AucSwap: A Vickrey auction modeled decentralized cross-blockchain asset transfer protocol

Weiwei Liu [a,c], Huaming Wu [b], Tianhui Meng [a,*], Rui Wang [a,c], Yang Wang [a], Cheng-Zhong Xu [d]

[a] Shenzhen Institute of Advanced Technology, Chinese Academy of Science, Shenzhen, China
[b] Tianjin University, Tianjin, China
[c] University of Chinese Academy of Science, Beijing, China
[d] State Key Lab of IoTSC & Department of Computer and Information Science, University of Macau, Macau, China

ARTICLE INFO

Keywords:
Blockchain
Cross-chain
Asset swap
Vickrey auction

ABSTRACT

With the rapid development of blockchain technology, the cross-blockchain asset transfer has been in great demand. However, most existing cross-blockchain solutions encounter low efficiency problems due to the centralized features, unfriendly development environment, and difficulty in cooperation. This paper proposes an interaction protocol for secure and efficient cross-blockchain transfer process, wherein the cross-blockchain asset transfer is modeled as an auction process. We design our protocol by leveraging the atomic swap technology and Vickrey auction scheme to achieve efficient cross-blockchain asset transfer, without sacrificing the decentralized control. To achieve the transfer efficiency, we optimize the Vickrey auction scheme to share data within the auction and delivery process synchronously. This results in a efficient user information exchange. The experimental results show that not only can our protocol achieve compatibility, but it also incurs little communication overhead in high throughput. A cross-blockchain transfer process can be accomplished in average 4 rounds of interaction. The difference between the transaction completion time and the bid waiting time is less than 1 second. Besides, our protocol guarantees the exchange rate at a reasonable range. The ratio of the cross-blockchain exchange rate to the real exchange rate converges to 0.9 for approximately 200 participants. The transaction fee decreases sharply with the increase of the number of auction participants.

1. Introduction

Since Blockchain technology was introduced in 2008, cryptocurrency systems continuously enlarged the community and exerted bigger impacts on our society [1]. The number of blockchain systems is increasing rapidly, which makes great demands for cross-blockchain asset transfers [2,3]. Besides, the deployment of smart-contract enriches the interaction approaches with the real world, based on which the traditional industry like finance and insurance can expand their scope dramatically [4,5]. We need to strengthen the interoperability between different blockchain systems to meet these diverse application patterns.

Specific to the cryptocurrency, it is necessary to strengthen the property of cross-blockchain asset transfer among separate blockchain systems [6]. As in the early days of the Internet, the interconnection of local area networks (LAN) greatly promoted the development of the network. The expansion of blockchain application demands the development of the transfer protocol, which specifies how an item on one blockchain can be shipped to the other with the same value.

The cross-blockchain asset transfer is a very common but important application scenario in reality applications [7,8]. Take the blockchain-enabled traffic accident automatic disposing as an example (Fig. 1). Supposing Alice has a car accident with Bob, and Alice needs to pay Bob $1000 with insurance and $500 cash. The sensors send the data to the accident disposing system, and the system confirms the responsibility. The accident disposing system collects Alice's payment from her bank account and the insurance payment system, and sends it to Bob. The information and assets flow among four systems in this case, which is slow and complex. Furthermore, the programmers need to deal with the complicated cooperation with different systems. These challenges of inefficient transaction and complex centralized collaboration are urgent to be solved.

To enable cross-blockchain operation, a lot of efforts have been made [9], e.g., the intermediary mechanism with a trusted third part, such as Ripple [10] and Binance [11]. In these schemes, the intermediary obtains the global information and uses it to make a deal [12]. The intermediary also entrusts and guarantees the transaction [13].

* Corresponding author.
E-mail address: th.meng@siat.ac.cn (T. Meng).

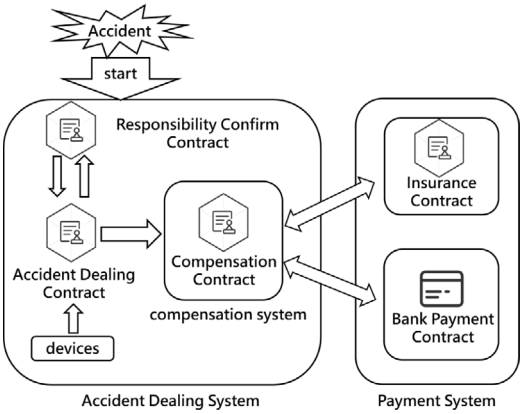

Fig. 1. The automatic accident processing with blockchain.

Another approach is developing a side chain or a relay chain to connect existing systems, represented by Cosmos [14] and Polkadot [15]. By developing a unified intermediate interactive interface, a new system is built between different blockchains [16]. It connects and interacts with the main chain system, transferring information among them [17]. Atomic swap mechanism is also developed for cross-blockchain operation [18,19]. This technology is mainly used in the asset swap scheme, and represented by the hash time lock contract. It utilizes the irreversibility of hash problem to realize atomicity and consistency during the asset swap process.

However, the existing blockchain interoperability schemes may not yield the best performance and decentralization for the following reasons. First, some schemes, e.g. Ripple and Binance, need to sacrifice the decentralization feature of the blockchain system, and transfers information through a trusted third party. However, a trusted third party is a centralized system, that goes against the decentralization of blockchains. Second, it often requires a large amount of developing work in some schemes to maintain a new entity, such as a side-chain or relay-chain system (Cosmos). This greatly increases the difficulty to maintain the blockchain system. Third, most of the existing schemes involve complex communication and coordination mechanisms. Distributed implementations of value transfer across blockchains are promising schemes, but it is still in the course of initial development [20,21]. Few systematic research literature could be found in this field. A Vickery auction is a sealed second price auction, which combines the bid process and auction process into one behavior [22]. This scheme has the advantages of decentralization, incentive fees and convenience in communication, that meet the demands of the cross-blockchain asset transfer problem well.

