IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 January 2024, accepted 15 February 2024, date of publication 26 February 2024, date of current version 14 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3370155

RESEARCH ARTICLE

Constructing a Secure Charity NFT Auction Platform Using Fisco Bcos Blockchain for Enhancing Transparency and Traceability

CHIN-LING CHEN[1,2], WAN-BING ZHAN[3], WOEI-JIUNN TSAUR[4,5], (Member, IEEE), DER-CHEN HUANG[6], AND LING-CHUN LIU[6]

[1]School of Information Engineering, Changchun Sci-Tech University, Changchun, Jilin 130600, China
[2]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 413310, Taiwan
[3]School of Computer and Information Engineering, Xiamen University of Technology, Xiamen, Fujian 361024, China
[4]Computer Center, National Taipei University, New Taipei City 237303, Taiwan
[5]Department of Computer Science and Information Engineering, National Taipei University, New Taipei City 237303, Taiwan
[6]Department of Computer Science and Engineering, National Chung Hsing University, Taichung 402202, Taiwan

Corresponding authors: Woei-Jiunn Tsaur (wjtsaur@mail.ntpu.edu.tw) and Ling-Chun Liu (d110056004@mail.nchu.edu.tw)

This work was supported in part by the National Science and Technology Council in Taiwan under Contract NSTC 112-2410-H-324-001-MY2 and Contract NSTC 112-2622-E-305-004.

ABSTRACT In the charity sector, fundraising and transparency have long been key issues. Charity NFT (Non-Fungible Token) auctions, an emerging charity fundraising model integrating blockchain and NFT concepts, bring opportunities and challenges. Blockchain provides distributed data integrity and transparency via cryptography-linked data blocks, while NFTs enable unique digital ownership representation. This study designs a charity NFT auction platform on the Fisco Bcos blockchain, using multi-signature algorithms to ensure NFT authenticity, ECDSA (Elliptic Curve Digital Signature Algorithm) signatures for transaction integrity and traceability, NFTs and virtual currencies to reduce costs, and IPFS (InterPlanetary File System) for storage. The implemented system achieves 2104 TPS throughput with 492-millisecond latency, increasing transaction processing with low latency. Overall, the platform aims to address charity issues like opaque fund flows, high costs, and fake initiatives through the strategic application of blockchain and NFT functionality.

INDEX TERMS Blockchain, security, InterPlanetary File System, NFT, multi-signature, ECDSA.

I. INTRODUCTION

A. BACKGROUND

The opacity of charity has been a persistent problem. It is estimated that between 4% and 6% of global charitable giving totaling $500 billion in 2022 is lost or misappropriated yearly [1]. In addition, the high cost of fundraising continues to plague the charity sector. Double the Donation's website shows charities will spend $0.21 on fundraising overhead for every dollar raised in 2022 [2]. This means nearly $105 billion is spent on fundraising rather than charity programs.

Emerging blockchain and NFT (Non-Fungible Token) technologies offer significant opportunities to improve philanthropy. Blockchain's distributed ledger and cryptographic algorithms ensure that the whereabouts and purpose of every donation are permanently and verifiably recorded [3]. This enhances the transparency and traceability of donations [4]. At the same time, smart contracts can automatically execute the donation agreement, greatly reducing manual operation costs [5]. On the other hand, NFT is the only digital asset represented on the blockchain, which provides a new fundraising channel for charitable organizations. By auctioning unique charitable NFT artworks, art collectors can be attracted to participate, and the proceeds can be directly 000used for charity [6]. Overall, blockchain and NFT provide an

The associate editor coordinating the review of this manuscript and approving it for publication was Junho Hong.

unprecedented, transparent, efficient, and open new model for philanthropy, expected to solve the long-standing problems in this field.

This paper examines the opacity problems and high fundraising costs associated with traditional charity fundraising auctions. Issues similar to those raised by BitGive have led to the application of blockchain technology to improve transparency in the charity sector. BitGive uses the Bitcoin blockchain to establish a transparent ledger to track the flow of donations, reduce administrative costs, and improve efficiency and transparency [7]. Projects such as Alice use the blockchain to allow users to track the progress of donations and achieve full transparency [8]. Both focus on the fact that the opaque flow of funds may lead to misappropriation or mismanagement of funds, which may not be used for public welfare. The high cost of fundraising auctions also seriously limits the efficiency of operating funds.

Secondly, the lack of effective connection between donors and beneficiaries in the traditional way cannot realize timely feedback and supervision, and it is also easy to false charity projects [9]. In the face of these problems, we can use the Fisco Bcos-based charitable NFT auction platform designed in this study to utilize the distributed ledger characteristics of the blockchain and encryption algorithms and other technical means to achieve transparent and traceable donation records, reduce the cost of fundraising operations, and establish a direct link between donors and beneficiaries and feedback mechanisms, to effectively solve the current dilemmas in the field of charity and indeed play the role of public welfare and charity.

B. RELATED WORKS

Traceability In recent years, research on the application of blockchain technology in the field of charity has gained significant development and presents a broad application prospect. Blockchain helps solve some of the problems in the traditional charity field through its distribution, transparency, traceability, and other technical characteristics. Shin et al. [10] proposed that blockchain technology can improve the transparency and efficiency of information sharing. It has been used to enhance the transparency of the donation platform and automation, which can help nonprofit organizations improve their operations. However, it needs to be summarized for existing organizations before proposing a specific application process. Omar et al. [11] designed a blockchain network auction solution based on Ethereum smart contracts that ensures the auction process's security, reliability, and transparency through decentralization and encryption mechanisms. However, the specific architecture of the platform is not given. Constantinides and Cartlidge [12] designed a periodic two-way auction protocol based on the Harmony blockchain using encryption and verifiable result publication to simultaneously protect order privacy and verify the correctness of the auction execution. Feki et al. [13] proposed a solution that combines the concepts of crowdfunding, donations, and philanthropic investing with the blockchain-based NFT, where smart contracts are used to manage the process of the registration, distribution, and ownership of NFTs. However, the security of the platform was not tested and analyzed. By using blockchain NFTs, Turki et al. [14] ensured and enforced data provenance and data integrity in the proposed IoT (Internet of Things) environment. Smart contracts and decentralized off-chain storage eliminate the need for middlemen and provide a trusted, secure, and immutable transaction history, but no tests have been made on system performance. Chen et al. [15] established a credit rating system based on the analytic Hierarchy Process (AHP) in the operational research theory to ensure the authenticity of the source data (not yet stored on the blockchain) on the blockchain traceability system. Through the literature of related studies mentioned in Table 1, we can identify the following pain points in the existing charity NFT auctions:

1. Non-transparent charitable auction transactions: The transaction history and prices are not open and transparent on the existing NFT auction platforms. This cannot avoid the possibility of price fraud and transaction laundering.

2. Uncertainty of ownership: buyers cannot prove ownership of the NFT, leading to copying and transaction disputes.

3. Untraceability of donations: Auction donations cannot be monitored by the general public, and there is no way to know where the donations are going or whether they are being used for other purposes.

4. High transaction costs: charitable organizations have high annual maintenance costs, which can result in spending a lot of money on maintenance.

Based on the above problems, we will use Fisco Bcos to build a coalition chain, which will establish a coalition of organizations or people related to the NFT charity auction, make all the transactions public, and determine the ownership of the NFT through digital signatures and smart contracts. IPFS stores NFT-related data; charitable tokens are issued to ensure the public can track donations; and the maintenance costs associated with direct monetary donations are reduced through NFT online auctions.

The objectives of this study that can be achieved in a traditional charity auction are as follows:

1. Design a transparent charitable NFT auction transaction system where all transactions and transaction histories are open and transparent. 2. Design a smart contract and digital signature system to ensure that all transactions and transaction histories are open and transparent.

2. Determine the unique ownership of NFTs through smart contracts and digital signatures.

3. Based on blockchain technology to achieve decentralized transactions, NFT auctions through charity tokens, user assets can be self-trusted throughout the whole process, and the money can be supervised by multiple parties to prevent money laundering and tax avoidance behavior.

The remainder of this article is organized as follows. Section II introduces the main technologies used in this system. Section III describes the main process and architecture of

TABLE 1. A comparative study of existing blockchain-based charity auction or NFT auction systems.

Authors	Year	Objective	Technologies	Merits	Demerits
Shin et al. [10]	2020	Blockchain technology can improve governance in non-profit organizations by enhancing information transparency and operational efficiency.	Blockchain Smart contract	Summarize the advantages of BitGive and AidChain and analyze how they can apply blockchain to philanthropy.	It only summarizes the existing organization without proposing a specific application process.
Omar et al. [11]	2021	This paper designs a blockchain network auction solution based on an Ethereum smart contract to ensure the auction process's security, reliability, and transparency through decentralization and encryption mechanisms.	Blockchain ETH Smart contract	The detailed algorithm is given, and the security and performance consumption are tested in detail.	The framework of the article topic platform is not discussed.
Constantinides et al. [12]	2021	A blockchain-based periodic two-way auction protocol that uses encryption and verifiable results publishing to simultaneously protect order privacy and verify the correctness of auction execution.	Harmony Blockchain ECIES	The protocol used is discussed mathematically in detail, the consumption of smart contracts is evaluated and calculated, and the deployment instructions in the harmony chain are given.	Individual users cannot thoroughly verify the execution of the auction and rely on the cooperative verification of all users.
Feki et al. [13]	2022	A platform that combines crowdfunding, donation, and philanthropic investment concepts with tokens based on blockchain-based irreplaceable Tokens (NFT) -BELONG.	Blockchain NFT Smart contract ETH	The system framework is detailed, and the platform's specific operating page and flow are given.	The platform's security is not tested, and there is no cryptography to guarantee security.
Turki et al. [14]	2023	Using blockchain Irreplaceable tokens (NFT) to ensure data provenance and data integrity.	Blockchain Smart contract NFT	Using smart contracts and decentralized off-chain storage eliminates the need for middlemen and provides a trusted, secure, and immutable transaction history.	The system's performance needs to be tested, and the security of the system encryption should be discussed in detail.
Chen et al. [15]	2023	Using the Analytic Hierarchy Process (AHP) from operations research theory, a credit rating system is established to ensure the authenticity of source data (not yet stored on the blockchain) in blockchain traceability systems.	Blockchain AHP NFT	A credit rating system is established by calculating each indicator's evaluation matrix and efficiency coefficient, enabling the assessment of user credit ratings in blockchain traceability.	It is not given which technical level of NFT the proposed method is implemented in this paper.

the system operation. Section IV performs the security analysis and Section V analyzes the performance and compares the proposed mechanism with other existing methods. Finally, we summarize our proposal in Section VI.

