Hindawi
Security and Communication Networks
Volume 2021, Article ID 4840253, 11 pages
https://doi.org/10.1155/2021/4840253

Research Article

A Regulatable Data Privacy Protection Scheme for Energy Transactions Based on Consortium Blockchain

Yufeng Li,[1] **Yuling Chen**,[1] **Tao Li**,[1] **and Xiaojun Ren**[2]

[1]*State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China*
[2]*Blockchain Laboratory of Agricultural Vegetables, Weifang University of Science and Technology, Shouguang 262700, China*

Correspondence should be addressed to Tao Li; litao_2019@qfnu.edu.cn

Received 6 October 2021; Accepted 10 November 2021; Published 7 December 2021

Academic Editor: Chien Ming Chen

Copyright © 2021 Yufeng Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the blockchain-based energy transaction scenario, the decentralization and transparency of the ledger will cause the users' transaction details to be disclosed to all participants. Attackers can use data mining algorithms to obtain and analyze users' private data, which will lead to the disclosure of transaction information. Simultaneously, it is also necessary for regulatory authorities to implement effective supervision of private data. Therefore, we propose a supervisable energy transaction data privacy protection scheme, which aims to trade off the supervision of energy transaction data by the supervisory authority and the privacy protection of transaction data. First, the concealment of the transaction amount is realized by Pedersen commitment and Bulletproof range proof. Next, the combination of ElGamal encryption and zero-knowledge proof technology ensures the authenticity of audit tickets, which allows regulators to achieve reliable supervision of the transaction privacy data without opening the commitment. Finally, the multibase decomposition method is used to improve the decryption efficiency of the supervisor. Experiments and security analysis show that the scheme can well satisfy transaction privacy and auditability.

1. Introduction

With the birth of Bitcoin [1], blockchain, as the underlying technology of Bitcoin [2], has been widely used in finance, medical data sharing, supply chain, energy trading, and other fields. Blockchain has the advantages of decentralization, tamper-proof, autonomy, traceability, and so on, which is regarded as the future of infrastructure. The subsequent emergence of Ethereum means that smart contracts can be used to settle the problem of decentralized applications in the currency fields [3, 4]. At present, the application mode of blockchain can be divided into three categories, public chain, consortium blockchain, and private chain. The public chain allows users to enter and exit freely, while the consortium blockchain and private chain require authorization and verification before joining. The consortium blockchain is a blockchain composed of multiple institutions. The designated members of the consortium blockchain participate in the consensus process and the maintenance of the ledger. The consortium blockchain has the advantages of fast transaction processing speed and high transaction efficiency. Therefore, it is widely used in energy trading, commodity traceability, supply chain management, and other fields. In the field of energy trading, blockchain technology is used to integrate scattered energy nodes to establish a distributed energy trading platform based on P2P transactions. It does not require third-party intermediaries and provides a low-cost trading platform for transactions between distributed energy nodes. The most important feature is that it can reasonably settle the trust problem in distributed energy transactions. Simultaneously, the blockchain-based transaction model can promote the fairness and openness of transactions in the Energy Internet and accelerate the circulation of data elements.

There are still some shortcomings existing in the practical application of energy trading. Specifically, miners and verification nodes in the blockchain can quickly verify the legitimacy of transactions due to the openness and

transparency of the ledger. However, information such as the users' identity and transaction details will be disclosed to all participants of the network in the process. Moreover, the external attackers [5, 6] can obtain information such as the account, geographic location, energy usage, and source location of the energy node from the transaction record [7]. When obtaining such information, attackers can predict users' next behavior by data mining, data analysis, machine learning, and other methods [8, 9]. Therefore, in the scenario of distributed energy transactions based on blockchain, the issue of data privacy protection in energy transactions has gradually become a new challenge. In transactions, privacy protection issues are mainly divided into two categories: identity privacy and transaction data privacy issues. Identity privacy means that attackers cannot obtain any useful information related to their identity only through the content of public data stored on the chain. Transaction data privacy refers to the fact that both parties to the transaction are considering their interests, and any node other than themselves cannot obtain the details of the transaction from public information. The contributions of this paper are as follows:

(1) There are two problems in the blockchain-based energy transaction scenario. The openness and transparency of the transaction ledger allow any participant to obtain transaction details, which poses the risk of private data leakage. Simultaneously, there needs to be a balance between transaction regulation and privacy protection. Therefore, we propose a supervisable energy transaction data privacy protection scheme to deal with the above problems.

(2) Combine Pedersen commitment and Bulletproof range proof to realize the concealment of the transaction amount. Adopt ElGamal encryption and zero-knowledge proof technology to ensure the authenticity of audit tickets. The reliability of the transaction can be supervised without executing the open commitment. The introduction of multibase decomposition technology in ElGamal improves the decryption efficiency of the supervisor.

(3) Security and performance analysis show that the scheme can audit a certain transaction or multiple transactions in the ledger and effectively protect the privacy of transaction amounts.

2. Related Works

At present, blockchain technology is developing rapidly, and the privacy protection issue in the blockchain has received extensive attention from a growing number of scholars. A variety of cryptographic technologies are applied in the blockchain system to settle the problems of identity privacy and transaction privacy, which also means that the supervision technology of blockchain transactions will face more challenges.