To address the issues of inefficient transaction and complex centralized collaboration in the existing cross-chain schemes, we propose an interactive protocol "AucSwap". Our protocol is designed by leveraging the atomic swap technology and Vickrey auction to achieve efficient and decentralized cross-blockchain asset transfer. The process of cross-blockchain transfer is abstracted into an auction problem and the basic principles that need to be observed during the transfer are pointed out. In order to enhance the support of blockchain applications, we optimize the Vickrey auction scheme by combining the bidding process with the selection process, which significantly simplifies the auction procedure. Moreover, the auction and delivery process are accelerated through automatic identical information sharing to reduce the redundant transmission. The experimental results show that our method has the advantages of compatibility, little communication overhead and high trading speed. Specifically, the main contributions are listed as follows:

1. The cross-blockchain asset transfer is modeled as an auction process. Through analysis, we leverage the auction mechanism to realize efficient cross-blockchain transfer without the sacrifice of decentralization;
2. By leveraging atomic exchange technology and Vickrey auction mechanism, we design AucSwap, an efficient, secure and decentralized cross-blockchain asset transfer protocol;
3. To the best of our knowledge, we are the first that proposes the general design principles for the cross-blockchain asset transfer system;
4. We implemented AucSwap in a testbed environment and the evaluation results proves its efficiency and consistency. The cross-blockchain transfer process can be accomplished in average 4 rounds of interaction with less than 1 s difference between the transaction completion time and bid waiting time. The ratio of the cross-blockchain exchange rate to the market exchange rate converges to 0.9 for approximately 200 participants.

The rest of the paper is organized as follows: The system model and the proposed scheme are introduced in Section 2. Section 3 describes the cross-chain transfer protocol. Section 4 shows the performance evaluation and discussion. Section 5 presents the related work. Finally, the paper is concluded in Section 6.

2. Preliminaries

2.1. Vickrey auction

Vickery Auction is a second price sealed auction scheme, first proposed by William Vickrey [23]. In the auction process, the bidders submit written bids secretly without knowing others' bidding price. Vickrey's original inquiry treated both auctions of a single item and auctions of multiple identical items, providing a mechanism in which it is a dominant strategy for bidders to report their values truthfully and in which outcomes are efficient [24]. For a single item, the mechanism is often referred to as the second-price sealed-bid auction, or simply the Vickrey auction. Bidders simultaneously submit sealed bids for the item. The highest bidder wins the item, but (unlike standard sealed-bid tenders) the winner pays the amount of the second-highest bid. With these rules, a winning bidder can never affect the price it pays, so there is no incentive for any bidder to misrepresent his value. From bidder n's perspective, the amount he bids determines only whether he wins, and only by bidding his true value can he be sure to win exactly when he is willing to pay the price.

Vickery Auction is a sealed and one-round auction scheme, which consists of three main steps:

(1) The bidders provide the intention price secretly to the auctioneer;
(2) The auctioneer publish all the bid data;
(3) The winning bidder of the highest price complete the transaction by the second-highest price.

According to the auction model, in the offering process, the optimal strategy for each buyer is to directly give its own actual price. Let m and n be the bidders who participate the auction, and ω_m be the bid of the bidder m. Let μ_m be the actual price of the auction goods considered by bidder-m, and $max_{n\neq m}(\omega_n)$ be the max bid of all bidders except m. Then, Bidder-m's earnings φ_m is given as

$$\varphi_m = \begin{cases} \mu_m - max_{n\neq m}(\omega_n), & when \quad \omega_m > max_{n\neq m}(\omega_n) \\ 0, & when \quad \omega_m \leq max_{n\neq m}(\omega_n) \end{cases} \tag{1}$$

where μ_m is the actual price of the auction goods considered by bidder-m, and $max_{n\neq m}(\omega_n)$ is the max bid of all bidders except m. Then, we have: $\omega_m > \mu_m$, the bidder makes the negative earning; $\omega_m < \mu_m$, the bidder losses the earnings when $\omega_m < max_{n\neq m}(\omega_n) < \mu_m$; $\omega_m = \mu_m$, the bidder reaches the optimal strategy.

Table 1
Notations.

Notation	Description
$tx(i)$	The i_{th} cross-blockchain asset transfer transaction
$n(i)$	The number of participants in the i_{th} cross-blockchain asset transfer process
α	The participant who initiates the transaction
β	The participant who responds to the transaction
S	The blockchain on which the participant initiates the transaction (i.e. source-blockchain)
D	The blockchain on which the participant responds the transaction (i.e. destination-blockchain)
ϱ	The time point corresponding to the state, $\varrho \in \{before, after\}$; $before$ is the time before the transaction, and $after$ after the transaction.
$\{R, I\}(x, Y)$	The changing in assets after the transaction, R means reduce and I increase, $x \in \{\alpha, \beta\}, Y \in \{S, D\}$
$Rate(S, D)$	The real exchange rate in the market for the value carrier between the source blockchain system and the destination one
$P(S, D)_{tx(i)}$	The value ratio relationship between the source blockchain system and the destination blockchain system in the actual i_{th} transaction
$Fee(S, D)_{tx(i)}$	The transaction fee paid to the responder during the i_{th} transaction

2.2. Problem formulation and system model

We consider the asset transfer problem between different blockchain systems. The value carrier and transfer are two key components in this problem. The *value carrier* is a kind of virtual asset entity existing in the system. A private key symbolizes the ownership of the asset. It is also the proof when participating in the blockchain system [25]. The *transfer* is the process of the value carriers' ownership alteration between different accounts. It accompanies with the alteration of the value carriers' ownership or the position. Thus the cross-blockchain asset transfer is a process of moving a user's asset into a different position and changing it into different value carriers between different blockchain systems.

In cross-chain transactions, the first things a user focuses on are the exchange rate (Eq. (2)) and the transaction fee (Eq. (3)).

$$P(S, D) = R(\alpha, S)_{tx(i)} : R(\beta, D)_{tx(i)} = I(\beta, S)_{tx(i)} : I(\alpha, D)_{tx(i)} \tag{2}$$

$$Fee(S, D)_{tx(i)} = \begin{cases} \left[Rate(S, D) - P(S, D)_{tx(i)}\right] * I(\beta, S) \\ \left[Rate(S, D) - P(S, D)_{tx(i)}\right] * R(\alpha, S) \\ \left[P(S, D)_{tx(i)} - Rate(S, D)\right] * I(\alpha, D) \\ \left[P(S, D)_{tx(i)} - Rate(S, D)\right] * R(\beta, D) \end{cases} \tag{3}$$

