A blockchain-based certifiable anonymous E-taxing protocol

Huimin Niu1, Ting Li2, Xiugang Gong3 *

1 Research Direction for Information Security, School of Computer Science and Technology, Shandong University of Technology, Zibo, Shandong, China, 2 Research Direction for Data Mining, School of Computer Science and Technology, Shandong University of Technology, Zibo, Shandong, China, 3 Research Direction for Embedded Systems, Detection and Control Technology, School of Computer Science and Technology, Shandong University of Technology, Zibo, Shandong, China

* gong_xg@sdut.edu.cn

Abstract

The security of the tax system is directly related to the development of a country. The conventional process of tax payment laborious steps, so this process becomes a cause of irregularities among taxpayers and tax authorities, increasing the rate of corruption in tax collection. Blockchain, as a distributed ledger technology, its unique advantages and promising applications in taxation offer an effective solution to the problems of electronic taxation. However, the transparency of blockchain exists the risk of privacy disclosure, the high degree of anonymity brings the problem of lack of user supervision. Therefore, for balancing the contradiction of taxpayer privacy and supervision, we propose a blockchain-based self-certified and anonymous e-taxing scheme, which uses blockchain as the underlying support, and utilizes cryptography technology such as self-certified public key, Diffie-Hellman, to reduce the taxpayer’s reliance on the certificate authority, and protects the taxpayer’s anonymity while realizing the tracking of the real identity of malicious taxpayers. The security analysis proves that the scheme has the properties such as anonymity, conditional privacy and unforgeability, etc. Finally, performance analysis shows that compared with similar schemes, the scheme significantly improves the registration efficiency, proving its practicability and implementability.

Introduction

At present, in many countries, taxation is an important avenue for governments to raise funds to finance their projects and programmes [1]. It has become a major source of public revenue, and its healthy and stable development plays an important role in the macroeconomic regulation of the country. Consequently, providing a secured system should be our first priority. Traditional paper tax is not only tedious and inefficient, but also cannot efficiently realize the cross-territory and cross-space taxation mode. Over the years, with the development of the economy and society and the diversification of market subjects, the mode of tax collection and management keeps pace with the times. Governments have invested a lot of resources to replace the traditional paper tax collection model by adopting electronic filing, which has not
only improved tax collection efficiency but also facilitated tax compliance [2]. However, with the diversification of taxpayer types, multidimensional demand and business diversification, tax collection has also brought new challenges: the opaqueness of data worsens the asymmetry of tax information; over-reliance on centralization makes it difficult to trace the nature of things in real time across regions and subjects. If tax authorities and taxpayers do not trust each other in handling data, it will be more difficult to implement a centrally administered tax system. In particular, a recent report shows that the European Union lost 152 billion euros only in 2015 due to inadequate tax collection systems (https://news.fx678.com/201709280602501445.shtml). In recent years, some multinational companies have taken advantage of the differences in tax rates between countries to evade tax, with Alphabet’s Google transferring 15.9 billion to Bermuda Shell companies in 2016, successfully avoiding $1 billion in taxes (https://www.yicai.com/news/5388587.html). Therefore, we urgently need a more complex, efficient and scientific tax system.

With the advent of the era of big data, blockchain technology came into being and attracted wide attention from various countries. Various countries began to study how to use blockchain technology to accelerate the pace of tax collection. Blockchain is not only a new carrier to improve tax efficiency and quality, but also provides new ideas for the future development of tax collection and management. Blockchain, as a distributed database, has the characteristics of anonymity, consensus, traceability, transparency, decentralization [3]. It fits perfectly with the tax system and provides new ideas for improving tax collection efficiency, informatization of taxation and perfecting the taxation system. The specific applicability is as follows: the distributed database solves the problems of data storage space limitation and data island between different systems; the decentralization of blockchain realizes tax information sharing, overcomes the problems of difficult verification of tax information and weakening of single centralized storage; the traceability and non-tamperability of transaction data solves the problems of data dispersion and difficult query, and helps to establish an open and transparent tax database.

Blockchain-based e-tax applications are currently receiving widespread attention. In [4–6], blockchain technology has been employed to create decentralized applications that track value-added tax (VAT) transactions of businesses, which can not only effectively track whether and where VAT has been paid, but also reduce tax compliance costs for businesses and individuals, improve taxpayer compliance and the ability of tax authorities to supervise microtransactions. Moreover, Saragih and Setyowati [7] discuss the benefits of blockchain in the tax administration, and the factors affecting blockchain technology in tax administration. In the tax system applied by blockchain technology, it provides effective solutions for the problems existing in e-tax, such as tax information disclosure, tax collection and tax service. Demirhan [8] proposes to create smart contracts with different types of tax algorithms in a blockchain-based tax model, which can coordinate records between multiple parties in real time and automatically, prevent inefficient tax operations and reduce or prevent fraud among parties involved in the management chain in e-tax. Tasca et al. [9] also mention that smart contracts in blockchain technology enable the validation and automation of tax returns, significantly reducing the risk of tax avoidance, fraud and evasion. Currently, many people consider that security, privacy, costs, and regulatory issues are the greatest challenges acing the current information age [10]. Preserving user privacy is a critical issue when it comes to collecting and handling highly sensitive personal data [11]. Many academics have discussed how to use blockchain to protect user privacy in various scenarios, for example, healthcare [12, 13], vehicular ad hoc networks (VANETs), e-ticketing, etc. However, while the anonymity of blockchain protects user privacy, it also provides an umbrella for some illegal and criminal acts. For example, in blockchain-based electronic tax applications, it is unable to track illegal transactions by
linking the transaction records to the relevant traders, which makes auditing difficult and tax evasion cannot be detected and stopped in time. The open and transparent function allows any node on the network to view and supervise the tax information on the blockchain. Although it solves the problem of difficult and slow detection of counterfeit tickets, there may be unscrupulous elements to infer the taxpayer’s wallet address, identity information and lifestyle habits by analysing the tax pattern [14]. Security is the most significant one where the user’s details are highly confidential from both legal and ethical sides. Article 34 of Act No. 28 of 2007 on general provisions and procedures for taxation sets out the importance of keeping tax data confidential [7]. The provisions described in the Act show that the security of taxpayers’ data is crucial and should be seriously considered.

**Our contribution**

Based on the aforementioned challenges, the main contributions of this paper are summarized as follows.

1. We propose a blockchain-based self-certified and traceable e-taxing scheme that verifies the authenticity of taxpayers without revealing their true identity, thus balancing the contradiction of taxpayer privacy and supervision.