The cryptocurrency based on the public chain emphasizes the privacy protection of transactions. For example, these works [10, 11] proposed a Mixcoin protocol, which uses a Mixcoin protocol to transfer funds from multiple input addresses to multiple output addresses to provide anonymity services. The connection between the user's real identity and address was interrupted. In Monero [12], the Pedersen commitment scheme is used to conceal transaction information. It uses ring signatures and one-time addresses to hide the identities of the sender and receiver in the transaction. Based on Monero, Li et al. [13] proposed a new cryptocurrency system, which can simultaneously achieve identity anonymity and traceability in Monero. However, excessive privacy protection strategies will cause the regulatory authorities to not effectively supervise the transaction content and identity. Zcash [14] uses noninteractive zero-knowledge proofs (zk-SNARKs) technology to verify private transactions and conceal the identity of the sender. However, the transaction efficiency of this scheme is unsatisfactory. An anonymous scholar named Tom Elvis Jedusor first proposed the MimbleWimble protocol in 2016 [15]. It uses confidential transaction technology to realize the shielding of transaction content and realizes the concealment of the identity of the transaction party by removing the transaction address. Although the agreement has regulatory functions, it cannot track transaction information and the identity of violators. In 2019, Beam and Grin were proposed. The scheme combines the MimbelWimble protocol and aggregated signature technology to achieve the purpose of protecting the privacy of blockchain transactions [16]. These works [17, 18] proposed a blockchain-based machine learning framework and secure key management scheme (BC-EKM). This scheme designs a secure cluster formation algorithm and a secure node movement algorithm to implement key management, where stake blockchain as a trust machine replaces the majority functions of the BS. In addition, this scheme is based on the SM2 public-key cryptosystem to protect data security and prevent data privacy leakage in edge services. Chen et al. [19] proposed a new ciphertext extension method that makes homomorphic encryption of ciphertext more efficient. However, the scheme requires both parties to the transaction to interact online, which will encounter difficulties in practice.

The above privacy protection scheme is a typical public chain application scenario. The privacy protection features they provide do not implement transaction supervision and cannot satisfy the supervision requirements of the application system. Therefore, privacy protection schemes with supervisory functions have also been proposed. Wüst et al. [20] proposed a new cryptocurrency PRCash in 2018. It uses zero-knowledge proof technology to generate range proof and regulatory proof for each transaction. The range proof is verified by the public node, which is used to guarantee the range of the user's transaction amount. The supervision certificate is verified by the supervisor, which is used to restore user identity information. The regulator in PRCash supervises the total amount of transactions made by users over a while. If the user's total transaction amount exceeds the quota specified by the system within a certain period, the supervisor can track the violating user. The supervisor obtains its true identity information based on the supervisory certificate. PRCash realizes the limitation of the user's transaction amount within a period and supervises violations, but it cannot obtain the specific value of each transaction. NeHa et al. [21] proposed a

comprehensive privacy auditable distributed ledger system Zkledger in 2018. The program uses a table ledger structure, which can conceal the identities of the sender and receiver of the transaction and the transaction amount simultaneously. Zkledger has set up a supervisor, and the supervisor needs to initiate an online inquiry to the user to obtain the sum of the user's assets over a while. However, the regulator cannot obtain the specific amount of each transaction during the entire process. Moreover, the user needs to open the commitment after responding to the supervision request, and the supervisor will obtain certain commitment secret value information in the process, which is not conducive to the security of the system. In 2019, Kang et al. [22] proposed the privacy protection smart contract Fabzk based on Zkledger. This scheme assigns the five zero-knowledge proofs generated in the transaction to system users and supervisors for verification. To improve transaction performance, the transaction verification process can be performed concurrently. However, the scheme requires the regulator to remain online at all times, and the transaction is considered valid only if all five verification equations are passed.

Regarding the transaction privacy issues in the energy transaction scenario based on the consortium blockchain, this paper proposes a supervisable energy transaction data privacy protection scheme. This scheme realizes the concealment of the transaction amount by the Pedersen commitment and uses the Bulletproofs range proof to guarantee the transaction amount range. Combining ElGamal encryption and zero-knowledge proof technology to ensure the authenticity of regulatory tickets, the regulation of transactions can be achieved without executing open commitments. The multibase decomposition technology is introduced in the scheme to improve the decryption efficiency of the regulator. The results of experiments and security analysis show that the scheme can achieve transaction privacy and auditability. The supervisor can audit the total transaction amount in a certain number of blocks, and it can also restore the specific amount in a transaction.

3. Preliminaries

3.1. Consortium Blockchain. Blockchain is a new technology system derived from the underlying technology of Bitcoin. Blockchain technology is developing rapidly, and it has derived consortium blockchain and private chains from public chains. The public chain is completely decentralized, and any user can join or exit freely, while the private chain is a completely private blockchain, and only internal personnel can use it. The degree of decentralization of the consortium blockchain is between the public chain and the private chain. It is mostly composed of offline enterprises and other alliances. Users need to achieve certain conditions and obtain permission to enter and exit. Additionally, the consortium blockchain can be completely open or only accessible by insiders of the consortium.

3.2. Zero-Knowledge Proof. The zero-knowledge proof system involves two parties, called the prover and verifier. Prover knows a certain secret, and prover hopes to convince verifier that he does have the secret without revealing the secret. The zero-knowledge proof system should satisfy the following three conditions: completeness, reliability, and zero-knowledge. Completeness means that if the prover knows a certain secret, the verifier will accept the prover's proof. Reliability means that if the prover can convince the verifier with a certain probability, the prover knows the corresponding secret. Zero-knowledge refers to the fact that the verifier cannot obtain any additional information during the interaction between the prover and the verifier. Zero-knowledge proofs can be classified into interactive and noninteractive knowledge proofs. Interactive zero-knowledge proof requires one or more communications between the prover and the verifier. Blum et al. [23] proposed a noninteractive zero-knowledge proof. The prover uses hash value instead of the interactive process, which avoids multiple communications between the prover and the verifier. Typical representatives of noninteractive zero-knowledge proof protocols are Bulletproofs [24] and ZK-SNARKs [25]. Bulletproofs have the characteristics of short proof time and no need to set up a trusted center.

Comparing the noninteractive zero-knowledge proof with the interactive zero-knowledge proof, the noninteractive zero-knowledge proof avoids multiple rounds of communication between participants. And any participant can verify the validity of the proof π. The Fait-Shamir [26] scheme provides a method to transform interactive zero-knowledge proofs into noninteractive zero-knowledge proofs. This feature fits perfectly with the decentralized environment of the blockchain, which can reach a consensus and establish a trust relationship between nodes that do not trust each other.