Table 1 presents the prominent notational conventions we use throughout this work. The exchange rate $P(S, D)$ is defined as the value ratio of the auction item on the source and the destination blockchain. If the process of generating value of the blockchain system is regarded as a primary market, the cross-blockchain asset transfer is an exchange behavior in the secondary market. Based on this knowledge, a cross-blockchain asset transfer process needs to observe the rules listed as follows:

- The total of the asset keeps the same during the cross-blockchain asset transfer process, i.e.

$$R(\alpha, S) = I(\beta, S) \tag{4}$$

$$I(\alpha, D) = R(\beta, D) \tag{5}$$

- $Rate(S, D)$ need to be formed by the market spontaneously, and is known by all the participants;
- The exchange rate in the real transaction need to be as close as possible to the $Rate(S, D)$, i.e.

$$\lim_{n(i)\to\infty} P(S, D)_{tx(i)} = Rate(S, D) \tag{6}$$

- There need to be some transaction fee in the transfer process to encourage users participating in the cooperation, i.e.

$$Fee(S, D)_{tx(i)} \neq 0 \tag{7}$$

and the transaction fee decreases with the increase of the participants, i.e.

$$\lim_{n(i)\to\infty} Fee(S, D)_{tx(i)} = 0 \tag{8}$$

Eqs. (4)–(8) describe the model situation of the asset cross-blockchain transfer problem. Eqs. (6) and (8) are the constraints for the exchange rate and the transaction fee in the model. We assume the user budget constraint is $\lambda\varepsilon$, where ε is the actual price and λ is the budget parameter ($1 < \lambda \leqslant 2$).

Our purpose is to make the cross-chain exchange rate close to the one in the market, while maintaining the transaction fee as low as possible. Taken the requirement and reality of the trading system into consideration, the *objectives* of the cross-blockchain asset transfer scheme are listed as follows:

- **Decentralization**. In the process of cross-blockchain asset transfer, the transaction is reached between two specific users. The decisions and price expectations in the transaction shall be determined by the participants themselves. And there is no other third parties involved in a specific transaction.
  That is $(Info, Op)_{transaction} \to 0$, where $Info$ is the market information and Op is the operation from other third parties.
- **Rational Exchange Rate**. An impeccable exchange scheme need to make the asset exchange rate as close as possible to the market rate;
- **Atomicity and Consistency** [18]. The state of the transaction is only between reached or not. The modification is consistent among all parties.
- **Privacy Protection** [26]. The necessary open information is specific to this transaction, and users' privacy information must not be disclosed.
- **High Efficiency**. The necessary transaction information transmission must be minimized, and transaction execution process is as simple as possible to reduce the transaction cost.
- **Incentive Mechanism**. There are necessary transaction fees in the process to encourage the participation and competition of all parties;
- **Isomerism Tolerance**. The transaction scheme can be operated among different blockchain systems, not just for a specific class of blockchain systems.
- **Forward Compatibility and Development Friendliness**. The transaction scheme should be compatible with the existing blockchain system, and developers can support the trading mechanism with a small amount of work.

Under the constraints of the above properties, the problem of cross-blockchain asset transfer can be well abstracted into an auction problem. The improved auction process can well meet the above criteria. The combined analysis of the auction model and the cross-blockchain asset transfer problem will be explained in detail in Section 3.

2.3. Vickrey auction based solution

According to the above analysis, the cross-blockchain asset transfer process can be abstracted into an auction process: the seller needs to sell

the assets on the source blockchain system, and restrict the transaction be made in the form of asset in a destination blockchain system. We resolve the problem in the approach of an auction scheme.

The analysis is based on four cognition points of the auction process: (1) The auction process is two-way interactive and decentralized; (2) The auction price can be close to the actual price by optimizing the auction mechanism; (3) The auction process only involves the transmission of information, thus it is easy to implement; (4) The auction process only involves a small amount of transaction information, which can well protect the privacy of all parties.

These properties make the auction model fit well with the cross-blockchain asset transfer model. With a detailed comparison between the cumulative auction, a sealed auction, Vickrey auction and other widely used auction mechanisms in economics [22,27], we find that Vickrey auction [24] is more consistent with the cross-blockchain asset transfer process. Vickrey auction is a sealed second-price payment auction scheme [24]. All buyers make their own offer for the seller's assets and this offer is sent to the seller in a sealed envelope. The offer is known only to the bidder until the seller opens envelope. After collecting all the offers, the seller opens the envelope and auctions the assets to the highest bidder. However, the highest bidder only needs to pay through the second highest offer to obtain the assets [22].

Eq. (1) describes the bidder m's earning. In this situation, the best strategy for a bidder is giving her actual price of the asset. This well meets the limits described in Eq. (5). When the number of participants increases, the condition of Eq. (7) can also be met.

Furthermore, we calculate the expected price of the asset $E\left(p_{tx(i)}\right)$ in the i_{th} transaction. It is not easy to directly solve the auction price, hence the idea is to use the difference between the minimum transaction fee and the highest market price to obtain the transaction price. The minimum transaction fee is a random variable that follows the normal distribution. What we need to solve is the expectation of its minimum value. Let $X_1, \ldots, X_n$ be independent random variables representing the transaction fees, with mean value of μ and standard deviation σ. Then, the expected fee that the buyer get $E\left(f_{tx(i)}\right)$ is given as:

$$E\left(f_{tx(i)}\right) = m * \varepsilon * [\rho - \delta * \int_{-\infty}^{\infty} t \frac{d}{dt} \varphi(t)^{n(i)} \, dt] \,, \tag{9}$$

where m is the amount of the asset need to be auctioned on the source blockchain and ε is the actual asset exchange rate between the source and destination in the transaction process. $\varphi(t)^{n(i)} = \prod_i^{n(i)} P[X_i > (\rho - t * \delta)]$ is the standard normal cumulative distribution function (CDF). Thus the expected price is given as:

$$E\left(p_{tx(i)}\right) = m * \varepsilon * [1 - \rho + \delta * \int_{-\infty}^{\infty} t \frac{d}{dt} \varphi(t)^{n(i)} \, dt] \,. \tag{10}$$

The larger ε is, the more close the expected assets' auction price to the actual price. This is also consistent with our common sense: when an auction has more bidders, the competition between the bidders will be more intense, the asset to be auctioned will have a higher final price. We model the cross-blockchain asset transfer as an auction process and present the strategies to achieve an efficient transfer.