II. PRELIMINARY

A. FISCO BCOS BLOCKCHAIN

Blockchain technology is a distributed database technology that links transactional data in the form of blocks and uses cryptography to protect the security and immutability of the data. Fisco Bcos [16] is an open-source blockchain platform led by the China Financial Blockchain Consortium. It has the following core features:

1. High performance: Fisco Bcos adopts the BFT-DPoS (Byzantine Fault Tolerance and Delegated Proof of Stake) consensus algorithm, which enables high-performance and low-latency transaction processing for high-throughput application scenarios [17].

2. Customizability: The platform supports multiple smart contract programming languages, such as Solidity, Java, and Python, allowing developers to create and deploy smart contracts according to specific needs [18].

3. Privacy: Fisco Bcos provides multi-layered privacy protection mechanisms [19].

Fisco Bcos, as a highly customizable and secure blockchain platform, opens up many new opportunities for the charity sector. It can be applied to solve fundraising and transparency problems the charity sector faces, reduce fundraising costs, provide timely feedback, and reduce fake charity programs.

The Charity NFT Auction Platform is a promising demonstration combining blockchain and NFT technology to improve how charitable fundraising and resource allocation are done.

B. INTERPLANETARY FILE SYSTEM (IPFS)

IPFS uses a distributed storage model where files are stored in a decentralized manner on multiple nodes on the network. This distributability helps increase files' availability and resilience to failures [20]. IPFS uses a content-addressing mechanism where each file has a unique hash identifier for retrieving the file. This ensures file integrity and uniqueness and prevents data tampering [21]. Charitable organizations can use IPFS to securely store critical documents and data to ensure that files are not tampered with or lost and to protect the integrity of generous data. The distributed nature of IPFS reduces the risk of data loss, provides the long-term accessibility of charitable data, and prevents a single point of data failure [22].

In this study, we will fully utilize IPFS technology by integrating it into the Fisco Bcos-based charity NFT auction platform. By synergizing IPFS with Fisco Bcos, we aim to provide a highly secure and accessible distributed file storage solution to support the operation of the Charity NFT platform. IPFS will ensure that the data related to charity NFT is reliably stored and accessed promptly, thus improving the transparency and efficiency of charity fundraising.

C. NON-FUNGIBLE TOKEN (NFT)

NFT, or non-homogenized tokens, represents a revolutionary technology in digital assets [23]. Its core feature is irreplaceability, with each NFT's unique identity and value. This characteristic has interested NFTs in various fields [24], including charity. Artists can auction off NFTs in donation auctions, associating them with specific projects or charitable causes, ensuring that the value of each NFT flows to a clear charitable goal. This increases the transparency of the flow of funds and allows donors to know exactly where their donations are going.

In our study, NFTs will be a key core component of the charitable NFT auction platform. We will use NFTs to represent charitable projects and digital artifacts to incentivize donors to participate in and support charitable causes. These NFTs will be backed by charitable virtual currencies and securely transacted and stored via the Fisco Bcos blockchain platform, ensuring transparency and traceability of charitable projects. By integrating NFT technology into the charity sector, we aim to address transparency in charity fundraising, reduce fundraising costs, provide timely feedback, and reduce fake charity projects. This innovative approach is expected to open new opportunities for the charity sector and promote wider social engagement and support.

1) D. MULTI-SIGNATURE

Multi-signature is an important security mechanism used to improve the security of transactions and digital assets and is also applicable to a variety of blockchain application scenarios to ensure the cooperation and trust of multiple participants [25]. We use the multi-signature mechanism in the auction preparation phase, where numerous entities sign the NFTs used for the auction to ensure the authenticity of the lots. First, we explain the parameters involved in multi-signature:

(G, p, g) p is a k-bit integer, G is a cyclic group of order p, and q is a generated element of G.

H_{com}: hash function $\{0,1\}^* \rightarrow \{0,1\}^l$, is used in the commitment phase.

H_{agg}: hash function $\{0,1\}^* \rightarrow \{0,1\}^l$, is used to compute the aggregated key.

H_{sig}: hash function $\{0,1\}^* \rightarrow \{0,1\}^l$, used to compute the signature.

$L = \{pk_1 = X_1, \cdots, pk_n = X_n\}$: n public key sets.

Step 1. Key generation: each signer generates a random private key $x \leftarrow Z_p$ and computes the public key $X = g^x$.

Step 2. Signing: $\{X_1, \cdots, X_n\}$ needs to sign the message m. Take a specific signer as an example. Take a specific signer X_1 as an example, X_1 who knows the public key X_i of other cosigners.

$$(1)\ X_1 \text{Calculate } a_i = H_{agg}(L, X_i) \quad i \in \{1, \cdots, n\} \tag{1}$$

$$X = \prod_{i=1}^{n} X_i^{a_i} (X \text{ is the aggregated public key}) \tag{2}$$

X_1 generates a random number $r_1 \leftarrow Z_p$, and computes:

$$R_1 = g^{r_i} \tag{3}$$

$$t_1 = H_{com}(R_1) \tag{4}$$

Then X_1 sends t_1 to cosigners $\{X_2, \cdots, X_n\}$.

(2) When X_1 received $t_2, t_3 \cdots, t_n$ from other cosigners, send R_1 to each other.

(3) When X_1 received $R_2, R_3 \cdots, R_n$ from other cosigners, check if all of the R_i meet the requirements:

$$t_i = H_{com}(R_i) \tag{5}$$

If any $R_2, R_3 \cdots, R_n$ does not conform to the above formula, terminate the signature. Otherwise, continue:

$$R = \prod_{i=1}^{n} R_i \tag{6}$$

$$c = H_{sig}(X, R, m) \tag{7}$$

$$s_1 = r_1 + ca_1x_1 \bmod p \tag{8}$$

Send s_1 to other cosigners.

(4) Wait until $s_2, s_3 \cdots, s_n$ is received and compute:

$$s = \sum_{i=1}^{n} s_i \bmod p \tag{9}$$

Finally X_1 computes the multi-signature $\sigma = (R, s)$.

Step 3. Verification: Role $L = \{X_1, \cdots, X_n\}$, message m, and signature $\sigma = (R, s)$. The verification steps are as follows:

$$a_i = H_{agg}(L, X_i), i \in \{1, \cdots, n\} \tag{10}$$

$$X = \prod\nolimits_{i=1}^{n} X_i^{a_i} \tag{11}$$

$$c = H_{sig}(X, R, m) \tag{12}$$

$$g^s \stackrel{?}{=} RX^c \tag{13}$$

If $g^s \stackrel{?}{=} RX^c$ holds, then the verification succeeds; otherwise, it fails.

2) E. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

Even The IEEE and NIST officially adopted the elliptic curve digital signature method as a standard in the year 2000 [26]. Unlike the integer factorization problem (IFP), no subexponential time solution is available for the elliptic curve discrete logarithm problem (ECDLP). ECDLP offers several advantages, such as shorter keys, more concise signatures, and faster computation times. When it comes to utilizing Fisco Bcos, ECDSA can be employed, which helps address the challenge of limited processing and storage resources to some extent.

Assume that role A signs the message with m in the signer's capacity, role B evaluates the message's legitimacy in the verifier's capacity, and A selects the elliptic curve's parameters as $y^2 = (x^3 + ax + b) \bmod p$, p, and G. This generates the roles of an A key pair (d_A, Q_A), a private key d_A, and a public key, each of which is $Q_A = d_AG$.

A uses the following signature procedure:

1. Role A chooses a base point G and an elliptic curve $E_p(a, b)$.

2. Role A picks the numbers $k \in [1, N-1]$, which are in random order.

3. Role A does the

$$H = hash(m) \tag{14}$$

information hash calculation.

4. Role A figures out a point

$$(x, y) = kG. \tag{15}$$

5. After role A calculates

$$r = x \bmod n \text{ and } r \neq 0 \tag{16}$$

it sends role B the result of its ECDSA signature, which is

$$s = k^{-1}(H + rd_A) \bmod n \text{ and } r \neq 0. \tag{17}$$

Following is the verification procedure for B:

1. Role B calculates the m, $H' = hash(m)$ hash.

2. Role B determines

$$u_1 = s^{-1}H' \bmod n \tag{18}$$

$$u_2 = s^{-1}r \bmod n \tag{19}$$

3. Role B determines

$$(x', y') = u_1G + u_2Q_A. \tag{20}$$

4. The verification of the signature is successful if $x' = r$.

III. PROPOSED ARCHITECTURE AND METHODS

A. SYSTEM ARCHITECTURE

In this study, we will build a federated chain on Fisco Bcos and use smart contracts to implement a tamper-proof and traceable charity auction system that connects the blockchain center with storage and application modules through Remote Procedure Calls (RPC) and channels. The system architecture of this charity auction system is shown in Figure 1. The participating roles in this system include Blockchain Center (BC), Charities (C), Donors (D), Bidders (B), and Regulators (R).

