A cross-chain trusted reputation scheme for a shared charging platform based on blockchain

Yunhua He, Cui Zhang, Bin Wu, Yigang Yang, Ke Xiao, Hong Li,

Abstract—With the development of electric vehicles, the shortage of charging piles has gradually been exposed. In response to this situation, charging pile (CP) operators have taken private charging piles into the shared charging system. Due to the lack of maintenance personnel for private charging piles that join shared charging, users often face the problems of damaged CPs and poor service attitudes of CP owners. Reputation solutions based on third-party platforms face a problem of single-point failures and reputation solutions based on blockchain face problems of storage and query efficiency. To improve storage and query efficiency, this paper proposes a multi-chain charging model that stores different types of information on different blockchains. However, it faces the problem of unreliable information called across chains, when calculating reputation across chains. Therefore, this paper proposes a cross-chain trusted smart contract (C_2T smart contract) to ensure the authenticity, real-time, and inter-chain write mutual exclusion of cross-chain information, making reputation calculation in the multi-chain charging model more convenient and more accurate. Specially, we propose a data mutual trust mechanism based on merkel proof to ensure the authenticity of cross-chain information and prevent forged information from participating in calculating reputation. Furthermore, we present a data structure composed of multiple counting bloom filters (MCBF) to verify the real-time of information and filter out non-real-time information, thereby ensuring the real-time of the calculated reputation. In addition, we put forward an algorithm to guarantee the inter-chain write mutual exclusion by hash mutexes, making the reputation calculation process more accurate and complete. The security analysis and experimental results demonstrate that C_2T smart contract is feasible in practice.

Index Terms—multi-chain, cross-chain, charging model, reputation, smart contract.

1 Introduction

With the rapid development of electric vehicles(EVs) [1], [2], [3], the problems of insufficient charging piles (CPs) and difficulty in finding CPs are being faced. Global EV Outlook reports [4], [5] made predictions on the scale of global CPs in 2030: by 2030, the global private CPs are expected to reach 245 million units respectively; the global public CPs are expected to reach 20 million units. The reports also pointed out: compared with public CPs, private piles are cheaper and more mature in technology. Therefore, the scale of private CPs in the United States, European countries, Japan, and other developed countries is much larger than that of public ones. The number of private CPs in China [6] has also increased from 8000 in 2015 to 703000 in 2019, with a compound annual growth rate of 206.17%.

Sharing private CPs is an innovative operation model that solves the dilemma of CP construction [7], [8], [9]. Incorporating private CPs into the shared charging system can effectively alleviate the difficulty in charging of EVs. However, due to the lack of maintenance personnel for private CPs, users often face the problems of damaged CPs and poor service attitudes of CP owners. The New Energy Vehicle Consumer Market Research Report in 2019 shows that current new energy vehicle users have the lowest satisfaction with the charging experience, with only 7.3 points, which indicates that the charging experience has become an urgent problem to be solved. To improve the charging experience of users, a reputation mechanism is proposed, in which the reputation of the CP is calculated based on user rating and high-reputation CPs are easier to be selected and get more charging rewards. At present, the private CP sharing platforms launched by various CP operators all adopt the third-party platforms, and the reputation calculation depends on user rating information collected by the third-party platforms. Although this method is efficient, it is vulnerable to problems of single-point failures and central deception.

Based on the characteristics of immutability and multi-party accounting, the emergence of blockchain [10], [11], [12] is expected to solve the problems of single-point failures and central deception [13], [14], [15], [16] in the charging model. Therefore, a reputation mechanism based on the blockchain is proposed, which record the reputation on the blockchain to prevent tampering. However, reputation calculation is also likely to be inaccurate, such as the ratings that are too high or too low of paid supporters. In order to obtain an accurate reputation, user authentication and charging records are needed to filter false ratings. In other words, user authentication, charging records, and rating information should all be recorded on the blockchain. But this will bring about the problems of low storage and query efficiency. To improve the efficiency of storing and searching the information, we propose a multi-chain charging model, in which identity information, charging information, and rating information are stored on different blockchains, because the storage and query efficiency of a

- *Yunhua He, Cui Zhang, Yigang Yang, Ke Xiao, were with School of Information Science and Technology, North China University of Technology, Beijing, China, 100144. E-mail: {heyunhua,xiaoke}@ncut.edu.cn; {zc19960917,yyg19988221}@163.com;*
- *Bin Wu, and Hong Li, were with Institute of Information Engineering Chinese Academy of Sciences.(Corresponding author: Bin Wu.) E-mail: {wubin,lihong}@iie.ac.cn*

Manuscript received March , 2021.

single information will be improved. Although multi-chain charging model addresses the issues of confusing storage and inefficient query, it also brings challenges to reputation calculation. The reputation calculation in the multi-chain charging model requires the use of cross-chain technology to call the information on multiple chains. At present, there are mainly three mainstream cross-chain technologies: notary schemes [17], [18], sidechains/relays [19], [20], [21], and hash-locking [22], [23]. However, most of the applications of these cross-chain technologies focus on asset transfer, rather than information call.

Inspired by cross-chain technology, we put forward a cross-chain trusted smart contract (C_2T smart contract) to address the issue in calling data on different blockchains to calculate reputation. Because each blockchain has its own internal security mechanism and does not participate in the consensus process of other blockchains [24], it is not easy to introduce the idea of cross-chain [25], [26], [27], [28] in calculating reputation. The introduction of cross-chain idea brings three important challenges as follows:

1) It is difficult to verify the authenticity of information. When calculating reputation of the multi-chain charging model, C_2T smart contract needs to call the information on different blockchains. Due to different consensus mechanisms adopted by different blockchains, the authenticity of the information cannot be mutually verified.
2) It is difficult to verify the real-time of information. Reputation is a real-time concept. To ensure the validity of reputation, real-time data need to be called from different blockchains. The authenticity of data is not the same as real-time: the authenticity of data can be verified by the information on the blockchain, while outdated real data cannot reflect its real-time performance.
3) The calculated reputation may be inconsistent with the information recorded in the blockchain. During the process of calculating reputation, information on blockchains is still being written, which will cause the calculated reputation to be inconsistent with the information on the blockchain, resulting in invalid reputation.

In this paper, to solve the challenges discussed above, we propose a C_2T smart contract, which is deployed on the evaluation information chain and can call the information of identity information chain and charging information chain for calculating reputation. In the process of calling information across chains, this smart contract uses a data mutual trust mechanism, a data structure, and hash mutexes to ensure information security. In summary, we make the following contributions:

1) To solve the problem of calculating reputation in the multi-chain charging model, we design a C_2T smart contract to implement information calls between different blockchains.
2) To verify the authenticity of information called between different blockchains, we propose a data mutual trust mechanism based on merkel proof. In the data mutual trust mechanism, one party can quickly prove the authenticity of specific data on other blockchains without obtaining the full data.
3) Considering the block size limitation issue [29], to achieve real-time validation of cross-chain information, we propose a new data structure called VerRealTime composed of multiple counting bloom filters (MCBF), which can ensure the real-time of cross-chain information and save space.
4) To ensure that the reputation is consistent with the information on blockchains, this paper utilizes hash mutexes to lock the information resources used in calculating reputation. After calculating reputation, C_2T smart contract unlocks the locked information to ensure a strong consistency of reputation.
5) We analyze the security of C_2T smart contract in theory. Besides, we conduct experiments on the consumption and effects of C_2T smart contract.

This paper is organized as follows. Section 2 introduces related work. In section 3, we give a description of the multi-chain charging model, threat model, and design goals. We describe the details of the operation process and scheme of C_2T smart contract in section 4, and carry out security analysis and experimental evaluation of the scheme in section 5. Finally, we conclude in section 6.

