IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 23 November 2022, accepted 9 December 2022, date of publication 12 December 2022,
date of current version 19 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3228787

APPLIED RESEARCH

Toward Achieving Anonymous NFT Trading

ZHANWEN CHEN[1] AND KAZUMASA OMOTE[1,2]
[1]Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8573, Japan
[2]National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan

Corresponding author: Zhanwen Chen (s2130132@s.tsukuba.ac.jp)

This work was supported by JSPS KAKENHI under Grant JP22H03588 and Grant JP22K19768.

ABSTRACT With the rapid development of Non-Fungible Token (NFT) market, various types of digital artwork are published via NFT in recent years for sale. In the current NFT system, owner's address of each NFT is stored in plaintext. This leads to a severe privacy problem: once a person's blockchain address is known, all his NFT assets are viewable, which may further cause problems related to the privacy of holding sensitive NFT or premeditated scams to high-value NFT owners. However, due to the limitation of Ethereum and smart contract, it is hard to prevent others from tracking the owner of NFT. Meanwhile, current state-of-the-art NFT research usually assumes the relation between blockchain address and owner's identity is unknown, thus creating the *so-called anonymity*. In this paper, based on the most popular NFT marketplace OpenSea's system, we propose a new exchange scheme to hides the address of NFT owner during trading. To achieve our goal, a proof of commitment scheme is exploited to bind the owner to an NFT while hiding the identity. Moreover, An anonymous payment method is designed to prevent attackers from tracing the Ether flow in NFT trading. Our scheme is proven to be secure against curious users and malicious active attackers. Implementation on testnet also shows that the increased gas cost is acceptable, meaning it is suitable for application.

INDEX TERMS Non-fungible token, owner privacy, blockchain, security.

I. INTRODUCTION

A. BACKGROUND

Non-Fungible Token (NFT) is a special type of cryptocurrency token that is first proposed by Ethereum team in their improvement proposal EIP-721 [1] and is then developed by EIP-1155 [2]. Unlike the previous ERC-20 token, which enables users to mint new cryptocurrency by leveraging Ethereum, EIP-721 proposes the idea of non-fungibility for minting a token. The most significant difference between NFT and other cryptocurrencies is that for cryptocurrencies like Ether, all the coins are equivalent and can be exchanged based on a fixed rate. For example, Alice's 1 Ether is equivalent to Bob's 1 Ether. And Alice can also separate her 1 Ether into several parts of change and only spend 0.1 Ether during a transaction. But things are different for NFT. An NFT is a token generated by a smart contract. Each NFT is represented by a unique token ID, and a corresponding smart contract records the only owner address of each NFT. Inside an NFT, there are generally two main components: One is called the Metadata, which contains JSON data that indicates a URI (Universal Resource Identifier) and other relevant information. In this way, one NFT refers to an online file, which can be a picture, music, video, virtual sportsman cards, items in online games, etc. The referred data give value to an NFT in its marketplace. Another component of NFT is a set of functions that supports returning the owner of a given token ID, and transferring the ownership to another address if the message sender is the current owner.

With the mushrooming of the NFT market in recent years, a growing trend of attention from individuals, industries, and academies is easily observed in recent years. In 2021, an NFT auction by Christie's auction house sold an NFT digital collage of artist Mike Winkelmann for $69.3 million [3], which breaks the record of Christie's. During the same year, the NFT market grew up to over $800 million of total traded volume within less than half a year by May, 2021 [4]. Apart from the commercial aspects, research around the NFT technology is also increasing. For example, Bal et al. proposed a non-fungible token tracking proof-of-concept based on

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

Hyperledger Composer and Hyperledger Fabric Blockchain [5]. However, research on the properties and value of NFT as a commodity is still mainstream compared with NFT-related technical research. Consequently, the development of NFT is still in its initiation phase, and it can be seen that NFT is still a prototype to be perfected.

B. PRIVACY PROBLEM OF NFT

From the perspective of security, We have observed a serious flaw in NFT that is currently being ignored and unaddressed. That is the privacy of NFT ownership. Currently, most NFT is highly embedded in the Ethereum blockchain since the mint and exchange of NFT are executed by its smart contract. To create a new NFT collection, one must design and deploy a smart contract in Ethereum so that EVM (Ethereum Virtual Machine) can execute it. Despite different methods of implementing NFT contracts, there must exist a ''list'' that stores all the existing token IDs with their owners. This raises the concern of owner-privacy: Blockchain is usually considered to provide a sense of anonymity since the link between a blockchain address and the owner's real-world identity is unknown, while in real-world financial systems an authority like the bank knows the account number of its customer. However, this anonymity is quite *fragile* when considering practical situations. One typical instance is that suppose Alice and Bob are real-world friends. One day, Alice transfers some Ether to Bob's account to pay for a dress she asked Bob to buy for her during his travel to a foreign country. In that case, Alice and Bob get to know each other's blockchain addresses. Furthermore, they can easily view all NFT assets possessed by each other via blockchain explorers like Etherscan. Another example is the blockchain-based payment of smart devices. There has been a great deal of research about this area [6], [7]. That is, if a person uses cryptocurrency in a real-world payment like shopping in a store, the relation between a blockchain address and a user is easily observed by the merchant, which may be later leaked to the public. Then, in the same way, people can view your NFT assets.

Although it appears that the exposure of NFT owners does not cause a heavy impact at first look, there are potential security concerns about it. For instance, if the buyer of a $69.3 million-worthy NFT artwork is known, Internet scammers can lock the target and commit fraud. Moreover, even if fraud is not considered, it is the owners' right to hide their personal belongings if they think it is sensitive. Take reality as an example, one may be willing to tell other people about his bank account for money transfers, but that does not mean he allows others to see what he has paid for using this account.

Despite many cryptographic papers investigating anonymous ownership transfer schemes, this problem faces different requirements in NFT [8]. For example, anonymous ownership transfer is widely studied in RFID systems [9], [10]. Many PKI schemes also aim at achieving anonymity (E.g. group signature [11]). But none of them are applicable for NFT. The most significant difference between NFT and other studies' circumstances is that all message interactions in Ethereum are recorded and viewable, and it is impossible to establish a session key with smart contract and conceal secret information. However, it is difficult to find an effective solution to the aforementioned problem. Therefore, we intend to do it ourselves to help the development of NFT technology.

Regarding NFT, most transactions happen in NFT marketplaces. The marketplaces provide a platform for sellers to list their NFT so that buyers can check. At present, OpenSea is the most popular NFT marketplace globally. It achieves NFT trading by using Wyvern protocol,[1] a third-party digital assets exchange protocol contract deployed on Ethereum. Wyvern ensures that the marketplaces have no way to interfere with the trading process. And the ownership of NFT is directly transferred to the buyer without going through the marketplace. We wish to propose a smart contract-based solution that is applicable to the current NFT trading mode without the requirement of modifying the blockchain itself.