3. Cross-chain transfer protocol

The characteristics of a Vickrey auction can well meet the requirements of the cross-blockchain asset transfer problem. In this section, we leverage Vickrey auction mechanism and atomic swap technology [18,28] to enable specific interaction process of cross-blockchain asset transfer protocol. It should be noted that the original Vickrey auction scheme is recomposed in the proposed protocol to meet the requirements of the cross-blockchain asset transfer process.

3.1. Protocol illustration

We illustrate to describe this interaction protocol. The protocol can be divided into two main processes. Considering the case that Alice needs to transfer some of her assets (assuming as m) from blockchain-A to blockchain-B. The disposed buyers are Bob, Carol, David, Eric and Flora on blockchain-B. They bid the price of n_1, n_2, n_3, n_4, n_5 and $n_1 > n_2 > n_3 > n_4 > n_5$. The proposed protocol consists of two main interaction processes, the Bidding Collecting Process and the Asset Exchange Process.

Bidding Collecting Process: The first step of the protocol is making an auction deal (Fig. 2). The seller broadcasts the bidding information and the buyers returning the bids to the seller.

(1) The seller (Alice) sends the cross-blockchain asset transfer request to all users on blockchain-B. The request has the asset of m and t_1, m is the amount of the asset to be transferred on blockchain-A and t_1 is the response deadline.

(2) The disposed buyers (Bob ~ Flora) bid for the asset before the response deadline t_1 after receiving the request. There is also the offer of the asset and the bidder's electronic signature in the response.

(3) Alice collects all the response after deadline t_1, and return the collection of the responses to all the bidders.

(4) After receiving the collections, Bob wins the auction and makes the intention of the transaction with the price n_2.

Algorithms 1 and Algorithm 2 describe the behavior of the seller and buyer during the bidding collecting process. Since this is a synchronize interaction protocol, we set a deadline in the Algorithm 1 to avoid the situation of dead-block. Algorithm 1 implements the seller's action of step 1, step 2 and step 4 in the bidding collecting process. The lines 12 in Algorithm 1 describes the determination of the clearing price. Since Vickery Auction is a second price sealed auction scheme, we first sort the buyer's price and use the second highest price as the clearing price.

Algorithm 2 implements the buyer's action of step 3. The winning price is announced automatically after the bidding step finished by broadcasting the bidding message. All bidders compare their bid price with the information returned to determine whether they have won the auction. During this process, the bidders' price, address and other information are shared. We use the copy of this information to simplify the procedure so as to accelerate the delivery process.

Algorithm 1: Find the disposed buyer and price by broadcasting

Input: SwapAssetAmount ξ , WaitTime τ , DestinationChain θ
Output: Collect of Buyers' Bids

```
1  Deadline = time.now() + τ;
2  for user x in θ do do
3  |  send < SwapRequest, ξ, Deadline > to x;
4  end
5  Initialize set allPrice, allBuyer to be empty;
6  while time.now() < Deadline do
7  |  GetPrice(buyerData ← θ);
8  |  allPrice.add(price);
9  |  allBuyer.add(buyer)
10 end
11 maxPrice = max(allPrice);
12 secondPrice=max(allPrice.remove(maxPrice)) ,
   Buyer=allBuyer.get(maxPrice);
13 for user γ in allBuyer do
14 |  send < secondPrice, maxPrice > to γ;
15 end
```

Asset exchange process: After making the auction deal, the seller and the selected buyer then exchange the asset by the method of hash-lock (Fig. 3). The interaction process lists as follows:

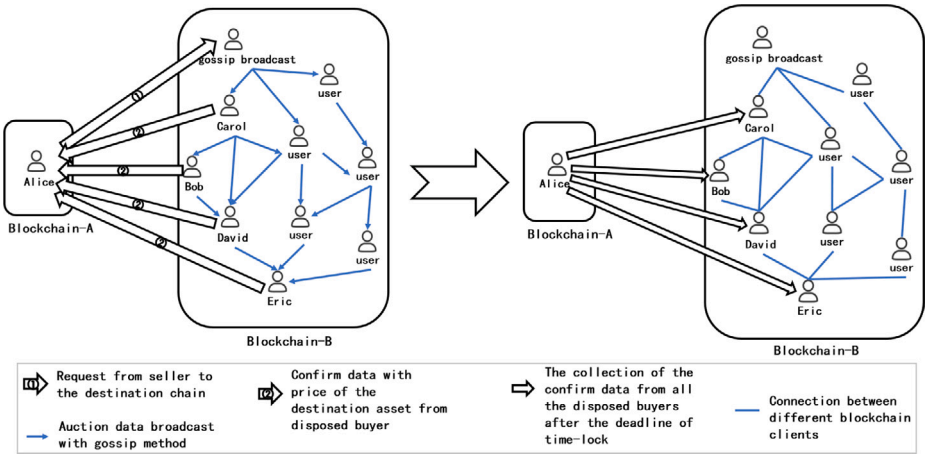

Fig. 2. Bidding collecting process.

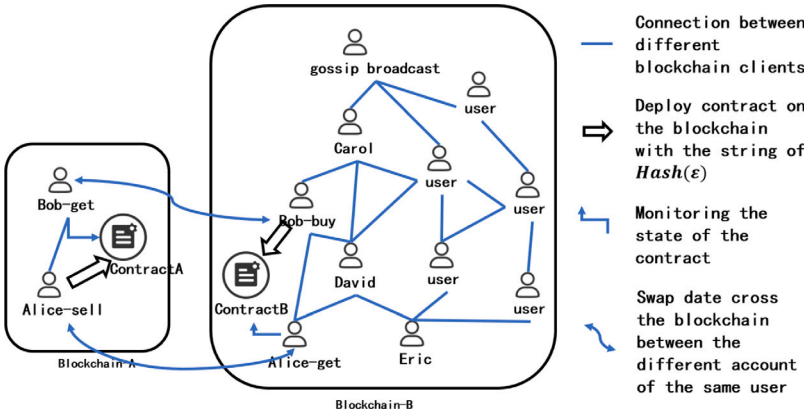

Fig. 3. Asset exchange process.