2 RELATED WORK

Recently, with the development of EVs, the demand for charging in the market is increasing. How to solve the trust issue in the charging model has been examined in many studies. Hua et al. [30] proposed a solution using blockchain technology to solve the problems about the fairness and justice of trade procedure, as well as the trust issue of battery information. Su et al. [31] optimized charge scheduling for a single EV aggregator based on a blockchain, which employs a reputation-based Byzantine fault tolerant (BFT) algorithm. In this case, EVs form nodes in the network and are assigned a reputation value that is tracked on the chain. This value is then used as a weight in a proof-of-stake based on consensus algorithm. Guo et al. [32] proposed a practical Byzantine fault-tolerant consensus mechanism based on reputation value to save consensus costs and improve efficiency. Wang et al. [33] proposed a proof of reputation to efficiently reach consensus in energy blockchain, where the reputation derivation is constructed based on the local trust computing and credibility computing. The trust solution mentioned above is only suitable for the trust issue in the single-chain charging model. For the multi-chain charging model, the above trust solutions are not completely suitable.

The multi-chain charging model brings challenges of calculating reputation. In the multi-chain charging model, in addition to paying attention to the trust issue in the charging process, it is also necessary to solve the problem of how to accurately call the information to calculate reputation. Most of the cross-chain studies focus on asset exchange. Li et al. [34] proposed a new cross-chain system based on multi-signature with better performance. This system is open to trading operators, who can be combined as several decentralized trading groups by locking tokens to ensure its credibility. Users can choose a reputable trading group and deposit assets to the trading group's multi-signature address

Cross-chain technology	Notary schemes	Sidechains/relays	Hash-locking
Trust model	Most notaries are honest	The chain will not fail or be 51%-Attack	The chain will not fail or be 51%-Attack
Interoperability	All	All with relay	Cross-dependence
Cross-chain asset exchange	Support	Support	Not support
Cross-chain asset transfer	Support	Support	Support
Multi-currency smart contract	Difficult	Difficult	Not support
Representative project	Ripple	BTC Relay/Poldadot/COSMOS	Lightning network

TABLE 1: Cross-chain technology comparison

on the existing blockchain. Herlihy et al. [35] proposed the notion of a cross-chain deal, a new way to structure complex distributed computations that manage assets in an adversarial setting. Van et al. [36] proposed the first cross-chain payment protocol that ensures termination in a bounded amount of time and works correctly in the presence of clock skew. In addition, some scholars have focused on cross-chain communication. Wang et al. [37] have investigated cross-chain communication, and introduced a blockchain router, which empowers blockchains to connect and communicate cross chains. However, the blockchain router can only act as a router, and the chains in this system cannot communicate messages between other chains directly, while in our work, the chain designed can communicate messages between each other directly. Lin et al. [38] designed a cross-chain protocol that enables two blockchains to communicate with each other and transmit transaction messages while dealing with each other.

The current mainstream cross-chain technologies and their representative projects are shown in Table 1. According to the above related work, the current cross-chain works mainly focus on asset exchange and cross-chain communication. Few studies have studied authenticity, real-time and inter-chain write mutual exclusion in the process of information exchange.

3 Model construction and design requirements

3.1 Multi-chain charging model

The number of EVs continues to increase with the country's strong support, and the infrastructure for shared charging has also been developed. At present, most of the blockchain-based shared charging models only contain one blockchain, which is used to store information during the charging process. However, due to the various information involved in the charging process and the differences between the confirmation and consensus of different types of information, we propose a multi-chain charging model to store the information involved in the charging process in this paper.

In our charging model, there are multiple entities: a shared charging service platform, CPs, EVs, and multiple chains, as shown in Fig. 1. The shared charging service platform is responsible for the interaction between CPs, EVs, and multiple chains. EVs can apply to the platform for charging. After charging is completed, the corresponding CPs can be evaluated and the ratings can be uploaded to the evaluation information chain C_3. CPs provide charging services for charging EVs. After charging is completed, the charging transaction is uploaded to charging information chain C_2. Multiple chains are used to store various types of information separately: identity information chain C_1 is responsible for storing the digital certificate and related operations such as creation and revocation of EVs and CPs; charging information chain C_2 is responsible for storing charging information; evaluation information chain C_3 is responsible for storing the service quality rating of the CPs. Since the bookkeepers and application scenarios of each blockchain are different, each chain can adopt a consensus mechanism that suits its own application scenarios. Readers can refer to related consensus algorithm papers [39], [40] for implementation. It should be noted that: although third-party platforms can also be used to create, store and revocate digital certificates, they can easily be the target of many attacks, such as, single point attack, malicious CA [41]. Therefore, this paper introduces C_1 to eliminate the limitation of the central CA and and ensure information security.

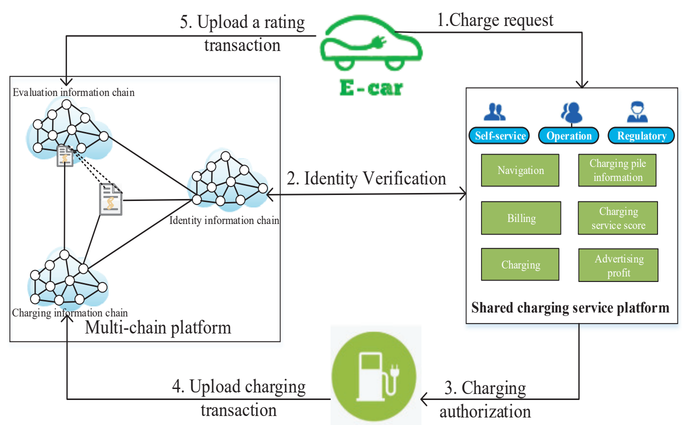


Fig. 1: Multi-chain charging model

In detail, before CPs and EVs enter the system, they first need to register on C_1. Then, when an EV needs to be charged, the EV applies to the shared charging service platform for charging. The service platform selects the optimal CP according to the reputation of CPs, and sends the information that needs to be authenticated to C_1. C_1 not only records the certificate information of CP and EV, but also records user registration, certificate issue, certificate query and certificate revocation. Although the probability of new user registration is relatively small, the operations of certificate query and certificate revocation need to be updated frequently [41]. After verification, the results are returned to the platform, and then the platform authorizes the charging of the selected CPs. After the charging is completed, the charging transaction is uploaded to C_2. Then the charging EV evaluates the charging service quality level, and uploads the rating information to C_3. There is a point worth noting here: in the process of calculating reputation, information on other blockchains needs to be called across chains. Therefore, we design a C_2T smart contract to ensure the authenticity, real-time, and inter-chain write mutual exclusion of the cross-chain information.

3.2 Threat model

In the process of calculating reputation of the CP, the information on different blockchains is involved. Generally, there are three forms of cross-chain attacks:

- **Authenticity attacks**
  In the process of invoking information by C_2T smart contract, an adversary will forge or tamper with the information, making the cross-chain information obtained by the smart contract untrue.
- **Real-time attacks**
  During the process of invoking information across chains, an adversary may send outdated information on the blockchains as the latest information to C_2T smart contract, causing the calculated reputation to expire.
- **Inter-chain write mutual exclusion attacks**
  After C_2T smart contract calls the required information, if an adversary changes the called information by writing, the final calculated reputation does not match with the information on the blockchains.

3.3 Design goals

- **Authenticity**
  Through the data mutual trust mechanism based on merkel proof, C_2T smart contract can quickly prove the authenticity of specific data on other blockchains without obtaining all the data on the blockchain.
- **Real-time**
  Blockchain can record the latest real-time information with a limited block space. In particular, when the information is called across chains, the real-time of the information can be verified by carrying a small amount of verification information.
- **Inter-chain write mutual exclusion**
  When C_2T smart contract calculates reputation, the called information needs to be locked. And after the calculation is completed, it is unlocked.

