C_a + nC_{HM}$
[14]	$4C_m + 2C_e + 2C_H$	$(n+1)C_p + nC_m + nC_a + nC_H$
[17]	$3C_H + 2C_a + 4C_m + C_{PK_E} + C_p$	$(5n+3)C_a + (2n+1)C_H + 2nC_m + 2C_p$
[34]	$4C_e + 3C_m + 2C_H$	$2(n+1)C_e + (3n+1)C_m + (n+2)C_H$
[33]	$4C_m + 3C_e + C_H$	nC_m

According to Fig. 7, it can be seen that the proposed scheme has higher computing efficiency both on user site and aggregator site.

B. *Comparison of Communication Cost*

The communications in the traditional smart grid mainly consist of users to the GW, and the GW to the CC. In order to solve the single point of failure, we introduce the blockchain, which is not mentioned in [33], [34]. Thus, we focus on the common parts of the comparison, *i.e.*, the communication overhead between users and the GW. The communication overhead in terms of the number of users of the above scheme is depicted in Fig. 8. It is obvious that the proposed scheme achieves much lower communication cost compared with [14], [17], [33], [34].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2021.3107301, IEEE Internet of Things Journal

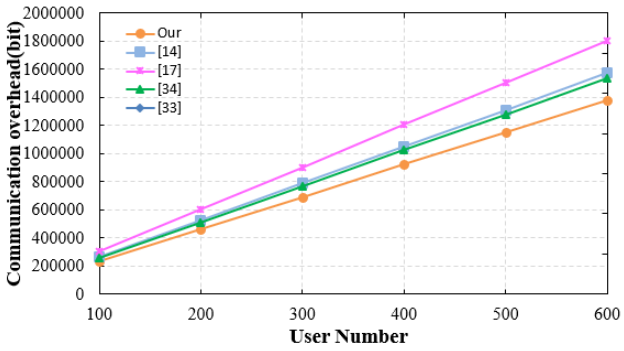


Fig. 8: Performance comparison of communication overhead

C. Node Reputation Analysis

In our consensus mechanism, we calculate the reputation of nodes utilizing the reputation model based on the subjective logic. TABLE VI and VII show the different settings of parameter weights in the model. Fig. 9 show the reputation values with different parameter weights. Here, we mainly analyze the weights of the positive/negative influence and the recent/past interaction. It should be noted that nodes are mainly divided into three types, *i.e.*, friendly node, intermediate node, and malicious node. Specifically, the friendly node always interacts successfully, the intermediate node is unable to interact successfully all the time, and the malicious node interacts unsuccessfully.

TABLE VI: Weight parameter 1

Parameter	1st E	2nd E	3rd E	4th E
P/N	0.4/0.6	0.3/0.7	0.2/0.8	0.1/0.9
F/S	0.6/0.4	0.6/0.4	0.6/0.4	0.6/0.4
W/U	0.6/0.4	0.6/0.4	0.6/0.4	0.6/0.4
R/P	0.7/0.3	0.7/0.3	0.7/0.3	0.7/0.3

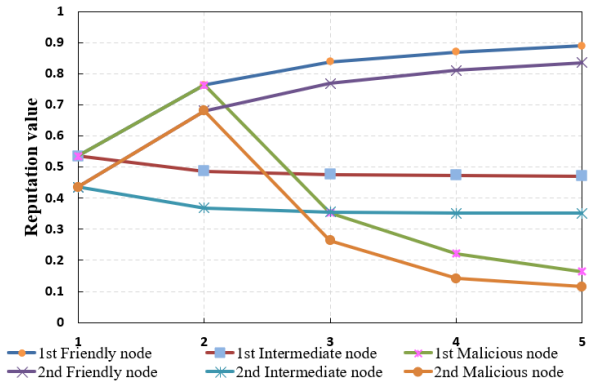
TABLE VII: Weight parameter 2

Parameter	5th E	6th E	7th E
P/N	0.4/0.6	0.4/0.6	0.4/0.6
F/S	0.6/0.4	0.6/0.4	0.6/0.4
W/U	0.6/0.4	0.6/0.4	0.6/0.4
R/P	0.6/0.4	0.8/0.2	0.9/0.1