C. OUR CONTRIBUTION

The contribution of this paper is listed as follows:

1) Based on the design of OpenSea's system, we propose a new NFT trading scheme that hides the identity of NFT owner to achieve anonymity even though the relationship between a user and his blockchain address is public.
2) Our new scheme is compatible with the existing NFT trading smart contract and its trading mode (non-anonymous) but adds the new option of anonymous trading.
3) In anonymous trading, there is a negligible possibility for a malicious attacker to trace the NFT owner's blockchain address based on publicly viewable information in the blockchain.
4) Our new scheme can be easily implemented by modifying the current system and adding necessary security-related contract codes. In evaluation, we give a proof-of-concept implementation of our scheme. And our scheme is proven to merely increase an acceptable additional transaction fee. Compared with the benefit it brings, the additional fee is worth it.

II. RELATED WORK

In 2008, the appearance of Bitcoin [12] brought about blockchain technology that expands the traditional financial system to a new type of form. Later on, the idea of blockchain also inspires the development and research of other cryptocurrency implementations, for example, Ethereum [13], Hyperledger Fabric [14] and Dogecoin. Blockchain is a digital ledger that is maintained by a network consisting of countless nodes. Each node is equivalent in status, thus creating a decentralized network. Nowadays, because of supporting smart contract, Ethereum becomes the most popular blockchain for NFT and related applications.

[1] https://wyvernprotocol.com

TABLE 1. Comparison of our scheme and related works.

Scheme	NFT support	Ethereum compatible	publicly verifiable ownership	conceal blockchain address
[24]	No	No	—	No
SNIP-721	Yes	No	Yes	—
[25]	Yes	No	Hard	—
[26]	Yes	Yes	Yes	No
Ours	Yes	Yes	Yes	Yes

The privacy problem of blockchain transactions has been studied by researchers in recent years. And some new cryptocurrencies are proposed with the characteristic of anonymity in their design. Monero is proposed with features about privacy and anonymity. Despite Monero being a public ledger, the information of transactions is obfuscated by introducing ring signature [15] technology to hide the transaction sender. Later on, ring confidential transactions (RingCT) [16] is applied to fully obfuscate the transaction information including the recipient and the amount of cryptocurrency. Apart from Monero, Zerocoin protocol [17] was proposed in 2013 as an improvement extension to Bitcoin that achieves Bitcoin transaction's anonymity by adding coin-mixing capabilities into the protocol. Zcash is another cryptocurrency that provides privacy protection. But some research found that the claimed anonymity of Zcash is questionable [18], [19]. In 2021, Wang et al. proposed a scheme to protect the privacy of blockchain where transactions are transparent to the public [20]. Despite it being close to what we wish to achieve, Wang's work merely hides the transaction's amount and does not benefit the data stored in smart contract. Coin mixer [21] is also a technology proposed to provide privacy preservation for cryptocurrencies without the original support of this property. However, the biggest problem is that the core of it heavily relies on the fungibility of tokens to obfuscate the flow of cryptocurrencies, meaning that a non-fungible token is immediately identified in the pool of coin mixers. In addition, Xu et al.'s work [22] investigates anonymity in electric vehicles. Chen et al. [23] explore the usage of blockchain regarding data sharing. But none of them suits the research in NFT. Therefore, none of these solutions are compatible with NFT transactions in Ethereum.

Currently, the security research about NFT is insufficient. Our survey found that a majority of research about NFT focuses on its economic property [27]. Apart from that, some of the only research available does not satisfy our needs either. Tewari's anonymous transferable E-cash system [24] achieves anonymity in Bitcoin network, while we intend to achieve anonymous transfer in Ethereum. The difference between E-cash and NFT also becomes an obstacle. This similar problem also occurs in SNIP-721[2] which is based on CosmWasm on the Secret Network, rather than Ethereum. Rao's private NFT scheme [25] considered the privacy of NFT, the proposed scheme is blockchain-agnostic. Instead, a group of validators takes the role of EVM and decide the winner of an auction. But the collusion of these validators can be worried. Also, it can be difficult to prove the ownership of an NFT in a blockchain-agnostic system. Ferone et al.'s work [26] uses NFT to construct an infection and notification system based on blockchain. Although privacy is a vital property of this system, it still relies on the unlinkability of blockchain addresses and users. Yet we have previously explained this unlinkability is fragile unless users never use their address in other cases, which is unreasonable for NFT trading. Table 1 shows the difference between our scheme and these works.

Other related works mainly exploit NFT as a component of a system. Regner et al. [28] use NFT to create an event ticketing application. Arcenegui et al. [29] introduce NFT in the secure management of IoT devices. García et al. [30] use NFT's metadata to embed copyright information against fake NFT. Krasnoselskii et al.'s Kramer [31] is designed for an online rarity meter for the Karnaia NFT collection. But none of the above schemes study the privacy problem we mentioned and propose an efficient solution. Another potential way of solving the anonymity problem in NFT trading is to construct a cross-chain system using cross-chain swap so that the anonymity of other cryptocurrencies can be exploited. Robinson et al. proposed a General Purpose Atomic Cross-chain Transactions protocol that allows composable programming across multiple Ethereum blockchains [32]. But it cannot be applied to cryptocurrencies with privacy protection like Monero. Other cross-chain swap schemes [33], [34] also suffer from this problem. Zamyatin et al proposed a scheme for communication across distributed ledgers [35]. However, it cannot hide the identity of the owners in NFT contract. Therefore, the existing works are hardly applied to the privacy problem we proposed.

III. PRELIMINARIES

A. DISCRETE LOGARITHM ASSUMPTION IN ELLIPTIC CURVE CRYPTOGRAPHY

For a group $\mathcal{G}$ with generator g and order q over an elliptic curve, there exists an efficient algorithm to calculate a point $Y = yg$ on the elliptic curve for any $y \in \mathbb{Z}_q$. However, given an element x of the group $\mathcal{G}$, there is no efficient way for any adversary to find $\alpha \in \mathbb{Z}_q$ such that $x = \alpha g$ within polynomial time. This is the discrete logarithm assumption that our scheme is based on.

Definition 1: The Discrete logarithm (DL) assumption holds in G if no polynomial time algorithm $\mathcal{A}$ has non-negligible advantage to solve the DL problem in G.

[2]https://github.com/SecretFoundation/SNIPs/blob/master/SNIP-721.md

B. NON-INTERACTIVE PROOF OF COMMITMENT

We use Pedersen's commitment [36] and Schnorr protocol [37] to construct a non-interactive proof for knowledge of the opening of a commitment.