4 Cross-chain trusted smart contract

Based on the consensus mechanism and cryptography technology, the blockchain has established a set of internal security mechanisms. Cross-chain scheduling information will break through the internal security boundaries of the blockchain, since blockchains do not participate in the consensus process of other blockchains. In the shared charging model, information between the different blockchains is involved, so it is necessary to rebuild a security mechanism to ensure the security of cross-chain information. Therefore, we design a C_2T smart contract to ensure the authenticity, real-time, and inter-chain write mutual exclusion of cross-chain information.

4.1 The process of C_2T smart contract

In the process of calculating reputation, it involves the invocation of information on multiple chains. To ensure the authenticity and reliability of cross-chain information, a C_2T smart contract is designed. The specific process is shown in Fig. 2.

After the charging is completed, EVs score and sign CPs according to the service quality level of the CPs. The bookkeepers collect the ratings of the EVs on the CPs, and then send an upload request to evaluation information chain C_3 to stimulate C_2T smart contract. To prevent the identity of CPs and EVs from being faked, C_2T smart contract sends the IDs of CPs and EVs to identity information chain C_1 and requests their identity information. After C_1 receives request which is signed by shared charging service platform, it verifies the signed request and searches for the identity information certificates of the relevant CPs and EVs on the blockchain. The queried identity information certificates are sent to C_2T smart contract for verification. If the identities of the EV and the CP are real, C_2T smart contract will send the ID of the CP to charging information chain C_2. And C_2 will query and return the latest charging information to C_2T smart contract. After verifying the authenticity of the charging information, C_2T smart contract uploads the rating information to C_3, then calculates the reputation of the CP, and stores the calculated reputation on C_3 so that the optimal CP can be selected next time. These things should be noted that: both the identity information verification and charging information verification in C_2T smart contract need to call cross-chain information. Additional proof information p is sent to the C_2T smart contract with the cross-chain information, which can verify the authenticity and real-time of the cross-chain information. In addition, C_2T smart contract ensures the integrity of the process of calculating reputation. In this paper, we make sure the authenticity of the information through a data mutual trust mechanism based on merkel proof, and verify the real-time of information by a data structure $VerRealTime$ composed of MCBF. Besides, the inter-chain write mutual exclusion algorithm is used to achieve the goal of inter-chain write mutual exclusion by hash mutexes. The specific scheme content is described below.

4.2 Cross-chain authenticity scheme

Because the trusted environment of blockchain only takes effect within the blockchain platform and cannot be trusted by another blockchain platform, additional proof information p needs to be introduced to achieve trusted interaction across blockchain platforms. Therefore, We design a data mutual trust mechanism based on merkel proof to verify the authenticity of the cross-chain data. Fig. 3 shows the specific process of the data mutual trust mechanism in C_2T smart contract.

In this data mutual trust mechanism, when C_2T smart contract is running, for the convenience of sending and receiving information, a proof module M_v used to prove the authenticity of data is set on C_v ($v \in \{1, 2, 3\}$). And there is no need to pay attention to its specific implementation details. When C_2T smart contract on C_3 sends a call request $CallReq\ q = \{C_j, Q\}$ ($j \in \{1, 2\},\ Q = (ID, c)$) to C_1 or

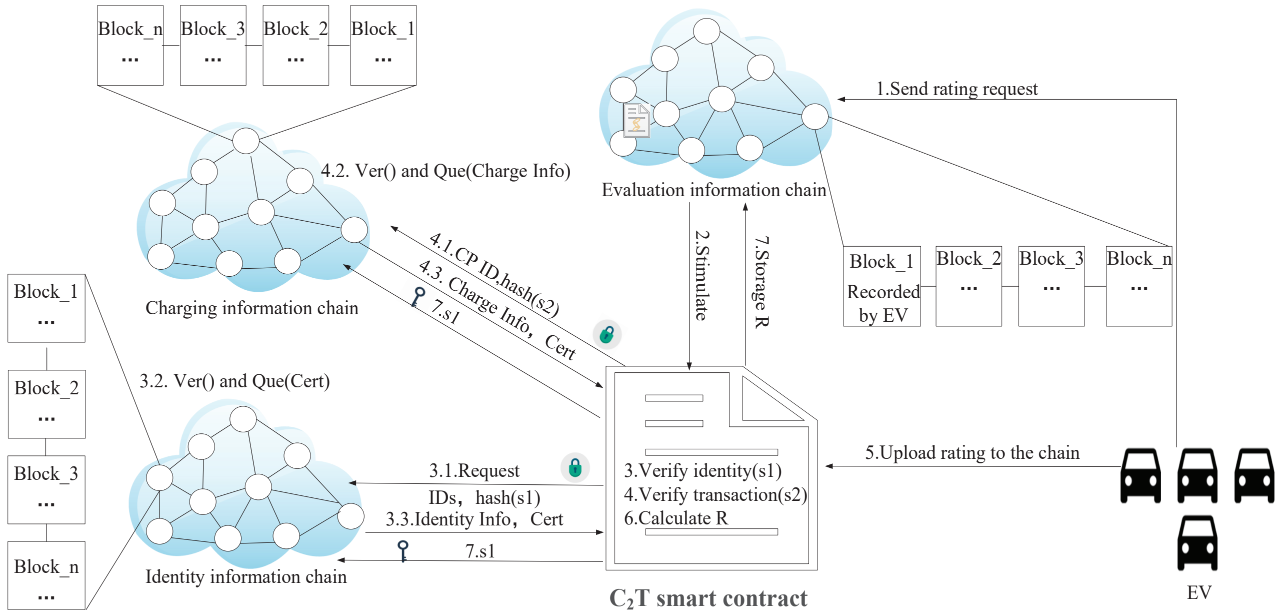


Fig. 2: The process of C_2T smart contract

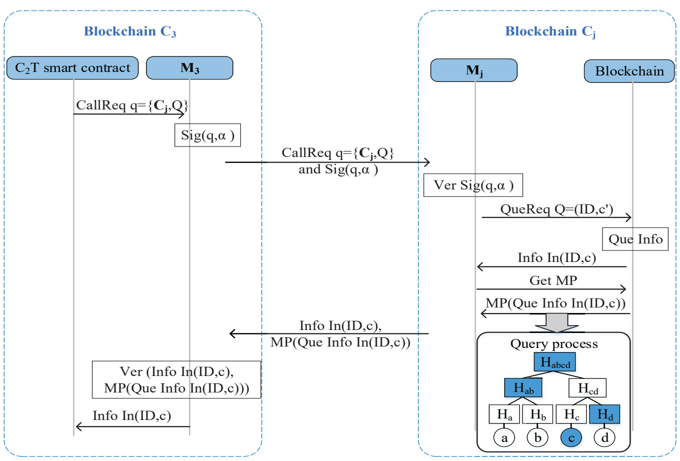


Fig. 3: The process of the data mutual trust mechanism

C_2, M_3 on C_3 is used to provide an authorized signature operation $Sig(q, \alpha)$ for q. $Q = (ID, c')$ represents a query request, and α represents the authorization identifier. Then q and $Sig(q, \alpha)$ are sent to C_j, and M_j on C_j will verify the authorization. After the authentication is passed, the query request $QueReq\ Q = (ID, c')$ in q is sent to the blockchain for information query. The queried information $Info\ In(ID, c)$ and the merkel proof of c query process $MP(Que\ Info\ In(ID, c))$ are returned to C_2T smart contract on C_3. ID represents the ID of the EV or CP; c' represents the content of the query request; and c is the specific content queried by c'. $MP(Que\ Info\ In(ID, c))$ is used as additional proof information p to ensure the authenticity of cross-chain data. Take the query process of c in Fig. 3 as an example, if you want to verify the authenticity of c, $MP(QueInfoIn(ID, c))$ only needs to include the verification path of c, which is H_d, H_{ab}, and H_{abcd}. The specific process is as follows: (1) calculate the hash according to c, and get $(H_c)'$; (2) calculate the hash according to $(H_c)'$ and H_d, and get $(H_{cd})'$; (3) calculate the hash according to $(H_{cd})'$ and H_{ab}, and get $(H_{abcd})'$; (4)compare whether $(H_{abcd})'$ and H_{abcd} are the same. If they are the same, the transmitted information c is correct. Otherwise, the information c has been tampered with. The above verification process is called merkel proof, which is additional proof information introduced in C_2T smart contract to verify the authenticity of the information.