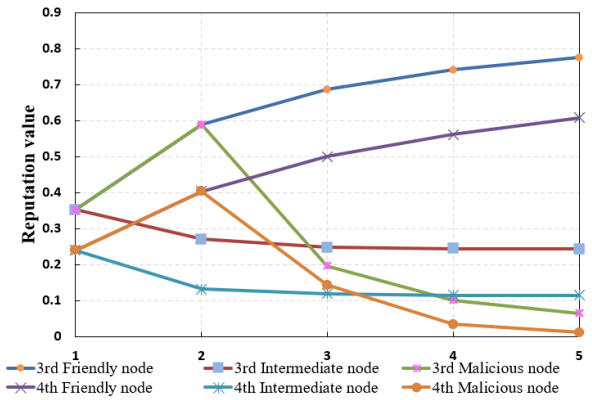
1st E: First experiment **2nd E:** Second experiment **3rd E:** Third experiment **4th E:** Fourth experiment **5th E:** Fifth experiment **6th E:** Sixth experiment **7th E:** Seventh experiment **P/N:** Positive/Negative influence **F/S:** Fast/Slow response for positive influence **W/U:** Wrong/Untimely signature sending in failed interaction **R/P:** Recent/Past interaction

Firstly, according to Figs. 9 (a) and (b), we can clearly draw the following conclusions.

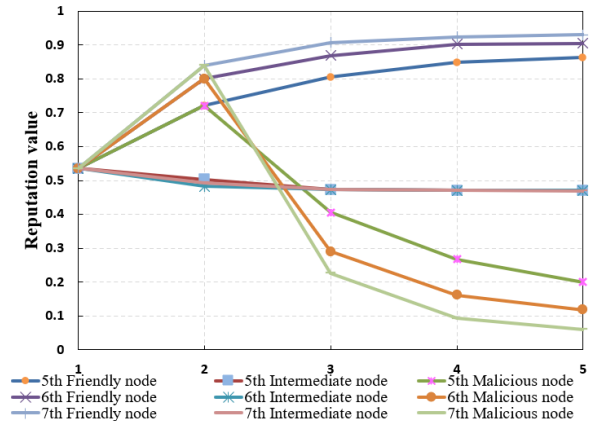
1) First of all, we take the 1st E as an example. The friendly node's reputation value increases from 0.53 to 0.89. The intermediate node's reputation value decreases from 0.53 to 0.47. The malicious node's reputation value decreases from 0.53 to 0.16. Therefore, our reputation model is realistic.
2) In addition, by comparing the influence of different weight values of the positive/negative influence on node reputation, it indicates that the selection of this factor is reasonable.
3) Finally, it can be observed that with the increase of the weight of negative influence, the node reputation value change more intensely. Simultaneously, to prevent the reputation value from changing too violently and maintain the stability of the whole reputation system, the



(a) The reputation of the first and second experiment nodes



(b) The reputation of the 3rd and 4th experiment nodes



(c) The reputation of the 5th, 6th and 7th experiment nodes

Fig. 9: Node reputation value experiment

reasonable parameter of the positive/negative influence is 0.4/0.6 through a large number of simulation experiments.

Subsequently, from Figs. 9 (a) and (c), it shows clearly that the differences in the weight of recent/past interaction affects the reputation values of nodes, especially for the malicious nodes. In the 5th, 6th, 7th E, the reputation values of the malicious nodes decrease from 0.53 to 0.20, 0.53 to 0.11, and 0.53 to 0.06, respectively. Meanwhile, in order to balance the influence of recent/past interaction weights on reputation value and ensure the stability and reliability of the reputation system, it is reasonable that the recommended parameters of recent/past interaction is 0.7/0.3 through a large number of simulation experiments.

D. *Primary Node Selection Analysis*

Without loss of generality, we assume that there are 100 consensus nodes in the system. We simulate three experiments, and each experiment contains 50 times of primary node selection, as shown in TABLE VIII and Fig. 10.