1) CHARITIES (C)

Charities is one of the core participants of the charity auction combined with the blockchain, responsible for creating the charity auction project, providing relevant project information, such as charitable objectives, lots, etc., and ensuring that the funds raised are used for appropriate charitable projects. The responsibilities of charities on the blockchain include valuing the donated items to draw up the starting price; saving the digital media information of the corresponding lots to IPFS; providing reports and feedback to stakeholders or the general public; and demonstrating the use and results of the charity funds.

2) AUCTION INSTITUTION (AI)

Responsible for organizing the auction activities of the charity NFT, including setting the auction time, handling the bidding requests, and closing the auction. Confirmation of Auction Results: Confirm the participant with the highest bid at the end of the auction event and transfer the ownership of

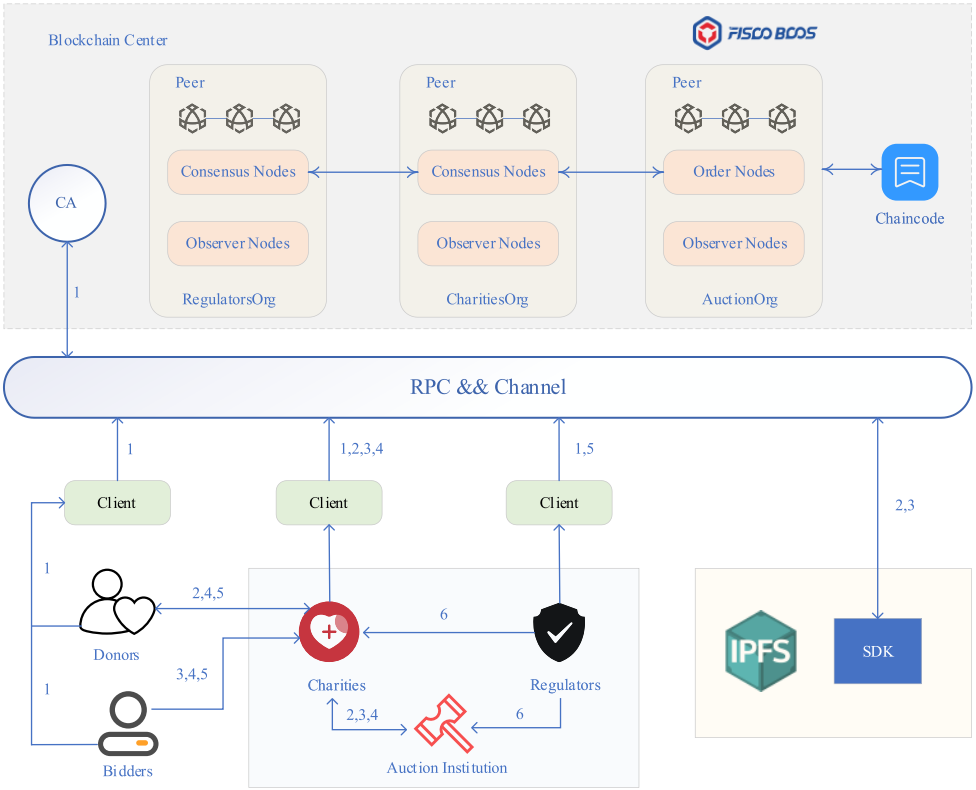

FIGURE 1. System architecture flow chart.

the NFT to the bidding winner. Transfer of Bidding Money: Transferring the bidding money to charitable organizations to support the implementation of charitable projects.

3) DONORS (D)

Donors are the parties that donate the bidding items. Their roles in the charity auction combined with blockchain include supporting auction items, such as cooperating with artists to issue NFTs and enjoying donations' satisfaction and social reputation.

4) AUCTION PARTICIPANT BIDDERS (B)

Auction participants are individuals or organizations participating in charity auctions by placing bids for items or services. Auction Participants increase auction fundraising by redeeming charity tokens to bid on items.

5) REGULATORS (R)

Regulators play a supervisory and regulatory role in charitable auctions combined with blockchain. Their responsibilities include formulating and enforcing relevant charity laws and regulations to ensure the compliance and legality of charity auctions and overseeing the behavior of charities and auction participants to prevent fraud and abuse. Review the charity auction platform transaction records to ensure their accuracy and legitimacy. Verify donation amounts and fund flow paths to ensure that donor funds are not abused or misappropriated.

6) FISCO BCOS BLOCKCHAIN CENTER (FBC)

Builds and maintains the charity auction blockchain platform, including accepting registrations for various roles, smart contracts, and charity token issuance. Track and record every donation and auction result and the flow of money used for charity, and ensure that the money is used for the designated charitable purposes.

Step 1. Registration Phase: In this phase, all entities participating in the charity auction must submit their registration information to the Certificate Authority (CA). Fisco Bcos will issue the corresponding identity certificates to the registered entities.

Step 2. Auction Preparation Stage: The charity organization creates the charity auction project, contacts potential auction donors, collects donated NFT digital collections, values the NFT lots, and stores the relevant media data of the lots, such as the set of settings, in IPFS. The auction item will be entrusted to the auction organization to start, and at the same time, the charity organization uses FBC to release charity tokens for bidding.

Step 3. Auction stage: the auction organization launches the auction on the blockchain, displaying the details of the auction items and the starting price. Bidders redeem charity

tokens and use them for bidding. The highest bidder wins the auction after the deadline.

Step 4. Asset Management Phase: Auction participants pay the appropriate amount of money based on the acquired items, and the payment transaction record is recorded on the blockchain. At the same time, the auction organization transfers the NFT token to the address of the successful bidder.

Step 5. Donation tracking phase: The auction organization sends the auction information to the charity, which can display the donation tracking information through the user interface on its application or website. This information can include the amount of money spent on each item, the identity of the bidder, the direction of the money, and reports on the progress and results of the charity's programs for the public and regulators to monitor.

Step 6. Supervision Stage: The supervisory organization supervises the whole process of the charity auction and inquires whether there are any irregularities or money laundering behaviors in the auction process.

B. NOTATIONS

The notation is illustrated in Table 2 below.

TABLE 2. Notations.

ID_X	The Identity of X
d_X	Party X's private key for the ECDSA
Q_X	Party X's public key for the ECDSA
$Cert_X$	A user X's digital certificate
k_i	The user selects a random number.
$Data_X$	Data at the heart of each transaction
NFT_{Token_D}	NFT assets belonging to D
$Auction_D$	Data on lots belonging to D
X_i	Multi-signature for user i
L	Signer's public key set
H_{Xi}	The ith hash that user X produced
H_{agg}	The hash function is used to compute the aggregated key.
H_{com}	Hash functions are used in the commit phase.
H_{sig}	The hash function is used to compute the signature.
X	public key aggregation (PKA)
M_D	Donor Donated Items Information
$Auction_D$	Auction item message
M_{Bi}	Bidder i Information
M_C	Indicates the transaction message uploaded to Hyperledger Fabric
(r_X, s_X)	The signature that user X created
C_X	Information encrypted by user X
$E_{Puk_X}(M_X)$	Use party X's public key puk_x to encrypt the message M.
$D_{Prk_X}(C_X)$	Use party X's private key prk_x to decode the message M.
T_{Sendn}	Timestamp of the message sent by the *nth* bidder in the auction phase
T_{Recn}	Timestamp of the bidding phase when the *nth* bidder message was received
ΔT	The standard for determining whether a timestamp is correct

C. REGISTRATION PHASE

At the registration stage, all participants (C, D, B, and R) involved in a charity auction must register with FBC when they first use the platform. The user fills in the information related to the registered identity through the client and then invokes Algorithm 1, which is audited by FBC's CA, which issues a digital certificate to the registered user after the audit is passed. At the same time, the system will generate the corresponding public or private key pair for the user and return it to the registered user. The registration contract includes generating public and private key pairs and digital certificates; the registration contract is shown in Algorithm 1.

We use '*Users X*' to represent the entity that needs to be registered in the blockchain network, as follows:

Step 1. The user sends registration data X to the CA node of the Fisco Bcos network through the X client.

Step 2. The CA node creates a unique private key d_X, determines the corresponding public key

$$Q_X = d_X G \tag{21}$$

by the ECDSA algorithm based on G, generates a private digital certificate $Cert_X$ based on the registration information provided by '*Users X*'and finally sends it back to the user.

Step 3. User x saves the public-private key pair $(ID_X, d_X, Q_X, Cert_X)$ generated by the system.