4.3 Cross-chain real-time scheme

One real-time method is to use the latest block to store the real-time information list, but the storage space of this information list will increase linearly with the increase of real-time information. Since the space of block is limited, bloom filter can be used to save space.

Bloom filter [42] is a binary-based data structure with good space efficiency and time efficiency. It is often used to judge the attribution of an element to a set. A bloom filter uses an m-bit array to represent a set $S = \{x_1, ..., x_s\}$ of s elements. Initially, all the bits in the filter are set to zero, and then we select k hash functions,$h_i(x)$, $(1 \leq i \leq k)$ used to map items $x \in S$ to random number uniform in range $1, ..., m$. An element $x \in S$ is inserted into the filter by setting the bits $h_i(x)$ to one for $1 \leq i \leq k$. When judging whether the element $y \in S$, we need to check each bit $h_i(y)$. If any one of them is zero, it means that the element y is not in this set. Besides, the standard bloom filter cannot delete elements. This function can be achieved by counting bloom filter (CBF). In CBF, every bit is replaced by a counter. When the element's hash is mapped to the counter, it increases by one. On the contrary, when deleting elements in the set, the counter is decreased by one.

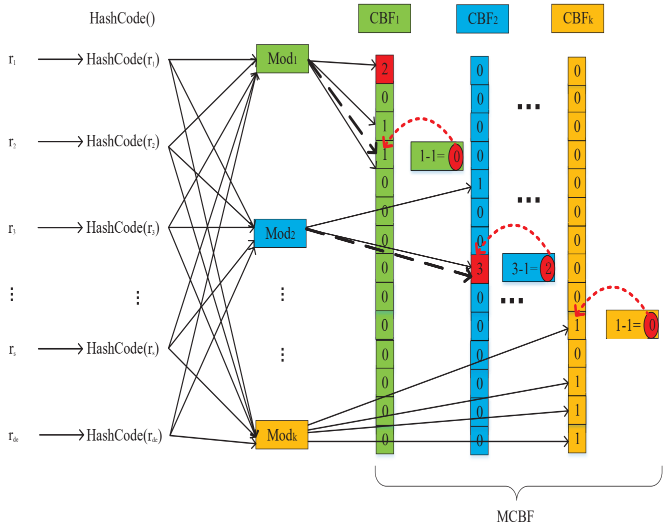


Fig. 4: Real-time initialization principle

In general, BF cannot delete elements, and CBF improves the shortcoming. However, whether it is BF or CBF, multiple hash functions need to convert the string to generate multiple values, and the numerical conversion of the hash function will bring a lot of running time. Therefore, in order to reduce the running time caused by multiple hash function value conversions, this paper designed a data structure $VerRealTime$ to solve this problem. In this solution, the string only needs to be converted once, and then multiple mod functions are used to take the remainder of the value, reducing the running time caused by multiple Hash function value conversions. Specifically, $VerRealTime$ uses multiple CBFs (MCBF) to represent the single-attribute domain of a multidimensional set. MCBF jointly complete the representation of the element and judge whether an element belongs to the set. In other words, all CBFs represent the real-time of the information together. And when real-time verification is performed, all CBFs in $VerRealTime$ determine whether the information is a real-time information together. The principle of real-time verification of cross-chain information is shown in Fig. 4.

1)**Real-time initialization of information**

When the genesis block is generated, a real-time data set R composed of the latest information r at that time is stored in the MCBF of the block header. The specific initialization process is shown in Algorithm 1.

Above all, a data structure $VerRealTime$ containing k CBFs where all elements are zero is initialized, and the content to be stored in k CBFs corresponds to the mapping results of k Mod functions respectively. When a real-time information r on the blockchain is stored in MCBF, it will go through the following process: first, r is hashed to obtain the corresponding hash value hc by $HashCode$ function. Then, hc is taken remainder by Mod function with k large prime numbers. The remainder m_i obtained by Mod_i is mapped to the relative position corresponding to CBF_i, and the value of this position is increased by one. When all the elements in R are added to the MCBF according to the above process, the MCBF that can be used to verify real-time information is finally generated.

Algorithm 1 Real-time initialization of information

Input: $R = \{r_f \mid 1 \leq f \leq s\}$
Output: MCBF
Initialize a data structure $VerRealTime$
for $f = 1; f \leq s; f++$ **do**
  $hc = HashCode(r_f)$
  //Add a real-time information
  for $i = 1; i \leq k; i++$ **do**
    $m_i = Mod_i(hc)$
    $CBF_i[m_i] += 1$
  end for
end for
return MCBF

Algorithm 2 Real-time query of information

Input: f
Output: Real-time or Non-real-time
$hc = HashCode(f)$
for $i = 1; i \leq k; i++$ **do**
  $m_i = Mod_i(hc)$
  if $CBF_i[m_i] == 0$ **then**
    return Non-real-time
  end if
end for
return Real-time

2)**Real-time query of information**

When C_2T smart contract calls information across chains, MCBF as additional proof of the real-time of information will return to the C_2T smart contract with cross-chain information. And C_2T smart contract verifies the real-time of the information according to the returned results. The specific process of verification is shown in Algorithm 2:

After calculating the hash value of returned information by $HashCode$ function, k Mod functions are used to perform the remainder operation on the hash value, and the result m_i of $Modi(hash)$ $(1 \leq i \leq k)$ corresponds to the i^{th} CBF respectively. We check whether the relative position m_i in CBF_i corresponding to the Mod_i is zero, if none of them are zero, the information f is real-time information, $f \in R$; otherwise, it is non-real-time information $f \in N$, N is a set

Algorithm 3 Real-time update of information

Input: r_{de}, r_{ad}, previous MCBF
Output: MCBF
Phase 1: Delete non-real-time element
$hc = HashCode(r_{de})$
$m_i = Mod_i(hc)$
for $i = 1; i \leq k; i++$ **do**
  $CBF_i[m_i] -= 1$
end for
Phase 2: Add real-time element
$hc = HashCode(r_{ad})$
$m_i = Mod_i(hc)$
for $i = 1; i \leq k; i++$ **do**
  $CBF_i[m_i] += 1$
end for
return MCBF

of elements that failed in real-time verification.

3)**Real-time update of information**

The generation of a new block means that some information in the previous MCBF is out of date. Therefore, when a new block is generated, the MCBF of the previous block is left and real-time information will be replaced on the basis of this MCBF. The specific process of update is shown in Algorithm 3:

In the process of real-time update of information, firstly, real-time information r_{ad} and outdated information r_{de} are determined according to the block information. Next, r_{de} is hashed to obtain the corresponding hash value hc by the $HashCode$ function. Then, hc is taken remainder by Mod function with k large prime numbers and the remainder m_i obtained by Mod_i is mapped to the relative position corresponding to CBF_i, and the value of this position is decreased by one. After deleting the non-real-time information, the real-time information is added to the MCBF according to the method of adding real-time information in algorithm 1, forming a new MCBF. The new MCBF is placed in the block header of the new block.