Algorithm 2: Bid for Some Disposed Destination Blockchain System and Make the Transaction Intention

Input: IntentionChain γ, IntentionRate δ ,
$< SwapRequest, \xi, Deadline >$,
$< Second\,Price\ \beta, MaxBuyer\ \xi >$
Output: The bid price

```
while chain = monitorSwapRequest() do
    if chain in γ then
        if time.now() < Deadline then
            price = δ.get(chain) * ξ;
        end
        wait(Deadline);
        if ξ = self && β = price then
            BuyerSwapAssetContract() continue;
        else
            continue;
        end
    end
end
```

(5) Alice makes a random String k and evaluates its Hash-String ($Hash(k)$). Alice makes a smart contract on blockchain-A by $Hash(k)$ and deadline t_2. In the contract, it stipulates that if someone provides the original string k of $Hash(k)$ before deadline t_2, he can freeze the asset in the smart contract.

Algorithm 3: Swap the Asset by Hash-Time Lock (Seller Operation)

Input: SwapAssetAmount ξ, String ϵ, WaitTime τ, SecondPrice β

```
hashString=Hash(ε);
Deadline=time.now() + τ;
makeContract(hashString, ξ, Deadline);
while monitorDesChainContract(hashString, β) do
    releaseDesChainContract(string, DesChainAddress);
    break;
end
```

(6) Bob makes the same contract with the asset $Hash(k)$ and t_3 ($t_3 < t_2$ and $t_3 \approx t_2/2$) on blockchain-B after monitoring the existence of the contract deployed on blockchain-A [29].

(7) Alice sends the string k to the contract on blockchain-B and gets the asset n_2 blocked in blockchain-B [29].

(8) Bob gets the string k after step 7. Then Bob sends the string to the contract deployed on blockchain-A before deadline t_2 and gets the asset m blocked in the contract.

Algorithms 3 and 4 describe the behavior of the seller and buyer during the asset exchange process. Algorithm 3 implements the seller's interaction of step 5 and step 7, and Algorithm 4 implements the buyer's interaction of step 6 and step 8.

Algorithm 4: Swap the Asset by Hash-Time Lock(Buyer Operation)

Input: HashString Hash(ε), Deadline τ, SecondPrice β, String ε
Output: Auctioned Asset

```
while monitorDesChainContract() do
    getData(Hash(ε), τ, β);
    break;
end
NewDeadline = (τ - time.now())/2 + time.now();
makeContract(Hash(ε), β, NewDeadline);
getString(ε);
releaseSourceChainContract(ε, SourceChainAddress);
```

These two interaction processes are asynchronous and binding together logically. The protocol only involves a small amount of information exchanges and local-blockchain operations. The global information is shared throughout the process, which makes the cooperation among different systems efficient and close. From the protocol, the winner and the winning price is organized automatically after the bidding step finished by broadcasting the bidding message. All bidders can determine whether they have won the auction by comparing their bid price with the information returned. During the process, the bidders' price, address and other information will be shared. We reuse the same copy of this information to simplify the interaction so as to accelerate the delivery process. The delivery process is implemented through smart contracts, which are transparent and efficient.

In the existing schemes, the exchange rates between different cryptocurrencies are collected through a trusted third-party monitoring market. The exchange rate in the market is obtained from the previous transactions. This does not reflect in real-time the market's rate of exchange for cryptocurrencies. Nevertheless, our scheme directly binds this pricing to the user's bidding behavior, which better represents the market's real-time exchange rate of the cryptocurrency. Moreover, the delay due to the centralized collection of exchange rate information is avoided in the proposed protocol.

There is a security problem that the malicious bidders might bid the asset at a higher price in the auction phase without paying for it in the asset exchange phase. To avoid this problem, a blacklist mechanism is designed. The blacklist is append-only and shared globally among all peers. When the bidders bid a price for the asset, the seller will check the blockchain account to verify whether the bidder's deposit can cover the payment and whether the bidder is on the blacklist. If the bidder's deposit is not enough or the bidder is on the blacklist, the bidding message will be invalid and ignored. When the malicious bidder comes to the asset exchange phase for the first time, his bad behavior will be recorded and broadcasted to all the users. The blockchain system will verify the message and make the consensus to add the malicious user on the blacklist. Each malicious user can only compromise one transaction. This reduces the possibility of the system being attacked by malicious users.

The proposed protocol is asynchronous. It only involves a little amount of information exchange and local-blockchain system operation. We divide the protocol into two steps, and the second step need to be triggered by the first step. These two steps are binding together logically, so that public information can be shared. Using our protocol, the cooperation among different blockchain systems will be efficient and close.

3.2. Exchange properties

Proposition 1. *The proposed AucSwap mechanism is allocatively efficient, dominant strategy truthful and individually rational.*

Proof. Assume we have a set of n agents i each of whom have a valuation function $v_i \in V$. We have a set of alternatives A we want to choose from. A pair of functions X and P defines the method of mapping agent's reported valuations to an outcome, where X is the choice rule and P is the payment rule.

First, AucSwap adopted the Vickrey–Clarke–Groves (VCG) mechanism and the Groves mechanism is *allocatively efficient* by definition [30]: for all $v_i \in V$, if $a = X(v)$, then for all $a' \in A$,

$$\sum_i v_i(a) \geq \sum_i v_i(a') \,. \tag{11}$$

Fix any agent i, and reports v_{-i} of the other players. We have the that agent i experiences:

$$u_i(X(v), P(v)) = v_i(a^*) + \sum_{j \neq i} v_j(a^*) - h_i(v_{-i}), \tag{12}$$

where $a^* = \arg\max_{a \in A}(\sum_{j \neq i} v_i(a^*) + v_i'(a))$. Agent i wishes to report v_i' to maximize his utility. Note that $h_i(v_{-i})$ has no dependence on his report, so equivalently, agent i wishes to report v_i' to maximize

$$v_i(a^*) + \sum_{j \neq i} v_j(a^*) = \sum_i v_i(a^*). \tag{13}$$

But note that if agent i truthfully reports $v_i' = v_i$, then a^* maximizes this quantity by definition. Hence, it is a dominant strategy for all agents to report *truthfully*.