2. We provide a conditional privacy protection, i.e. certificate authority can track misbehaving taxpayers in e-tax and revoke the true identity of misbehaving taxpayers from causing any further damage.

3. We propose an efficient self-certified scheme that self-certified public key [15] system instead of the certificate-based public key system. The scheme not only reduces the amount of public key storage and computation, improves the registration efficiency of the system, but also reduces the security risk by reducing the dependence on the certificate authority, so that the scheme has higher security.

**Organization**

The remainder of this paper is organized as follows. First is an introduction that the necessary preparations. Next, we describes the related work, the system model and security requirements. This is followed by construction of the scheme. The next section describes the security analysis of the protocol. The conclusions of protocol are presented at the end of the article.

**Related works**

The lack of privacy protection and data leakage will raise many problems for blockchain-based e-tax systems. Some scholars have also taken measures to improve the privacy of taxpayers. Considering that efficient tax models require a trade-off between privacy and transparency, Hoffman et al. [16] propose a blockchain that can implement an access control policy by deploying a set of global smart contracts on a federal ledger managed on the chain, defining each node’s role and access to data. This policy not only solves a single point of failure for the entire system, but also avoids errors and delays in processing tax data on a global scale. Fatz et al. [17] propose a conceptual design of confidentiality and distributed tax document exchange system, stating that zero-knowledge proofs solves the dilemma between transparency and confidentiality in tax systems. Magdalena [18] achieved taxpayer anonymity by adding a serial number to the e-ticket, thus avoiding the reuse of tax slips by malicious users and tying the taxpayer’s identity information to the tax slip to prove its uniqueness. Li and Niu [19] established a federated block-based chain-based e-ticketing system that not only uses ring
signatures to achieve anonymity in a hybrid currency protocol, but also guarantees the unforgeability of tickets through multiple signatures.

Although the above scheme improve the protection of user privacy, it does not consider how to balance the contradiction between anonymity and accountability, and still face the challenge of difficult supervision. However, in the existing work, some scholars have discussed the application of balancing anonymity and traceability in other scenarios, such as, wireless body area networks (WBANs) [20], roaming service [21]. In addition, in [22] proposed conditional tracking mechanisms for VANETs, and used an efficient anonymous two-way authentication scheme. In addition, in [23] proposed an anonymous authentication scheme for wireless body area networks based on low-entropy password, which proved its security in the random oracle model. In [24] through secure authentication code transfer between the consecutive roadside unit. In fact, these anonymity schemes are based on the Diffie-Hellman problem under discrete logarithms, whereas the security of our scheme is based on the Diffie-Hellman assumption under elliptic curves, which is much more difficult than the Discrete Logarithm Problem over Finite Fields [25]. Furthermore, different from [23], the security proof in our scheme on anonymity is under the generic group model.

Preliminaries

One-Way Hash Function Assumption (OWHF)

Let $H(\cdot)$ be a one-way hash function [26]. We assume that the input of the hash function is randomly and uniformly distributed, and the output is also randomly and uniformly distributed. For given a arbitrary message $M$, it is easy to calculate $H(M)$. The following tasks are computationally infeasible:

1. Given an integer $H(M)$, it is infeasible to calculate $M$.
2. Given an integer $H(M)$, it is infeasible to find another message $M'$ satisfying that $H(M) = H(M')$.

Elliptic Curve Diffie-Hellman (ECDH)

It is a simulation of Diffie-Hellman [27] key change in a finite field and based on Elliptic Curve Discrete Logarithm Problem (ECDLP). In elliptic curve the public parameters $P$ as a generate in group $G$, given any point $(P, aP, bP) \in G$, $a, b \in [1, n - 1]$. It is difficult to compute $abP$. The advantage of adversary $A$ in solving ECDH problem is defined as:

$$\text{Adv}_{ECDH}^A(\lambda) = \Pr[abP \leftarrow (aP, bP)]$$

For any polynomial-time, no adversary $A$ can solve the ECDH problem with non-negligible advantage.

Non-interactive zero-knowledge proofs

Non-interactive Zero-knowledge Proofs (NIZK) [28] is a delicate cryptographic protocol, which usually studied in the common reference string (CRS) model.

Let $(\omega, x) \in R$ be a binary relation, where $x$ is a common reference string and $\omega$ is a witness for $x$. A prover to generate a proof and convince the verifier that he indeed knows a certain quantity $\omega$ satisfying $(\omega, x) \in R$ without leaking any additional knowledge of the secret. Informally, the NIZK satisfies the following properties [29].
Completeness. A prover can generate a proof such that it can be passed through the verification by the verifier with probability 1.

Computational soundness. No polynomial-time adversary is capable of forging a valid attestation that can be accepted by the verifier with non-negligible probability.

Zero-knowledge. The procedure only reveals the statement rather than any secret.

Smart contact

Smart contacts are automatically stored and executed in the blockchain as part of a transaction, which has a better security system than the traditional paper contacts [30]. The necessary fairness and credibility can be ensured directly through the performed partially or fully self-executing of contractual clauses.

In [31], it is discussed that the new data capabilities and possibilities of smart contract applications in tax management. In the blockchain distributed network [32], each node, i.e., the tax authority, deploys the relevant smart contract and publishes the taxpayer’s tax payment information. Then the user executes the smart contract to know the amount of tax to be paid. All the execution results are recorded as a transaction, which is irreversible and traceable. Meanwhile, each node will update the duplicate locally based on the current execution result after running the smart contract. Its secure distributed environment makes smart contract widely used in practice.

System model and security requirements

In this section, we describe the system model and system components of the blockchain-based certifiable anonymous e-taxing protocol. Then we introduce the related security requirements.

System model

As shown in Fig 1, four entities are involved in our system, namely, the certificate authority, the tax authority, the taxpayer and the smart contract.

- **Certificate Authority**, identified by CA, is mainly to initialization of system parameters. Moreover, CA is responsible for issuing certificates and maintaining the list of eligible registrations, authenticating and managing taxpayers’ identity, and revealing the true identity of misbehaved taxpayers.

- **Tax Authority**, identified by TA, deploys smart contracts and publishes the tax payment information of the corresponding taxpayer to smart contracts.

- **Taxpayer**, identified by TU, registers with CA to become a legal taxpayer and executes the smart contract to know the tax amount.

- **Smart Contract**, identified by SC, resemble the third-parties (e.g. brokers) involved in a deal, ensuring trust among the parties. Specify detailed rules for each role based on pre-determined set of conditions.