4.4 Inter-chain write mutual exclusion scheme

Algorithm 4 Inter-chain write mutual exclusion

for $j = 1; j \leq 2; j++$ **do**
  $s_j = sand()$
  $store\ s_j$
  $h_j = hash(s_j)$
end for
// Phase 1: Lock identity information resources
$q^{id} = (C_1, Q), Sig(q^{id}, \alpha)\ and\ h_1 \to C_1$
$Ver\ Sig(q^{id}, \alpha)$
if $Ver\ Sig(q^{id}, \alpha) == 1 \bigcup h_1\ exists$ **then**
  $Query\ \omega_{id} \in \Omega_{ID}$
  $lock\ \omega_{id}$
  $\omega_{id} \to C_2T\ smart\ contract$
end if
// Phase 2: Lock charging information resources
$q^{ch} = (C_2, Q), Sig(q^{ch}, \alpha)\ and\ h_2 \to C_2$
$Ver\ Sig(q^{ch}, \alpha)$
if $Ver\ Sig(q^{ch}, \alpha) == 1 \bigcup h_2\ exists$ **then**
  $Query\ \omega_{ch} \in \Omega_{CH}$
  $lock\ \omega_{ch}$
  $\omega_{ch} \to C_2T\ smart\ contract$
end if
// Phase 3: Calculate reputation
// Phase 4: Unlock all information resources
$s_1 \to C_1$
if $h_1 == hash(s_1)$ **then**
  $Unlock\ \omega_{id}$
end if
$s_2 \to C_2$
if $h_2 == hash(s_2)$ **then**
  $Unlock\ \omega_{ch}$
end if

In the process of calculating reputation, if the relevant information of the CP or EV for reputation calculation is updated, the calculated reputation is non-real-time. It does not match the information of the CP and the EV, causing the calculation invalid. Therefore, we use hash mutexes to lock the blockchain information resource for calculating reputation to achieve inter-chain write mutual exclusion. Compared with traditional mutexes, hash mutexes use random numbers s_j and $hash(s_j)$ to unlock and lock reputation computing resources $\omega_\gamma \in \Omega$. Ω is all blockchain resource. The specific unlocking and locking resource process is shown in Algorithm 4.

In the process of verifying the identity and the transaction, C_2T smart contract generates random numbers s_1 and s_2. s_1 and s_2 are stored and hashed, $h_1 = hash(s_1)$, $h_2 = hash(s_2)$. Then, the hash values h_j are sent to C_j respectively. The called identity resource $\omega_{id} \in \Omega_{ID}$ and the called charging resource $\omega_{ch} \in \Omega_{CH}$ are locked after receiving h_1 and h_2 respectively, and are unlocked when receiving s_1 and s_2. Ω_{ID} is all resources of C_1 and Ω_{CH} is all resources of C_2. After ω_γ is locked, it is sent to C_2T smart contract for verification. After calculating reputation, s_j is sent to C_j to unlock ω_γ. This process ensures the inter-chain write mutual exclusion.

5 SECURITY ANALYSIS AND EXPERIMENTAL EVALUATION

In this section, we first conduct a security analysis of C_2T smart contract proposed in this paper, including the security analysis of the authenticity attacks, real-time attacks, and inter-chain write mutual exclusion attacks that exist in the cross-chain process of the multi-chain charging model. Then, the effect of the solution proposed in this paper on resisting these attacks was verified through experiments.

5.1 Security analysis

In order to solve the cross-chain security problems of information, this paper proposes a scheme of C2T smart contract to realize the cross-chain interaction of information. This scheme is composed of three basic methods: Merke proof algorithm to achieve authenticity scheme, $VerRealTime$ data structure to achieve real-time scheme, and hash mutexes to achieve inter-chain write mutual exclusion scheme. In this section, we list some proofs to demonstrate that the authenticity scheme can resist the authenticity attack, the real-time scheme can resist the real-time attack, and the inter-chain write mutual exclusion scheme can resist the inter-chain write mutual exclusion attack. In summary, C_2T smart contract can resist authenticity attacks, real-time attacks and inter-chain write mutual exclusion attacks in the threat model, and achieve security goals.

Authenticity attacks. C_2T smart contract uses the merkel proof algorithm as its basic algorithm to ensure the authenticity of the information, when it calls information on other blockchains. The data mutual trust mechanism based on merkel proof enables C_2T smart contract to quickly prove the authenticity of the called information without obtaining the full amount of data of the block, when it calls the information of C_1 and C_2 across chains. When data are verified in authenticity, if an attacker forges or tampered with information $In(ID, c)_A$ and turns it into $In(ID, c)_B$ in the process of cross-chain transmission, then $MP(Que\ \ Info\ \ In(ID,c)_A) \neq MP(Que\ \ Info\ \ In(ID,c)_B)$. Thus, the operation $Ver\ (Info\ In(ID,c)_B,\ \ MP(Que\ \ Info\ \ In(ID,c)_A))$ will fail when verifying the authenticity of the information $In(ID,c)_A$.

Real-time attacks. $VerRealTime$ composed of MCBF can query the real-time of information. When data are verified in real-time, if an attacker passes the outdated information n as real-time information r to C_2T smart contract in the process of calling information, then $HashCode(n) \neq HashCode(r)$, $Mod_i(HashCode(n) \neq Mod_i(HashCode(r))$ $(1 \leq i \leq k)$. The data structure cannot find the real-time performance of n, which indicates that n is non-real-time information.

Inter-chain write mutual exclusion attacks. During the cross-chain process, C_2T smart contract uses hash mutexes to lock and unlock ω_γ to ensure the integrity of the multi-chain shared data operation. When calling ω_γ on C_j for calculating reputation, C_2T smart contract sends h_j to the C_j to lock ω_γ. If an attacker wants to modify ω_γ, the resource has already been locked and cannot be accessed.

5.2 Experimental evaluation

In the previous part, we have theoretically analyzed the security of C_2T smart contract for attacks in the threat model. In this part, we get the gas consumption of C_2T smart contract and the effects of C_2T smart contract against various attacks in the threat model in this charging scenario. In addition, we also compare and analyze the difference between the MCBF used in the authenticity scheme and other filters. At the same time, the influence of the number of different functions on false positive (FP) rate is also tested in the cross-chain authenticity scheme. The final results of authenticity attacks, real-time attacks, and inter-chain write mutual exclusion attacks must be reflected in rating and reputation. Therefore, to make the experiments simple and the effects obvious, we directly use MATLAB to simulate the change of reputation when encountering various attacks.

Regarding reputation calculation of C_2T smart contract, this paper adopts the calculation method in literature [43], and the specific calculation is shown in formula (1)

$$\begin{cases} E_n = R_{cp,n-1}/D \\ \Phi(R_{cp,n-1}) = 1 - \frac{1}{1+e^{\frac{-(R_{cp,n-1}-D)}{\sigma}}} \\ R_{cp,n} = R_{cp,n-1} + \frac{1}{\mu}\Phi(R_{cp,n-1})R_v(W_n - E_n) \end{cases} \tag{1}$$

In (1), $R_{cp,n-1}$ represents the $n-1^{th}$ transaction service rating of the CP. $\mu > 1$ is the adjustment coefficient that can determine the speed of change of service rating after transaction rating. Its value can be adjusted so that the rating of CPs with low ratings will not always be affected by past bad ratings after the service capacity is improved. $W_n \in \{1,2,3\}$ is the score provided by users with reputation R_v; E_n is the score expected by the CP; D is the highest level in the service rating.(Set $D = 3$ in this paper); $\Phi(R_{cp,n-1})$ is the damping function because of which the charging service rating value changes gently; and σ is the acceleration factor in the damping function.

5.2.1 Overheads of C_2T smart contract

C_2T smart contract involves the call of information between multiple chains. We build three blockchains locally: an identity information chain, a charging information chain, and an evaluation information chain, and program smart contract through the solidity programming language. In C_2T smart contract, the whole reputation calculation process of CP includes cross-chain information verification and reputation calculation. The focus of cross-chain information verification is mainly on verifying the authenticity and real-time of information and the immutability of occupied resources. Therefore, for the sake of simplicity, we directly save the information needed by reputation calculation of the CP to the local, and call it by C_2T smart contract. We deploy C_2T smart contract to the Remix IDE to measure its gas consumption. The main gas consumption of C_2T smart contract is shown in Fig. 5 and Fig. 6. Fig. 5 shows the main gas consumption in the cross-chain verification process. But when verifying the authenticity of the information, the amount of block information and the location in the merkel tree have a significant impact on gas consumption. Therefore, we verify the authenticity of the information in different locations on different merkel trees, and record the gas consumption. The result is shown in Fig. 6. Because the information verification and the process of reputation calculation involve a large number of interactions which consume a lot of gas, they occupy the main consumption of smart contract.