A commitment scheme is conducted between a committer C and a receiver R. The committer first commits to a secret message and sends the commitment to the receiver. In the future, this secret message is opened to the receiver, and there is an efficient algorithm to verify that the opened message is the exact message used in generating the commitment. To do so, a group $\mathcal{G}$ with the order q and two generators G and H are published as public parameters. C randomly choose $r \in \mathbb{Z}_q$ and commit to the m by generating $com = mG + rH$, where com is sent to R. C opens this commitment by revealing (m, r) so that R can check whether $com = mG + rH$ holds.

There are two properties of the Pederson commitment: perfectly binding and computational hiding. Perfectly binding represents that for Alice, the possibility of outputting $Commit(m, r) = Commit(m', r')$ where $m \neq m'$ is negligible even if Alice has unbounded computational power. This means once a commitment is made, the commitment com is uniquely linked to the commit message m. On the other hand, computational hiding represents that for $m \neq m'$, the probability ensembles $Commit(m, R)$ and $Commit(m', R)$ with R being a uniform distribution over 2^k are computationally indistinguishable. It means for a probabilistic polynomial-time adversary, it cannot extract any useful information about m before the opening.

However, to prevent the secret message m from being known by others, C can generate a proof of knowledge for the opening instead of revealing it based on the following scheme. Notice that the random oracle used for generating h will be replaced by a collision-resistant hash function in practice.

$Proof(m, r)$:

1) $x, y \longleftarrow \mathbb{Z}_q$
2) $P = xG + yH$
3) $h \longleftarrow RO(P)$
4) $x' = x + hm, y = y + hr$
5) Return (P, x', y')

$Verify(com, P, x', y')$:

1) $h \longleftarrow RO(P)$
2) if $P + hCom = x'G + y'H$ holds, the proof is accepted.

C. ETHEREUM AND SMART CONTRACT

One of the most well-known blockchain implementations that support smart contract is Ethereum. An Ethereum account consists of the following entities: Address, Ether balance, Contract code, and Storage. And there exist two types of accounts: One is the externally owned account (EOA), which is owned by a user with a corresponding private key and is used for generating transactions. Another is the contract account, which is not owned by a user but a pre-written contract code deployed on Ethereum. The contract code controls the behavior of a contract account. Since the smart contract cannot be rewritten after being deployed on Ethereum blockchain, and anyone inside the Ethereum network can check the contract code, people always trust the code to execute as expected. It is this characteristic that stimulates the development of various open-source, decentralized projects and applications on Ethereum. The exchange of NFT and other crypto assets is also achieved by smart contracts.

IV. WORKFLOW OF OPENSEA

In this section, the workflow of OpenSea, a typical NFT marketplace based on Ethereum and Wyvern protocol, is demonstrated for a better understanding of how we modify it into our scheme. Figure 1 shows the brief process of a NFT transaction in OpenSea.

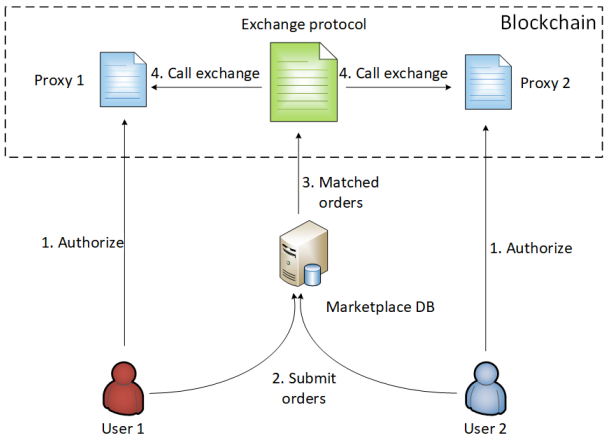

FIGURE 1. The workflow of OpenSea.

A. CREATE AND LIST NFT

The NFT trade begins by minting and listing a new NFT token. OpenSea provides a method of creating a new NFT contract through its website. But it also accepts NFT contracts that are already deployed. Considering the real world's situation, transactions may take a variety of forms. NFTs can be sold at a fixed price or by an auction. As the auction is mainly concerned with the functional design of smart contract, we will just illustrate our proposed scheme in the fixed price model, where a seller submits a selling order of a certain NFT and lists it on OpenSea's website, and after browsing OpenSea's website, a buyer submits a corresponding order to buy it.

B. AUTHORIZE PROXIES

Since the time of listing a certain NFT is usually different from the time of purchasing, it is not practical to let the seller keep waiting for a potential buyer to submit a buy-side order and then transfer the NFT to the corresponding buyer. To solve this problem of inconvenience, each OpenSea user is required to have a one-to-one matched proxy on the Ethereum blockchain. A proxy is instantiated through the proxy registry contract to help the automatic exchange by generating transactions on behalf of buyers or sellers correspondingly. After submitting an order, a user authorizes his proxy access

to the target NFT by calling proxy functions, thus delegating this proxy to deal with asset exchange.

C. PROCEED ORDERS

While buyers and sellers submit their orders, they are submitting to the order book of OpenSea through OpenSea's front end. These orders contain information including the order maker, proxy registry, target, price, calldata, etc. Calldata is a configurable predicate that usually consists of segments about delegating some action and is used for the proxy's execution. Configurability enables the replacement of calldata array guarded by a bitmask so that the seller does not need to include the address of the buyer in the order or vice versa. The submitted orders are uploaded to the exchange smart contract in the form of bundles. An exchange protocol is in charge of matching buy-side and sell-side orders based on the price. If there is a match, the protocol will complete the calldata and call the proxies of both sides to conduct the exchange procedure. After that, the ownership of digital assets (Ether and NFT) is exchanged.

V. SYSTEM MODEL AND THREAT MODEL

A. SYSTEM MODEL

We start by demonstrating by introducing each party's role in the proposed scheme. Detailed construction will be given after it.

1) NFT MARKETPLACE

The NFT marketplace (e.g. OpenSea) maintains an online website for blockchain users to create or list and sell their NFT assets. During transactions, users submit their NFT orders through the marketplace's front end. Regarding the blockchain part, several smart contracts are deployed by the marketplace on the blockchain network, conducting NFT transactions including minting new tokens, matching NFT orders, and transferring ownership of existing tokens. Moreover, we assume the NFT marketplace is almost entirely trusted. Therefore, some key information that leads to the exposure of identity is kept a secret in marketplaces' databases.

2) EXCHANGE PROTOCOL

The exchange protocol is a deployed contract on the blockchain that mainly deals with order-matching affairs. It receives bundles of orders from the marketplace and checks if any two orders are matched regarding the target token, price settings, and other relevant information. If so, the exchange protocol will first fill in the omitted segments of calldatas according to the bitmask (The construction of matching calldata can also be done in any fashion off-chain, for example by the marketplace). After then, the proxies from buy-side and sell-side are involved to conduct the pre-defined transfer actions. This will also emit corresponding events in the blockchain network for listeners. Finally, proxies of both sides finish their exchange operation and the transaction is confirmed by the blockchain. Thus the ownership of the target NFT is transferred.