3.3. Pedersen Commitment. The cryptographic commitment scheme is a two-stage interactive protocol involving two parties, and the two parties are the promiser and the receiver, respectively. The first stage is the commitment stage. The promiser chooses a message m and sends it to the receiver in the form of ciphertext, which means that it will not change m. The second stage is the opening stage, where the promiser discloses the message m and the blinding factor, and the receiver uses this to verify whether it is consistent with the message received in the promise stage. The commitment scheme has two basic properties: hiding and binding. Hiding is the commitment and will not reveal any information about the message m. Binding means that no malicious promiser can open the commitment to m and pass the verification, which means that the receiver can be sure that m is the message corresponding to the commitment. Pedersen promises to be an important cryptographic component in blockchain technology, and its structure consists of the following three stages:

Setup**:** select the elliptic curve $E(F_p)$ with G and H, where G and H are the two generators of the elliptic curve, and the order is q. Public parameters are (G, H, q).

Commitment**:** the promiser chooses a random number k as the blind factor, calculates the commitment

Com = $kG + vH$, and then sends the commitment Com to the receiver.

Open: the promiser sends (v, k) to the receiver, and the receiver verifies whether the commitment is equal to $kG + vH$ and accepts if they are equal; otherwise, it rejects the commitment.

The homomorphic characteristics of Pedersen commitment are embodied as follows: $\mathrm{Com}(v_1) + \mathrm{Com}(v_2) = (k_1 + k_2)G + (v_1 + v_2)H = \mathrm{Com}(v_1 + v_2)$. According to this feature, the verifier can calculate the transaction commitment without knowing the specific secret.

3.4. Elliptic Curve Cryptography. Elliptic curve cryptography was first proposed by Neal Koblitz and Victor Miller in 1985, and it is called ECC for short. It is a public-key cryptosystem that is currently widely used. The security of the ECC algorithm is mainly based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). Under the same security requirements, its required parameters and key size are shorter. Compared with other public-key cryptosystems, elliptic curve cryptography has the advantages of higher security, short key length, small storage space, and fast calculation speed.

Let Z_p denote the domain of integers, where p is a large prime number; thus, an elliptic curve $E(F_p)$ can be defined. It can usually be expressed as $y^2 = x^3 + ax + b \pmod p$, where the coefficients $a, b \in Z_p$. a and b are two constants satisfying $4a^3 + 27b^2 \pmod p \neq 0$. $P = (x, y)$ represents a point on the elliptic curve, where $x, y \in Z_p$ represents the abscissa and ordinate of the corresponding point on the elliptic curve, respectively. There is a special point $\boldsymbol{O}$ on the elliptic curve, called the point of infinity, which forms the elliptic curve $E(F_p)$ together with the whole point P.

3.5. ElGamal Encryption Algorithm. ElGamal encryption is a common asymmetric encryption algorithm. Its security is based on the finite field discrete logarithm problem [27], and it is indistinguishable under selected plaintext attacks (IND-CPA). ElGamal encryption mainly includes three algorithms: key generation algorithm, encryption algorithm, and decryption algorithm.

Key generation algorithm: select the finite field cyclic group G of order p, where p is a large prime number. The generator of the finite field cyclic group G is g. Randomly select $x \in Z_p$ as the private key, calculate the public key $y = g^x \bmod p$, and make it public.

Encryption algorithm: the encrypting party chooses a plaintext message m, and the plaintext message m needs to satisfy $m < p$ and then choose a random number $k < p$, where k and $p - 1$ are relatively prime. Calculate the ciphertext $A = g^k \bmod p$ and $B = \mathrm{my}^k \bmod p$. The ciphertext consists of two parts $C = (A, B)$.

Decryption algorithm: the decryptor uses his private key x to decrypt the ciphertext (A, B) and restore the plaintext by calculating $m = B/A^x \bmod p$.

In addition, the relevant symbols and explanations involved in this paper are listed in Table 1.

4. Supervisable Privacy Protection Scheme Model

The scheme satisfies the primary principles of privacy and supervisability of transactions, which are required to prevent the leakage of sensitive user information to ensure transaction privacy. The Pedersen commitment based on the elliptic curve is applied to the scheme to hide the transaction information, and the zero-knowledge range proof ensures that the transaction amount hidden in the commitment is in the legitimate interval. We combine homomorphic encryption technology, Pedersen commitment, and zero-knowledge proof technology to ensure that the transaction amount is consistent with the amount in the ciphertext. To further improve transaction performance, multibase decomposition technology is used to improve the efficiency of encryption and decryption by regulatory authorities. Based on these cryptography technologies, we have designed a regulatory privacy protection scheme to achieve privacy and regulations.

4.1. Transaction Structure. There are mainly five entities in this program, as shown in Figure 1, which are the certification body (CA), regulatory (RA), energy aggregator, energy buyer EB, and energy seller ES. The role of each entity is as follows:

Certification authority (CA): Its role is to issue a certificate for the user. Any user who wants to enter the blockchain network must be authorized by the certification authority and obtain the certificate *Cert* promulgated by the certification authority to the certificate *Cert*.

Regulatory authority (RA): It is responsible for auditing transaction content. Once suspicious transactions are found, the supervisor can obtain ciphertext and decrypt the specific one after the transaction information is decrypted from the transaction information and interact with the CA to obtain real-name information of the transaction. It is worth noting that this scheme can be audited in this scheme, which means that there is no need to travel online.

Energy buyers (EB): It uses the initiator of the transaction to launch a transaction as a sender in the transaction. It uses the private key to sign the transaction proposal during the transaction process, which is a transaction commitment, supervision ciphertext, and zero-knowledge used to prove the effective effectiveness. Before generating a complete transaction, it is necessary to make a chain interaction with the recipient of the transaction, and the purpose is to consent with the two parties. Moreover, in the actual transaction process, ES can also initiate a transaction as a transaction sender. To describe convenience, only EB is considered as a sender, and ES is considered as a reception party.

Table 1: Nomenclature.