In order to prove AucSwap mechanism is *individually rational*, we need to show that agent i's utility satisfies:

$$u_i(o) = v_i(a^*) + \sum_{j \neq i} v_j(a^*) - \sum_{j \neq i} v_j(a^*_{-i}) \geq 0. \tag{14}$$

Or equivalently

$$\sum_i v_j(a^*) \geq \sum_{j \neq i} v_j(a^*_{-i}). \tag{15}$$

But note that if this is not the case, since v_i is non-negative, we would have:

$$\sum_i v_i(a^*_{-i}) \geq \sum_{j \neq i} v_j(a^*_{-i}) > \sum_i v_i(a^*) \tag{16}$$

But this would contradict the allocative efficiency of a^*. ■

For the budget balance property, we have the following claim. Let p^0_{bid} denote the smallest successful bid and p^{-1}_{bid} denote the largest unsuccessful bid. Similarly, let p^0_{ask} denote the largest successful ask and p^{-1}_{ask} denote the smallest unsuccessful ask.

Claim 1. *The proposed AucSwap mechanism is budget balanced if and only if one (or more) of the following conditions hold: (1) $p^0_{bid} = p^0_{ask}$; (2) $p^0_{bid} = p^{-1}_{bid}$; (3) $p^0_{ask} = p^{-1}_{ask}$.*

Proof sketch: In our cross-blockchain scenario, budget balance holds if and only if $\max(p^0_{ask}, p^{-1}_{bid}) \geq \min(p^0_{bid}, p^{-1}_{ask})$, leading to cases: (1) $p^0_{ask} \geq p^{-1}_{bid}$ and $p^0_{bid} \leq p^{-1}_{ask}$; (2) $p^0_{ask} < p^{-1}_{bid}$ and $p^0_{bid} \leq p^{-1}_{ask}$; (3) $p^0_{ask} \geq p^{-1}_{bid}$ and $p^0_{bid} > p^{-1}_{ask}$.

4. Evaluation

In order to evaluate the proposed cross-blockchain asset transfer scheme, an Ethereum-based experiment platform is developed to implement the protocol. Our protocol can be implemented on any blockchain system with the features of virtual assets, transfer functions and smart contracts. Developers only need to define a programming interface to support the protocol in their own blockchain systems. We make the general procedure for implementing this protocol on two Ethereum test networks. This protocol can be also supported for other heterogeneous blockchain systems (Bitcoin, Ethereum, Hyperledger Fabric and so on). For a developed blockchain system, it can integrate such an auction platform to support the protocol. For a developing system, this protocol can be supported by embedding inside a blockchain system.

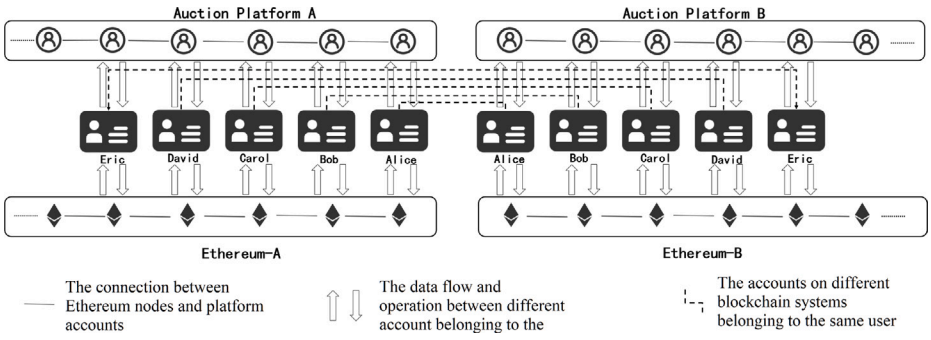

Fig. 4. The architecture of the designed auction platform.

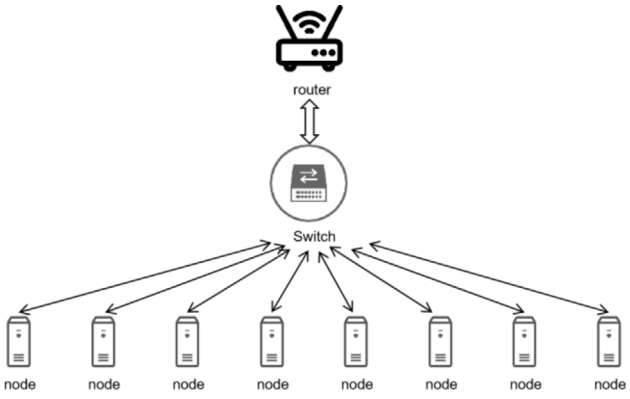

Fig. 5. Network setup for the empirical evaluation.

4.1. Experiment setup

The architecture of the system is shown in Fig. 4. We built up two Ethereum networks (Ethereum-A and Ethereum-B). There are several accounts on each blockchain and each user has an account on both Ethereum networks. Users have a wallet application outside the Ethereum network, and this wallet is tied to an accountant on the Ethereum. Each wallet has the function of broadcasting auction information and collecting bids from potential buyers on the corresponding Ethereum auction platform. Our experimental environment is: PC (CPU: Xeon e3-1230-v5, memory: DDR4 3000-16G * 2, 250G SSD) and Laptop (CPU: i5-8250u, Memory: DDR4 2400-8G, 250G SSD). In order to verify the protocol's heterogeneous devices tolerance, we also use some devices to simulate the behavior of light nodes, including Raspberry Pi, mobile phones, virtual machines, etc.

In the experiment, we implement our protocol in a network topology described in Fig. 5. All nodes are connected with each other through a 1 Gbps switch (D-Link DGS-105). The network latency is less than 10 ms, and the network bandwidth usage is less than 10%. These network peaks are well below the network's maximum capacity. We call it "an ideal network condition". The simulation code and the raw data are published here.[1]

4.2. Performance results

We analyze the protocol from the following aspects: the transaction completion time, the protocol I/O size, the ratio between the cross-blockchain exchange rate and the real exchange rate, and the tolerance for heterogeneous devices. The analysis of the network situation's impact is given in Appendix. Global parameters and variables used in the evaluation are listed as follows. The *Purchase Possibility* indicates the users' purchase intention of the asset, reflecting the market's popularity of the asset. The *Number of Participants* is the number of active users on a blockchain system. It symbolizes the activity of the community. The *Communication Size* indicates the number of communications carried out by an account during the protocol. Since each communication only involves little information transmission of coordination, we use the number of communications to describe the I/O situation. The *Exchange-rate Ratio* is the ratio between the cross-blockchain exchange rate and the real exchange rate in the market.

