A Lightweight NFT Auction Protocol for Cross-chain Environment

Hongyu Guo, Mao Chen, and Wei Ou(✉)

School of Cyberspace Security (School of Cryptology), Hainan University,
Haikou 570228, Hainan, China
ouwei@hainanu.edu.cn

Abstract. The NFT market has been booming in recent years. In 2021, digital artist Pak's newest creation, The Merge, fetched US$91.8 million on Nifty Gateway. Since then, many NFT owners have turned to auctions to gain more profits through their collections. Ethereum covers the majority of NFT transactions at the moment. However, it will be hard for them to make profits if they have only one way to sell. To settle this situation, we propose an auction protocol for NFTs which works in a cross-chain environment. We design our protocol by using hash time lock and adding strategies to control users' malicious behaviors. We also optimize the cross-chain asset exchange process to ensure both auction and exchange are successful. Through testing in Ethereum and FISCO BCOS networks, the experimental results show that our scheme is capable of completing auctions in heterogeneous blockchain networks and maintaining low communication costs. The transactions can be confirmed in an average of 4 blocks, and the contract strategies will filter out invalid transactions. We also do additional experiments to prove that our protocol can resist reentrancy.

Keywords: Non-fungible token · Electronic auction · Cross chain · Asset swap

1 Introduction

Non-fungible token (NFT [1]) is a type of cryptocurrency and was firstly proposed in Ethereum Improvement Proposals (EIP-721 [2]). Unlike the traditional ones, NFT is unique, which means it cannot be exchanged equivalently. When an NFT is minted, it also records information about its owner, the time it was minted, etc. It can be traded, but it cannot be split or replaced. This type of token is now widely used to prove the ownership of virtual assets such as images, videos, etc. It emphasizes the unique characteristics that attract the creator's

This work was supported in part by the Hainan Provincial Natural Science Foundation of China (621RC508), Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A16), the Science Project of Hainan University (KYQD(ZR)-21075).

Y. Xu et al. (Eds.): ML4CS 2022, LNCS 13655, pp. 133–146, 2023.
https://doi.org/10.1007/978-3-031-20096-0_11

and the public's attention, indicating the asset's potential value. Collins Dictionary has also selected "NFT" as its word of the year for 2021, reflecting its influence to a certain extent. According to Forbes, the NFT market generated more than $23 billion in volume in 2021, which is an explosive increase from 2020 that has been sustained to date. However, some investors see the NFT market in 2021 as a speculative bubble likely to collapse quickly. However, to this day (May 2022), the NFT market remains highly active. Although the overall volume of transactions has decreased, the number of transactions has increased rather than decreased, which indicates that the value of a single NFT is rising. Compared to NFT, bitcoins and tokens generated based on ERC-20 are homogeneous. For example, the first bitcoin block was mined by Satoshi Nakamoto, who received the bitcoin reward for that block. However, this earliest bitcoin is now lost in the Bitcoin network and is no different from the bitcoin generated by the block just mined. Smart contracts manage NFTs, and over 97% of NFT smart contracts are deployed in the Ethereum leading network. However, the thousandfold return on its increasing market draws vast attention worldwide. Due to the staggering growth volume, the Ethereum network can no longer meet the needs of all users. Those who own NFTs wish that they can trade their NFTs in other blockchain networks, which involve the technologies of cross-chain asset exchange and electronic auction.

First, to solve the problem of blockchain data silos, researchers have developed several ways to realize the exchange of assets or information between different blockchain networks. The existing cross-chain approaches are divided into four basic methods [3]: notary schemes, sidechains/relays, hash-locking, and distributed private key control. The notary mechanism is essentially a kind of intermediary, and this mutually trusted intermediary verifies and forwards cross-chain messages. In a sidechain scheme, miners need to use Simplified Payment Verification (SPV) to verify transactions on other chains, resulting in a soft fork of the main chain that does not easily support cross-chain exchange. Hash-locking technology, the idea of which is to create a micro-payment channel to lock deposits for a specific time, has been applied to the Lightning Network. However, it allows malicious users to request transactions frequently but refuses to redeem them, resulting in some tokens being locked for a long time. In the distributed private key control scheme, multiple verifiers realize currency exchange based on secure multi-party computation and threshold signature technology. Tesseract [4] is a system that utilizes a Trusted Execution Environment (TEE), SGX. However, the trading accounts of all clients of that project are managed by SGX, which is of significant risk.