System components

A blockchain-based certifiable anonymity e-taxing protocol consists of the following polynomial-time algorithms Setup, Register, Declare, Audit and Trace.
• Setup(λ) → (PP, (P_{CA}, S_{CA}))(P_{TA}, S_{TA})). The setup algorithm is a function that takes as input a security parameter λ, and outputs the system public parameters PP, CA’s key pair (P_{CA}, S_{CA}) and TA’s key pair (P_{TA}, S_{TA}).

• Register(PP, (P_{CA}, S_{CA}), RID_i) → (ID_i, S_{TU_i}, c_i). This is an interactive protocol between a taxpayer and CA, which takes the system public parameter PP, a taxpayer’s real identifier RID_i, CA’s key pair (P_{CA}, S_{CA}) as input, and outputs the taxpayer’s pseudoidentity ID_i (i.e. tax identification number), private key S_{TU_i} and self-certified key c_i.

• Declare(PP, S_{TU_i}, P_{TA}, ID_i, M_i, T_i) → (σ_i, C_i). This is an interactive protocol between a taxpayer and TA, which takes the system public parameter PP, taxpayer’s private key S_{TU_i}, tax authority’s public key, P_{TA} taxpayer’s pseudoidentity ID_i, the tax return M_i ∈ {0, 1}^* and timestamp T_i. It outputs a signature σ_i and ciphertext C_i.

• Audit(PP, P_{CA}, ID_i, T_i, c_i, σ_i) → (0/1). The algorithms takes the system public parameter PP, the CA’s public key P_{CA}, the taxpayer’s ID_i, timestamp T_i and its self-certified key c_i, signature σ_i, ciphertext C_i as input. It outputs 1 if the tuple is valid and 0 otherwise.

• Trace(PP, S_{CA}, ID_i) → RID_i. This algorithm is performed by CA. It takes the system public parameter PP, CA’s private key S_{CA}, and the taxpayer’s pseudoidentity ID_i as input. It outputs the corresponding a malicious taxpayer’s real identifier RID_i.

Security requirements
A blockchain-based certifiable anonymous e-taxing protocol requires the following properties.
• Anonymity. Taxpayers should be kept anonymous when paying taxes, and no one can link a tax return to a true identity of taxpayer.
• Unforgeability. No one can forge taxpayer’s certificate and signature, only certified taxpayers can generate a tax return correctly.
• **Traceability.** When an illegal tax return is found, the misbehaved taxpayer’s identity can be tracked and exposed by the certificate authority.

**Anonymity.** Anonymity of a blockchain-based certifiable anonymous e-taxing protocol is an essential security property. Given a tax identification number, no adversary except CA could associate the true identity of the taxpayer with the tax identification number with non-negligible probability.

Anonymity for e-taxing schemes is defined as the following game between the Challenger $C$ and the Adversary $A$. $A$ is given access to an *register oracle*. Here $A$ is functional in two phases, a choose phase and a guess phase.

**Definition 1 (Anonymity).** A blockchain-based certifiable anonymous e-taxing protocol satisfies anonymity if for any polynomial-time adversary $A$, its advantage $\text{Adv}^\text{Anon}_A(\lambda)$ is negligible in winning the following game.

\[
\text{EXP}^\text{Anon}_A(\lambda)
\]

1. $(PP, (P_{CA}, S_{CA}), (P_{TA}, S_{TA})) \leftarrow \text{Setup}(\lambda)$
2. **Choose**

\[
(ID_1, ID_2) \leftarrow A^{\text{O}_{\text{reg}}(\lambda)}(\text{choose}, PP, RID);
\]

$j \in \{0, 1\}; \quad (A_j, ID_j) \leftarrow \text{Register}(PP, RID)$
3. **Guess**

\[
\hat{j} \leftarrow A(\text{guess}, A_j, ID_j)
\]
4. $A$ wins if $\hat{j} = j$. We denote by

\[
\text{Adv}^\text{Anon}_A(\lambda) = |Pr[A \text{ wins the game}] - \frac{1}{2}|
\]

The $ID_1, ID_2$ were not queried to *register oracle* in the choose stage.

**Unforgeability.** We now provide a rigorous definition of security by defining the *Unforgeability, Experiment*, which requires that no adversary can forge a valid signature, even if it obtain one or more certified address by compromise the CA/Taxpayer.

Unforgeability for e-taxing schemes is defined as the following game between the Challenger $C$ and the Adversary $A$. In this game, our definition is adaptive and allow the adversary to adaptively choose a tax return existing in the forgery. $A$ is given access to an *register oracle* and a *sign oracle*. Here $A$ is functional in two phases, a choose phase and a guess phase.

**Definition 2 (Unforgeability).** A blockchain-based certifiable anonymous e-taxing protocol satisfies Unforgeability if for any polynomial-time adversary $A$, its advantage $\text{Adv}^\text{Unfo}_A(\lambda)$ is negligible in winning the following game.

\[
\text{EXP}^\text{Unfo}_A(\lambda)
\]

1. $(PP, (P_{CA}, S_{CA}), (P_{TA}, S_{TA})) \leftarrow \text{Setup}(\lambda)$, and set $L \leftarrow \emptyset$, $S \leftarrow \emptyset$
2. **Choose**

\[
(ID_j, c_j) \leftarrow A^{\text{O}_{\text{reg}}(\lambda)}(\text{choose}, PP, RID); \quad \text{Update } L \leftarrow L \cup c_j;
\]

\[
\sigma_i \leftarrow A^{\text{O}_{\text{sig}}(\lambda)}(\text{choose}, PP, c_i, M_i); \quad \text{Update } S \leftarrow S \cup (c_i, M_i, \sigma_i)
\]
3. **Guess**

\[ \sigma^* \leftarrow \mathcal{A}(\text{guess}, M^*, c^*) \]

4. \( \mathcal{A} \) wins if

\[ \text{Verify}^{\text{ECDSA}}(M^*, \sigma^*) = 1 \quad \text{and} \quad c^* \notin L, \quad \text{and} \quad (c^*, M^*, \sigma^*) \notin S \]

We denote by

\[ \text{Adv}^{\text{Unfo}}(\lambda) = \Pr[\mathcal{A} \text{ wins the game}] \]

**Traceability.** Traceability for the proposed protocol is also a core security requirement, this ensures that even if all tax authority and malicious taxpayer collude, they cannot produce a signature that traces to an honest taxpayer whose personal secret key has not been learned by the adversary.