First, we evaluate the *Communication Size* of the proposed protocol. The number of communications is used as the indicator of the communication size. Fig. 6(a) shows the number of communications changes with the number of bidding participants. Since the buyer's communication during the transaction is constant, we only count the number of the seller's communications. One can see that the number of communications increases with the number of participants and the purchase possibility. Among these two factors, the popularity of the auction asset is more important. It can be seen in Fig. 6(a) that number of communications grows approximately linearly with the number of participants. But the increase in purchase popularity augment the transaction communication time greatly.

Fig. 6(b) shows the relationship between the transaction completion time and the bid waiting time. According to the analysis of the protocol, the transaction completion time is mainly spent on the auction period. The duration of this phase is set by the user. The time for distributing auction messages is directly proportional to the number of participants. However, it can reach in a constant time under the ideal network conditions. Thus we conclude that the auction completion time should be substantially proportional to the bid waiting time and slightly increased as the number of participants increases. In the experiment, we set up 100 common users on two Ethereum blockchains and purchase possibility is set to 0.2. When the purchase possibility and the participants gradually increase, the time spent on the distribution auction increases. However, compared to the bid waiting time, it is still a smaller part.

Then, the *Exchange-rate Ratio* is evaluated in Fig. 6(c) and (d). This ratio eventually converges to 1 as the number of participants and the popularity of the asset increases. Since we count the price ratio of a specific auction, there may be some price fluctuations. Fig. 6(c) is the case where a lower price limit is set, and Fig. 6(d) is the case where limits no starting price. In both figures, it can be seen the trend that the ratio gradually converges to 1. By compared the two graphs, one can see that without starting price, although the ratio also eventually converges, the price fluctuations are relatively large, and the convergence rate is much slower. In the same situation, the higher the popularity of auction assets, the faster the convergence rate. The purchase possibility is set as 0.4 in Fig. 6(c), which is at a relatively lower level. After limiting a lower starting price, the amplitude of price fluctuations is reduced, and the rate of convergence is greatly

[1] https://github.com/mth1haha/Aucswap.

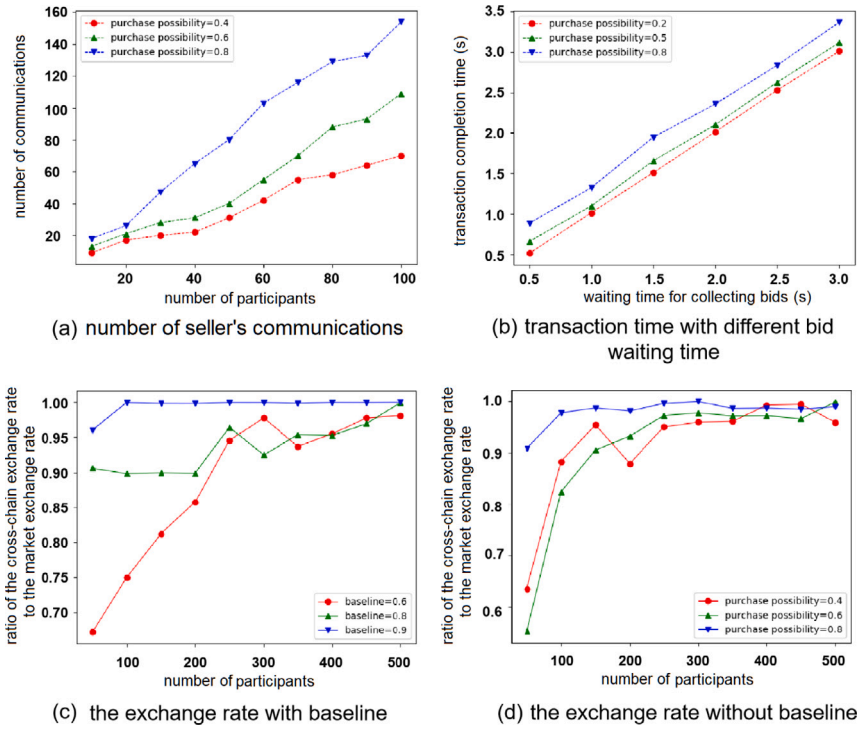

Fig. 6. The comparing results of the experiments.

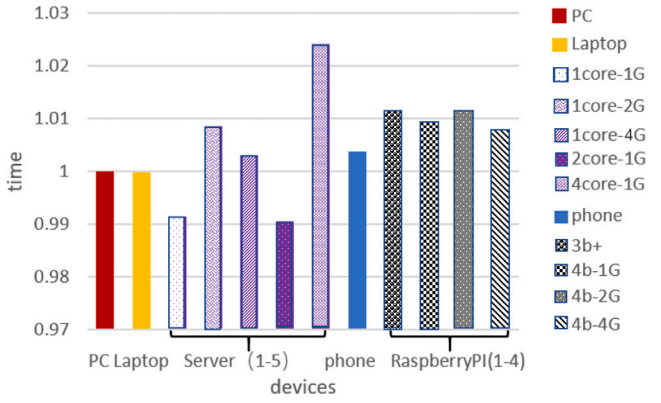

Fig. 7. Transaction time of heterogeneous devices.

accelerated. It can be seen that when the starting price is set to 0.9, it can reach near 1 with the participation of merely 100 people.

Based on the analysis of the results in Fig. 6(b)–(c), we can find that in an ideal network environment, the protocol can well realize the assets cross-blockchain transfer. It is possible to change the ownership of assets without breaking the original closure of the system. This process is realized point-to-point and can be achieved during constant-level communication interaction. The interaction process is synchronous but controllable, thus it has the characteristics of decentralization, efficiency, and heterogeneity tolerance.

Furthermore, the heterogeneity tolerance of the protocol is analyzed through comparing the transaction time with different devices for the same transaction process. As shown in Fig. 7, we take the processing time of PC as the base point 1, and compare the time between the PC and other devices. We have counted the transaction on a laptop, virtual servers with different configurations, mobile phones and Raspberry Pis. Experimental results have shown that the time taken for various devices to reach a transaction is basically the same. The transaction completion time difference for various devices is within 3%. This shows that the protocol we designed only consumes very little computing resources in the working process, and the protocol has the character of heterogeneity tolerance.

Since there is no distributed cross-blockchain transfer implementation available, we compare the performance of AucSwap with the most famous cryptocurrency exchange Binance [31].