In terms of the electronic auction, blockchain and secure multi-party computation play an active role, especially in reverse auctions [5] and double auctions [6]. Traditional auctions are managed by a central auction service structure called the auctioneer. It coordinates the auction process and holds most of the data and power. Nevertheless, it can also lead to severe consequences when the auctioneer act maliciously. Through blockchain, users can participate in an auction without any auctioneers. As long as the corresponding contracts are deployed, users need no one to trust. Furthermore, researchers have proposed sealed-bid schemes using secure multi-party computation. The MPC protocol allows multiple users to perform collaborative computing under mutual distrust leaking their privacy. However, such schemes are usually very complex and can hardly be used in existing blockchain networks. At present, there is very little research on the cross-chain auction protocol. According to our investigation, AucSwap [7] proposed a cross-chain asset swap protocol based on the Vickrey [8] auction model, which has the characteristics of atomicity and decentralization. However, its experimental environment is limited to homogeneous Ethereum, and it cannot overcome the shortcomings of the Vickrey auction model itself. As a second-price auction model, it cannot defend against joint attacks by bidders nor maximize the auctioneer's revenue. To address such issues, we propose a lightweight auction protocol aiming at NFT, which works in a cross-chain environment. We use hash time lock contracts to achieve cross-chain asset transfer, which makes it efficient and decentralized. Smart contracts conduct the process of the bidding parts, and bidding strategies are included in the contracts to enhance the support of blockchains and simplify the auction procedure. The experiment results show that our scheme is competent for isomorphic and heterogeneous cross-chain auctions and requires less communication cost. The main contributions are listed as follows:

- By using atomic exchange technology, we propose an NFT auction protocol for cross-chain conditions. It does not need any third-party trusted auctioneers, thereby preventing the harm of user collusion.
- The auction process is conducted during the asset exchange to ensure the interests of both parties. As long as the auction successes, the cross-chain asset exchange is bound to implement.
- We use blockchain anonymity to protect the user's identity and temporarily lock the user's amount in the smart contract to ensure that the user cannot deny it.
- We provide some interfaces to help users learn essential information about the bidding process, such as the highest bid at now and which address will benefit from it. We completed the tests in the Ethereum-Ethereum and Ethereum-FISCO BCOS environments, respectively, which proved that our protocol has a certain tolerance for heterogeneous cross-chain environments and achieved a good performance at 509.8TPS.

The rest of the paper is organized as follows: We summarize the related works in Sect. 2 and then illustrate our method in Sect. 3. Section 4 does the experiment evaluation, and the final part discusses the conclusion.

2 Related Works

2.1 Cross-Chain Schemes

There are currently four mainstream cross-chain schemes, including a notary scheme mechanism, relay chain/side chain, hash time lock, and distributed private key control.

Notary Scheme. The notary scheme is a technical framework created based on the Interledger [9] protocol, similar to the real-world intermediary mechanism. This mechanism assumes that the two sides of a transaction cannot trust each other and introduces a third party trusted by both sides of the transaction to act as a notary. The notary scheme is divided into single-signature notary scheme, multi-signature notary scheme, and distributed signature notary scheme. The single-signature notary scheme operates with relatively high processing efficiency, which is the simplest but also the model with the highest risk of a single point of failure. This system has the problem of centralization. The security of the central node is the key to the system's stability; once the notary itself is maliciously attacked, the transaction becomes untrustworthy, and the whole system will have a security vulnerability. The distributed signature notary scheme uses the idea of secure multi-party computing [10], which is more secure but more challenging to implement.

Sidechains and Relays. BTC-Relay [11] is the first sidechain of Bitcoin [12] and Ethereum [13]. In a sidechain mechanism, a sidechain is another blockchain system with a completely independent function. Then the sidechain can actively sense and act on information from the main chain. A sidechain is essentially a cross-blockchain solution that enables the transfer of digital assets from one blockchain to another. The concept of sidechaining first appeared in Bitcoin, and now its representatives are Cosmos [14] and Polkadot [15]. Sidechain technology allows for the transfer of assets between Bitcoin and other currencies, allowing users to use assets they already own by accessing the new cryptocurrency system. Because the sidechain system is independent of the main chain, technological innovation on the sidechain is not hindered. At the same time, the damage to the sidechain does not affect the performance and security of the main chain.