$E_p(a,b)$	An elliptic curve with parameters a, b, p
H, G, n	Generator and order
P_a, x_a	Supervisor public key and private key
paramas	Public parameters
v	Transaction amount
k, r	Blinding factor and random number
$Rf(v)$	Range proof of transaction amount
$C(k, v)$	Transaction commitment
bill	System audit ticket
S	Transaction balance signatures
e, σ	Challenge value
Cert	Identity certificate
C_x, D_x, B_x	Regulatory ciphertext
π	Zero-knowledge proof
V_x, E_x, T_x	ZK auxiliary information
η_x, k_x, r_x	An element in vectors η, k, r

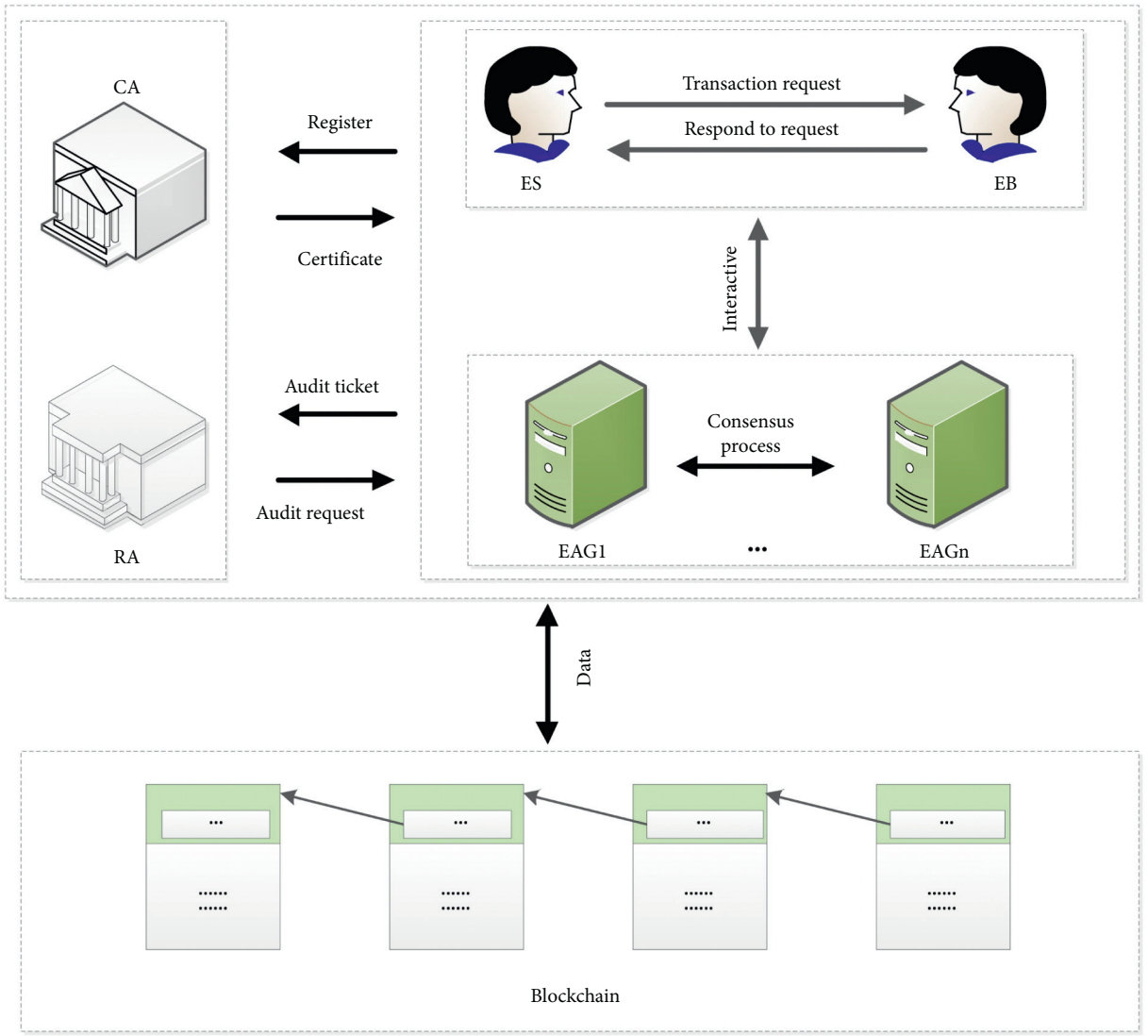

Figure 1: Scheme architecture.

Energy seller (ES): It serves as a receiver of the transaction. During the generation of the transaction, there is an interactive process between the recipient and the sender to generate some interaction information.

EAG: It sends an audit request to the user, verifies the user's audit notes, and interacts with the supervisor.

4.2. Transaction Process. The transaction process consists of two stages: system initialization and interaction between buyers and sellers.

4.2.1. System Initialization. Our scheme is combined with the Pedersen commitment and ElGamal encryption technology. The system parameters are needed to generate a scheme in the initialization phase. Select an elliptic curve $E_p(a,b)$, one generating element G on the curve, and its order is n. Randomly select k, $x_a < n$, calculate $H = kG$ and $P_a = x_aG$, and the system deletes the discrete logarithm k of H. Therefore, the discrete logarithm of H is unknown to the outside world. We use x_a as the private key of the regulator and P_a as the public key of the regulator. Finally, the public parameters may be represented as params = $(E_p(a,b), n, G, H, P_a)$.

4.2.2. Interactive Process. In the energy transaction payment phase, EAG returns the results of the bid to energy buyer A and energy seller B. v_3 is the transaction price between buyer A and seller B. Subsequently A checks if the amount in all the addresses is greater than the transaction amount v_3; otherwise, the trading will be terminated. Assume that the amounts v_1 and v_2 in the two addresses of A are satisfied with $v_3 = v_1 + v_2$, where $v_1, v_2, v_3 \in [0, 2^n - 1]$. The detailed trading steps are as follows:

Step 1: A initiates a transaction to B. Specifically, A pays v_1 and v_2 from B, which is the amount that matches in advance. A selects blind factors $k_1, k_2 < n$ and a random number $r_a < n$ at random and calculates the necessary information and range proof. Among them, the range proof proves that $Rf_{\text{in1}}(v_1)$ and $Rf_{\text{in2}}(v_2)$ are generated by Bulletproof technology. The specific calculation process is as follows:

$$R_a = r_aG, \tag{1}$$

$$K_a = (k_1 + k_2)G, \tag{2}$$

$$C_{\text{in1}}(k_1, v_1) = v_1H + k_1G, \tag{3}$$

$$C_{\text{in2}}(k_2, v_2) = v_2H + k_2G. \tag{4}$$

Then compose the above result into m_1. And send $m_1 = (\text{params}, K_a, R_a, Rf_{\text{in1}}, Rf_{\text{in2}}, C_{\text{in1}}, C_{\text{in2}})$ and certificate $Cert_A$ to B by the secure channel.