D. AUCTION PREPARATION PHASE

The auction preparation phase starts with donors submitting their NFT artwork as a donation item on the system. They are required to provide a detailed description of the work, the story behind the artwork or creation, as well as any relevant supporting or authentication documents and the NFT wallet address, which stores the above information via IPFS with the corresponding IPFS address when submitting the

Algorithm 1 Registration

Struct Entity:
Name ID
Address address
Public key publicKey
Private key privateKey
Digital certificate digitalCertificate
Function registerEntity:
If (mapping already has entity for caller address)
Return error: "Entity already registered."
Generate key pair and certificate:
Private key: generate a random number from the current block info
Public key: derive from a private key
Digital certificate: simple string "Sample Digital Certificate"
Store entity info in mapping:
Address: caller address
Other info: input parameters and generated key pair & certificate

FIGURE 2. IPFS example diagram.

donated item. The charity values the NFT donation; at the end of the pricing process, the donation is converted into an auction item; the charity creates an auction item to be consigned to the auction house; and AI, D, and C multi-sign the lot and its value. Multi-signature increases security: multi-signature requires multiple authorized parties to approve the transaction, which reduces the risk of a single point. Even if one private key is compromised, confirmation from the other signing parties is still required to execute the transaction, reducing the risk of potentially malicious behavior or error. Enhanced Trust: The need for multiple parties to participate and confirm reduces the risk of potential fraud, especially in the charitable sector, which is key for both donors and charities. And it is up to C to issue charity tokens through FBC. The specific steps are as follows:

Step 1. D first stores the donation details of NFT in IPFS, and then IPFS returns the address ads_{NFT} as shown in Fig 2. D submits the donation information to the system

$$M_{\text{D}} = \left(ID_D || NFT_D \left|\right| ads_{NFT} \left|\right| T1\right) \tag{22}$$

Step 2. After receiving M_D it, C accesses the details of the donated item ads_{NFT}. After verifying its authenticity, it prices and values the item and ultimately combines the pricing and C's authentication information with the donated item to form the lot information

$$Auction_D = (M_{\text{D}} || ID_C || \Pr ice) \tag{23}$$

Step 3. $\{\text{X}_D,\text{X}_C,\text{X}_{AI}\}$ Sign $Auction_D$. In this section, take X_D as an example,

$$L = \{Q_D = X_D, Q_C = X_C, Q_{AI} = X_{AI}\} \tag{24}$$

(1) X_D computes

$$a_i = H_{agg}(L, X_i), i \in n\{D, C, AI\} \tag{25}$$

$$X = \prod_{i=1}^{n} X_i^{a_i} \tag{26}$$

$\text{X}_D$chooses a random number $r_D \leftarrow Z_p$ to compute

$$R_D = g^{r_i}, t_D = H_{com}(R_D) \tag{27}$$

and then X_D sends t_D to cosigners $\{X_C, X_{AI}\}$.

(2) When X_D received $t_i \in (t_C, t_{AI})$ from the other cosigners (generated by the other participating signing actors), it is sent R_D to C and AI.

(3) When X_D receives $\{X_C, \text{X}_{AI}\}$ sent by $\{R_C, R_{AI}\}$, check whether all $t_i = H_{com}(R_i)$ meet the requirements; the checking formula is X. If any one X does not meet the checking formula, terminate this signature and generate the multi-signature only when all of them pass.

$$R = \prod_{i=1}^{n} R_i \tag{28}$$

$$c = H_{sig}(X, R, Auction_D) \tag{29}$$

$$s_D = r_D + ca_D d_D \bmod p \tag{30}$$

Then, send s_D to the other cosigners.

(4) Calculate

$$s = \sum_{i=1}^{n} s_i \bmod p \tag{31}$$

after receiving s_C, and finally, calculate the co-signature $\sigma = (R, s)$, and all the roles participating in the co-signature are calculated to be the same and unique.

Step 4. FBC creates and manages charity tokens through ERC-20 contracts, which the bidders use to bid for the lots in the subsequent phases, and sets the time of this auction $T_{Auction}$.

E. AUCTION PHASE

The auctioneer invokes Algorithm 3 on the blockchain to launch the auction, displaying details of the items up for auction and the starting price. Bidders use the charity tokens after redeeming them to bid on the auction. The highest bidder wins the auction item after the deadline.

Step 1. The AI sets the auction time $\{T_{\text{now}}, T_{Auction}\}$ and then displays the details of the auction item and the starting price

$$Auction_D = (M_{\text{D}} || ID_C || \Pr ice) \tag{32}$$

B first obtains charity tokens issued by the charity platform by exchanging fiat currencies or other cryptocurrencies, and the charity tokens will be used to pay for the auction item. At this stage, there are multiple B's, with i referring to different B's. To participate in the auction, one needs to provide the number of charitable coins held by the individual CT_{Bi},

the amount of deposit P_{Bi}, the amount of bid Bid_{Bi}, and the credentials ID_{Bi}, as well as the timestamp T_{Sendi}, as bidding information

$$M_{Bi}\,(CT_{Bi}||P_{Bi}||Bid_{Bi}||ID_{Bi}||T_{Sendi}) \tag{33}$$

Step 2. B chooses a random number k_{i1}, computes the hash value

$$H_{M_{Bn}} = hash\,(M_{Bi}) \tag{34}$$

of the bidding message and subsequently generates a signature by calling the signature function of Algorithm 2.

$$(r_{Bi}, s_{Bi}) = Sign\,(M_{Bi}, k_{i1}, d_{Bi}) \tag{35}$$

B uses the public key encryption of AI to generate the encrypted message

$$C_{Bi} = E_{Puk_{\text{FAI}}}\,(M_{Bi}) \tag{36}$$

and send it to AI.

Step 3. When AI receives the bidding information at T_{Reci} a time, it verifies the validity of the bidder's signature through the verification function of Algorithm 1.

$$H'_{M_{Bi}} = hash\,(M_{Bi}) \tag{37}$$

$$Verify\left(H'_{M_{Bi}}, r_{Bi}, s_{Bi}\right) \tag{38}$$

After verification, AI uses its private key to decrypt

$$M_{Bi} = D_{\text{Pr}\,kAI}\,(C_{Bi}) \tag{39}$$

verifies the validity of the timestamp

$$T_{Recn} - T_{Sendn} \leq \Delta\text{T} \tag{40}$$

and obtains Bi's bidding information.

Step 4. AI broadcasts Bi's bidding information; at this time, other bidders can continue to raise bids on this basis, and the bidding process follows the above two steps. Finally, the bidding closes when the next time exceeds the bidding time after.

F. ASSET MANAGEMENT PHASE

Auction participants pay the appropriate amount of money based on the acquired items, and a record of the payment transaction is recorded on the blockchain. The auction organization simultaneously transfers the attributed token of NFT to the address of the successful bidder.

Step 1. At the end of the bidding, the highest bidder needs to make a payment in charitable virtual currency. B sends the corresponding amount of charitable virtual currency to the specified wallet address. Once the payment is successful, the payment system will verify and generate the corresponding transaction record

$$M_{tra} = \{ID_{tra}, ID_B, ID_C, \text{Pr}\,ice, ads_B, ads_C, ads_{NFT}\} \tag{41}$$

The AI selects a random number k_1, calculates the hash value

$$H_{M_{tra}} = hash\,(M_{tra}) \tag{42}$$

Algorithm 2 ECDSA's Process

```
func Signature(k string, d string, H string)
(rstring,sstring){
    (x,y)=k*G
    r=x/n
    if(r!=0)
    s=(H+r*d)/k mod n
    else
    return false
return r,s
}
func Verify(H string,r string,s string)(res string){
    u1=(H mod n)/s
    u2=(r mod n)/s
    Q ←cert.PublicKey
    (x,y)=u1*G + u2*Q
}
```

Algorithm 3 Auction Contract

```
Struct Auction:
    address donor;
    address the highest bidder;
    uint the highest bid;
    uint auctionEndTime;
    bool ended;
    uint tokenId;
mapping(uint => Auction) auctions; // Map auction ID to
auction info
event AuctionStarted(uint indexed auctionId,address indexed
donor,uint indexed tokenId, uint auctionEndTime);
event HighestBidIncreased(uint indexed auctionId,address
indexed bidder,uint amount );
event AuctionEnded(uint indexed auctionId,address indexed
winner,uint amount);
address nftContract; // NFT contract address
function createAuction(uint auctionId,uint tokenId,uint bid-
dingTime
) {
 auctionEndTime = now + bidding time
 Create Auction object
 auctions[auctionId] = Auction object
 Transfer NFT from donor to contract
 Emit AuctionStarted event
}
function placeBid(uint auctionId) {
 Check bid higher than highest bid
 If old highest bid, refund old highest bidder
 highestBidder = msg.sender
 highestBid = msg.value
 Emit HighestBidIncreased event
}
```

of the transaction information and subsequently generates a signature by calling the signature function of Algorithm 1.

$$(r_{AI}, s_{AI}) = Sign\,(M_{tra}, k_1, d_{AI}) \tag{43}$$

Finally, the AI deposits the transaction record into the FBC ledger without encryption, which can be viewed and monitored by alliance chain members at any time.

Step 2. At the end of the auction, the winner is identified as the buyer who owns the NFT, and the asset transfer of the NFT is performed between the buyer and the seller. The transfer of ownership of NFTs is performed using smart contracts, as shown in Algorithm 4. The requestNFTTransfer function is used to initiate an NFT transfer request. During execution, it checks whether the seller owns the specified NFT, ensures that the contract is authorized to transfer the NFT, and then creates a TransferRequest structure containing the relevant information and stores it in the mapping transferRequests. Finally, the function emits an NFTTransferRequested event, indicating that the NFT transfer request has been submitted.

The executeNFTTransfer function is used to perform the actual transfer of the NFT. It first gets the TransferRequest structure associated with the request ID, then ensures that the NFT has not yet been transferred, checks that the message sender is the buyer, and ensures that the message value equals the transfer price. If all conditions are met, it transfers the NFT from the seller to the buyer, updates the transfer flag, and issues the NFTTransferred event to indicate that the NFT has been successfully transferred.

The cancelNFTTransfer function is used to cancel an outstanding NFT transfer request. It checks to see if the NFT has not yet been transferred by obtaining the TransferRequest structure associated with the request ID, ensures that the message sender is the seller, and then deletes the request. This function allows the seller to cancel the transaction before the transfer is complete to ensure the security and flexibility of the contract.

The smart contract can automatically perform the asset transfer after the buyer pays the corresponding price of the charity currency to C. The smart contract can be used to transfer the assets of the NFT to the seller by calling requestNFTTransfer.The buyer initiates the NFT transfer request by calling the requestNFTTransfer function and passing parameters such as the seller, buyer, NFT token ID, and price. The buyer must ensure that it has been authorized for the NFT transfer.