Traceability for e-taxing schemes is defined as the following game between the Challenger \( \mathcal{C} \) and the Adversary \( \mathcal{A} \). \( \mathcal{A} \) is given access to a **register oracle** and a **sign oracle**. Here \( \mathcal{A} \) is functional in two phases, a choose phase and a guess phase. \( \mathcal{A} \) corrupts a set \( \mathcal{C} \) of taxpayers adaptively.

**Definition 3 (Traceability).** A blockchain-based traceable certified e-taxing protocol satisfies traceability if for any polynomial-time adversary \( \mathcal{A} \), its advantage \( \text{Adv}^{\text{Trace}}(\lambda) \) is negligible in winning the following game.

\[ \text{EXP}^{\text{Trace}}(\lambda) \]

1. \((\mathcal{P}, (\mathcal{P}, \mathcal{C}, \mathcal{S}), (\mathcal{P}, \mathcal{S}, \mathcal{T})) \leftarrow \text{Setup}(\lambda), \text{and set} \mathcal{C} \leftarrow \emptyset.\)

2. **Choose**

\[ (ID, c) \leftarrow \mathcal{A}^{\text{Reg}(\mathcal{C}, \cdot)}(\text{choose}, \mathcal{P}, \mathcal{S}, c, c'); \]

\[ \text{Update} \mathcal{C} \leftarrow \mathcal{C} \cup \{ID, c\} \]

3. **Guess**

\[ (M', \sigma') \leftarrow \mathcal{A}^{\text{Reg}(\mathcal{S}, \cdot)}(\text{guess}, \mathcal{P}, \mathcal{P}, \mathcal{S}, \mathcal{U}, c, c'); \]

4. \( \mathcal{A} \) wins if

\[ \text{Verify}^{\text{ECDSA}}(M', \sigma') = 0; \quad (c', ID') \notin \mathcal{C} \]

\[ \text{Trace}(\mathcal{P}, \mathcal{S}, \mathcal{C}, \mathcal{S}) = \perp \]

We denote by

\[ \text{Adv}^{\text{Trace}}(\lambda) = \Pr[\mathcal{A} \text{ wins the game}] \]

**The proposed scheme**

In this section, we introduce the concrete construction of a blockchain-based certifiable anonymous e-taxing protocol. The protocol consists of five parts: **Setup, Register, Declare, Audit and Trace**.
A. System initialization

To setup the tax system, CA initializes the system parameters and generates his public/private key pair, and TA deploys the smart contract on the blockchain. Specifically, the following steps are executed.

- Pick a random \( \lambda \) as the security parameter, and \( M \in \{0, 1\}^* \) as a identifier of the tax return.
- CA chooses a cyclic group \( G_1 \) with prime order \( q \), where \( G_1 \) is generated by \( P \). TA chooses an elliptic curve \( E \) defined over \( Z_p^2 \) where \( p \) is a prime. Let \( G \in E(Z_p) \) be a base point of order \( n \) which is a prime. The reduction function be some function \( f: G \rightarrow [0, n-1] \), and \( f(R) = x_R \mod n \) where \( x_R \) is an integer representation of the \( x \)-coordinate of the elliptic curve point \( R \).
- CA selects \( S_{CA} \in Z_q^* \) at random as CA’s private key, and computes \( P_{CA} = S_{CA} \cdot P \) as CA’s public key. TA selects \( S_{TA} \in Z_q^* \) as TA’s private key, and computes \( P_{TA} = S_{TA} \cdot P \) as TA’s public key.
- CA chooses a secure hash function \( h(.) \), TA also selects a cryptographic hash \( H(.):[0, 1]^* \rightarrow [0, n-1] \) denotes as a secure hash function.

At the end of setup phase, each party keeps their own private keys, and CA preloads with the public parameters \( \{G_1, q, P, E, p, n, f, G, P_{TA}, P_{CA}, h(.), H(.)\} \).

B. User registration

A user needs to register to become a legitimate taxpayer \( TU_t \). First, taxpayer generates a random pseudoidentities(i.e. tax identification number) based on ECC, which is unique, then performs the process of registration phase based on self-certified public key.

- Taxpayer’s real identity \( RID_i \in G_1 \), each taxpayer randomly selects \( k_i \in Z_q^* \) and computes \( A_i = k_i \cdot P \), let \( ID_i^1 = h(A_i) \), and \( ID_i^2 = RID_i \oplus h(k_i \cdot P_{CA}) \cdot P \). Taxpayer’s pseudoidentity \( ID_i = (ID_i^1 \parallel ID_i^2) \), which allows only CA to reveal the real identity \( RID_i \) of taxpayer. Each taxpayer stores a pseudoidentity \( ID_i \), and sends \( \{ID_i, A_i\} \) to CA.
- CA maintain an initially-empty registry list. CA randomly selects \( k_i \in Z_q^* \) and computes the components of taxpayer’s secret keys by \( c_i = A_i + k_i \cdot P, \ e_i = h(ID_i^1 \parallel c_i), \ x_i = (k_i + e_i \cdot S_{CA}) \mod q \).

After that, CA sends the value \( x_i \) and \( c_i \) to taxpayer.
- Taxpayer computes the private keys \( x_i = (x_i \mod q) \cdot P \), and extracts public key \( y_i \) by computing the following equation

\[
y_i = c_i + e_i \cdot P_{CA}
\]

- The certified address A is the value \( h(c_i) \).
- CA adds \( \{ID_i, c_i\} \) to the maintained registry list.

The correctness of the public key derivation follows.

\[
x_i \cdot P = c_i + e_i \cdot P_{CA} = (k_i + k_i \cdot P_{CA}) \cdot P = (k_i + k_i) \cdot P + e_i \cdot P_{CA} = c_i + e_i \cdot P_{CA}
\]
C. User declaration \(TU_i\) executes the SC in the blockchain and views the corresponding tax return. The tax return \(M_i \in \{0, 1\}^*\), which we denote by \(M_i\) contains: tax payment amount, tax payment time, \(TU_i\)'s certified address \(A\), and \(TA_i\)'s address, etc.

- \(TA_i\) maintains an initially-empty users list. \(TU_i\) first proves his/her legal identity to the \(TA_i\) by sending his/her public key \(y_i\), along with a NIZK(non-interactive zero-knowledge) proof \(NIZK_i = \{(x_i, y_i = x_i \cdot P)\}\) to prove the knowledge of \(x_i\) satisfying \(y_i = x_i \cdot P\), as shown in Fig 2. If the NIZK holds, \(TA_i\) adds \((ID_i, y_i)\) to the maintained users list.