Step 2: After receiving the transaction request, B immediately verifies the legitimacy of the certificate, whether the scope certification and commitment are correct. If any verification fails, the transaction is terminated. Among them, the verification commitment is equivalent to the verification equation (5). If the verification is passed, it means that the transaction initiator has correctly calculated the commitment according to the rules. B randomly selects the blinding factor and random number $k_3, r_b < n$ and calculates the commitment $C_{\text{out}}(k_3, v_3)$, the range proof $Rf_{\text{out}}(v_3)$, the transaction balance signature S_b, and the audit ticket bill_{out} (the construction of the audit ticket will be detailed in Section 4.4). The specific calculation process is as follows:

$$C_{\text{in1}}(k_1, v_1) + C_{\text{in2}}(k_2, v_2) = v_3H + K_a, \tag{5}$$

$$R_b = r_bG, \tag{6}$$

$$K_b = k_3G, \tag{7}$$

$$C_{\text{out}}(k_3, v_3) = v_3H + k_3G, \tag{8}$$

$$\begin{aligned} K &= K_a + K_b, \\ R &= R_a + R_b, \end{aligned} \tag{9}$$

$$e = \text{Hash}(\text{params}, R, K), \tag{10}$$

$$S_b = r_b + ek_3, \tag{11}$$

$$\text{bill}_{\text{out}} = (C_{\text{out}}, D_{\text{out}}, \pi_{\text{out}}). \tag{12}$$

Then compose the above result into m_2. And send $m_2 = (\text{params}, K_b, R_b, Rf_{\text{out}}, C_{\text{out}}, S_b, e, \text{bill}_{\text{out}})$ and certificate Cert_B to A by the secure channel.

Step 3: when A accepts and receives the reply, it will verify the validity of the certificate. If the verification is passed, then extract K_b and Rb from the message m_2 to calculate $K = K_a + K_b, R = R_a + R_b$. Verify whether equation (13) is established. If the verification is passed, calculate the transaction balance signature S and audit bill $\text{bill}_{\text{in1}}, \text{bill}_{\text{in2}}$; otherwise, terminate the transaction. The specific calculation process is as follows:

$$\text{Hash}(\text{params}, R, K) = e, \tag{13}$$

$$S_a = r_a + e(k_1 + k_2), \tag{14}$$

$$S = S_a + S_b, \tag{15}$$

$$\text{bill}_{\text{in1}} = (C_{\text{in1}}, D_{\text{in1}}, \pi_{\text{in1}}), \tag{16}$$

$$\text{bill}_{\text{in2}} = (C_{\text{in2}}, D_{\text{in2}}, \pi_{\text{in2}}). \tag{17}$$

Finally, combine the above results into a private transaction $Tx = (\text{params}, (C_{\text{in},i}(k_i, v_i), \text{Rf}_{\text{in},i}(v_i), \text{bill}_{\text{in},i})_{i\in[1,2]}, (C_{\text{out},j}(k_j, v_j), \text{Rf}_{\text{out},j}(v_j), \text{bill}_{\text{out},j})_{j=1}, R, K, S, e, \text{Cert}_A, \text{Cert}_B)$ and send Tx to EAG.

Step 4: EAG will verify its correctness after receiving the Tx. It mainly includes the legality of the certificates Cert_A and Cert_B, the correctness of the scope certification, and the correctness of the signature (S, e). Among them, verifying the correctness of the signature is equivalent to verifying whether the equation $SG = R + eK$ is established, which means that the sum of the input of the transaction is equal to the sum of the output; otherwise, the transaction is discarded.

4.3. Supervision Process. The supervision process mainly consists of three entities: RA, EAG, and CA. (1) RA: it has supervision and audit functions. In the supervision process, the specific amount in a certain transaction can be audited. (2) EAG: it provides audit-related transaction information for regulators. (3) CA: when the supervisor finds that the transaction is abnormal, it can extract the certificate Cert from the transaction information and interact with the CA to trace the identity of the trader. Specifically, it consists of the following steps:

Step 1: Verify the correctness of the zero-knowledge proof in the audit ticket. After submitting an audit request to EAG, the supervisor obtains a transaction Tx and extracts the audit bill $\text{bill}_{\text{in},i}$, $\text{bill}_{\text{out},j}$ from it. For the convenience of description, we simplified the audit ticket as bill $= (C, D, \pi)$. For the zero-knowledge proof $\pi = \text{PK}\{(\eta_x, k_x, r_x)_{x\in[0,l-1]}: C_x = \eta_x H + k_x G \wedge D_x = \eta_x H + r_x P_a \wedge B_x = r_x G\} = \{(Z_{\eta x}, Z_{kx}, Z_{rx})_{x\in[0,l-1]}, \sigma\}$ (its generation process will be described in detail in Section 4.4), calculate the following values, respectively:

$$E_x = Z_{rx} G - \sigma B_x, \tag{18}$$

$$T_x = Z_{\eta x} H + Z_{rx} P_a - \sigma D_x, \tag{19}$$

$$V_x = Z_{\eta x} H + Z_{kx} G - \sigma C_x, \tag{20}$$

$$\sigma' = H\left(\text{params}, (V_x, E_x, T_x)_{x\in[0,l-1]}\right). \tag{21}$$

Verify that equation $\sigma' = \sigma$ is established. If the verification is passed, it means that the ciphertext and the commitment calculation in the audit ticket are correct. Otherwise, it means that there are violating nodes participating in the transaction, which requires interaction with the CA through the certificate in the transaction information to track the identity of the suspicious transaction initiator.

Step 2: The supervisor uses its private key x_a to decrypt the ciphertext to obtain the specific transaction amount. To improve the efficiency of encryption and decryption, the supervisor precomputes a table $(0H, 1H, \ldots, (u-1)H)$ and stores it locally. The supervisor calculates $y_x = D_x - x_a B_x$ by extracting the ciphertext $D = (B_x = r_x G, D_x = \eta_x H + r_x P_a)_{x\in[0,l-1]}$ from the audit ticket. According to y, the auditor uses a precomputation table containing t to find out the value of η_x. Finally, the specific amount in each transaction is restored by calculating $v = \sum_{x=0}^{l-1} \eta_x u^x$.