If the payment request is met, b calls the executeNFTTransfer function to perform the NFT transfer. The contract verifies that the buyer's payment amount matches the price requested by the FBC and executes the NFT ownership transfer. If there is no match, the FBC calls the cancelNFTTransfer function to cancel the transfer request.

G. DONOR TRACKING PHASE

The auctioneer sends the auction information to the charity, which can display the tracking information of the funds in C's books through the user interface on its application or website, which can be queried ID_{tra}. The charity can display the tracking information for the funds. This information may include the amount of money for each bid item, the identity of the bidder, the direction of the money, and a report on the progress and results of the charitable program, which C stores in the IPFS and which can be queried by the general public and the regulator through ads_{Info} in the IPFS.

Algorithm 4 NFT Transfer Contract

Struct TransferRequest:
Seller address seller
Buyer address buyer
NFT tokenId tokenId
Transfer price price
If transferred transferred
Mapping requestId => TransferRequest transferRequests
NFT contract address nftContract Function requestNFTTransfer:
Check seller owns NFT
Check contract approved to transfer NFT
Create TransferRequest
transferRequests[requestId] = TransferRequest
Emit NFTTransferRequested event
Function executeNFTTransfer:
Get TransferRequest
Check not transferred
Check msg.sender is buyer
Check msg.value equals price
Transfer NFT from seller to buyer
Update transferred flag
Emit NFTTransferred event
Function cancelNFTTransfer:
Get TransferRequest
Check not transferred
Check msg.sender is seller
Delete request

Step 1: C selects a random number k_2, calculates the hash value

$$H_{M_{don}} = hash\,(M_{don}) \tag{44}$$

of the fund usage transaction information and then generates a signature by invoking the signature algorithm.

$$(r_C, s_C) = Sign\,(M_{don}, k_2, d_C) \tag{45}$$

C Signs the fund flow information and, uploads it to the ledger, and provides a query interface for the public to query, which can be realized by calling Algorithm 5.

Step 2. D can obtain the corresponding charity currency after the charity money is used, and the charity virtual currency can be used to participate in the next charity auction. It can also encourage community participation and governance. People holding the virtual currency can participate in the decision-making process, such as voting for charitable projects, making suggestions, or participating in the governing body's decision-making to ensure the rational allocation of resources and maximize the benefits of charitable activities.

H. SUPERVISORY PHASE

The regulator supervises the whole process of a charity auction and inquires whether there is any violation or money laundering in the auction process.

Step 1. R initiates a request to view the transaction information in the chain

$$M_{req} = (ID_R || ID_{tra} || T_{send}) \tag{46}$$

Selects a random number k_3, calculates the hash value

$$H_{M_{req}} = hash\left(M_{req}\right) \tag{47}$$

of the transaction information and subsequently generates a signature by calling the signature function of Algorithm 2.

$$(r_R, s_R) = Sign\left(M_{req}, k_3, d_R\right) \tag{48}$$

R uses the public key encryption of FBC to generate the encrypted message

$$C_{req} = E_{Puk_{\mathrm{FBC}}}\left(M_{req}\right) \tag{49}$$

and send it to FBC.

Step 2. FBC receives the bidding information at the moment T_{Rec}. FBC verifies the validity of the bidder's signature through the verification function of Algorithm 2.

$$H'_{M_{req}} = hash\left(M_{\mathrm{req}}\right) \tag{50}$$

$$Verify\left(H'_{M_{req}}, r_R, s_R\right) \tag{51}$$

FBC uses its own private key to decrypt

$$M_{req} = D_{\mathrm{Pr}\,k}\left(C_{req}\right) \tag{52}$$

verifies the validity of the timestamp

$$T_{Rec} - T_{Send} \leq \Delta \mathrm{T} \tag{53}$$

and gets ID_{tra}.

Step 3. FBC returns the entire fund flow of the auction information through ID_{tra} to encapsulate it as $\mathrm{M}_{\mathrm{supervise}}$. The FBC chooses a random number k_4, computes the hash value

$$H_{M_{\mathrm{sup}\,ervise}} = hash\left(M_{\mathrm{sup}\,ervise}\right) \tag{54}$$

of the transaction message, and subsequently generates a signature by calling the signature function of Algorithm 2

$$(r_{FBC}, s_{FBC}) = Sign\left(M_{\mathrm{sup}\,ervise}, k_4, d_{FBC}\right) \tag{55}$$

FBC uses R's public key encryption to generate the encrypted message

$$C_{\mathrm{sup}\,ervise} = E_{Puk_R}\left(M_{\mathrm{sup}\,ervise}\right) \tag{56}$$

and sends it to R on time T_{sendR}.

Step 4. R receives the bidding information at the time T_{RecR}. R verifies the validity of the bidder's signature through the verification function of Algorithm 2.

$$H'_{M_{\mathrm{sup}\,ervise}} = hash\left(M_{\mathrm{sup}\,ervise}\right) \tag{57}$$

$$Verify\left(H'_{M_{\mathrm{sup}\,ervise}}, r_{FBC}, s_{FBC}\right) \tag{58}$$

Algorithm 5 Query Interface

```
import org.fisco.bcos.channel.client.Contract;
import org.fisco.bcos.web3j.protocol.Web3j;
import org.fisco.bcos.web3j.protocol.core.RemoteCall;
import org.fisco.bcos.web3j.tuples.generated.Tuple4;
import org.fisco.bcos.web3j.tuples.generated.Tuple2;
import java.math.BigInteger;
import java.util.List;
 @Override
 public
RemoteCall<List<Tuple2<String,BigInteger>>> getDona-
tionsForAuction(BigInteger auctionId) {
 return contract.getDonationsForAuction(auctionId);
}
 @Override
 Public RemoteCall<List<Tuple2<String,
BigInteger>>> getWithdrawalsForAuction(BigInteger auc-
tionId) {
 return
 contract.getWithdrawalsForAuction(auctionId);
 }}
```

R uses its private key to decrypt

$$M_{\mathrm{sup}\,ervise} = D_{\mathrm{Pr}\,k}\left(C_{\mathrm{sup}\,ervise}\right) \tag{59}$$

and verify the validity of the timestamp

$$T_{Rec} - T_{Send} \leq \Delta \mathrm{T}. \tag{60}$$

Verification $\mathrm{M}_{\mathrm{supervise}}$ of all the auction funds and processes to regulate the auction process to prevent violations or money laundering behavior.

IV. ANALYSIS

A. TRACEABILITY

The application of blockchain technology and smart contract technology helps to improve the traceability of the system. By incorporating blockchain technology into the systems of charitable organizations, the organization's details and each charitable project can be saved as tamper-proof proof.

Scenario: The public is particularly concerned about the use of funds by charitable organizations, and they track the flow of funds for each charitable project. Charities upload this critical information to the blockchain to ensure that the information cannot be tampered with.

Analysis: The public can verify whether the information provided by the charity is consistent with the original information recorded on the blockchain. The verification process is as follows:

1. The regulator sends a verification request to the charity.
2. The blockchain center returns information about a specific charity NFT auction item after verifying the validity of the request.
3. The public verifies the authenticity of the item through the validation function of Algorithm 2, thus achieving trace-

ability and sufficient transparency.

$$M_{req} = (ID_R || ID_{tra} || T_{send}) \tag{61}$$
$$H_{M_{req}} = hash\left(M_{req}\right) \tag{62}$$
$$u_1 = \mathrm{H}'_{M_{req}} s_{FCC}^{-1} \bmod n \tag{63}$$
$$u_2 = r_{FCB} s_{FBC}^{-1} \bmod n \tag{64}$$
$$(x'_{FBC}, y'_{FBC}) = u_{FBC} G + u_{FBC} Q_{FBC} \tag{65}$$

If validation fails, the charity may have altered the information. This helps donors to have a clear picture of whether their donations are being used accurately for those in need and also enables recipients to have a clear picture of whether the charitable organization has misappropriated the funds they receive. In addition, the public will be able to monitor the flow of funds for charitable organizations to ensure the transparency of their management practices. In addition, regulators can also use this information to conduct fair and impartial reviews and assessments of the operations of charitable organizations.

B. TRANSPARENCY

The transparency of Fisco Bcos ensures the fairness and integrity of charitable NFT auctions, as well as the transparency of the flow of money. All transactions and auction activities are recorded on the tamper-proof blockchain, allowing anyone to verify information, build trust, and attract more participants, including charities, donors, and NFT purchasers. Additionally, transparency helps track where donations and auction monies go, ensuring that they are used for appropriate charitable programs and reducing the risk of misuse of funds. It also assists regulators in effectively monitoring compliance, as information is publicly available to ensure that auctions comply with the law. We provide two Java interfaces generated by the Fisco Bcos Java SDK (Software Development Kit) in Section III-E that can be called for querying.