- \(TU_i\) signs on the \(M_i\), randomly selects \(d_1, 2 \in [0, n-1]\), then computes \(\sigma_1, 2\). The specific steps are as follows.

\[
\begin{align*}
R(x, y) &= d_1 \cdot G \\
\sigma_1 &= f(R) \mod n \\
\text{Hash}_i &= H(M_i, ID_i, T_i) \\
\sigma_2 &= (d_1^{-1} \cdot (\text{Hash} + x_i \cdot \sigma_1)) \mod n
\end{align*}
\]

- \(TU_i\) encrypts the \(M_i\) with the \(P_{TA_i}\), randomly selects \(d_2 \in [0, n-1]\), then computes \(C_1 = M_i + d_2 \cdot P_{TA}, C_2 = d_2 \cdot P\).

Where the signature on tax return \(M_i\) is \(\sigma_i = (\sigma_1, 2)\), the ciphertext is \(C_i = (C_1, C_2)\) and sends \((T_i, c_i, \sigma_i, C_i, NIZK_i)\) to \(TA_i\).

D. Auditing \(TA_i\) verifies the information received. First check the validity of \(TU_i\)'s certified address \(A\), then look up \(ID_i\)'s public key \(y_i\) by the maintained list. If it holds, the \(ID_i\) is an certified legal taxpayer; otherwise, this step is terminated. \(TA_i\) computes as follows.

- check that

\[A = h(c_i) \text{ and } y_i = c_i + e_i \cdot P_{CA}\]

- decrypt the tax return by computing

\[M_i = C_1 - S_{TA_i} \cdot C_2\]

- verify

\[\sigma_i = f(\sigma_2^{-1} \cdot (\text{Hash}_i \cdot G + y_i \cdot \sigma_i))\]

Fig 2. Zero-knowledge proof for legal identity.

https://doi.org/10.1371/journal.pone.0270454.g002
If the equation holds, the signature is accepted; otherwise the signature is invalid.

**E. Trace** CA traces the identity of illegal taxpayer with his private key $S_{CA}$. Consequently, the malicious taxpayer’s real identity can be easily derived by locating the registry list maintained by CA.

- Firstly, $TA$ runs the **Auditing** algorithm to verify the given signature. If the signature is invalid, it terminates.
- After $TA$ submits the illegal taxpayer's $ID$, to CA, then CA computes $RID_i = ID_i \oplus h(A_i \cdot S_{CA}) \cdot P$ by using his private key.

**Security analysis**

In this section, we describe the security analysis of proposed protocol by giving some theorem and security proofs. Theorem 1 are against the anonymity. Theorem 2 targets the identity privacy protection. Theorem 3 and 4 are against the unforgeability, and Theorem 5 are against addresses conditional privacy protection. We shall prove that the proposed schemes can satisfy these security properties and successfully withstand the corresponding attacks.

**Theorem 1.** The proposed protocol satisfies anonymity if ECDH problem and OWHF assumption holds.

**proof.** Assume that $A_{anony}$ is an adversary against the anonymity of the proposed protocol with an non-negligible probability $\lambda$ in the probabilistic polynomial time, then we can construct an example the ECDH problem $(aP, bP, abP)$, where $a, b \in Z_q^*$, the algorithm $I_{anony}$ simulate the challenger to solve the ECDH problem.

**Setup Phase.** $I_{anony}$ executes the initialization algorithm to generate system public parameters and sends to $A_{anony}$, $A_{anony}$ can operate a polynomial-bounded number of the following queries the register oracle and sign oracle while the $I_{anony}$ returns the corresponding response as follows.

**Register Phase.** Firstly, $A_{anony}$ randomly selects the identity index $i \in I_1$, where $I_1$ is a group of users, and sends to $I_{anony}$ for registration query. $I_{anony}$ calls the registration algorithm and returns $(ID_i, A_i, c_i)$. $A_{anony}$ could make at most $m$ register queries.

**Hash Query.** $I_{anony}$ will maintain a hash list, $A_{anony}$ randomly selects $Q_i$ to query the hash oracle $O_{Hash}$. If tuple $(i, Q_i, Z_i)$ exits in the hash list, then $I_{anony}$ returns the corresponding $Z_i$ as the response result. Otherwise, $I_{anony}$ returns a randomly selected element $Z_i \in Z_q^*$ as a response. Meanwhile, $I_{anony}$ will maintain a hash list and update after each query to ensure identical response to repeated hash queries. $A_{anony}$ could make at most $n$ register queries.

**Challenge Phase.** In the phase, the $A_{anony}$ chooses two taxpayer $(RID_h, RID_l)$ to request anonymity challenge. $I_{anony}$ runs register algorithm and randomly selects $j \in \{0, 1\}$ to generate corresponding $(ID_j, A_j, c_j)$, then sends $A_{anony}$.

**Guess Phase.** $A_{anony}$ outputs a bit $f$. Then $I_{anony}$ outputs $f$ as the answer to its ECDH challenge. We note that $I_{anony}$ wins the anonymity game. The probability of solving the ECDH problem with success is $Pr[I(aP, bP) \rightarrow abP] = Adv_{anony}(A_{anony}) \cdot Pr[j = f] \cdot Pr[|I(Z_i)|]$.

If $I_{anony}$ successfully solves the ECDH problem, the following conditions need to be met:

1. $A_{anony}$ correctly chose $f$, that is $Pr[j = f] = 1/2$;
2. \( Z_j \) satisfies \( (j, Q_j, Z_j) \), so \( \Pr[\mathcal{I}(Z_j)] \geq 1/n \). Then

\[
\Pr[\mathcal{I}(aP, bP) \rightarrow abP] = \text{Adv}_{\text{unfo}}(\mathcal{A}_{\text{unfo}}) \cdot \Pr[j=f] \cdot \Pr[\mathcal{I}(Z_j)] \\
\geq \lambda \cdot (1/2) \cdot (1/n) = \lambda / 2n
\]

The advantage of \( \mathcal{I}_{\text{unfo}} \) in breaking the \( \text{ECDH} \) is non-negligible, which contradicts the \( \text{ECDH} \) hypothesis, so the scheme satisfies anonymity.

**Theorem 2.** The proposed protocol satisfies identity privacy preserving if no \( \mathcal{A} \) can obtain the taxpayer’s secret identity information form the public information.