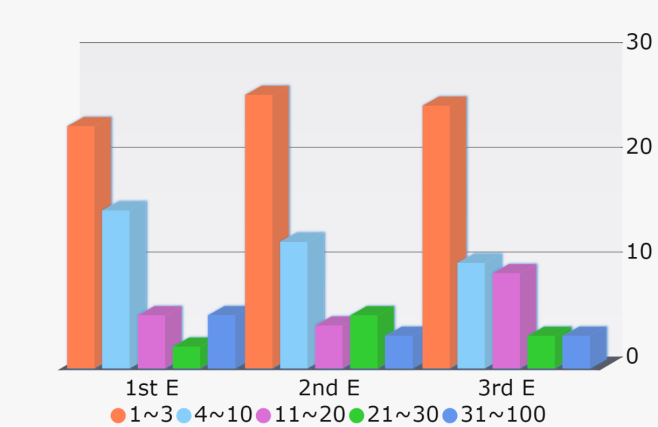


Fig. 10: The primary node selection

TABLE VIII: Primary node reputation ranking

Rr	1 ∼ 3	4 ∼ 10	11 ∼ 20	21 ∼ 30	31 ∼
1st E	23	15	5	2	5
2nd E	26	12	4	5	3
3rd E	25	10	9	3	3

Rr: Reputation ranking **1st E**: First experiment **2nd E**: Second experiment **3rd E**: Third experiment **31** ∼: The node reputation ranks after the 31st

From Fig. 10, the experiment results indicate that the node with higher credibility has a higher probability of being selected as the primary node. Meanwhile, the results also show that the node with high credibility cannot always be selected as the primary node, which ensures the fairness of the primary node selection mechanism.

VII. Conclusions

In this paper, we have proposed a novel BBNP scheme achieving privacy preservation, data integrity, communication confidentiality, high utility, and fairness simultaneously. Firstly, the user's data are efficiently encrypted and aggregated utilizing the modular-addition-encryption mechanism. Secondly, a new authentication technique is proposed, which integrates the MAC to achieve data integrity. Thirdly, we integrate the blockchain into the smart grid, which effectively solves the single point of failure. By introducing the subjective logical reputation model, the fairness of the primary node selection mechanism is ensured. Finally, through comparative performance analysis, it reveals that the proposed scheme outperforms the state-of-the-art similar schemes in terms of computation complexity and communication cost. The simulation experiments show that the property of fairness is fully guaranteed by the proposed primary node selection mechanism. In the future, we plan to design the reasonable incentive mechanism based on machine learning or game theory.

References

[1] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in internet of vehicles," *Future Generation Computer Systems*, vol. 92, pp. 644–655, 2019.

[2] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[3] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving and verifiable querying scheme in vehicular fog data dissemination," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1877–1887, 2018.

[4] Q. Kong, R. Lu, M. Ma, and H. Bao, "Achieve location privacy-preserving range query in vehicular sensing," *Sensors*, vol. 17, no. 8, p. 1829, 2017.

[5] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in lte-advanced networks," *IEEE internet of things journal*, vol. 4, no. 1, pp. 29–39, 2016.

[6] C. Guo, X. Jiang, K.-K. R. Choo, X. Tang, and J. Zhang, "Lightweight privacy preserving data aggregation with batch verification for smart grid," *Future Generation Computer Systems*, 2020.

[7] H. M. Khan, A. Khan, F. Jabeen, and A. U. Rahman, "Privacy preserving data aggregation with fault tolerance in fog-enabled smart grids," *Sustainable Cities and Society*, vol. 64, p. 102522.

[8] M. Badra and S. Zeadally, "Lightweight and efficient privacy-preserving data aggregation approach for the smart grid," *Ad Hoc Networks*, vol. 64, pp. 32–40, 2017.

[9] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3pda) scheme for smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1767–1774, 2018.

[10] J. Ni, K. Alharbi, X. Lin, and X. Shen, "Security-enhanced data aggregation against malicious gateways in smart grid," in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2015.

[11] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*, pp. 223–238, Springer, 1999.

[12] J. B. Hur, D. Y. Koo, and Y. J. Shin, "Privacy-preserving smart metering with authentication in a smart grid," *Applied Sciences*, vol. 5, no. 4, pp. 1503–1527, 2015.

[13] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 29–39, 2020.

[14] H. Fan, Y. Liu, and Z. Zeng, "Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain," *Sensors*, vol. 20, no. 18, p. 5282, 2020.