3) PROXY REGISTRY AND PROXY

For the convenience of NFT trading, each user exploits a proxy in the blockchain network to handle NFT orders on behalf of the user. The function of proxy is defined inside a deployed contract called the registry. And every new proxy instance is generated via calling the registry. Inside the proxy, a temporary address, representing the owner of this proxy, is stored for verifying the message from its owner. When the owner wants to delegate the NFT trading to the proxy, he authorizes proxy access to target digital assets by a command with a temporary key's signature. After then, once a valid order with the owner's signature is sent to the exchange protocol and causes the asset exchange, the proxy will conduct the corresponding action based on the calldata in the order. In that way, the seller-side proxy transfer the ownership of the target NFT to the buyer by changing the ownership to the buyer.

4) DECOY ACCOUNT

Decoy accounts are a large group of blockchain accounts managed by the marketplace. From the perspective of other users, decoy accounts seem not different from other EOA accounts that are held by individuals. However, the private key of decoy accounts is actually managed by the marketplace. Decoy accounts are proposed to isolate the cryptocurrency payment from NFT transfer, thus making it difficult to link a buyer and seller to an NFT transfer. While the whole system is running, the buyer pays to decoy $\mathfrak{D}_1$, and another decoy $\mathfrak{D}_2$ transfers the same amount of cryptocurrency to the seller. Such a procedure makes others impossible to find a link between the buyer, the seller, and the transferred NFT. And the payment looks like two separate regular blockchain transactions between EOA, which is why we call it a decoy account.

5) NFT BUYER

NFT buyers can view all buyable items through marketplaces' websites and submit an order of buying certain NFT. While buying an NFT artifact, the buyer is free to choose the anonymous or non-anonymous mode. While in anonymous mode, the buyer submits an anonymous order and contributes to the randomness of commitment's generation. Since the non-anonymous mode does not require any protection of buyer identity, we only demonstrate the process of anonymous mode in this paper. To purchase an NFT, the buyer submits an order with an Elliptic Curve Digital Signature Algorithm (ECDSA) [38] signature signed by the temporary key. The buyer also transfers Ether to a given decoy address. After the exchange, the buyer pays the money. And a commitment to the buyer's blockchain address is recorded as the new holder of that token.

6) NFT SELLER

NFT sellers refer to some NFT holders who want to sell their NFT collections to other people in an NFT trade. They bought NFT from other NFT creators or sellers as buyers.

If a seller is non-anonymous, he can completely act like an NFT creator while selling an NFT to others. Thus we only consider the situation where an NFT seller's ownership is anonymous. In this case, the NFT marketplace takes the role of intermediator and the transaction becomes a three-parties transaction: During the off-chain part, the seller lists NFT items on the marketplace and sends an order. There are two purposes of this order: one is to indicate the purpose of selling a target NFT with a price. Another is to prove the ownership of target NFT to the exchange protocol. The seller also approves the proxy to transfer the ownership of the target NFT to another address when two orders are matched, via authorization with the signature generated by the temporary key. After the exchange, the ownership of NFT is transferred and the seller obtains Ether from a decoy account later.

B. THREAT MODEL

In threat model, we assume the following: The NFT marketplace deploys smart contract on the mainnet of Ethereum such that the contract code is viewable to the public. Moreover, exchange-related functions on smart contract only process inputs from the marketplace, which is achieved by checking the message sender's address. In addition, marketplace maintains a front-end server and a database for users to publish and store orders. The server, database and communication between users and the server are considered secure. And the marketplace is assumed *almost fully trusted*. It will process all defined operations according to the workflow. And Although it knows the blockchain address of all buyers, it will never leak these private information.

There are two attackers in the threat model: an adversary from the perspective of blockchain users and the marketplace. Their abilities and target are described as follows:

- A blockchain-user adversary is financially rational with strong computational power to have access to the smart contract. Hence, it is able to read the *privacy processing* owner of NFT tokens as well as each function call to the smart contract. But the adversary cannot compromise the security model of Ethereum itself. The adversary wins if he extracts the hidden owner's address of any NFT, or if he proves fake ownership of any NFT to sell others' NFTs.
- Compared to blockchain-user adversary, the extra advantage of marketplace is the accessibility of exchange-related functions on smart contract. There is a small chance that the marketplace is corrupted when high-price NFT occurs. The marketplace tries to manipulate the order and use the exchange contract to buy this NFT at an irrational price.

VI. OUR SCHEME

In this section, we demonstrate the concrete construction of our scheme. The workflow of our scheme is described based on an example that Alice is the owner of a listed NFT and Bob wants to purchase it. The exchange is conducted through a marketplace that utilizes our proposed scheme.

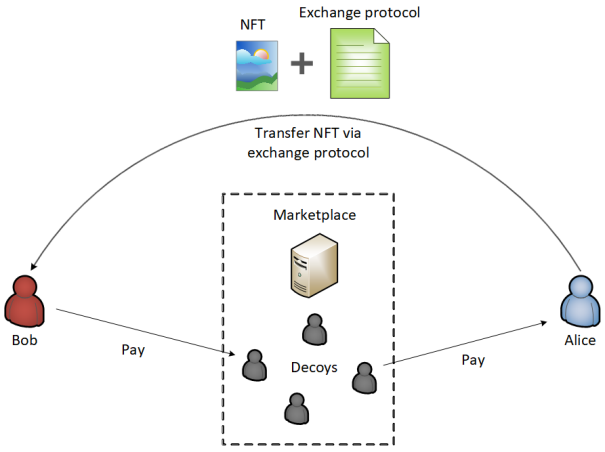

FIGURE 2. Our proposed scheme.

We also assume that every off-chain communication is executed through an end-to-end secure channel against an eavesdropping attack. Moreover, a group $\mathcal{G}$ over finite elliptic curve field with order q, two generators G and H, a collision-resistant hash function $h()$ is chosen by the marketplace and published as public parameters. Figure 2 demonstrates the frame of our scheme. The NFT transfer is executed by smart contract. And the payment is through decoy accounts controlled by marketplace. Figure 3 shows how our scheme works. Note that only the sell-side requires a proxy, and the seller has no direct interaction with their proxy.