Hash-Locking. Hash locking is a technical implementation model proposed in the Lightning Network, widely used in the Lightning Network technical architecture. The Lightning Network is a typical application of hash locking technology, essentially a mechanism to perform zero-confirmation transactions using HTLC securely. Herlihy M et al. [16] propose a hash-locking scheme to support asset exchange between two chains. Two users from different chains who need to exchange can each exchange assets on their blockchain using hash time-locked contracts.

Distributed Private Key Control. Distributed private key control is a technology through private key generation and control technology. This technology maps cryptocurrency assets to a chain with built-in asset templates based on blockchain protocols. And then deploy smart contracts based on cross-chain transaction information to create cryptocurrency assets. Fusion [17], for example, uses distributed key generation algorithms and threshold signature technology in cryptography to ensure the security of cross-chain assets. All nodes participating in the system consensus decide the locking and unlocking of assets in the cross-chain process. Therefore, no node or a few nodes jointly have the right to use the assets in the process.

2.2 Blockchain-Based Electronic Auction

The decentralized, tamper-evident, and open and transparent features of blockchain are beneficial to solving the traditional auction scenario of problems, such as un-trustworthy tripartite. Therefore, many researchers try to deploy electronic auctions in blockchain [18,19] networks to conduct them. Existing blockchain-based e-auction protocols can be broadly classified into two categories:

The first solution is to rely on digital currency. In this type of solution, the logic in a smart contract is often used to manage the entire auction process. Bidders are given a limited time to bid by providing a deposit held in a smart contract that handles the auction process. At the end of the bidding period, the contract compares all the bids and determines the winner, seizes the winner's funds, and returns the deposit to the others. Since the blockchain address does not reflect the bidder's real identity, this scheme has certain anonymity. However, this makes it difficult to expose or punish malicious bidders. In addition, bidders generally use digital currency to bid through transactions so that the blockchain network can guarantee that they cannot double-spend or reverse their bids. However, the amount of the bid is publicly transparent and less private.

If they do not rely on digital currency, auctions are generally conducted by sending cryptographic values, such as those electronic auction schemes based on secure multi-party computation [20]. These schemes [21,22] rely on cryptographic techniques such as group signatures and homomorphic encryption to enable anonymous and verifiable auctions between semi-trusted entities. Since there is no need to send digital currency directly, this scheme avoids some financial risk, but the winning bidder may renege after winning the auction and not send the money. In addition, because it relies on more cryptographic technologies and the protocols are more complex, cause corresponding computational overhead is significantly increased. It will make it challenging to be implemented on a large scale in existing blockchain networks.

2.3 Cross-Chain NFT

In multi-chain development, cross-chain has become a hot spot for market and academic research. NFT is also blooming on multiple chains, but cross-chain NFT is still an immature concept. In 2021, the NFT cross-chain exchange protocol ENVELOP went live and currently supports public chains such as Ethereum, Cryptocurrency Smart chain, and Polygon. ENVELOP's approach is to store the original NFT as a cryptocurrency or other NFT, that is, to encapsulate the original NFT in a new NFT until the owner decides to open the NFT. After opening it (like opening an envelope), the owner of the original NFT can sell, store or repackage the NFT.

Although the Ethereum leading network is often congested, it is still the preferred rooting place for NFT players. Because it has the most active NFT market, the latest and most exciting things generally appear here, and the best liquidity is also here. For example, it can be observed from Etherscan that Gh0stly, a chain that can store NFTs, only called the function of traverseChains nine times within a month. This means that only nine transfers of NFTs from the Ethereum leading network to this chain occurred during this period. This shows that the public does not yet accept the current scenario of cross-chain NFTs, and ordinary users tend to transfer their NFTs through auctions or sales in Ethereum.

3 Cross-Chain Auction Protocol

3.1 Protocol Illustration

The protocol consists of three contracts and implements the following functions, and Fig. 1 describes its process.