C. DATA INTEGRITY

In this paper, data integrity is ensured through hashing algorithms. First, data hashing hashes the data that needs to be protected from tampering. The hashing algorithm converts the data into a fixed-length, unique hash value that produces a different hash value even if the data is altered in a small way. Next, the hash value is stored. The calculated hash value of the data is stored on the blockchain to ensure that it cannot be tampered with. We show the verification of data integrity in table 3. Scenario: If an auction participant tries to falsify the bidding information, such as personal credentials, to conduct a fake auction, Analysis: An entity at the FBC, such as the AI, receives the bidding information and uses the validation function in Algorithm 2 to verify its authenticity. If the verification is successful, the AI will record the bidding information of the current bidder. The validation process is as follows:

$$H'_{M_{Bn}} = hash\left(M_{Bn}\right) \tag{66}$$
$$u_1 = s_{Bn}^{-1} h'_{M_{Bn}} \bmod n \tag{67}$$
$$u_2 = s_{Bn}^{-1} r_{Bn} \bmod n \tag{68}$$
$$(x'_{Bn}, y'_{Bn}) = u_1 G + u_2 G \tag{69}$$

D. TRUSTWORTHINESS

We use a multi-signature mechanism for NFT lots in the preparation phase of the auction. Multi-signatures enhance the security of charitable NFT auctions. Each transaction requires multiple authorized parties' approval, ensuring the transaction's authenticity and legitimacy. This reduces the risk of fraud and misconduct. Decentralized control and multi-signatures require multiple participants to provide authorization, which means no single controller can manipulate the entire process, ensuring the fairness of charity NFT auctions. Trust building: multi-signature creates trust in the lot as multiple independent entities must agree to the transaction. This helps build trust and attracts more participants, including charities, charitable donors, and NFT purchasers. Here is an example of the multi-signature steps he performed from the donor's perspective.

$$a_i = H_{agg}\left(L, X_i\right), R_D = g^{r_i}, t_D = H_{com}\left(R_D\right) \tag{70}$$
$$R = \prod_{i=1}^{n} R_i \tag{71}$$
$$c = H_{sig}\left(X, R, Auction_D\right) \tag{72}$$
$$s_D = r_D + c a_D d_D \bmod p \tag{73}$$
$$s = \sum_{i=1}^{n} s_i \bmod p \tag{74}$$
$$\sigma = (R, s) \tag{75}$$

E. NON-REPUDIATION

The system also applies ECDSA to ensure the non-repudiation of data. Each user uses his private key to sign the message content when sending a message. When the receiver receives the message, the sender's public key is used to verify the message's signature. If the verification is successful, the sender cannot deny the content of the message they sent. In Table 3, we describe the non-repudiation of each character in the proposed scheme. For example, in the charity tracking phase, the sender and receiver use the ECDSA signature algorithm to compute a signature

$$(r_C, s_C) = Sign\left(M_{don}, k_2, d_C\right) \tag{76}$$

using a random number k_2, a hash value

$$H_{M_{don}} = hash\left(M_{don}\right) \tag{77}$$

and a private key d_C. Then, the receiver charitable organization computes the hash value using the received message and verifies the signature. If the verification is successful, the receiver sends the message.

We show the non-repudiation description of the proposed scheme in table 4.

F. REPLAY ATTACK

During the communication process, there is a potential risk that malicious attackers may intercept the content of the communication between the sender and the receiver. These attackers may attempt to masquerade as legitimate users, spoof the system, and perform replay attacks by sending the

same content to the receiver. Replay attacks can be accomplished by the message's originator or by a hostile entity that intercepts and sends the data again.

The system employs a timestamping mechanism to defend against this type of attack. During the approval phase of a charitable project, the sender and receiver send the necessary information containing the timestamp. When the charitable organization receives the message, the timestamp is verified (e.g., timestamp). The completeness and correctness of the data can only be confirmed if the timestamp is successfully verified; otherwise, the validity of the data cannot be confirmed, thus effectively preventing the attack.

G. MAN-IN-THE-MIDDLE ATTACK(MITM)

During communication, the system ensures that public keys are not transmitted in clear text. The public keys of all users are stored on the blockchain network for easy access by all users. This practice effectively prevents the risk of an attacker intercepting the communication and then replacing the public key. For example, the sender will use the receiver's public key to encrypt the communication content, and the attacker will not be able to decrypt the content because they do not have access to the receiver's private key. The information related to each phase is detailed in Table 5.

H. NFT VALUE

NFT stands for uniqueness and scarcity, so donors can contribute one-of-a-kind assets such as digital artwork, musical works, or virtual land. Such scarcity attracts more donors because they know that their contribution is of unique value to the charitable organization. NFT is digital and global. NFTs are digital assets that can be easily transferred and stored online. This allows charitable donations to be made globally without being restricted by geographic location. This helps to expand a charity's audience. NFTs also have a strong social presence, as the NFT market attracts a wide range of attention, and donors can increase their social presence by donating NFTs to promote their charitable causes to a wider audience.

V. DISCUSSION

A. PERFORMANCE ANALYSIS

This section evaluates the performance of chaincode contract calls for the scenario presented in this study. The testing tool uses the Java SDK provided by Fisco Bcos to stress test the Fisco Bcos nodes. The Java SDK Demo of Fisco Bcos provides a contract compilation function that converts the Solidity contract file into a Java contract file. We tested an AMD R7 5800H@3.2GHz CPU with a 32GB RAM configuration. This test is mainly for querying and writing contracts to try the different performance metrics of reading data into the blockchain and writing data to the blockchain. The number of node connections is set to 4 nodes. The metrics include transactions per second, the performance bottleneck of the system in processing transactions; latency (average response time: the response time and performance bottleneck

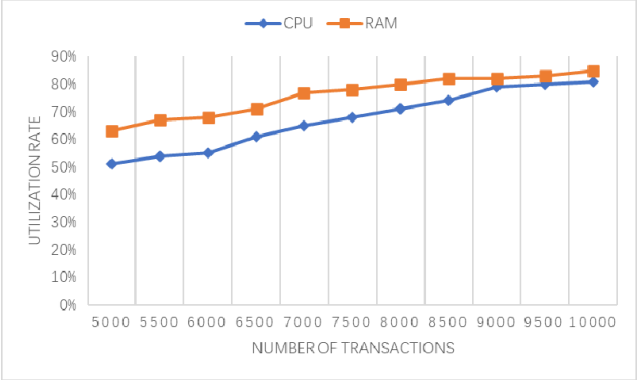

FIGURE 3. Graph of CPU and RAM usage changes.

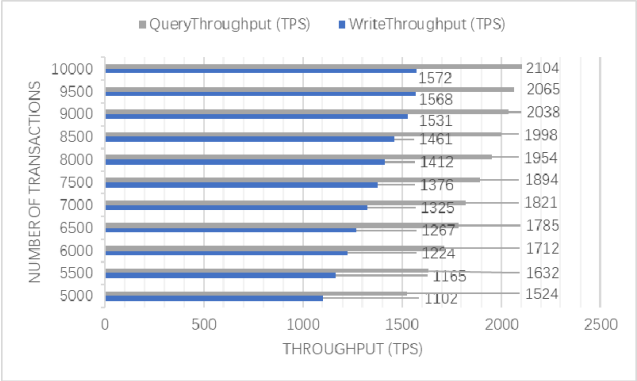

FIGURE 4. Throughput for different workloads.

of the system); resource utilization (the resource utilization and performance bottleneck of the system in processing transactions); transaction pool utilization; and block processing time.

We investigate the relationship between the number of transactions and CPU and memory consumption in Figures 3 and 4. As the number of transactions increases, we observe a gradual increase in CPU and memory usage, which suggests that the system's processing capacity may be limited as the workload increases.

Figure 4 explores the correlation between the number of transactions and throughput. It is observed that as the number of transactions increases, the number of write transactions and read transactions also increases gradually. When the number of transactions is 5000, the write transactions reach 1102 TPS (throughputs), and the read transactions reach 1524 TPS. whereas when the number of transactions increases to 10,000, the write transactions increase to 1672 TPS, and the read transactions increase to 2104 TPS.

We stress-tested Fisco Bcos, focusing on the correlation between the utilization of the trading pool and the number of trades. We gradually increased the number of trades and simulated different load scenarios to gain insight into the system's performance in the face of varying trade volumes. With the gradual increase in the number of trades, we observed a

TABLE 3. Verification of data integrity of the proposed scheme.

Item / Phase	Party: Sender	Party: Receiver	Message	Hash Value	Verification
Auction Phase	B	AI	M_{Bn}	$H_{M_{Bn}} = hash(M_{Bn})$	$Verify(H'_{M_{Bn}}, r_{Bn}, s_{Bn})$
Asset management phase	AI	FBC	M_{tra}	$H_{M_{tra}} = hash(M_{tra})$	$Verify(H'_{M_{tra}}, r_{AI}, s_{AI})$
Donor tracking phase	AI	C	M_{Don}	$H_{M_{Don}} = hash(M_{Don})$	$Verify(H'_{M_{Don}}, r_C, s_C)$
Supervisory phase	R	FBC	M_{req}	$H_{M_{req}} = hash(M_{req})$	$Verify(H'_{M_{req}}, r_R, s_R)$
	FBC	R	$M_{supervise}$	$H_{M_{supervise}} = hash(M_{supervise})$	$Verify(H'_{M_{supervise}}, r_{FBC}, s_{FBC})$

TABLE 4. Non-repudiation description of the proposed scheme.

Item / Phase	Party: Sender	Party: Receiver	Signature	Verification
Auction Preparation Phase	D	C and AI	$s_D = r_D + ca_D d_D \bmod p$	$s = \sum_{i=1}^{n} s_i \bmod p$
	C and AI	D		
Auction Phase	B	AI	$(r_{Bn}, s_{Bn}) = Sign(M_{Bn}, k_{n1}, d_{Bn})$	$Verify(H'_{M_{Bn}}, r_{Bn}, s_{Bn})$
Asset management phase	AI	FBC	$(r_{AI}, s_{AI}) = Sign(M_{tra}, k_1, d_{AI})$	$Verify(H'_{M_{tra}}, r_{AI}, s_{AI})$
Donor tracking phase	C	FBC	$(r_C, s_C) = Sign(M_{don}, k_2, d_C)$	$Verify(H'_{M_{don}}, r_C, s_C)$
Supervisory phase	R	FBC	$(r_R, s_R) = Sign(M_{req}, k_3, d_R)$	$Verify(H'_{M_{req}}, r_R, s_R)$
	FBC	R	$(r_{FBC}, s_{FBC}) = Sign(M_{supervise}, k_4, d_{FBC})$	$Verify(H'_{M_{supervise}}, r_{FBC}, s_{FBC})$

gradual increase in the utilization of the trading pool. As the transaction volume increases, more unconfirmed transactions accumulate in the pool, causing the pool to become more crowded. This may affect the processing speed of transactions and the response time of the whole system. The specific data is shown in Figure 5.