**Proof.** We will discuss our security properties in the following two different scenarios.

**Scenario 1.** This scenario occurs mainly in the registration phase, if the \( \mathcal{A} \) wants to get the components of the private key from the CA, which means \( \mathcal{A} \) needs to deduce the equation \( x_i = k'_i + e_i \cdot S_{\text{CA}} \). However, there is two unknown values \( k'_i \) and \( S_{\text{CA}} \), where \( k'_i \) is randomly and uniformly distributed, and solving the \( S_{\text{CA}} \) is comparable to solving the \( \text{ECDLP} \). Therefore, it is impossible for an adversary to get a portion of the taxpayer’s private key.

**Scenario 2.** This process occurs mainly between the \( \mathcal{A} \) and the taxpayer \( \mathcal{T}_U \), where \( \mathcal{T}_U \)'s private key \( P \). In registration phase, \( \mathcal{A} \) needs to deduce the equation \( x_i = P = c_i + e_i \cdot P_{\text{CA}} \), apparently, it is as difficult as breaking \( \text{ECDLP} \) to obtain taxpayer’s private key \( x_i \). Even though in the first scenario, the \( \mathcal{A} \) successfully obtains a portion of the \( \mathcal{T}_U \)'s private key from the CA, \( x_i = x_i + k_i \), where \( k_i \in Z_q \) is uniformly randomly distributed. Therefore, in this scenario, the probability of a successfully attacked adversary is negligible.

The proof of unforgeability in this section can be divided into certificate unforgeability and signature unforgeability.

**Theorem 3.** The proposed protocol satisfies certificate unforgeability if \( \text{ECDLP} \) assumption holds in Generic Group Model (GGM) [33]

**Proof.** Inspired by the proof of certificate unforgeability in [34], our proof is shown as follows.

**Setup Phase.** \( \mathcal{I}_{\text{cert-unfo}} \) generates public parameters by executing setup algorithm. Then it forwards the system public parameters \( PP \) to \( \mathcal{A}_{\text{cert-unfo}} \).

\( \mathcal{A}_{\text{cert-unfo}} \) can operate a polynomial-bounded number of the following queries and \( \mathcal{I}_{\text{cert-unfo}} \) returns the corresponding response as follows.

**Register Queries.** In the register phase, \( \mathcal{A}_{\text{cert-unfo}} \) randomly makes register query to the register oracle \( \mathcal{O}_{\text{reg}} \) for the public/private key pair of the taxpayer at index \( i \). The \( \mathcal{I}_{\text{cert-unfo}} \) returns \( (x_i, c_i) \) following register algorithm and maintains a list \( \varphi_i \) of coding, let the current query number of its list be \( m \). Note that in this case, the verification equation implies that \( c = \varphi(x - e \cdot S_{\text{CA}}) \), where \( e = h(ID || c) \) and \( S = x - e \cdot X \). If \( S \) is not in the list of oracle queried executed by the algorithm, augment the list by adding \( S = F_{m+1} \) at the end, and increase the number of queries \( m \) to \( m + 1 \).

**Hash Queries.** \( \mathcal{A}_{\text{cert-unfo}} \) can query the hash oracle \( \mathcal{O}_{\text{hash}} \) at any time. \( \mathcal{I}_{\text{cert-unfo}} \) returns a randomly a selected element a response. \( \mathcal{I}_{\text{cert-unfo}} \) maintains a hash list \( \mathcal{H} \) and updates \( \mathcal{H} \) after each query to ensure identical response to repeated hash queries.

**Forge.** Finally, the \( \mathcal{A}_{\text{cert-unfo}} \) forges a corresponding key pair \( (c_j, x_j) \), where \( (c_j, x_j) \) has never been queried. Let \( F_i \) be the unique appearance in the list, without loss of generality. From the hardness of \( \text{ECDLP} \), there does not exist a index \( i \) such that \( F_i = F_j \mod q \), a random
value is returned by the oracle, because $F_j$ represents a query for a new encoding at step $j$ when the encoding oracle is called. In other words, the probability of successful forgery, that $\sigma(F_j) = c_j$, is negligible. Therefore, no efficient, generic adversary forged successful if given only a polynomial number of queries.

**Theorem 4.** The proposed protocol satisfies signature unforgeability if OWHF assumption and ECDLP assumption holds.

**Proof.** Suppose that in polynomial time, an adversary $A_{sig-unfo}$ forges the valid signature of tuple $\{M_i, ID_i, T_i\}$ with an non-negligible advantage, then we can construct the algorithm $I_{sig-unfo}$ to break the ECDLP. Given an example of ECDLP question about $(P, Q = xP)$, where $P, Q \in G_q, x \in Z_q^*$, $I_{sig-unfo}$ calls adversary $A_{sig-unfo}$ as a subroutine to solve the ECDLP.

**Setup Phase.** $I_{sig-unfo}$ runs the initialization algorithm to generate the system public parameter $PP$, and sends it to $A_{sig-unfo}$. In addition, $I_{sig-unfo}$ initialize two empty lists $L_H, L_S$, where $L_H, L_S$ respectively represents the query of adversary $A_{sig-unfo}$ to hash oracle $O_{Hash}$ and signature oracle $O_{sig}$.

**Hash Queries.** $A_{sig-unfo}$ can query the hash oracle $O_{Hash}$ at any time in the form of list $\{M_i, ID_i, T_i\}$, if the list exits, $I_{sig-unfo}$ returns the form of $\{M_i, ID_i, T_i, Hash\}$ to $A_{sig-unfo}$ as the response result. Otherwise, $I_{sig-unfo}$ randomly selects element $Hash \in Z_q$ as a response, while updates the $L_H$ after each query to ensure the same response to repeated hash queries.