A. PROXY REGISTRATION

A deployed proxy registry contract on blockchain is in charge of registering a new proxy and memorizing a map of proxies and corresponding owners, which is identical to the Wyvern protocol. However, unlike the current Wyvern protocol where users directly register proxies via interacting with the contract, the marketplace is in charge of every interaction with the registry in our proposed scheme. When registering a new proxy, each user generates a new key pair (pk_t, sk_t) called **temporary key** by the key generation algorithm of Ethereum. sk_t is kept as a secret, and an address $addr_t$ generated by pk_t is submitted through the request of applying for a new proxy to the marketplace through an off-chain channel. Notice that the format of temporary key is identical to a blockchain key pair. But a user should never use it except for the NFT transaction situation. Next, for the marketplace side, let $\mathcal{U}$ be the space of all blockchain users and $\mathcal{T}$ be the space of all temporary addresses $addr_t$. The marketplace will record the mapping relationship $\mathcal{UT} \subseteq \mathcal{U} \times \mathcal{T}$ which represents the temporary address and to whom they belong. The relation $\mathcal{UT}$ is kept by the database of the marketplace as a secret, meaning the owner of a given temporary address is only known by the marketplace and the owner himself. After then, the marketplace calls the registry function and initiates a new proxy by forwarding the temporary address to the proxy as the owner's address. And the owner of this newly generated proxy is

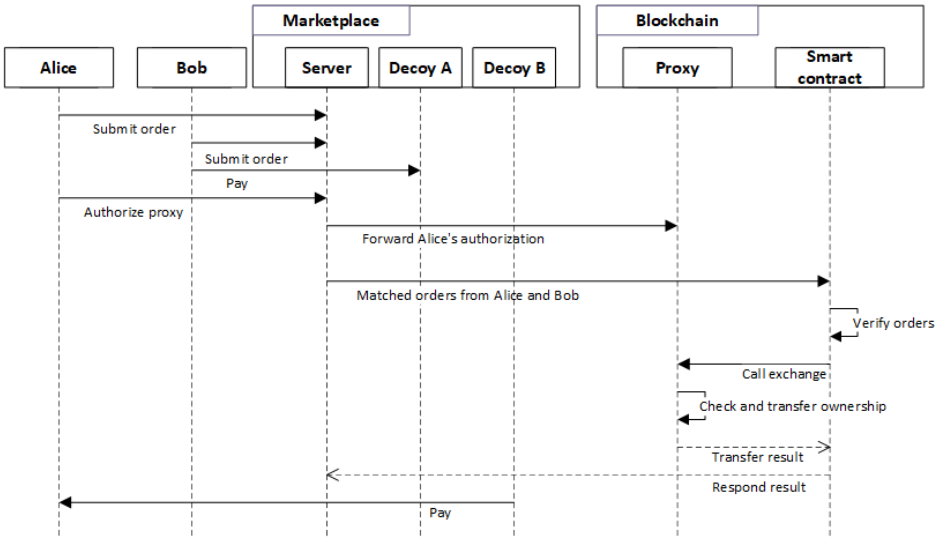

FIGURE 3. The workflow of our scheme.

recorded as $addr_t$. By this means, the link between proxy and owner is maintained by the knowledge of a temporary secret key.

B. NFT OWNERSHIP

A commitment to the owner's address is used to bind the ownership of NFT to a certain user. The commitment is generated as follows: Given a public group $(G, \cdot)$ of a large order p, the marketplace randomly chooses two generators g and $h = g^{\alpha}$ of G and publish (G, g, h, p) as public parameters, where α is held as a secret. For an NFT M's owner Alice with address $addr_1$, she calculates the commitment to her address by randomly choosing a secret value $r_1 \in \mathbb{Z}_p$ and calculates:

$$C_{Alice} = g^{addr_1} h^{r_1} \tag{1}$$

In a non-anonymous mode, the NFT contract stores a list of token IDs with the corresponding owner's address. When the anonymous mode is adopted, instead of the owner's address, C_{Alice} is stored to indicate that the owner of M exists but is hidden.

C. ORDER GENERATION

The generation of orders starts in the off-chain environment. For the sell-side, Alice generates an order which indicates her willingness to sell. It contains the required information including token ID, price, listing time, expiration time, call-data, and proof of knowledge for commitment, attached by a signature for all above-mentioned messages signed by the temporary secret key $sk_{t,Alice}$. The generation of proof is shown below:

1) $x, y \longleftarrow \mathbb{Z}_q$
2) $P = xG + yH$
3) $t \longleftarrow h(order)$
4) $x' = x + tm, y' = y + tr$
5) $Proof = (P, x', y')$ is generated

The order is first submitted to the marketplace through a secure end-to-end channel. After receiving it, the marketplace completes it as table 2 shows before submitting it to the exchange protocol. As for the buy-side, Bob starts by communicating with the marketplace's front end to be assigned an address of the decoy account. Before generating a buyer order to the marketplace, Bob must transfer sufficient Ether for purchasing to this decoy. After then, Bob also generates an order including target token, bid, listing time, expiration time, new commitment to Bob's address as equation 2, and signs on all previous messages using his temporary secret key $sk_{t,Bob}$. This order is sent to the marketplace's server via off-chain channel as well.

$$C_{Bob} = G \cdot addr_2 + H r_2 \tag{2}$$

Notice that the order submissions to the marketplace from Alice and Bob are not required to be simultaneous. And Bob can submit a buy-side order in advance as well. After receiving the order from Bob, the marketplace's server checks whether Bob has transferred enough Ether to the designated decoy account. Then it also completes the order as shown in table 3. Eventually, two orders are stored off-chain in the database of the marketplace, waiting for being uploaded to the exchange protocol.

D. AUTHORIZE THE PROXY

Apart from the order, Alice also generates another message with her signature to authorize the proxy to access the target NFT. To do so, Alice generates a message about the order and signs on it using the temporary key:

$$m_{au} = "AUTH" || target\ NFT || timestamp \tag{3}$$

$$sig_{au} = sign(m_{au}, sk_{t,Alice}) \tag{4}$$

(m_{au}, sig_{au}) is sent to the marketplace off-chain. And then the marketplace forwards it to the proxy registry via calling

TABLE 2. Order from Alice.

maker	$pk_{t,Alice}$
registry	Registry to be used
proxy	Corresponding proxy
target	Target NFT token
price	Price for purchase
listing time	The time after which the purchase is available
expiration time	The time after which listing is not valid
calldata	erc721c.methods.transferFrom(Alice, Bob, token_id).encodeABI()
proof	Proof of the knowledge for opening

TABLE 3. Order from Bob.

maker	$pk_{t,Bob}$
target	Target NFT token
bid	The maximum affordable Ether
listing time	The time after which the purchase is available
expiration time	The time after which listing is not valid
new commitment	$C_{Bob} = g^{addr_2} h^{r_2}$

the related function. On receiving the message and signature, the registry checks whether the time stamp is valid. And the signature is then verified. If sig_{au} is accepted, the registry will add the corresponding proxy and NFT as a new entry to a list that stores all delegated proxies with their target NFT.