4.4. Construction of Audit Ticket. This section will describe in detail the construction of an audit ticket. For large transaction amounts, to improve supervision efficiency and system performance, multibase decomposition is used to achieve efficient decryption of ciphertext by regulatory agencies. The generation of audit tickets consists of the following three steps:

Step 1: Decompose a transaction amount v into a set of vectors $\eta = (\eta_0, \ldots, \eta_{l-1})$, $\eta_x \in [0, u-1]$, where u represents the basis of multibase decomposition, satisfying $v = \sum_{x=0}^{l-1} \eta_x u^x$.

Step 2: For each element η_x in the vector η, calculate the ElGamal ciphertext $D = (B_x = r_x G, D_x = \eta_x H + r_x P_a)_{x\in[0,l-1]}$ and the commitment $C = (\eta_x H + k_x G)_{x\in[0,l-1]}$, where r_x and k_x satisfy $r = \sum_{x=0}^{l-1} r_x u^x$ and $k = \sum_{x=0}^{l-1} k_x u^x$.

Step 3: For each element η_x in the vector η, calculate the zero-knowledge proof $\pi = \text{PK}\{(\eta_x, k_x, r_x)_{x\in[0,l-1]}: C_x = \eta_x H + k_x G \wedge D_x = \eta_x H + r_x P_a \wedge B_x = r_x G\}$. The specific details are as follows: randomly select v_x, t_x, s_x, calculate $V_x = v_x H + t_x G, E_x = s_x G, T_x = v_x H + s_x P_a$, calculate $\sigma = H(\text{params}, (V_x, E_x, T_x)_{x\in[0,l-1]})$, and calculate $Z_{\eta x} = v_x + \sigma\eta_x, Z_{kx} = t_x + \sigma k_x, Z_{rx} = s_x + \sigma r_x$. Obtain a zero-knowledge proof $\{(Z_{\eta x}, Z_{kx}, Z_{rx})_{x\in[0,l-1]}, \sigma\}$ with a transaction output amount of v. Finally, we get the audit bill bill $= (C, D, \pi)$.

5. Security Analysis

5.1. Security Requirements. The security goals of the scheme will be defined as follows: (1) Transaction balance: it means that the total input of a transaction is equal to the total output, which means that users cannot create or destroy a transaction arbitrarily. (2) The privacy of the transaction: except for the parties to the transaction and the supervisor, other users cannot obtain specific information about the transaction amount based on public information such as transaction balance signatures, commitment values, and audit tickets. (3) Auditability of transactions: when the supervisor needs to review a certain transaction or multiple transactions in a certain block, the supervisor can audit the corresponding transaction amount and trace the user identity.

5.2. Analysis

5.2.1. Transaction Balance. Suppose H is a random oracle. If the discrete logarithm problem of transaction balance signature is difficult and the commitment scheme satisfies the binding property, then this scheme satisfies the transaction balance.

The proof process is an interactive game between the algorithm opponent A and the mathematical problem

opponent B. B receives a random DLP problem instance $H = xG$, and his goal is to calculate x. B uses A as a subroutine to calculate x, and the mathematical problem opponent B plays the challenger of the algorithm opponent A.

System initialization phase: B sends the system public parameters params to A. B has to maintain two tables L_c and L_s, which are empty at the initial moment. L_c is used to simulate the query of the algorithm opponent A on the commitment value and L_s is used to simulate the transaction balance signature query.

Inquiry stage: the algorithmic opponent A, respectively, inquires the commitment $C(v_i)$ and the transaction balance signature S_i to the commitment oracle and the transaction balance signature oracle for a limited number of times. If there is no corresponding value in L_c and L_s, B randomly selects the parameter to calculate the corresponding value, returns it to A, and updates L_c and L_s.

Forgery stage: suppose the algorithm opponent A successfully forged a transaction $(C(v'), K', R', S', e')$ by the above query and the forged transaction balance signature is (S', e', K'), where $K' = v'H + e'G + K$. It can be verified that the equation $S'G = R' + e'K'$ holds. During the interrogation process, the adversary of the algorithm also obtains a correct signature (S, e, K) and can also verify that the equation $SG = R + H(R, K)K$ is established.

The discrete logarithm x corresponding to H can be solved by combining the above two equations. It can be seen that algorithmic opponent A can successfully break the trading balance. Mathematical problem opponent B can use A to settle the discrete logarithm problem, which contradicts the DLP assumption of this scheme. Therefore, this scheme satisfies the transaction balance.

5.2.2. The Privacy of Transactions. Transaction input and output are stored in the blockchain in the form of commitment. Because the blinding factor is unknown and the discrete logarithm is difficult, other participants cannot know the specific amount of the transaction except for the two parties in the transaction. Simultaneously, EAG will mix all inputs and outputs, which breaks the logical connection between the transaction input address, transaction output address, and change address, thereby ensuring the privacy of transactions.

5.2.3. Auditability of Transactions. This scheme uses Bulletproof to ensure that the transaction amount is within a specific range. The supervisor can obtain the specific details of a transaction by its private key. When the supervisor needs to verify the information of a certain transaction, it uses the private key to decrypt the audit ticket to obtain detailed information of a certain transaction. If suspicious behavior is discovered, the user's identity information can be obtained by interaction with CA for accountability.

6. Performance Analysis

We analyze our scheme based on throughput and latency. Throughput and latency are the two most important indicators for analyzing the performance of a blockchain system. We analyze this scheme based on these two indicators. Transaction delay and throughput are affected by transaction zero-knowledge proof generation time, verification time, audit ticket generation time, supervisor audit time, and transaction size. The comparative analysis between this scheme and the existing scheme is shown in Table 2.