**Signature Queries.** $A_{sig-unfo}$ can request that $I_{sig-unfo}$ sign arbitrary messages $M_i$ of his choice, and query the signature oracle $O_{sig}$ to get the form of the list $\{M_i, ID_i, T_i, \sigma\}$, where $\sigma = (\sigma_1, \sigma_2)$. If not exists, $I_{sig-unfo}$ computes the signature of message $\{M_i, ID_i, T_i\}$ and adds the tuple $\{M_i, ID_i, T_i, \sigma\}$ to the list $L_S$. The reply message needs to meet the following equation:

$$\sigma_1 = f(\sigma_2^{-1} \cdot (Hash \cdot P + y \cdot \sigma_1))$$

**Forge.** Adversary $A_{sig-unfo}$ saves the tuple $\{M_i, ID_i, T_i, \sigma\}$ and forges a new signature of known message $\{M_i, ID_i, T_i\}$, that is, the $A_{sig-unfo}$ outputs $\{M_i, ID_i, T_i, \sigma'_i\}$ in polynomial time. Where the hash value of the message in the two signatures constructed is the same. According to the forked Lemma [35], two signatures need to satisfy:

$$d_1 \cdot P = \sigma_2^{-1} \cdot P \cdot (H(M_i, ID_i, T_i) + x \cdot \sigma_1)$$

$$d'_1 \cdot P = \sigma_2'^{-1} \cdot P \cdot (H(M_i, ID_i, T_i) + x \cdot \sigma'_1)$$

Through the above formula, we can get

$$\sigma_2 \cdot d_1 - x \cdot (\sigma_1 - \sigma'_1) = \sigma_2' \cdot d'_1$$

$I_{sig-unfo}$ needs to compute $d'_1 = (\sigma_2 \cdot d_1 - x \cdot (\sigma_1 - \sigma'_1))/\sigma_2'^{-1} mod q$, which is equivalent to solving the ECDLP problem. Therefore, there is no efficient, generic adversary $A_{sig-unfo}$ that achieves a non-negligible probability of break the signature unforgeability.

**Theorem 5.** The proposed protocol satisfies conditional privacy preserving if ECDLP assumption holds.

**Proof.** Here, we elaborate the security properties similar to traceability. Conditional privacy preserving means that honest $TU_i$ are anonymous to everyone, and malicious $TU_i$ are traced by CA. During the audit phase, the $TU_i$’s signature verification fails, the $TA$ reports to the $CA$ about the malicious $TU_i$’s identity information.
Only the CA can reveal the real identity of the taxpayer based on the unique tax identification number. The pseudoidentities $ID_i$ consists of $ID_1^i$ and $ID_2^i$, where $ID_2^i = RID_i \oplus h(k_i \cdot P_{CA}) \cdot P$. No one knows CA’s private key $S_{CA}$ unless the $A$ solves ECDLP, so no one except CA can decrypt to get the $TU_i^j$ real identity. Whenever the authentication fails, our solution could make his/her identity to be forcibly disclosed to the public in an ingenious way so as to enable the illegal actions can be avoided, thus balancing accountability and anonymity, achieving the security property of conditional privacy.

**Implementation**

In this section, we analyze its security advantages and disadvantages of the proposed protocol by comparing with other scheme. In addition, we tested the time cost of each phase in the simulation experiment, which proves its practicability and implementability.

**Safety comparison**

In the scheme proposed in [18], RSA signatures and group signatures are used to achieve identity anonymity and transaction unforgeability, but the certificate unforgeability is not provided. The scheme proposed in [19] is based on multi-signature to realize the anonymity of users and the unforgeability of transaction, which also does not have the security property of unforgeability of certificates and does not provide traceability. Combined with the security analysis of the previous section, we derive the comparison of the security performance of the three scheme. As shown in Table 1.

**Performance analysis**

1. **Environment.** We conducted the implementation on a desktop loaded with Win 10 operating system and Intel(R) Core(TM) i5–8265U CPU 1.60GHz, 8.00GB RAM. All our evaluations were performed by programs in Python language.

2. We evaluate the time cost of operations in each phase for each taxpayer, including Setup, Register, Declare, Audit, Trace, and running 100 times to take an average. As shown in Fig 3. The time cost of Setup is about 0.140s, containing system setup, CA and TA generates his key pair separately. A user who want to become a legal taxpayer has to register, which takes about 0.355s, also tested the time costed for NIZK proof is 0.253s. We evaluate the specific time consumption of each step in declare and audit phase, including signature and verify of the tax return, where the time cost is the 0.064s and 0.126s, and the encryption and decryption times were 0.198s and 0.128s respectively. Finally, the time cost of the tracing phase is 0.124s.

3. we increase the number of taxpayers to test time cost. In the registration phase, the time cost of self-certified public key technology and certificate based public key technology are compared, as shown in Fig 4. The results show that the time costs of both increase almost

| scheme  | Anonymity | Certificate unforgeability | Signature unforgeability | Traceability |
|---------|-----------|----------------------------|--------------------------|--------------|
| [18]    | Yes       | No                         | Yes                      | Yes          |
| [19]    | Yes       | No                         | Yes                      | No           |
| Our scheme | Yes       | Yes                        | Yes                      | Yes          |

https://doi.org/10.1371/journal.pone.0270454.t001
linearly with the number of users, but the self-certified public key technology is more efficient and has better performance in the multi-user case.

4. Testing the time cost of multi-user at each phase. Because the initialization algorithm is executed only once in the whole process, the implementation of the initialization algorithm with multi-user is not considered here. As shown in Figs 5 and 6, where the time consumption of each algorithm tends to increase as the number of users increases. And, in the whole scheme, the zero-knowledge proof algorithm and the encryption algorithm take longer time compared with other phase, but on the whole, the execution time of scheme have higher efficiency.
Conclusion

In this paper, we propose a blockchain-based certifiable anonymous e-taxing protocol, that guarantees the security requirements of anonymity, unforgeability, and traceability. Our scheme preserve the main merits of elliptic curve cryptography and self-certified public keys, there is no digital certificates, which reduces the reliance on certificate authority, and tax authority can implement implicit verification of certificates while verifying signatures, thus reducing security risks. In addition, the scheme takes advantage of pseudoidentities to achieve conditional privacy, further balancing anonymity and traceability. Finally, we list the security
features and some security proofs, the security analysis proves that the scheme has the properties such as anonymity, conditional privacy and unforgeability, etc. Meanwhile, the performance analysis shows that compared with similar schemes, the scheme significantly improves the registration efficiency, proving its practicability and implementability.

Supporting information
S1 File.
(ZIP)

Acknowledgments
The authors would like to thank the anonymous referees for their valuable comments.

Author Contributions
Methodology: Huimin Niu.
Supervision: Xiugang Gong.
Visualization: Ting Li.
Writing – original draft: Huimin Niu.