E. EXCHANGE

If two orders are matched based on the target token, price, etc., they will be simultaneously submitted to the exchange protocol as a bundle (sell order, seller signature, buy order, buyer signature) by the marketplace. When receiving this bundle, the exchange protocol proceeds as follows:

1) Check whether two orders are matched by comparing the target token, price and bid, and validity time.
2) Lock the transaction status of the target NFT.
3) Verify the validity of signatures.
4) Verify the proof from sell-side.
5) Check whether the proxy of buyer has been authenticated.
6) If any of the above procedures fail, the exchange phase aborts and emits error information. If all the above procedures succeed, the exchange protocol checks whether the proxy is authenticated by the seller. If so, it calls the sell-side proxy and passes the calldata for execution.
7) The calldata is executed by the proxy and the ownership field of the target NFT is replaced by C_{Bob}. And an event of the completion of this exchange is emitted as a transaction receipt.

Algorithm 1 shows the exchange function in the deployed smart contract. The procedure of proxy is shown in Algorithm 2 where *Proxy* is defined by Wyvern library to allow the proxy to execute the ownership transfer command created by Alice. After detecting the completion event, the marketplace uses another decoy to pay Ether to Alice as the income for selling NFT.

Algorithm 1 Pseudocode for Exchange Contract

Upon receiving ($Order_1$, $Order_2$):
- Assert $message.sender = marketplace$
- Assert $Order_1.target = Order_2.target$
- Assert $Order_2.bid \geq Order_1.price$
- Assert $t > listing\ time \parallel expiration\ time > t$
- Lock($Order_1.target$)
- Verify($Order_1.sig$)
- Verify($Order_2.sig$)
- Assert (VerifyProof($Order_1.proof$) $= 1$)
- Assert $Registry[proxy] = approved$
- $r = Call(proxy, Order_1.calldata, Order_2.commit)$
- Unlock($Order_1.target$)
- Return r and emit event

Algorithm 2 Pseudocode for Proxy

Upon receiving ($calldata$, $commit$):
- Verify($calldata.sig$, pk_t)
- $calldata.receiver = commit$
- $r = Proxy(calldata)$
- Return r

VII. DISCUSSION: DILEMMA ABOUT ANONYMITY AND MARKETPLACE

In this section, we will discuss a dilemma regarding hiding the identity of NFT owners, and the reason why NFT marketplaces like OpenSea must be almost fully trusted.

Currently, a large proportion of NFT is minted and traded on Ethereum because of the convenience of smart contracts. For verification, each transaction is bound to an issuer address so that the miners can verify its signature in Ethereum-like blockchains. Therefore, it is easy for anyone to obtain the owner's address of a given NFT. Other privacy-preserving blockchains like Monero may use cryptography technologies like RingCT to hide the address of transactions' sender and recipient, but lack the support of the smart contract, making it difficult to mint and trade NFT. As a consequence, the owner's privacy and the feasibility of NFT trade become contradictory to each other.

For the coexistence of owner privacy and NFT trade, a compromise has to be made. We solve it by letting marketplaces act as intermediator of information exchange. The transaction link: User A→exchange contract→User B is fuzzily processed by the marketplace via creating a virtual user (temporary key), and the Ether flow from Alice to Bob also becomes indirect by introducing decoys. Accordingly, the cost of this compromise is that marketplace knows virtual identities of all users. And the Ether transfers to sellers are not executed by the smart contract. Therefore, an *almost fully trusted* marketplace is required for our scheme. But considering the real-world situation, this assumption is reasonable: Although it is theoretically possible that the marketplace misappropriates the ether from Bob to Alice, this will largely influence the marketplace's credit and make it loses

market share. Apart from that, all transactions are traceable in blockchain. Victims can use it as evidence for arbitration. That means, despite the feasibility of illegal behavior, marketplaces are not willing to conduct it since evidence cannot be erased. Further analysis will only discuss a special situation where the marketplace leaves no crime evidence.

VIII. EVALUATION

A. SECURITY ANALYSIS

In our proposed scheme, there are three main security requirements:

1) Anonymous ownership: No one except the marketplace can learn the hidden address of any NFT owner.
2) NFT security: It is infeasible for anyone other than the owner to change the ownership to another address.
3) Anti-forgery: Even with the ability to access the exchange contract, the marketplace cannot forge or manipulate an order to maliciously buy any listed NFT at a low price or for free.

The analysis is described from the perspective of different attacks as follows.

1) EXTRACT THE OWNER FROM NFT CONTRACT

This attack can be launched by an adversary in blockchain as described in section V-B. Intuitively, The most direct way to extract the owner of an NFT is by investigating the NFT contract. Since the contract stores a list of every minted token with the owner's address, and blockchain serve as a digital ledger that keeps the history of all transactions, the attacker can search the information of all owners after an NFT is minted. Although the address of NFT owner is encoded as a commitment in our scheme, $C_{Bob} = G \cdot addr_2 + Hr_2$ still contains information $addr_2$ which is Bob's blockchain address. From this perspective, a direct way is to extract $addr_2$ from C_{Bob}. However, this is prevented by the security of commitment itself. The computational hiding property of commitment guarantees that a probabilistic polynomial-time attacker has no way to extract the committed information since it contains solving the discrete logarithm problem. This protects anonymous ownership.

2) SEARCH FOR THE OWNER OF PROXIES

One significant property of Ethereum is public-by-default, meaning each transaction is in plaintext and viewable in Ethereum. Note that in the NFT exchange procedure, the proxy of buyer is involved and bound to a specific NFT transfer transaction. In the meantime, each proxy is assigned to a unique user. Therefore, instead of extracting the owner address from the commitment, the adversary may try to find the owner of a proxy. Once succeed, the proxy's owner is also the present or former owner of an NFT. Nevertheless, the proxy is linked to a temporary key generated by the real owner, and there is no algebraic relationship between this temporary key and the owner's address. Moreover, there is no direct interaction between the proxy and its owner in our scheme. The authorization command is sent to the marketplace in a secure off-chain channel and then forwarded to the proxy. In the records of blockchain, it is always the marketplace that interacts with proxies. Therefore, an attacker cannot find any relationship between the owners and proxies. Therefore, anonymous ownership is protected.

3) INVESTIGATE ETHER FLOW

This is also an adversary's attack based on side information. For payment, the Ether flow starts from the buyer to the marketplace, and later to the seller, which may expose the fact that they are engaged in an NFT exchange. Furthermore, by investigating the amount of transferred Ether and recently sold NFT, the traded NFT may be specified by its price. This works especially for high-value NFT. But the mechanism of decoy accounts makes it difficult to trace the link between buyers and sellers. During the payment, Bob pays to decoy A at first. After the ownership is transferred, the marketplace use decoy B to pay the same to Alice. Thus no direct ether flow from Bob to Alice can be observed. And there are two advantages of using decoys: One is that the marketplace controls a large group of decoys, and the generation of new decoys can easily be done offline. As a result, the attacker cannot distinguish between a normal user account and a decoy account. Another is that the decoys used for a buyer and a seller are different. And there is no direct link between the two decoys either. Since all decoys are controlled by the marketplace, the huge network of decoys can easily achieve complicated transfer of Ether. From the perspective of attackers, these transactions look the same as other normal transactions between blockchain users. Thus, the attacker cannot find an obvious link between a buyer and a seller that indicates the NFT exchange. And the infeasibility of the previously discussed three attacks indicates the anonymous ownership.