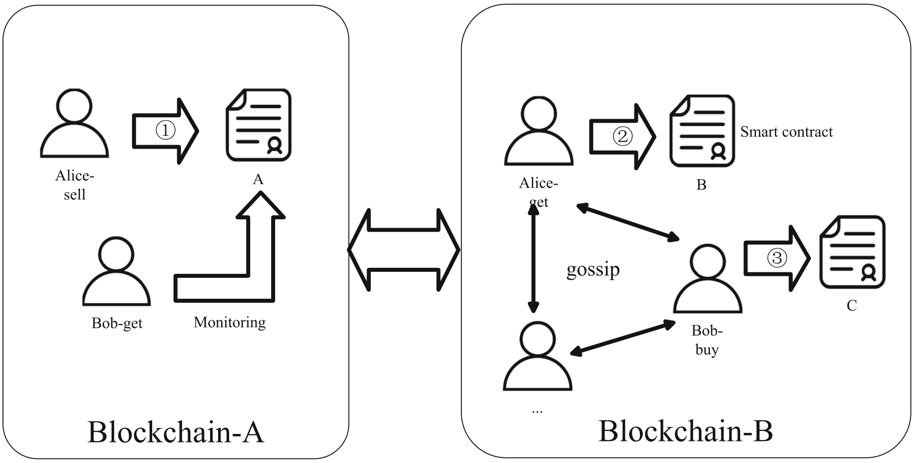

Fig. 1. The process of the protocol.

Step 1: First, the seller passes a random string z, and the Hash encrypts this string to generate a Hash(z). According to Hash (z), the hash time lock contract (HTLC) can be written to lock the NFT assets on the account and deployed on the Ethernet. And then broadcast to the whole network to prove the authenticity of the NFT assets. The transaction deadline in the HTLC can be set to half an hour after the auction end. And then, if a user on the blockchain can provide the secret z before the deadline, the user can access the NFT assets. **Step 2:** The seller sends an auction request across the blockchain to all users on the blockchain (including Ethereum and FISCO BCOS) via Algorithm 1. The initialization parameters require the input of the auctionend (up to three hours) and the beneficiary address. **Step 3:** Once the bidder receives auction information, the user can make an offer through Algorithm 2 before the end of the auction. The price offered must be an actual bid based on the available assets, and all unrealistic bids will be denied service. **Step 4:** The user can obtain the address of the user with the highest current bid and the current highest price through the function in the bidding contract. If the previous bid is surpassed, the previous bid can be retrieved through Algorithm 3. Users can determine whether to continue with a new round of bidding based on the current situation. **Step 5:** The seller receives the information and offer of the highest bidder after the auction ends and broadcasts the results of that auction. **Step 6:** After the auction ends, the winner is asked to generate the corresponding HTLC for asset exchange. The winner can base on the auction's price bid and the seller's HTLC to deploy the NFT asset to generate the contract.

3.2 NFT Locking Process

The first step in the protocol is that sellers need to lock the NFT they wish to auction to a specific contract. Assuming that user A owns an NFT on chain A, the contract address of its minting is Contract address A. Through this address, any user can find the current state information of the NFT, including who minted it, the current owner, and whether the NFT is in the state of sale.

3.3 NFT Auction Process

The auction process of NFT is the core process of this protocol. The seller sends an auction request to the B chain (another chain) and creates a corresponding contract. The transaction is spread in the blockchain network. And then, interested buyers can interact with the contract account generated by the transaction to compete for bidding. The buyer sends the bid amount as a transaction to the contract during the bidding process. To filter out invalid offers, the logic inside the contract will reject all bids that are less than the current highest bid. In addition, by interacting with the contract, users can view the current maximum bid amount at any time and adjust their bids. The sender can call the interface to retrieve the deposit if the bid is not accepted. Because the flow of money in the blockchain is open and transparent, each user can verify the legitimacy of the entire process by querying the transaction data of the contract.