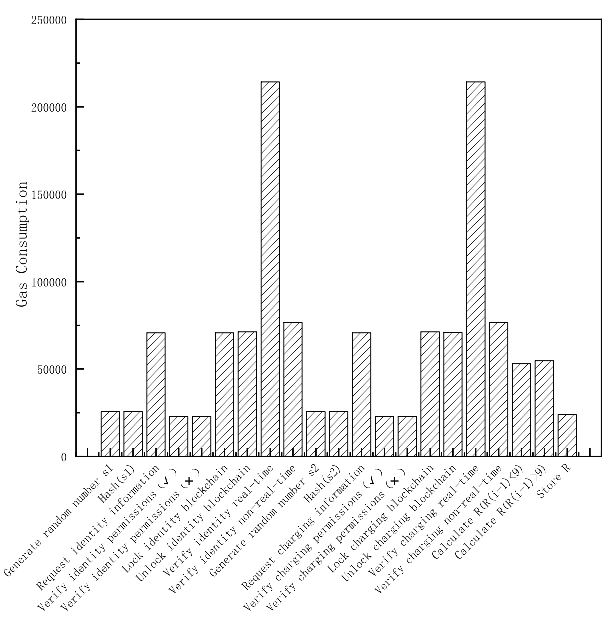


Fig. 5: The Main Gas Consumption of C_2T Smart Contract

5.2.2 Cross-chain authenticity scheme evaluation

In the absence of authenticity verification, an attacker may launch two authenticity attacks: the first one is that a CP operator or private pile owner employs paid supporters to scour their own CPs to improve their own CP's reputation value; the second one is that when a CP operator competes with other operators, it employs paid supporters to score maliciously on CPs to combat other operators. In this part,

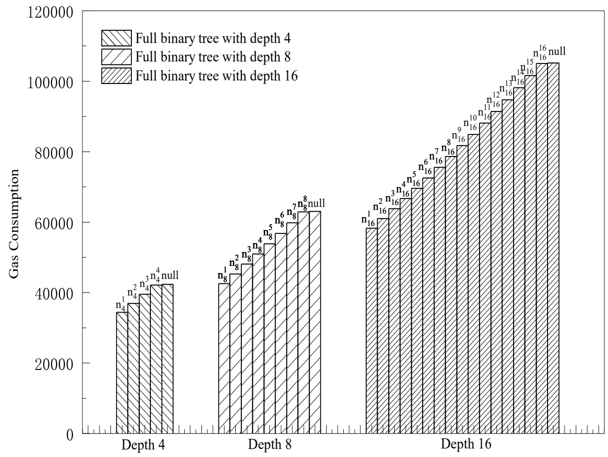


Fig. 6: Gas consumption to verify authenticity in different situations

we conduct two sets of experiments. The first set of experiments tests the impact on reputation calculation when the rating obeys normal distributions with different variance. The second set of experiments verifies the effect of the cross-chain authenticity scheme in C_2T smart contract on two authenticity attacks. In the first set of experiments, we assume that the rating obeys $N(2, \sigma^2)$ after the authenticity scheme verification; the rating obeys $N(3, \sigma^2)$ after the first attack; and the rating obeys $N(1, \sigma^2)$ after the second attack.

The first set of experiments includes three experiments: the first experiment tests the effect of normal distributions with different variance on the reputation of overestimation rating; the second experiment tests the effect of normal distributions with different variance on the reputation of normal rating; the third experiment tests the effect of normal distributions with different variance on the reputation of underestimation rating; The specific effect is shown in Fig. 7. Observing the results of the set of experiments, we can see that variance σ^2 in normal distribution has almost no effect on the reputation calculation for first authenticity attack and normal rating. For the second authenticity attack, the amplitude of the fluctuation is within a controllable range and the trend is consistent.

Therefore, in the second set of experiments, we assume that the rating obeys $N(2, 0.6)$ after the authenticity scheme verification, the rating obeys $N(3, 0.6)$ after the first authenticity attack, and the rating obeys $N(1, 0.6)$ after the second authenticity attack. The set of experiments includes two experiments. The first experiment includes two charging piles that suffer the first authenticity attack: one charging pile has been verified for authenticity, the other was not. The effect comparison is shown in Fig. 8(a). The second experiment includes two charging piles that suffer the second authenticity attack: one charging pile has been verified for authenticity, and the other was not. The effect comparison is shown in Fig. 8(b).

It can be seen from Fig. 8(a) and Fig. 8(b): if the authenticity of the information is not verified, the information may be vulnerable to authenticity attacks during invoking information across chains, resulting in inaccurate information.

Filter	BF	CBF	MCBF
Number of filters	1	1	multiple
Function type	Hash	Hash	Hash and Mod
Data type of bit	Bool	Int	Int
Delete element	No	Yes	Yes
FP rate	High	Low	Lower

TABLE 2: BF vs. CBF vs. MCBF

Num(Mod)	Num(FP)	Rate(FP)
3	1018	1.02×10^{-5}
4	85	8.5×10^{-7}
5	10	1×10^{-7}
6	2	2×10^{-8}
7	0	0

TABLE 3: The relationship between the number of Mod function and FP rate

5.2.3 *Cross-chain real-time scheme evaluation*

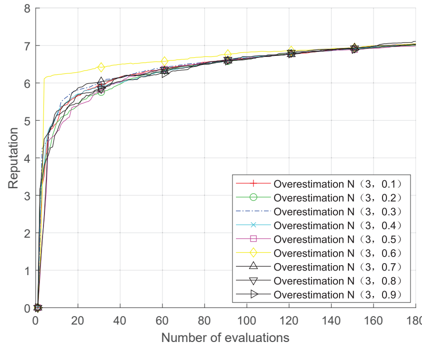
In this part, we first compare the differences between MCBF, BF (Bloom filter), and CBF. The specific comparison is shown in Table 2. Bit type in BF is bool type, which only stores two values of zero and one. In order not to affect the existing elements in the set, BF can only add elements but not delete them, and the FP rate is high. Compared with BF, bit type in CBF is int type, which increases the deletion operation and reduces the FP. The MCBF used in the $VerRealTime$ in this paper is composed of multiple CBFs. The information is converted into value once, and then multiple Mods are used to take the remainder of the value, which can reduce the running time caused by the conversion of hash functions.

Besides, in this cross-chain real-time scheme, FPs of real-time information are related to the number of Mod functions. We will query the deduplicated 100 million pieces of data in MCBF. The maximum available memory is 1G. The experimental results are shown in Table 3, which shows the relationship between the number of Mod functions and FP rate.

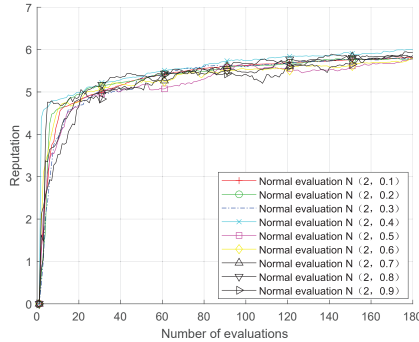
In addition, we select two CPs to verify the real-time of information during the cross-chain process. In the beginning, the behaviors of these two CPs are reliable until it reaches a high reputation, and then it starts abusing its reputation for fraud. In the process of cross-chain information extraction, the rating information of one CP has been verified in real-time, while the other has not been verified in real-time. From the results shown in Fig. 9, it can be seen that CPs have not been verified in real-time may cause a time delay in reputation calculation.