6.1. Experimental Configuration. This experiment was conducted on a computer with 8G memory, Inter (R) Core (TM) i5-65003.20 GHz CPU and GeForce GT 730 graphics card, and 64-bit Windows10 operating system. The scheme is implemented in C language, in which the Hash algorithm uses the cryptographic hash algorithm SM3, and the elliptic curve selects the more efficient SM2. We set $n = 64$; that is, we use a 64-bit positive integer to represent the transaction amount. This setting is to be the same as Bitcoin and Monero. In our experiments, we mainly consider the following two aspects, time overhead and storage overhead. Storage overhead is mainly the size of a transaction. Time overhead mainly includes transaction generation time, verification time, and audit time. We compare the above indicators with another similar scheme.

6.2. Results and Analysis. The time cost and storage cost of a single transaction mainly consider the classic transaction scenario of 2 inputs and 2 outputs. We compared our scheme with similar schemes, as shown in Table 3.

In our scheme, the size of the audit ticket is approximately 320 bytes. For each output, the range proved to be about 738 bytes in size. The committed size for each transaction is 64 bytes. The transaction generation time cost is about 90 ms, the transaction verification time cost is about 10 ms, and the transaction audit time cost is about 43 ms.

For [12], it uses ring signature technology. For more convenience, we set the size of the ring signature to 4. In a transaction with 2 inputs and 2 outputs, its total storage cost is 12710 bytes, and the time cost of the sender and verifier is approximately 300 ms.

For [14], all the proofs can be combined into a 288-byte zk-SNARK proof through aggregation technology. The total proof size of a classic transaction with 2 inputs and 2 outputs becomes about 576 bytes. Since the zk-SNARK proof is adopted, the time cost of generating the proof will be very large, about 2 minutes. And zk-SNARK proves that a large amount of memory RAM >rbin 3 GB needs to be consumed during the generation process. It will cause long delays in the blockchain system. However, the verification time overhead of the zk-SNARK proof is considerable, about 10 ms.

For the privacy of transactions, we set 64-bit transaction data, which means that the data range is $v \in [0, 2^{64} - 1]$. We use the multibase decomposition method to improve the efficiency of encryption and decryption, taking $u = 2^8 = 256$, $l = 8$. Figures 2 and 3 show the comparison of encryption time and decryption time between Elgamal and MBD_Elgamal (Elgamal encryption based on multibase decomposition). From the figure, we can see that, with the increase of transaction data length, the encryption efficiency

Table 2: Scheme comparison.

Schemes	Main technique	Transaction privacy	Offline supervision	Public verification	Single transaction audit
[12]	CryptoNote protocol Ring signature	Yes	No	No	No
[14]	zk-SNARKs Pedersen commitment	Yes	No	No	Yes
This paper	Pedersen Commitment, Bulletproofs, and ElGamal	Yes	Yes	Yes	Yes

Table 3: Comparison of privacy-preserving blockchain schemes.

Schemes	Storage overhead (bytes)	Transaction time	Verification time	Audit time
[12]	12710	300 ms	300 ms	—
[14]	576	120 s	10 ms	55 ms
This paper	4488	90 ms	10 ms	43 ms

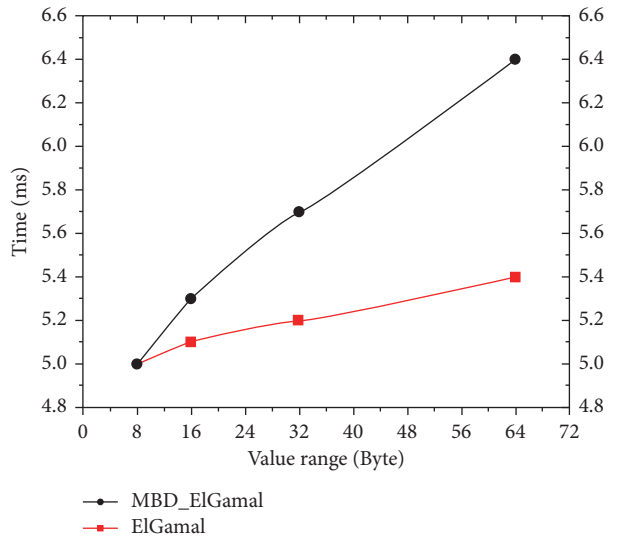

Figure 2: Encryption time.

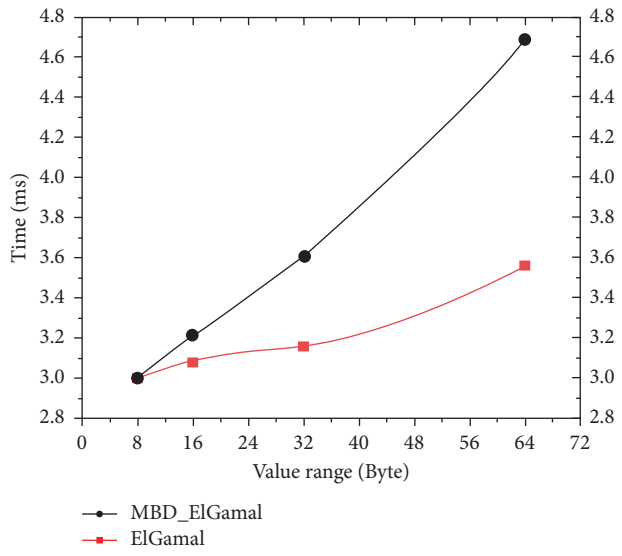

Figure 3: Decryption time.

Table 4: Encryption scheme comparison.

Schemes	Setup time	Enc time	Dec time
This paper	52 s	5.4 ms	3.4 ms
Paillier	403 ms	27 ms	7 ms

of ElGamal based on multibase decomposition can be increased by more than 1.2 times. The decryption time can be increased by more than 1.3 times.

For transaction data privacy, we compare this scheme with the Paillier encryption scheme with the same security level. As shown in Table 4, we only compare the encrypted and decrypted parts. It can be seen from the figure that our scheme is about 5 times and 2 times higher than Paillier's encryption efficiency. This is because our solution requires a longer initialization time and sacrifices the time overhead of initial parameters in exchange for more efficient encryption and decryption time.