[15] M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," in *Cryptographers' track at the RSA conference*, pp. 191–208, Springer, 2005.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," tech. rep., Manubot, 2019.

[17] M. Fan and X. Zhang, "Consortium blockchain based data aggregation and regulation mechanism for smart grid," *IEEE Access*, vol. 7, pp. 35929–35940, 2019.

[18] S. Chen, L. Yang, C. Zhao, V. Varadarajan, and K. Wang, "Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid," *Engineering*, 2020.

[19] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[20] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[21] K. Aberer and Z. Despotovic, "Managing trust in a peer-2-peer information system," in *Proceedings of the tenth international conference on Information and knowledge management*, pp. 310–317, 2001.

[22] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in *2010 Eleventh International Conference on Mobile Data Management*, pp. 85–94, IEEE, 2010.

[23] Y. Wang and J. Vassileva, "Bayesian network-based trust model in peer-to-peer networks," in *Proceedings of the Workshop on Deception, Fraud and Trust in Agent Societies*, pp. 57–68, Citeseer, 2003.

[24] G. Choquet, "Theory of capacities," in *Annales de l'institut Fourier*, vol. 5, pp. 131–295, 1954.

[25] A. Josang, "Conditional reasoning with subjective logic," *Journal of Multiple-Valued Logic and Soft Computing*, vol. 15, no. 1, pp. 5–38, 2008.

[26] A. Jøsang and J. Golbeck, "Challenges for robust trust and reputation systems," in *Proceedings of the 5th International Workshop on Security and Trust Management (SMT 2009), Saint Malo, France*, vol. 5, Citeseer, 2009.

[27] M. Castro, B. Liskov, *et al.*, "Practical byzantine fault tolerance," in *OSDI*, vol. 99, pp. 173–186, 1999.

[28] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual international cryptology conference*, pp. 213–229, Springer, 2001.

[29] A. Joux, "A one round protocol for tripartite diffie–hellman," in *International algorithmic number theory symposium*, pp. 385–393, Springer, 2000.

[30] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[31] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in *Proceedings of the 33rd annual Hawaii international conference on system sciences*, pp. 9–pp, IEEE, 2000.

[32] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[33] S. Li, K. Xue, Q. Yang, and P. Hong, "Ppma: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462–471, 2017.

[34] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "Effect: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Science China Information Sciences*, vol. 62, no. 3, p. 32103, 2019.

[35] R. Li, C. Sturtivant, J. Yu, and X. Cheng, "A novel secure and efficient data aggregation scheme for iot," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1551–1560, 2018.

[36] M. Scott, "Miracl–multiprecision integer and rational arithmetic c/c++ library, 2007."

[37] B. Lynn *et al.*, "Pbc: The pairing-based cryptography library," *http://crypto. stanford. edu/pbc*, 2011.

HAIYONG BAO received the PhD degree in computer science from Shanghai Jiao Tong University, China, in 2006. Since February 2011, he has been an Associate Professor and a Full Professor with the School of Computer Science and Information Engineering, Zhejiang Gongshang University, and the Software Engineering Institute, East China Normal University, China. From June 2014 to May 2015, he worked as a Postdoctoral Research Fellow at Nanyang Technological University, Singapore. Dr. Bao's research interests include network and information security, applied cryptography, and big data security.

BINBIN REN received the B.S. degree in information and computing science from Ningbo University of Technology, China. He is currently pursuing his master degree in Zhejiang Gongshang University, China. His current research interests include computer network and information security.

Beibei Li received the B.E. degree in communication engineering from Beijing University of Posts and Telecommunications, China, in 2014, and the Ph.D. degree from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2019. He is currently an associate professor with the College of Cyber Science and Engineering, Sichuan University, China. His research interests include cyber-physical system security, intrusion detection, artificial intelligence, and applied cryptography.

Qinglei Kong received her PhD degree from the School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore, in 2018, and the M.Eng. degree in electronic and information engineering from Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China, in 2015. Now she is working in The Chinese University of Hong Kong, Shenzhen (CUHK-Shenzhen), as a postdoc researcher. Her research interests include applied cryptography, blockchain, VANET, and game theory.