5.2.4 *Inter-chain write mutual exclusion scheme evaluation*

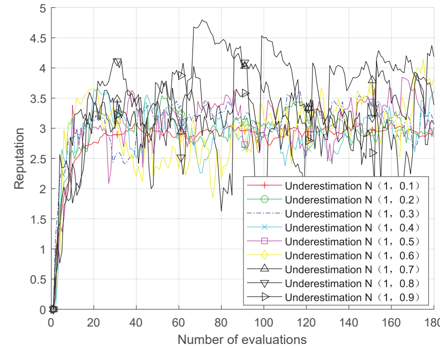
The experiment verifies the delay time of inter-chain write mutual exclusion when the effective rating rate δ is 100%, 80%, and 50%. The delay of inter-chain write mutual exclusion is the lock time of other blockchains when the C_2T smart contract calculates reputation, which is determined by the calculation time of the reputation. When information is transmitted across chains, the effective rating rate represents the rating ratio of the transmitted information that participates in reputation calculation, which determines the length of the time delay. It can be seen from Fig. 10 that the higher



(a) The effect of normal distribution on overestimation rating

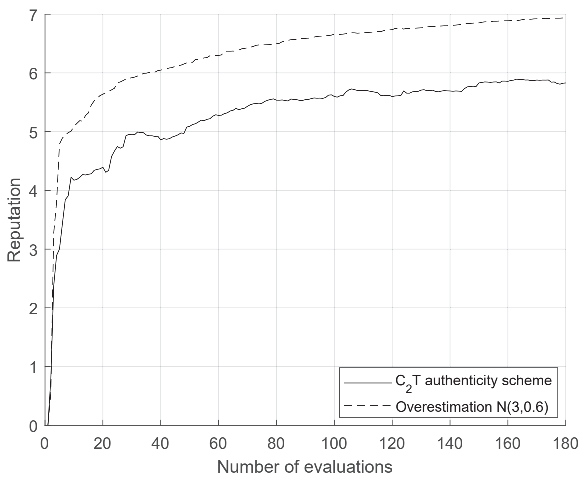


(b) The effect of normal distribution on normal rating

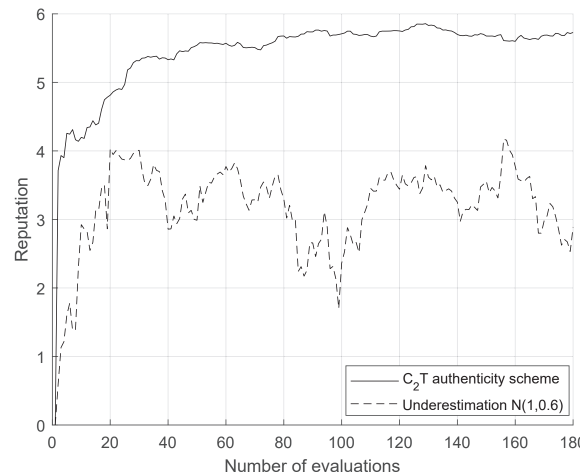


(c) The effect of normal distribution on underestimation rating

Fig. 7: The effects of normal distributions with different variance on reputation calculation in various authenticity attacks and normal rating



(a) The effect of C_2T authenticity scheme on first authenticity attack



(b) The effect of C_2T authenticity scheme on second authenticity attack

Fig. 8: The effects of C_2T authenticity scheme on various attacks

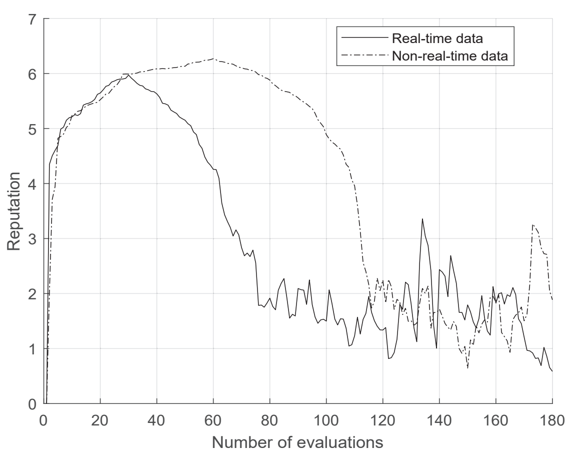


Fig. 9: Effect comparison with or without real-time verification

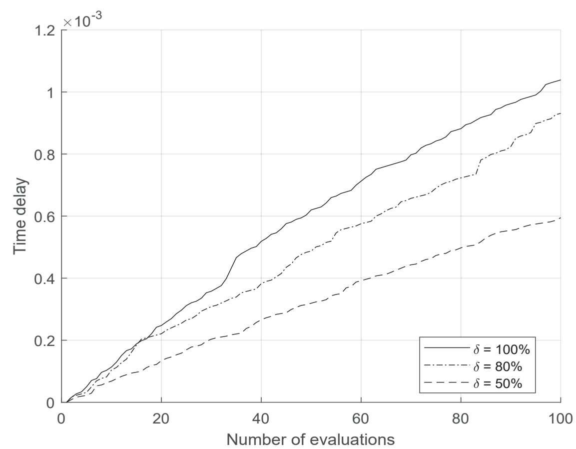


Fig. 10: Time delay with the change of δ

the effective rating rate is, the higher the time delay is; and vice versa.

6 Conclusion and Future Work

To ensure the accurate transmission of information among C_3, C_1, and C_2, we propose a C_2T smart contract to call information on multiple blockchains and perform reputation calculation. In particular, we propose a data mutual trust mechanism that uses merkel proof as the underlying algorithm to ensure the authenticity of information. Besides, we put forward a data structure, $VerRealTime$, to ensure the real-time of information. To guarantee the inter-chain write mutual exclusion of information, we present an algorithm that utilizes hash mutexes to lock block resources. Security analysis and experimental results show that C_2T smart contract is actually feasible. The solution proposed in this paper also has certain limitations. There are too many interactions between different blockchains, causing a lot of resource consumption. Therefore, in future research work, we will deploy a smart contract on each blockchain to be responsible for the calculation process of blockchain where it is located. After the calculation is completed, we only need to transfer the calculation results between smart contracts deployed in different blockchains. This improvement saves transmission resource consumption.

Acknowledgments

This work was supported by Natural Science Foundation of China (61802005), Joint of Beijing Natural Science Foundation and Education Commission(KZ201810009011).

References

[1] L. Situ, "Electric vehicle development: the past, present & future," in *2009 3rd International Conference on Power Electronics Systems and Applications (PESA)*. IEEE, 2009, pp. 1–3.

[2] C. Chan, "The past, present and future of electric vehicle development," in *Proceedings of the IEEE 1999 International Conference on Power Electronics and Drive Systems. PEDS'99 (Cat. No. 99TH8475)*, vol. 1. IEEE, 1999, pp. 11–13.

[3] B. Frieske, M. Kloetzke, and F. Mauser, "Trends in vehicle concept and key technology development for hybrid and battery electric vehicles," in *2013 World Electric Vehicle Symposium and Exhibition (EVS27)*. IEEE, 2013, pp. 1–12.

[4] P. Cazzola, M. Gorner, R. Schuitmaker, and E. Maroney, "Global ev outlook 2016," *International Energy Agency, France*, 2016.

[5] T. Bunsen, P. Cazzola, M. Gorner, L. Paoli, S. Scheffer, R. Schuitmaker, J. Tattini, and J. Teter, "Global ev outlook 2018: Towards cross-modal electrification," 2018.

[6] J. Chen, F. Li, R. Yang, and D. Ma, "Impacts of increasing private charging piles on electric vehicles' charging profiles: A case study in hefei city, china," *Energies*, vol. 13, no. 17, p. 4387, 2020.