4) MALICIOUSLY CHANGE THE OWNERSHIP OF AN NFT

Instead of extracting the owner's identity from commitment, another perspective of attack for the adversary is to change the ownership of others' NFT. One way is to attack Ethereum itself and create a malicious block, which is also known as a 50 percent attack. Since it requires enormous computational power, it is usually considered impossible in blockchain research. Another way is to forge the proof of ownership of an NFT, thus making it possible to impersonate the owner and sell the NFT. In that case, the problem transforms into generating valid proof of a given commitment without the knowledge of opening. The introduced proof scheme is a common extension of Schnorr's protocol. Therefore, we give a brief proof idea: Let $\mathcal{A}$ be an adversary that convinces the honest verifier for two challenges c_1, c_2 under rewind. The corresponding two proofs are (x_1, y_1) and (x_2, y_2). Then $addr = \frac{x_2 - x_1}{c_2 - c_1}, r = \frac{y_2 - y_1}{c_2 - c_1}$. This contradicts to fact that $\mathcal{A}$ do not know the opening of commitment. Therefore, the only way to generate valid proof is by knowing the owner's address and nonce. Thus an attacker has no advantage in forgery.

5) SECURITY AGAINST THE MARKETPLACE

As is explained before, the marketplace is *almost fully trusted* in our scheme. The term ''almost'' represents marketplace will not leak the owner's address of NFTs. But when a superiorly-high price NFT occurs, there is a possibility that the marketplace may become corrupted and wants to obtain this NFT through the exchange contract through its privilege. The previous contents already discussed the feasibility of forging a proof of commitment. Although *addr* is known by the marketplace, a valid proof cannot be generated without the knowledge of r. However, another advantage of marketplace is the access to exchange protocol. If the marketplace manipulates a submitted sell-side order to an abnormally low price, it can create a buy-side order and buy it *legally*. But this is prevented because each order is attached with an ECDSA signature generated by the temporary secret key, thus providing the authentication for exchange contract. To successfully impersonate another order, the marketplace must produce a valid signature without the knowledge of the corresponding secret key. However, according to the security of ECDSA, the probability of success is negligible for the marketplace. This guarantees that the marketplace cannot sell a high-value NFT at an abnormally low price and claim it is authenticated by the NFT seller. Therefore, users do not have to worry about their losses while using the marketplace.

B. PERFORMANCE ANALYSIS

In EVM, the execution of smart contracts can be separated into several basic operations. These operations are executed by validators and require computation resources (gas). Besides the price of tokens, launcher of transactions also needs to pay corresponding gas costs to miners. The more complex operations and contract space are involved, the more transaction fee it requires. Therefore, the transaction fee is an important factor in investigating the performance of blockchain applications. On the other hand, the runtime of smart contract is determined by the block time of Ethereum, which is considered fixed. For our heavily contract-based scheme, the bottleneck regarding time cost depends on the scalability of blockchain itself. Improving the scalability of blockchains is a crucial issue. However, blockchain scalability depends on the underlying blockchain (e.g., Ethereum) of the NFT system. We are premised on using Ethereum employed by OpenSea. So, it is outside the scope of our study, and time cost will not be evaluated consequently.

Since our scheme is a modification on top of the NFT exchange system used by OpenSea, the functionality of existing parts is not influenced by our work. Hence we only estimate the additional gas cost of modified parts. The less our scheme adds to the gas cost of trading NFT in OpenSea's system, the more acceptable it will be. We implement our scheme and simulate a complete NFT-to-Ether match transaction to estimate the gas cost in Rinkeby testnet. Since elliptic curve cryptography is applied in our scheme, the Elliptic-curve-solidity library[3] is included in our contract to achieve efficient elliptic curve calculation. The adopted elliptic curve is secp256k1 ($y^2 = x^3 + 7$). The estimation of gas cost is shown in both Ether and USD. Note that the Ether price was obtained on 20 November 2022.

TABLE 4. Gas cost of each process.

Functions	Gas cost (Ether)	Gas cost (USD)
Verify proof	0.000730	0.88
Authorize: verify signature	0.000025	0.03
Exchange: verify signature	0.000025	0.03
Summary	0.00078	0.94

It can be observed from Table 4 that for each NFT trading, the most gas-consuming operation is verifying the proof. This operation only occupies calculational power without leveraging any storage space of smart contract, which is usually considered to be the most expensive operation in smart contract. Thus, assigning the proof's verification to smart contract only increases a little extra cost. In addition, a summary of all the gas costs indicates that for each transaction bundle, the gas cost of a successful NFT trading only increases by 0.00078 Ether or 0.94 USD. For comparison, we introduce the transaction of an NFT collection called Otherdeed. For the sale of a single token,[4] the transaction fee is 0.0044 Ether (5.32 USD). Therefore, the extra expense for the sake of privacy is completely acceptable for nowadays blockchain users. Moreover, although various related schemes are compared in table 1, none of the listed schemes achieves the essential privacy property (i.e. Anonymous ownership) as ours does. For this reason, it is meaningless to compare the gas cost with theirs. As long as our scheme accomplishes an acceptable result in OpenSea's NFT system, it is proven to be suitable.

IX. CONCLUSION

The privacy of personal belongings should be protected. However, the anonymity of Ethereum heavily relies on the unlinkability of blockchain address and user's identity, making it possible to expose NFT assets of users in current NFT trading. In this paper, we studied the trading process of the most popular NFT marketplace, and improved it by adding the feature of hiding the identity of NFT owner so that no one other than the owner himself and the marketplace knows the owner of a given NFT. Also, this new scheme is compatible with the current mechanism, which means the current NFT trading will not be influenced at all if changing to the modified system. We then give a detailed analysis of the security and performance. For attackers, the probability of extracting the identity of any NFT is negligible. This perfectly protects the privacy of NFT owners. As for performance, the

[3]https://github.com/witnet/elliptic-curve-solidity. Open-source project under the MIT license

[4]Transaction Hash: 0x97125659eeaf717963541ebe7e9035513cf47f5b0c8650bab8a433c9c57cf938.

newly added security part in smart contract only increases 0.94 USD per trade for NFT buyers and sellers, which proves our scheme is suitable for the application.