Algorithm 1. Auction Contract Setup

```
Input: auctionend, profots, price
Output: transactionStatus, contractAddress
  if auctionend $\leq$ 10800 then
    set bidding.time = block.timestamp + auctionend
    if len(profits) == 42 then
      set beneficiary = profits
      set startingPrice = price
    end if
  end if
  return contractAddress
```

Algorithm 1 describes the initial parameters required to deploy the contract, including auctionend, profits, and price. Among them, "auctionend" represents the time when the auction ends we need to initialize, and the "auctionend" must be no more than three hours. Profits said that we need to enter the address of the NFT holder (the address of the NFT owner on different chains is subject to the actual situation) and determine whether the address is legal. Next, the seller needs to enter the expected price for the NFT. After the deployment is successful, the status information of the current contract (whether the deployment is successful or not), the transaction hash, and the contract address will be displayed.

Algorithm 2. Bid for NFT

```
Input: amount
Output: transactionStatus
  while auctionend > time.Now do
    while amount > highestBid do
      if highestBid != startingPrice then
        returnsBid[highestBidder]+= highestBid
      end if
      highestBidder = msg.sender
      highestBid = amount
    end while
  end while
```

When users bid for NFT, they will first enter a price they think is reasonable or call the function with the highest bid to query the highest bid of the current auction as a basis for bidding. In Algorithm 2, the timestamp of the current bid auction is compared with the timestamp of the end of the auction. If the period of the current transaction is during the auction period, the current user bid amount and the highest auction price will be judged. Suppose it is greater than the current highest bid price. In that case, the highest bid price will be mapped to the address of the highest bidder first and wait for the bidder to call up the bid amount manually. Because of the grammatical feature of solidity, when the user's bid is automatically returned to the account, the malicious contract can intercept the user's assets by calling the function body. Therefore, the amount after the bid is exceeded must be manually retrieved by the user to ensure security. And then, the address of the highest bidder will be changed to the address of the current user. Correspondingly, the highest price is also changed to the price offered by the current user.

When the user's bid is exceeded, the bid amount will be placed in the mapping of its address, and the user needs to call the function to retrieve the bid amount manually. When calling the function, the user does not need to enter the address where he wants to withdraw the amount. The function body will judge whether the user's address and the input address are consistent. Only when the addresses are consistent can the amount be withdrawn. Then it will determine whether

Algorithm 3. Withdraw

```
Input: accountAddress
Output: transactionStatus
  if address != msg.sender then
    set amount = returnsBid[address]
    if amount > 0 then
      set returnsBid[address] = 0
      if !address.send(amount) then
        returnsBid[address] = amount
      end if
    end if
  end if
```

there is an amount in the current address map and if so, it will first clear the amount in the address map. This is because, as part of accepting the call, the receiver can call the function again before 'send' returns, so first, set the amount in the address map to zero). And then send the corresponding amount to the current user's address.

3.4 Asset Exchange

Since NFT can only be deployed on Ethereum, for a successful bidder, the user's blockchain is first determined (Ethereum or FISCO BCOS, accounts for receiving assets differ on different chains). Assets can then be exchanged via HTLC. According to the traditional hash time lock method, the buyer and seller must create a hash time lock contract with the exact string. However, in our protocol, the seller has deployed the hash time lock contract before the auction, and the hash string Hash(z) is hosted in the auction contract. When the seller successfully deploys a hash time lock contract that locks the NFT assets, the smart contract will broadcast to the entire network. All users participating in the auction have received this network broadcast and confirmed the NFT assets before the bidding starts. The buyer actively calls a function to deposit the bids into the hash time lock contract after the auction ends. The seller performs two confirmations when it detects the presence of the same contract:

4 Experiment and Analysis

4.1 Experiment Setup

In order to verify and evaluate the cross-chain auction protocol for NFT proposed in this paper, we wrote the corresponding Solidity smart contracts to implement the logic process on the Ethereum private network and FISCO BCOS.