On the Fisco Bcos platform, we have deeply investigated the relationship between the number of transactions and transaction latency. The results in Figure 6 show that as the number of transactions increases, the latency tends to increase for both write and read transactions. Specifically, the minimum write latency is 682 ms and the maximum latency is 3998 ms, while the minimum read latency is 492 ms and the maximum latency is 768 ms.

These observations suggest a significant trend: as the load gradually increases, the performance capability of the Fisco Bcos system may be somewhat limited. It is worth noting that, for the same number of transactions, the latency of write transactions is generally higher than that of read transactions since write transactions involve more computational and storage operations. However, as the number of transactions continues to increase, the latency gap between write and read transactions decreases. This may imply that the system is approaching its performance limit and cannot effectively cope

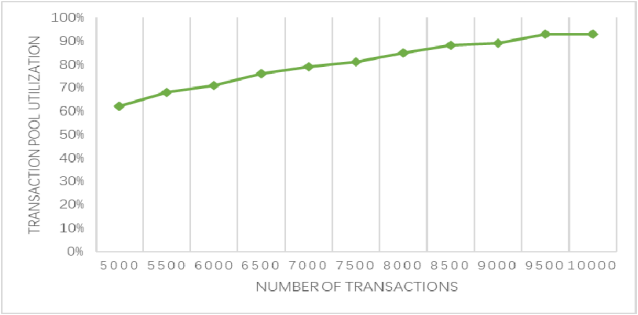

FIGURE 5. Trade pool utilization of different volumes.

TABLE 5. Prevention of man-in-the-middle attack.

Phase \ Item	Party: Sender	Party: Receiver	Encryption	Decryption
Auction Preparation Phase	D	C and AI	N/A	N/A
	C and AI	D	N/A	N/A
Auction Phase	B	AI	$C_{Bn} = E_{Puk_{\mathrm{FAI}}}\left(M_{Bn}\right)$	$M_{Bn} = D_{\mathrm{Prk}AI}\left(C_{Bn}\right)$
Asset management phase	AI	FBC	N/A	N/A
Donor tracking phase	C	FBC	N/A	N/A
Supervisory phase	R	FBC	$C_{req} = E_{Puk_{\mathrm{FBC}}}\left(M_{req}\right)$	$M_{req} = D_{\mathrm{Prk}}\left(C_{req}\right)$
	FBC	R	$C_{\mathrm{supervise}} = E_{Puk_R}\left(M_{\mathrm{supervise}}\right)$	$M_{\mathrm{supervise}} = D_{\mathrm{Prk}}\left(C_{\mathrm{supervise}}\right)$

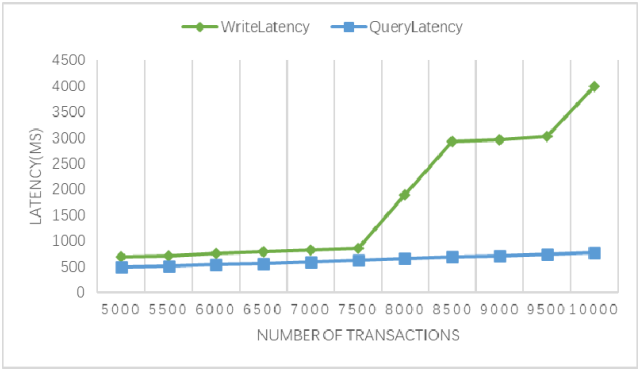

FIGURE 6. Latency with the changing workload.

with more requests, and further optimization is needed to improve processing efficiency.

B. COMPUTATIONAL COST

Firstly, we have performed a computational cost analysis for each system phase. In this process, we used asymmetric encryption to perform decryption operations, data processing using hash functions, and multiplication computation as the basic computational cost. The computational costs for each specific stage are shown in Table 6.

During the auction preparation phase, donors will perform one multi-signature, three hashes, one signature, and one signature verification operation; charities and auction institutions require to complete one multi-signature, three hashes, one signature, and one signature verification operation, respectively. In the auction phase, bidders perform one hash, one signature, and one encryption operation; auction institutions perform one hash, one signature verification, and one decryption operation. In the asset management phase, auction institutions perform one hash and one signature operation. In the donor tracking phase, charities perform one hash and one signature operation. In the supervisory phase, regulators perform two hashes, one signature, one signature verification, one encryption, and one decryption operation. The Fisco Bcos blockchain center executes two hashes, one signature verification, one signature, one encryption, and one decryption operation.

During the auction process, the highest computational costs occur mainly in the auction preparation and the supervisory phases. In the auction preparation phase, donors, charities, and auction institutions perform complex cryptographic operations such as multi-signature, hash, signature, signature verification, etc., which leads to higher computational costs. On the other hand, the supervisory phase involves regulators and Fisco Bcos blockchain center performing multiple hashing, signing, signature verification, encryption, and decryption operations to ensure regulatory security and transparency, further increasing computational costs.

C. COMPARISON

In this section, we will compare our proposed scheme with other previous systems and present the results in Table 7. Through the comparison, we can see that our scheme has corrected the deficiencies that existed in the previous systems.

Shin et al. [10] proposed that blockchain technology can improve the transparency and efficiency of information sharing and has been used to enhance the transparency and automation of donation platforms, which can help non-profit organizations improve their operations. However, it did not provide specific organizational structures and processes and did not specify what kind of sound regulatory feedback mechanism. Omar et al. [11] proposed an auction system framework based on Ethereum smart contracts, decentralized storage systems, and trusted prophecy machines, which utilized smart contracts to realize automation and disintermediation in the auction process while ensuring data security, traceability, and transparency. But there is no regulation or feedback mechanism involved. Constantinides and Cartlidge [12] proposed a framework for a double auction system based on blockchain technology, which can be applied to various periodic double auction mechanisms and can be

TABLE 6. Computational cost of the proposed scheme.

Item / Phase	1st Role	2nd Role
Auction Preparation Phase	D: $T_{Mul\text{-}sig}+3T_H+1T_{Sig}+1T_{Ver}$	C and AI: $2T_{Mul\text{-}sig}+6T_H+2T_{Sig}+2T_{Ver}$
Auction Phase	B: $1T_H+1T_{Sig}+1T_{Enc}$	AI: $1T_H+1T_{Ver}+1T_{Dec}$
Asset management phase	AI: $1T_H+1T_{Sig}$	N/A
Donor tracking phase	C: $1T_H+1T_{Sig}$	N/A
Supervisory phase	R: $2T_H+1T_{Sig}+1T_{Ver}+1T_{Enc}+1T_{Dec}$	FBC: $2T_H+1T_{Ver}+1T_{Sig}+1T_{Dec}+1T_{Enc}$

Notes: $T_{Mul\text{-}sig}$: time needed for multi-signature operation. T_H: time needed for hash function operation. T_{Dec}: time needed for decryption operation. T_{Enc}: time needed for encryption operation. T_{Sig}: time needed for signature generation. T_{Ver}: time needed for signature verification.

TABLE 7. Comparisons among existing charity donation system surveys.

Author	Year	1	2	3	4	5	6	7
Shin et al. [10]	2020	Y	Y	N	Y	Y	N	N
Omar et al. [11]	2021	Y	Y	Y	Y	Y	N	N
Constantinides et al. [12]	2021	Y	N	Y	Y	Y	Y	N
Feki et al. [13]	2022	Y	Y	Y	Y	Y	N	N
Turki et al. [14]	2023	Y	Y	Y	Y	Y	Y	N
Chen et al. [15]	2023	Y	N	N	Y	Y	N	N
Ours	2023	Y	Y	Y	Y	Y	Y	Y

Notes: 1: Blockchain-focused, 2: smart contracts, 3: Putting forward the system framework, 4: Traceability, 5: Unforgeability, 6: Providing supervision mechanism, 7: Providing online feedback and evaluation. Y: Yes, N: No.

easily transformed into a commercial system where traders can verify the correctness of the auction mechanism, thus providing a supervision mechanism. However, there is no detailed description of smart contracts and no feedback mechanism. Feki et al. [13] proposed the BELONG platform architecture and smart contracts for managing NFT registration, distribution, and ownership, as well as the unforgeability of NFT and tracking of fund use, without providing supervision or feedback mechanisms. Turki et al. [14] proposed to eliminate the need for middlemen by using smart contracts and decentralized off-chain storage to ensure and enforce the use of blockchain irreplaceable tokens in the proposed IoT environment, but it did not make an online feedback mechanism. Chen et al. [15] proposed a credit rating system based on AHP (Analytic Hierarchy Process) and discussed the application of blockchain in the traceability system and supervision mechanism, but this system did not directly involve ‘‘unforgeability’’ and ‘‘online feedback and evaluation’’ and did not elaborate on the system architecture and smart contracts.

Our proposed mechanism ensures open and transparent access to all transactions and transaction histories. We introduce smart contracts and digital signature systems to ensure NFT's unique ownership and strengthen transaction histories' transparency. By leveraging blockchain technology for decentralized transactions, we auction NFT through charitable tokens, enabling users' assets to trust themselves throughout the process. This system enables multi-party supervision and effectively prevents money laundering and tax avoidance. At the same time, we provide a detailed architectural solution flow to ensure the understandability and operability of the system.