References
1. Faccia A, Mosteanu NR. Tax evasion information system and blockchain[J]. Journal of Information Systems & Operations Management, 2019, 13(1), 65–74.
2. Okunogbe O, Pouliquen V. Technology, taxation, and corruption: evidence from the introduction of electronic tax filing[J]. American Economic Journal: Economic Policy, 2022, 14(1):341–72.
3. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.
4. Nguyen V C, Hoai-Luan P, Thi-Hong T, et al. Digitizing invoice and managing vat payment using blockchain smart contract[C]// 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2019: 74–77.
5. Xiaoqing D, Tao L, Xiaoyuan D. Research on the intelligent settlement cloud platform of electric power materials based on the electronization of blockchain VAT special invoice[C]// 2021 China International Conference on Electricity Distribution (CICED). IEEE, 2021: 948–952.
6. Wijaya D A, Liu J K, Suwarsono D A, et al. A new blockchain-based value-added tax system[C]// International conference on provable security. Springer, Cham, 2017, 471–486.
7. Setyowati M S, Utami N D, Saraghi A H, et al. Blockchain Technology Application for Value-Added Tax Systems[J]. Journal of Open Innovation: Technology, Market, and Complexity, 2020, 6(4): 156.
8. Demirhan H. Effective Taxation System by Blockchain Technology[M]// Blockchain Economics and Financial Market Innovation. Springer, Cham, (2019), 347–360.
9. Tasca P. Insurance under the blockchain paradigm[M]// Business Transformation through Blockchain. Palgrave Macmillan, Cham, 2019: 273–285.
10. Maria A, Pandi V, Lazarus JD, et al. BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs[J]. Security and Communication Networks, 2021, 2021. https://doi.org/10.1155/2021/6679882
11. Gaurav Akshat and Psannis Konstantinos and Peraković Dragan. Security of Cloud-Based Medical Internet of Things (MIoTs): A Survey[J]. International Journal of Software Science and Computational Intelligence (IJSSCI), 2022, 14(1): 1–16. https://doi.org/10.4018/IJSSCI.285593
12. Nguyen GN, Le Viet NH, Elhoseny M, et al. Secure blockchain enabled Cyber-physical systems in healthcare using deep belief network with ResNet model[J]. Journal of Parallel and Distributed Computing, 2021, 153: 150–160. https://doi.org/10.1016/j.jpdc.2021.03.011
13. Gupta BB, Li KC, Leung V C M, et al. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system[J]. IEEE/CAA Journal of Automatica Sinica, 2021, 8(12): 1877–1890. https://doi.org/10.1109/JAS.2021.1004003
14. Au MH, Liu JK, Fang J, et al. A new payment system for enhancing location privacy of electric vehicles [J]. IEEE transactions on vehicular technology, 2013, 63(1): 3–18. https://doi.org/10.1109/TVT.2013.2274288

15. Girault M. Self-certified public keys[C]// Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1991: 490–497.

16. Hoffman M R. Can blockchains and linked data advance taxation[C]// Companion Proceedings of the The Web Conference 2018. 2018: 1179–1182.

17. Fatz F, Hake P, Fettke P. Confidentiality-preserving Validation of Tax Documents on the Blockchain [C]// Wirtschaftsinformatik (Zentrale Tracks), 2020: 1262–1277.

18. Payaras-Capellà M M, Mut-Puigserver M, Castellà-Roca J, et al. Design and performance evaluation of two approaches to obtain anonymity in transferable electronic ticketing schemes[J]. Mobile Networks and Applications, 2017, 22(6): 1137–1156. https://doi.org/10.1007/s11036-016-0732-6

19. Li X, Niu J, Gao J, et al. Secure electronic ticketing system based on consortium Blockchain[J]. KSII Transactions on Internet and Information Systems (TIIS), 2019, 13(10): 5219–5243.

20. Vijayakumar P, Obaidat MS, Azees M, et al. Efficient and secure anonymous authentication with location privacy for IoT-based WBANs[J]. IEEE Transactions on Industrial Informatics, 2019, 16(4): 2603–2611. https://doi.org/10.1109/TII.2019.2925071

21. Wei F, Vijayakumar P, Jiang Q, et al. A mobile intelligent terminal based anonymous authenticated key exchange protocol for roaming service in global mobility networks[J]. IEEE Transactions on Sustainable Computing, 2018, 5(2): 268–278. https://doi.org/10.1109/TSUSC.2018.2817657

22. Vijayakumar P, Chang V, Deborah LJ, et al. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks[J]. Future generation computer systems, 2018, 78: 943–955. https://doi.org/10.1016/j.future.2016.11.024

23. Wei F, Vijayakumar P, Shen J, et al. A provably secure password-based anonymous authentication scheme for wireless body area networks[J]. Computers & Electrical Engineering, 2018, 65: 322–331. https://doi.org/10.1016/j.compeleceeng.2017.04.017

24. Maria A, Pandi V, Lazarus JD, et al. BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs[J]. Security and Communication Networks, 2021, 2021. https://doi.org/10.1155/2021/6679882

25. Galbraith S D, Gaudry P. Recent progress on the elliptic curve discrete logarithm problem[J]. Designs, Codes and Cryptography, 2016, 78(1): 51–72 https://doi.org/10.1007/s10623-015-0146-7

26. Quynh H Dang et al. Secure hash standard[J]. 2015.

27. Gura N, Patel A, Wander A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]// International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2004: 119–132.

28. Agrawal S, Ganesh C, Mohassel P. Non-interactive zero-knowledge proofs for composite statements [C]// Annual International Cryptology Conference. Springer, Cham, 2018: 643–673.

29. Lu Y, Tang Q, Wang G. Zebralancer: Private and anonymous crowdsourcing system atop open blockchain[C]// 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS). IEEE, 2018: 853–865. https://doi.org/10.1109/TPDS.2018.2881735

30. Muh J, Laurence T. Blockchain fur Dummies[M]. John Wiley & Sons Incorporated, 2017.

31. Fiorentino S, Bartolucci S. Blockchain-based smart contracts as new governance tools for the sharing economy[J]. Cities, 2021, 117: 103325.1. https://doi.org/10.1016/j.cities.2021.103325

32. Li M, Weng J, Yang A, et al. Crowdbc: A blockchain-based decentralized framework for crowdsourcing [J]. IEEE Transactions on Parallel and Distributed Systems, 2018, 30(6): 1251–1266. https://doi.org/10.1109/TPDS.2018.2881735

33. Brown, Daniel RL. The exact security of edcsa[C]. Advances in Elliptic Curve Cryptography. 2000.

34. Atieniese G, Faonio A, Magri B, et al. Certified bitcoins[C]// International Conference on Applied Cryptography and Network Security. Springer, Cham, 2014: 80–96.

35. Pointcheval D, Stern J. Security proofs for signature schemes[C]// International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 1996: 387–398