We built an Ethereum private network and deployed the NFT on the Ethereum test network. As you can see from Fig. 2, there are few accounts on each blockchain, and each user controls at least one account. We conducted

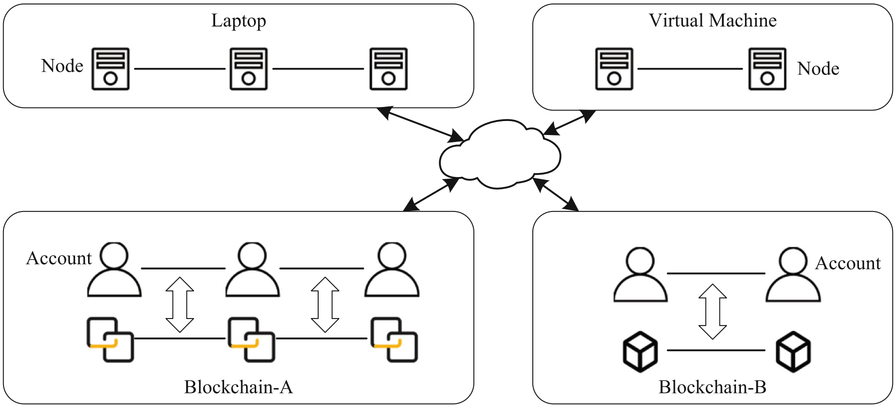

Fig. 2. Network topology for cross-chain auction experiment.

experiments on a laptop (CPU: i7-11800h, memory: DDR4 3200 8G*2, 500G SSD) and ran a few light nodes on virtual machines. After that, we also built up a FISCO BCOS network to simulate heterogeneous conditions. The data of transactions were recorded on the blockchain, and we exported it into tables. We implemented two experiments to test our protocol: the Ethereum-Ethereum cross-chain auction and the Ethereum-BCOS cross-chain auction. In each experiment, the NFT is always deployed in one Ethereum, and the auction contract will be initiated in another test chain. Finally, the exchange of cross-chain assets will be completed through the hash time lock contracts. We analyze and evaluate the performance and security of the protocol from the following aspects: transaction completion time, bid strategy control, heterogeneous cross-chain tolerance, and comparison with existing schemes. We first conduct the Ethereum-Ethereum cross-chain auction. There are four users in this process, one of which created the auction contract, and the rest can bid freely. During this process, we first manipulate the users to bid and withdraw legally and test the availability of the interfaces provided in the contracts. Then we focus on several key issues. For example, we let some users use reentrancy while he calls to see if our scheme can resist it.

Moreover, we also send some carefully designed transactions to examine the effectiveness of our bidding strategy. When the auction ends, we will also check if the cross-chain asset exchange succeeds. The block number and time are recorded so that we can see the efficiency of our protocol. The following experiment occurs in the Ethereum-BCOS networks, and the auction is completed in the FISCO BCOS network. There are four groups of users, and their asset changes are similar to those in the former experiment. In the BCOS network, there are few interfaces currently implemented. We first deploy asset contracts in the BCOS network, register enough assets for each user, and then finish the auction. The bidding and withdrawal operations of the auction are simulated. It is a method by which money can transfer from one account to another. We collect the experiment results and do the work of calculation and comparison.

4.2 Results

These are the transaction records for the first Ethereum-Ethereum cross-chain auction. There are four users in the auction process, among which user1 is the initiator of the auction, who creates the bidding contract and sets the auction duration. The other three users can bid continuously. For the convenience of analysis, we take the first transaction block as the initial block height and time when processing data. It can be seen that the entire auction lasted for 1532 s, and 21 transactions were completed during the period, which does not reflect the performance of the network because the bidding needs to be manually initiated by users. Most of the time, we are waiting for users to bid. The user interacts with the contract to send quotations through Bid. After the contract accepts a new quotation, it will update the current highest quotation and the address of the current highest quotation user. The purpose of providing these two interfaces is to facilitate users to view the current highest valid quotation to adjust their quotation strategy and avoid invalid quotations. Our protocol does not limit the address from which the quotation is initiated, except for the limit on the quotation amount. Moreover, the contract provides an interface to query the address of the auction initiator, which is. By comparing the address with the highest bid address, the user can know whether the auction initiator is trying to raise the price, making it difficult to cheat maliciously (Table 1).

Table 1. The Ethereum-Ethereum cross-chain auction details.