REFERENCES

[1] W. Entriken, D. Shirley, J. Evans, and N. Sachs, "EIP-721: ERC-721 non-fungible token standard," Standard ERC-721, Ethereum Improvement Proposals, 2018.
[2] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and A. R. Sandford, "EIP 1155: ERC-1155 multi token standard," Standard ERC-1155, Ethereum, 2018.
[3] K. Crow and C. Ostroff, "Beeple NFT fetches record-breaking 69 million in Christie's sale," *Wall Street J.*, 2021. [Online]. Available: https://www.wsj.com/articles/beeple-nft-fetches-record-breaking-69-million-in-christies-sale-11615477732
[4] 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.
[5] M. Bal and C. Ner, "NFTracer: A non-fungible token tracking proof-of-concept using hyperledger fabric," 2019, *arXiv:1905.04795*.
[6] A. Xu, M. Li, X. Huang, N. Xue, J. Zhang, and Q. Sheng, "A blockchain based micro payment system for smart devices," *Signature*, vol. 256, no. 4936, p. 115, 2016.
[7] H. Hata and S. Teramoto, "A payment system for regional transport services by blockchain with IC card and the application for transaction settlement of local economy," *IEEJ Trans. Electron., Inf. Syst.*, vol. 141, no. 8, pp. 903–908, 2021.
[8] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding security issues in the NFT ecosystem," 2021, *arXiv:2111.08893*.
[9] Z. Sun and M. Wei, "PUF-based anonymous RFID system ownership transfer protocol," in *Proc. Chin. Control Conf. (CCC)*, Jul. 2019, pp. 6367–6373.
[10] K. H. S. S. Koralalage, S. M. Reza, J. Miura, Y. Goto, and J. Cheng, "POP method: An approach to enhance the security and privacy of RFID systems used in product lifecycle with an anonymous ownership transferring mechanism," in *Proc. ACM Symp. Appl. Comput.*, 2007, pp. 270–275.
[11] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2004, pp. 41–55.
[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, p. 21260, 2008. [Online]. Available: https://bitcoin.org/en/bitcoin-paper
[13] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2017.
[14] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, and Y. Manevich, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.
[15] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Berlin, Germany: Springer, 2004, pp. 325–335.
[16] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, Dec. 2016.
[17] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from Bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411.
[18] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in Zcash," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 463–477.
[19] C. Ye, C. Ojukwu, A. Hsu, and R. Hu, "Alt-coin traceability," Cryptol. ePrint Arch., 2020. [Online]. Available: https://eprint.iacr.org/2020/593
[20] H. Wang and J. Liao, "Blockchain privacy protection algorithm based on Pedersen commitment and zero-knowledge proof," in *Proc. 4th Int. Conf. Blockchain Technol. Appl.*, Dec. 2021, pp. 1–5.
[21] I. A. Seres, D. A. Nagy, C. Buckland, and P. Burcsi, "MixEth: Efficient, trustless coin mixing service for ethereum," Cryptol. ePrint Arch., 2019. [Online]. Available: https://eprint.iacr.org/2019/341
[22] S. Xu, X. Chen, and Y. He, "EVchain: An anonymous blockchain-based system for charging-connected electric vehicles," *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 845–856, Dec. 2021.
[23] X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao, and W. Kong, "*AQ—ABS*: Anti-quantum attribute-based signature for EMRs sharing with blockchain," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2022, pp. 1176–1181.
[24] H. Tewari and A. Hughes, "Fully anonymous transferable Ecash," Cryptol. ePrint Arch., 2016. [Online]. Available: https://eprint.iacr.org/2016/107
[25] V. Rao, "Paras—A private NFT protocol," Cryptol. ePrint Arch., 2022. [Online]. Available: https://eprint.iacr.org/2022/976
[26] A. Ferone and A. Della Porta, "A blockchain-based infection tracing and notification system by non-fungible tokens," *Comput. Commun.*, vol. 192, pp. 66–74, Aug. 2022.
[27] F. Valeonti, A. Bikakis, M. Terras, C. Speed, A. Hudson-Smith, and K. Chalkias, "Crypto collectibles, museum funding and OpenGLAM: Challenges, opportunities and the potential of non-fungible tokens (NFTs)," *Appl. Sci.*, vol. 11, no. 21, p. 9931, Oct. 2021.
[28] F. Regner, N. Urbach, and A. Schweizer, "NFTs in practice—Non-fungible tokens as core component of a blockchain-based event ticketing application," 2019. [Online]. Available: https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1045/wi-1045.pdf
[29] J. Arcenegui, R. Arjona, and I. Baturone, "Secure management of IoT devices based on blockchain non-fungible tokens and physical unclonable functions," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* Cham, Switzerland: Springer, 2020, pp. 24–40.
[30] R. García, A. Cediel, M. Teixidó, and R. Gil, "Semantics and non-fungible tokens for copyright management on the metaverse and beyond," 2022, *arXiv:2208.14174*.
[31] M. Krasnoselskii, Y. Madhwal, and Y. Yanovich, "KRAMER: Kanaria NFT collection rarity meter," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2022, pp. 1–2.
[32] P. Robinson and R. Ramesh, "General purpose atomic crosschain transactions," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 61–68.
[33] M. Herlihy, "Atomic cross-chain swaps," in *Proc. ACM Symp. Princ. Distrib. Comput.*, Jul. 2018, pp. 245–254.
[34] J. Gugger, "Bitcoin-monero cross-chain atomic swap," Cryptol. ePrint Arch., 2020. [Online]. Available: https://eprint.iacr.org/2020/1126
[35] A. Zamyatin, M. Al-Bassam, D. Zindros, E. Kokoris-Kogias, P. Moreno-Sanchez, A. Kiayias, and W. J. Knottenbelt, "SoK: Communication across distributed ledgers," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2021, pp. 3–36.
[36] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1991, pp. 129–140.
[37] C.-P. Schnorr, "Efficient identification and signatures for smart cards," in *Proc. Conf. Theory Appl. Cryptol.* New York, NY, USA: Springer, 1989, pp. 239–252.
[38] 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.

ZHANWEN CHEN received the joint master's degree in computer technology from the University of Wollongong (UOW) and Central China Normal University (CCNU), in 2019. He is currently pursuing the Ph.D. degree with the University of Tsukuba. His research interests include blockchain security, applied cryptography, and privacy-preserving in network applications.

KAZUMASA OMOTE received the Ph.D. degree in information science from the Japan Advanced Institute of Science and Technology (JAIST), in 2002. He worked at Fujitsu Laboratories Ltd. From 2002 to 2008, he was engaged in research and development for network security. He was a Research Assistant Professor at JAIST, from 2008 to 2011, where he was an Associate Professor, from 2011 to 2016. He was an Associate Professor at the University of Tsukuba, from 2016 to 2022, where he has been a Professor, since 2022. His research interests include applied cryptography, network security, and blockchain security. He received the WISTP 2019 Best Paper Award. He was the General Co-Chair of ACNS 2021 International Conference.