VI. CONCLUSION

Through this research, we have successfully designed and implemented a charity NFT auction trading system based on

Fisco Bcos blockchain, IPFS, multi-signature, and ECDSA, introducing a higher level of transparency, credibility, data accuracy, traceability, and non-repudiation of transactions to the charity field. Our research results include innovations in transparent auction trading systems, ensuring open and transparent transaction histories, protecting the unique ownership of NFT through smart contracts and digital signature systems, enhancing performance with IPFS, ensuring accurate information by multi-signature, and enabling traceability and non-repudiation of transactions by ECDSA signatures.

In future work, we expect to expand the application areas of the charity NFT auction trading system, enhance the functionality and adaptability of smart contracts, promote interoperability between different blockchain platforms, strengthen the protection of security and privacy, focus on the social impact of charitable behavior, and further improve regulatory compliance. Through continuous technological innovation and comprehensive consideration of the needs of all parties, we will strive to build a more just, transparent, and efficient charity ecosystem and contribute more possibilities to the sustainable development of social welfare undertakings.

REFERENCES

[1] (2023). *CivilSociety*. Accessed: Nov. 25, 2023. [Online]. Available: https://www.civilsociety.co.uk/news/charity-fraud-losses-up-44-in-2022-data-shows.html

[2] (2023). *Double the Donation*. Accessed: Nov. 25, 2023. [Online]. Available: https://doublethedonation.com/nonprofit-fundraising-statistics/

[3] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017, doi: 10.1007/s12599-017-0467-3.

[4] M. S. Farooq, M. Khan, and A. Abid, "A framework to make charity collection transparent and auditable using blockchain technology," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106588, doi: 10.1016/j.compeleceng.2020.106588.

[5] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020, doi: 10.1016/j.future.2019.12.019.

[6] L. Ante, "The non-fungible token (NFT) market and its relationship with bitcoin and ethereum," *FinTech*, vol. 1, no. 3, pp. 216–224, Jun. 2022, doi: 10.3390/fintech1030017.

[7] (2023). *Bitgive*. Accessed: Nov. 25, 2023. [Online]. Available: https://www.bitgivefoundation.org/

[8] (2023). *Alice*. Accessed: Nov. 25, 2023. [Online]. Available: https://alice.si/

[9] O. Stapleton, L. N. Van Wassenhove, and R. Tomasini, "The challenges of matching corporate donations to humanitarian needs and the role of brokers," *Supply Chain Forum, Int. J.*, vol. 11, no. 3, pp. 42–53, Jan. 2010, doi: 10.1080/16258312.2010.11517239.

[10] E.-J. Shin, H.-G. Kang, and K. Bae, "A study on the sustainable development of NPOs with blockchain technology," *Sustainability*, vol. 12, no. 15, p. 6158, Jul. 2020, doi: 10.3390/su12156158.

[11] I. A. Omar, H. R. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Implementing decentralized auctions using blockchain smart contracts," *Technol. Forecasting Social Change*, vol. 168, Jul. 2021, Art. no. 120786, doi: 10.1016/j.techfore.2021.120786.

[12] T. Constantinides and J. Cartlidge, "Block auction: A general blockchain protocol for privacy-preserving and verifiable periodic double auctions," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 513–520, doi: 10.1109/Blockchain53845.2021.00078.

[13] E. Feki, K. Boukadi, F. Loukil, and M. Abed, "BELONG: Blockchain based platform for donation & social project funding," in *Proc. IEEE/ACS 19th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Dec. 2022, pp. 1–8, doi: 10.1109/AICCSA56895.2022.10017836.

[14] M. Turki, S. Cheikhrouhou, B. Dammak, M. Baklouti, R. Mars, and A. Dhahbi, "NFT-IoT pharma chain: IoT drug traceability system based on blockchain and non fungible tokens (NFTs)," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 35, no. 2, pp. 527–543, Feb. 2023, doi: 10.1016/j.jksuci.2022.12.016.

[15] C. Chen, H. Huang, B. Zhao, D. Shu, and Y. Wang, "The research of AHP-based credit rating system on a blockchain application," *Electronics*, vol. 12, no. 4, p. 887, Feb. 2023, doi: 10.3390/electronics12040887.

[16] (2023). *Fisco Bcos*. Accessed: Nov. 25, 2023. [Online]. Available: https://fisco-bcos-documentation.readthedocs.io/zh-cn/latest/

[17] H. Li, Y. Chen, X. Shi, X. Bai, N. Mo, W. Li, R. Guo, Z. Wang, and Y. Sun, "FISCO-BCOS: An enterprise-grade permissioned blockchain system with high-performance," in *Proc. Int. Conf. High Perform. Comput., Netw., Storage Anal.*, Nov. 2023, pp. 1–17, doi: 10.1145/3581784.3607053.

[18] M. Ren, F. Ma, Z. Yin, Y. Fu, H. Li, W. Chang, and Y. Jiang, "Making smart contract development more secure and easier," in *Proc. 29th ACM Joint Meeting Eur. Softw. Eng. Conf. Symp. Found. Softw. Eng.*, Aug. 2021, pp. 1360–1370, doi: 10.1145/3468264.3473929.

[19] J. Huang, T. Huang, H. Wei, J. Zhang, H. Yan, D. S. Wong, and H. Hu, "ZkChain: A privacy-preserving model based on zk-SNARKs and hash chain for efficient transfer of assets," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 12, pp. 1–11, Dec. 2022, doi: 10.1002/ett.4709.

[20] (2023). *IPFS*. Accessed: Nov. 25, 2023. [Online]. Available: https://ipfs.tech/

[21] D. Saraswat, F. Patel, P. Bhattacharya, A. Verma, S. Tanwar, and R. Sharma, "UpHaaR: Blockchain-based charity donation scheme to handle financial irregularities," *J. Inf. Secur. Appl.*, vol. 68, Aug. 2022, Art. no. 103245, doi: 10.1016/j.jisa.2022.103245.

[22] N. S. Sirisha, T. Agarwal, R. Monde, R. Yadav, and R. Hande, "Proposed solution for trackable donations using blockchain," in *Proc. Int. Conf. Nascent Technol. Eng. (ICNTE)*, Jan. 2019, pp. 1–5, doi: 10.1109/ICNTE44896.2019.8946019.

[23] H. Nobanee and N. O. D. Ellili, "Non-fungible tokens (NFTs): A bibliometric and systematic review, current streams, developments, and directions for future research," *Int. Rev. Econ. Finance*, vol. 84, pp. 460–473, Mar. 2023, doi: 10.1016/j.iref.2022.11.014.

[24] M. Nadini, L. Alessandretti, F. Di Giacinto, M. Martino, L. M. Aiello, and A. Baronchelli, "Mapping the NFT revolution: Market trends, trade networks, and visual features," *Sci. Rep.*, vol. 11, no. 1, pp. 1–11, Oct. 2021, doi: 10.1038/s41598-021-00053-8.

[25] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme," in *Proc. Public Key Cryptogr. (PKC)*, 2003, pp. 31–46, doi: 10.1007/3-540-36288-6_3.

[26] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001, doi: 10.1007/s102070100002.

CHIN-LING CHEN received the Ph.D. degree from National Chung Hsing University, Taiwan, in 2005. From 1979 to 2005, he was a Senior Engineer with Chunghwa Telecom Company Ltd. He is currently a Distinguished Professor. He has published more than 170 articles in SCI/SSCI international journals. His research interests include cryptography, network security, and electronic commerce.

WAN-BING ZHAN is currently pursuing the master's degree in electronic information and computer technology with the School of Computer and Information Engineering, Xiamen University of Technology. His main research interests include blockchain supply chain traceability, cryptography, and information security.

WOEI-JIUNN TSAUR (Member, IEEE) received the Ph.D. degree in electrical engineering from the National Taiwan University of Science and Technology, Taiwan, in 1998. From 1994 to 2003, he was a Project Manager and a Technology Consultant with the Research and Development Division, Syscom Computer Engineering Company, a research center of software development in Taiwan. From 2010 to 2015, he was a Distinguished Professor with the Department of Information Management, Da Yeh University, Taiwan. Since 2016, he has been with the Computer Center, National Taipei University, Taiwan, where he is currently a Distinguished Professor. His research interests include blockchain, network security, artificial intelligence applications, and information security management.

DER-CHEN HUANG received the B.S. degree in electronic engineering from Feng Chia University, Taiwan, in 1983, the M.S. degree in computer engineering from Florida Institute of Technology, USA, in 1991, and the Ph.D. degree in computer engineering from the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan, in 2000. From 1983 to 1989, he was a Design Engineer with the Computer Communication Laboratory (CCL)/Industrial Technology Research Institute (ITRI) and Chung-Shan Institute and Science of Technology (CSIST) when he was assigned to a partnership project with General Dynamics, Fort Worth, TX, USA. He was an Associate Professor with the Department of Electronic Engineering, National Chin-Yi Institute of Technology, Taichung, Taiwan, from 1991 to 2004. In 2004, he joined the Department of Computer Science and Engineering, National Chung Hsing University, Taichung. He was the Director of the Computer and Information Center, National Chung Hsing University, from 2007 to 2011. He is currently a Full Professor with National Chung Hsing University. His research interests include VLSI design for testability and diagnosis, communication, security, and image and artificial intelligence. He was a member of the Editorial Board of *Journal of Internet Technology*. He received the Best Paper Award from the 5th International Conference on Future Information Technology, South Korea, in 2010. He served as a reviewer for various technical journal and conferences.

LING-CHUN LIU is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, National Chung Hsing University. Her research interests include blockchain application, cryptography, blockchain of things, and information security.