Transaction number	Block number	Timestamp	From	Value	Method	Status
1	0	0	user1	0	contract created	success
2	5	75	user2	10	bid	success
3	12	180	user3	10	bid	fail
4	14	210	user3	50	bid	success
5	18	270	user4	99	bid	success
6	20	300	user4	100	bid	success
7	22	330	user4	99	withdraw	success
8	26	390	user2	10	withdraw	success
9	29	390	user2	123	bid	success
10	31	465	user3	50	withdraw	success
11	33	495	user3	144	bid	success
12	37	555	user3	0	withdraw	success
13	39	585	user4	100	withdraw	success
14	42	630	user4	500	bid	success
15	48	720	user4	0	withdraw	success
16	53	795	user4	0	withdraw	success
17	67	1005	user3	144	withdraw	success
18	75	1125	user1	0	auctionEnd	fail
19	86	1292	user1	500	auctionEnd	success
20	88	1322	user2	123	withdraw	success

It can be seen from transactions 2 and 3 that user2 and user3 have sent the exact quotation successively because the quotation strategy of this agreement does not accept all quotations lower than the current highest quotation. Hence, transaction 3 fails, and the corresponding quotation is also invalid. Users can also send bids consecutively, as long as the later bid is higher than the previous one, such as transactions 5 and 6. Once an offer is sent, the corresponding amount is temporarily held in the contract, and all but the current highest bid can be withdrawn, whether the auction is in progress (transactions 7, 8, etc.) or has ended (transactions 20, 21). When the contract returns the user's invalid quotation, it does not transfer again. However, it directly returns the quotation through the function "revert" to circulate the user's funds safely and quickly. Users with insufficient funds can retrieve the original invalid quotations and then submit quotations again (transactions 8, 9), which effectively increases the flexibility of capital flow. At the end of the bidding process, we complete the exchanges of cross-chain assets through hash time lock contracts. Assume that the accounts of both parties to the swap are Alice and Bob in Fig. 1, and both have accounts for receiving and transferring assets. In our protocol, since the buyer's funds will be locked in the bidding contract, the auctioneer must lock the NFT asset to a specific contract before the auction, assuming its original image is ε and the locking time is t_1. After the auction, the winner generates a hash time lock contract with the same original image by calling "auctionEnd", passing in the hash string and locking time t_2. (It is required that $t_1 \gg t_2$ to ensure that the auction and exchange have enough time to proceed). At this time, A can obtain the auction revenue by offering the secret, and B can also obtain the NFT assets on another blockchain (Table 2).

Table 2. Testing results of transfer in the Ethereum-BCOS cross-chain auction.

Name	Succeed	Fail	SendRate (TPS)	Maxlatency (ms)	Minlatency (ms)	Avglatency (ms)	TPS
Transfer	10000	0	976.7	18.35	10.35	12.23	509.8

It can be seen from the table that on the BCOS network, the Send Rate (TPS) of the method based on this protocol is 976.7, of which a total of 10,000 transactions were sent, 10,000 times were successfully verified without failure, and the average delay in verifying transactions was 12.23 ms, which can maintain good performance.

5 Conclusion

In this paper, we combine the process of hash locking and cross-chain auction to designing a decentralized protocol to complete the cross-chain auction of NFT assets. The scheme has no third-party auctioneer and can filter invalid bids through in-contract strategies. Through testing in Ethereum-Ethereum and

Ethereum-BCOS, it can be proved that our protocol is compatible with a heterogeneous cross-chain environment, with an average of 4 blocks to confirm transactions. We also reached 509.8 TPS in the Ethereum-BCOS network. Nevertheless, there are still some shortcomings in our work, such as not being able to run on blockchains that do not support solidity; the degree of automation of the protocol is not high. It can be seen from the table that on the BCOS network, the Send Rate (TPS) of the method based on this protocol is 976.7, of which a total of 10,000 transactions were sent, 10,000 times were successfully verified without failure, and the average delay in verifying transactions was 12.23 ms, which can maintain good performance.

Our next step will try to implement secret auctions in a cross-chain environment. Since the transaction amount on the blockchain is publicly queryable, it is difficult to hide the bid amount. There are some secret bidding schemes based on secure multi-party computation. However, due to the anonymity of blockchain identities, users participating in the auction can choose to bid a high price to influence the auction and refuse to pay at the payment stage. Even if the address is blocked, malicious users can create new addresses at a small cost. Therefore, for the secret bid-ding protocol adapted to the blockchain, more research is needed on overcoming the contradiction between secret bidding and denial of payment.