[7] S.-C. Ma and Y. Fan, "A deployment model of ev charging piles and its impact on ev promotion," *Energy Policy*, vol. 146, p. 111777, 2020.

[8] Y. Hou, Y. Chen, Y. Jiao, J. Zhao, H. Ouyang, P. Zhu, D. Wang, and Y. Liu, "A resolution of sharing private charging piles based on smart contract," in *2017 13Th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (Icnc-Fskd)*. IEEE, 2017, pp. 3004–3008.

[9] Y. Wang, Z. Su, and K. Zhang, "A secure private charging pile sharing scheme with electric vehicles in energy blockchain," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 648–654.

[10] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.

[11] S. S. Gupta, "Blockchain," *IBM Onlone (http://www. IBM. COM)*, 2017.

[12] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[13] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2019.

[14] C. Gorenflo, L. Golab, and S. Keshav, "Mitigating trust issues in electric vehicle charging using a blockchain," in *Proceedings of the Tenth ACM International Conference on Future Energy Systems*, 2019, pp. 160–164.

[15] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2016.

[16] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, 2019.

[17] A. Hope-Bailie and S. Thomas, "Interledger: Creating a standard for payments," in *Proceedings of the 25th International Conference Companion on World Wide Web*, 2016, pp. 281–282.

[18] T. Koens and E. Poll, "Assessing interoperability solutions for distributed ledgers," *Pervasive and Mobile Computing*, vol. 59, p. 101079, 2019.

[19] M. Westerkamp and J. Eberhardt, "zkrelay: Facilitating sidechains using zksnark-based chain-relays," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2020, pp. 378–386.

[20] P. Frauenthaler, M. Sigwart, C. Spanring, and S. Schulte, "Testimonium: A cost-efficient blockchain relay," *arXiv preprint arXiv:2002.12837*, 2020.

[21] P. Frauenthaler, M. Sigwart, C. Spanring, M. Sober, and S. Schulte, "Eth relay: A cost-efficient relay for ethereum-based blockchains," in *2020 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2020, pp. 204–213.

[22] B. Dai, S. Jiang, M. Zhu, M. Lu, D. Li, and C. Li, "Research and implementation of cross-chain transaction model based on improved hash-locking," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2020, pp. 218–230.

[23] Z. Li and Z. Zhang, "Research and implementation of multi-chain digital wallet based on hash timelock," in *International Conference on Blockchain and Trustworthy Systems*. Springer, 2019, pp. 175–182.

[24] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," *arXiv preprint arXiv:1906.11078*, 2019.

[25] M. Herlihy, "Atomic cross-chain swaps," in *Proceedings of the 2018 ACM symposium on principles of distributed computing*, 2018, pp. 245–254.

[26] Y. Jiang, C. Wang, Y. Wang, and L. Gao, "A cross-chain solution to integrating multiple blockchains for iot data management," *Sensors*, vol. 19, no. 9, p. 2042, 2019.

[27] L. Deng, H. Chen, J. Zeng, and L.-J. Zhang, "Research on cross-chain technology based on sidechain and hash-locking," in *International Conference on Edge Computing*. Springer, 2018, pp. 144–151.

[28] N. Shadab, F. Houshmand, and M. Lesani, "Cross-chain transactions," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2020, pp. 1–9.

[29] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*. IEEE, 2015, pp. 104–121.

[30] S. Hua, E. Zhou, B. Pi, J. Sun, Y. Nomura, and H. Kurihara, "Apply blockchain technology to electric vehicle battery refueling," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

[31] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4601–4613, 2018.

[32] S. Guo, Y. Qi, Y. Jin, W. Li, X. Qiu, and L. Meng, "Endogenous trusted drl-based service function chain orchestration for iot," *IEEE Transactions on Computers*, 2021.

[33] Y. Wang, Z. Su, and N. Zhang, "Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3620–3631, 2019.

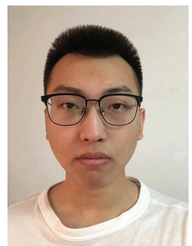
[34] D. Li, J. Liu, Z. Tang, Q. Wu, and Z. Guan, "Agentchain: A decentralized cross-chain exchange system," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data

Science And Engineering (TrustCom/BigDataSE). IEEE, 2019, pp. 491–498.
[35] M. Herlihy, B. Liskov, and L. Shrira, "Cross-chain deals and adversarial commerce," *arXiv preprint arXiv:1905.09743*, 2019.
[36] R. van Glabbeek, V. Gramoli, and P. Tholoniat, "Cross-chain payment protocols with success guarantees," *arXiv preprint arXiv:1912.04513*, 2019.
[37] H. Wang, Y. Cen, and X. Li, "Blockchain router: A cross-chain communication protocol," in *Proceedings of the 6th international conference on informatics, environment, energy and applications*, 2017, pp. 94–97.
[38] T. Lin, X. Yang, T. Wang, T. Peng, F. Xu, S. Lao, S. Ma, H. Wang, and W. Hao, "Implementation of high-performance blockchain network based on cross-chain technology for iot applications," *Sensors*, vol. 20, no. 11, p. 3268, 2020.
[39] B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, and Y. Li, "Performance analysis and comparison of pow, pos and dag based blockchains," *Digital Communications and Networks*, vol. 6, no. 4, pp. 480–485, 2020.
[40] Y. Li, B. Cao, M. Peng, L. Zhang, L. Zhang, D. Feng, and J. Yu, "Direct acyclic graph-based ledger for internet of things: performance and security analysis," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1643–1656, 2020.
[41] Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized public key infrastructures atop blockchain," *IEEE Network*, vol. 34, no. 6, pp. 133–139, 2020.
[42] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, "Theory and practice of bloom filters for distributed systems," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, pp. 131–155, 2011.
[43] M. T. Alam, H. Li, and A. Patidar, "Bitcoin for smart trading in smart grid," in *The 21st IEEE International Workshop on Local and Metropolitan Area Networks*, 2015.

Yunhua He (Member, IEEE) received the Ph.D. degree in Computer Science from Xidian University, Xi'an, China, in 2016. He was a visiting scholar at the Department of Computer Science, the George Washington University, Washington. DC from 2014 to 2016. He has been serving as an associate Professor with the School of Information Science and Technology, University of Engineering and Technology. His current research interests include Blockchain Technology, IoT Security and Privacy, Industrial Internet security.

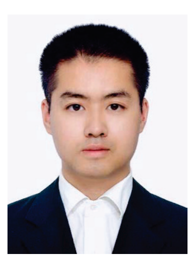
Cui Zhang, received the bachelor's degree in the Software College of Qufu Normal University, Jining, China, in 2019. She is studying for her master's degree in Computer Science and Technology of North China University of Technology, Beijing, China. Her current research interests include blockchain technology and security.

Bin Wu received his BS degree in automation and MS degree in computer science from the Ocean University of China in 2003 and 2006, respectively. He received his Ph.D. degree in information security from the Graduate University of Chinese Academy of Sciences in 2010. Now, he is an associate professor in State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His research interests include network security, covert communication, and blockchain.



Yigang Yang received the bachelor's degree in North China University of Technology, Beijing, China, in 2020. He is working toward his master's degree at the North China University of Technology. His current research interests includes blockchain security and smart contracts.

Ke Xiao received the Ph.D. degree in circuits and systems from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008. He has been a Professor with the North China University of Technology, China, since 2018. His research interests include IoT security and industrial Internet security. He is a member of the IEEE Communications Society and the IEEE VTS Society. He serves as a Reviewer for the IEEE Communications Letters, the IEEE Communications Magazine, and the IEEE Internet of Things (IoT) Journal.



Hong Li received the BA degree from the Xi'an Jiaotong University, and the PhD degree from the University of Chinese Academy of Sciences. He is an associate professor with the Institute of Information Engineering, Chinese Academy of Sciences. His primary research interests include IoT security, privacy-aware computing and blockchain.