7. Conclusion

In this paper, we have designed a supervisable transaction data privacy protection scheme, which settles the problem of transaction privacy and effective supervision in the blockchain-based energy transaction scheme. Specifically, we combine Pedersen commitment and zero-knowledge proof technology to ensure the authenticity of transaction data, which effectively prevents malicious users from using random amounts for encryption to defraud the regulator. Simultaneously, the transaction data can be verified in a ciphertext environment. In the process of generating audit tickets, we introduced the ElGamal encryption and decryption method based on multibase decomposition to improve the efficiency of encryption and decryption. And the Bulletproofs range proof technology is introduced in the transaction creation process, which improves the efficiency of transaction verification. Security and performance analysis show that the scheme can audit a certain transaction or multiple transactions in the ledger and effectively protect the privacy of transaction amounts.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported by the Natural Science Foundation under Grant nos. 61962009 and 62162008; Major Scientific and Technological Special Project of Guizhou Province under Grant nos. 20183001 and 20193003; Science and Technology Support Plan of Guizhou Province ((2020) 2Y011); Foundation of Guangxi Key Laboratory of Cryptography and Information Security (GCIS202118); and Shandong Provincial Natural Science Foundation (ZR202103050289).

References

[1] C. S. Wright, "Bitcoin: a peer-to-peer electronic cash system," *SSRN Electronic Journal*, no. 9, 2008.

[2] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, and X. Yu, "Semi-selfish mining based on hidden Markov decision process," *International Journal of Intelligent Systems*, vol. 36, no. 7, pp. 3596–3612, 2021.

[3] A. Singh, R. M. Parizi, Q. Zhang, K.-K. R. Choo, and A. Dehghantanha, "Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities," *Computers & Security*, vol. 88, Article ID 101654, 2020.

[4] V. Aleksieva, H. Valchanov, and A. Huliyan, "Application of smart contracts based on ethereum blockchain for the purpose of insurance services," in *Proceedings of the 2019 International Conference on Biomedical Innovations and Applications (BIA)*, pp. 1–4, IEEE, Varna, Bulgaria, November 2019.

[5] T. Li, Y. Chen, Y. Wang et al., "Rational protocols and attacks in blockchain system," *Security and Communication Networks*, vol. 2020, Article ID 8839047, 11 pages, 2020.

[6] Y. Wang, G. Yang, T. Li et al., "Optimal mixed block withholding attacks based on reinforcement learning," *International Journal of Intelligent Systems*, vol. 35, no. 12, pp. 2032–2048, 2020.

[7] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "Psspr: a source location privacy protection scheme based on sector phantom routing in wsns," *International Journal of Intelligent Systems*, 2021.

[8] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, "Is semi-selfish mining available without being detected?" *International Journal of Intelligent Systems*, 2021.

[9] G. Yang, Y. Wang, Z. Wang, Y. Tian, X. Yu, and S. Li, "Ipbsm: an optimal bribery selfish mining in the presence of intelligent and pure attackers," *International Journal of Intelligent Systems*, vol. 35, no. 11, pp. 1735–1748, 2020.

[10] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: anonymity for bitcoin with accountable mixes," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 486–504, Springer, Christ Church, Barbado, March 2014.

[11] X. Yu, Z. Wang, Y. Wang et al., "Impsuic: a quality updating rule in mixing coins with maximum utilities," *International Journal of Intelligent Systems*, vol. 36, no. 3, pp. 1182–1198, 2021.

[12] S. Noether, "Ring signature confidential transactions for monero," *IACR Cryptol. ePrint Arch*, vol. 1, p. 1098, 2015.

[13] Y. Li, G. Yang, W. Susilo, Y. Yu, M. H. Au, and D. Liu, "Traceable monero: anonymous cryptocurrency with enhanced accountability," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 679–691.

[14] E. B. Sasson, A. Chiesa, C. Garman et al., "Zerocash: decentralized anonymous payments from bitcoin," in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, pp. 459–474, IEEE, Berkeley, CA, USA, May 2014.

[15] G. Fuchsbauer, M. Orrù, and Y. Seurin, "Aggregate cash systems: a cryptographic investigation of mimblewimble," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 657–689, Springer, Darmstadt, Germany, May 2019.

[16] G. Betarte, M. Cristiá, C. Luna, A. Silveira, and D. Zanarini, "Towards a formally verified implementation of the mimblewimble cryptocurrency protocol," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 3–23, Springer, Rome, Italy, October 2020.

[17] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in iiot," *IEEE Transactions on Industrial Informatics*1 page, 2021.

[18] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in dwsns," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, 2020.

[19] Chen, Y. Dong, S. Li, T. Wang, Y. Zhou, and Huiyu, "Dynamic multi-key FHE in asymmetric key setting from LWE," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021.

[20] K. Wüst, K. Kostiainen, V. Čapkun, and S. Čapkun, "Prcash: fast, private and regulated transactions for digital currencies," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 158–178, Springer, Frigate Bay, St. Kitts and Nevis, February 2019.

[21] N. Narula, W. Vasquez, and M. Virza, "zkledger: privacy-preserving auditing for distributed ledgers," in *Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, pp. 65–80, Renton, WA, USA, April 2018.

[22] H. Kang, T. Dai, N. Jean-Louis, S. Tao, and X. Gu, "Fabzk: supporting privacy-preserving, auditable smart contracts in hyperledger fabric," in *Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pp. 543–555, IEEE, Portland, OR, USA, June 2019.

[23] M. Blum, A. De Santis, S. Micali, and G. Persiano, "Noninteractive zero-knowledge," *SIAM Journal on Computing*, vol. 20, no. 6, pp. 1084–1118, 1991.

[24] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: short proofs for confidential transactions and more," in *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP)*, pp. 315–334, IEEE, San Francisco, CA, USA, May 2018.

[25] J. Groth and M. Maller, "Snarky signatures: minimal signatures of knowledge from simulation-extractable snarks," in *Proceedings of the Annual International Cryptology*

Conference, pp. 581–612, Springer, Santa Barbara, CA, USA, August 2017.

[26] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Proceedings of the Conference on the Theory and Application of Cryptographic Techniques*, pp. 186–194, Springer, Santa Barbara, CA, USA, August 1986.

[27] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.