Acknowledgements. This work was supported in part by the Hainan Provincial Natural Science Foundation of China (621RC508), Henan Key Laboratory of Network Cryptography Technology (LNCT2021-A16), the Science Project of Hainan University (KYQD(ZR)-21075).

References

1. Wang, Q., Li, R., Wang, Q., Chen, S.: Non-fungible token (NFT): overview. Evaluation, Opportunities and Challenges. arXiv (2021)
2. Entriken, W., Shirley, D., Evans, J., Sachs, N.: EIP-721: ERC-721 non-fungible token standard. Ethereum Improvement Proposals (721) (2018)
3. Deng, L., Chen, H., Zeng, J., Zhang, L.-J.: Research on cross-chain technology based on sidechain and hash-locking. In: Liu, S., Tekinerdogan, B., Aoyama, M., Zhang, L.-J. (eds.) EDGE 2018. LNCS, vol. 10973, pp. 144–151. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-94340-4_12
4. Smith, R.: An overview of the tesseract OCR engine. In: Ninth International Conference on Document Analysis and Recognition (ICDAR 2007), vol. 2, pp. 629–633. IEEE (2007)
5. Gumussoy, C.A., Calisir, F.: Understanding factors affecting e-reverse auction use: an integrative approach. Comput. Hum. Behav. **25**(4), 975–988 (2009)
6. Liu, L., Du, M., Ma, X.: Blockchain-based fair and secure electronic double auction protocol. IEEE Intell. Syst. **35**(3), 31–40 (2020)
7. Liu, W., Wu, H., Meng, T., Wang, R., Wang, Y., Xu, C.Z.: AucSwap: a Vickrey auction modeled decentralized cross-blockchain asset transfer protocol. J. Syst. Architect. **117**, 102102 (2021)
8. Ausubel, L.M., Milgrom, P., et al.: The lovely but lonely Vickrey auction. Combin. Auctions **17**, 22–26 (2006)

9. Neisse, R., et al.: An interledger blockchain platform for cross-border management of cybersecurity information. IEEE Internet Comput. **24**(3), 19–29 (2020)
10. Chaofan, Y., Wang, L., Zhou, A., Zhang, N., Tian, H., Xiao, J.: Method and apparatus for performing multi-party secure computing based-on issuing certificate. US Patent 11,038,699, 15 June 2021
11. Chow, J.: BTC relay. BTC-relay (2016)
12. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Decentralized Bus. Rev. 21260 (2008)
13. Wood, G., et al.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. **151**(2014), 1–32 (2014)
14. Scoville, N., et al.: The cosmic evolution survey (COSMOS): overview. Astrophys. J. Suppl. Ser. **172**(1), 1 (2007)
15. Wood, G.: Polkadot: vision for a heterogeneous multi-chain framework. White Pap. **21**, 2327–4662 (2016)
16. Herlihy, M.: Atomic cross-chain swaps. In: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, pp. 245–254 (2018)
17. Yang, G., Zang, C., Chen, J., Guo, D., Zhang, J.: Distributed fusion cross-chain model and architecture. IET Blockchain (2022)
18. Sánchez, D.C.: Raziel: private and verifiable smart contracts on blockchains. arXiv preprint arXiv:1807.09484 (2018)
19. Galal, H.S., Youssef, A.M.: Verifiable sealed-bid auction on the ethereum blockchain. In: Zohar, A., et al. (eds.) FC 2018. LNCS, vol. 10958, pp. 265–278. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-662-58820-8_18
20. Lindell, Y.: Secure multiparty computation. Commun. ACM **64**(1), 86–96 (2020)
21. David, B., Gentile, L., Pourpouneh, M.: FAST: fair auctions via secret transactions. In: Ateniese, G., Venturi, D. (eds.) ACNS 2022. LNCS, vol. 13269, pp. 727–747. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-09234-3_36
22. Shi, R.H.: Anonymous quantum sealed-bid auction. IEEE Trans. Circ. Syst. II express briefs **69**(2), 414–418 (2021)