The performance comparison results are shown in Fig. 8. We first compare the cross-blockchain asset transfer latency with Binance. From Fig. 8(a), one can see the latency of the proposed scheme is more stable. However, for Binance exchange, the transfer latency is high when the transaction statistics are low, that is due to the delay caused by the centralized collection and processing of the exchange rates and other information. With an increase in the number of transactions, the Binance latency decreases and converges to the AucSwap level.

Fig. 8(b) shows the transaction fee varying with the different number of auction participants in different schemes. It is notable that in AucSwap, the transaction fee decreases sharply with the increase of the number of auction participants. But the transaction fees of ETH to BTC and BTC to ETH remain nearly constant in Binance exchange because the transaction fees of the exchange are derived from the previous transactions.

Our protocol is decentralized and atomic in its ability to transfer assets across the blockchain directly between two users without the help of other tools. In the process of the protocol, the exchange behavior and incentiveness are organized spontaneously with the fluctuation of the transaction. As a result, the protocol has a reasonable exchange rate. During the auction process, only the necessary messages and operations are involved. Therefore, the user's personal information is rarely exposed, with strong privacy protection and transaction security. In addition, the efficiency of the proposed method is high since our approach is an interoperable protocol and does not require additional

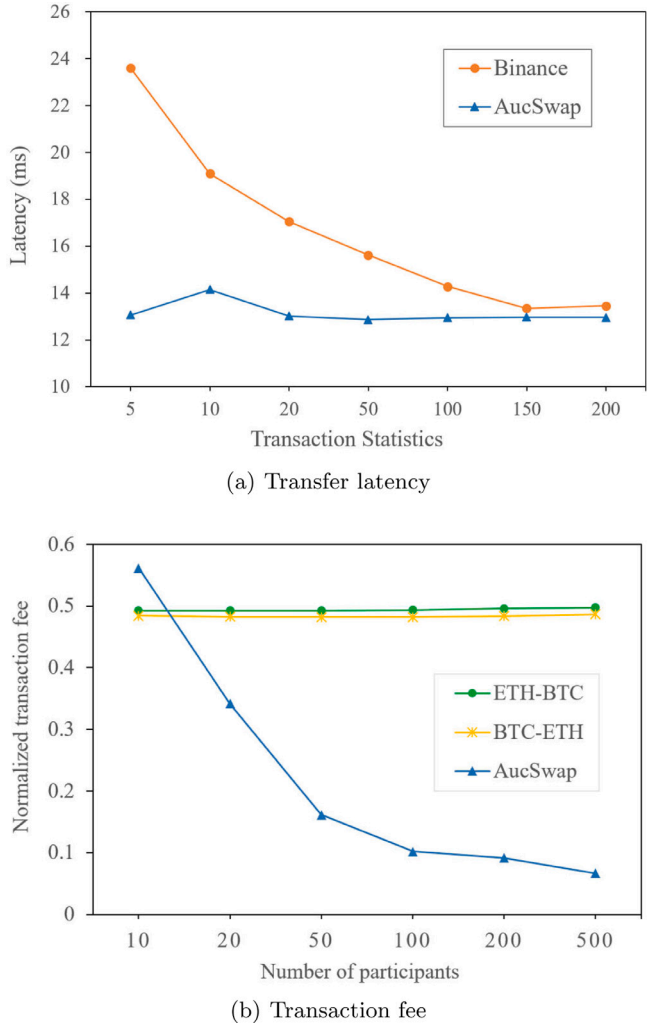

Fig. 8. Performance comparison of AucSwap and Binance exchange.

middleware to support of existing blockchain systems. Developers who want to add this method to their own systems simply need to build an open interface based on this protocol, so as to perform asset transfer operations with other blockchain systems. We find that our design maintains some good characters among them.

5. Related work

There have been some previous research efforts on the cross-blockchain asset transfer. BTC-Relay [32] is the first sidechain of Bitcoin [33] and Ethereum [34]. By implementing the smart contract of Bitcoin SPV (Simplified Payment Verification) wallet on the Ethereum 9, the scheme of BTC-Relay can verify the transactions between Bitcoin and Ethereum easily [35]. However, the BTC-Relay scheme only supports asset transfers between bitcoin and Ethereum, not other blockchain platforms, which is lack of universality. It also needs large amount of development and maintenance.

Binance [11] is a blockchain asset exchange with a centralized trading center. When users need to buy and sell blockchain assets, they first pass the demand to the exchange. After receiving the request, the exchange matches the request with the most recent trading information to find the appropriate trading pair. Then the exchange matches two trades on an operating platform to reach a deal. Transactions are requested and completed on the exchange platform.

As to multi-party swap, Shapley and Scarf consider the situation that certain kinds of swap have strong equilibriums [36]. Kaplan describes a polynomial-time algorithm that given a set of proposed swaps, constructs a swap digraph if one exists [37]. Decker and Wattenhofer present a protocol for improving the scalability of Bitcoin by enabling off-chain transactions between untrusted parties [38]. Moreover, Herlihy shows that an atomic swap protocol has time complexity proportional to the graph's diameter and communication complexity proportional to the amount of value exchanges.

Interledger [19] is an atomic swap based cross-blockchain scheme. It applies the scheme of the hash-locking and time-locking [18,39]. However, it remains the problem of lacking transaction proceeding information. This makes the transaction only can be finished after the disposing information matching process.

Our work aims to combine the transaction information matching process and asset cross-blockchain transfer process into one protocol. The protocol makes the transaction occurred point-to-point, ensuring the decentralization and cooperation among participants.

6. Conclusion

In this paper, we abstract the cross-blockchain asset transfer problem into an auction model, and design an interaction protocol to solve it. We point out the general rules need to be obeyed during a cross-chain protocol design. An auction platform is developed to implement the proposed protocol. We employ a combination of analytical calculations and experiments to investigate our scheme, and demonstrate that it has the advantages of efficiency, decentralization, rational exchange rate, and isomerism tolerance. The experimental results show that our protocol can be implemented in only 4 rounds of interaction. In an ideal network environment, the difference between the transaction completion time and the bid waiting time is less than 1 s. Our protocol also ensures that the exchange rate is within a reasonable range. The ratio between the cross-blockchain exchange rate and the real exchange rate converges to 0.9 for approximately 200 participants.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by the Key-Area Research and Development Program of Guangdong Province (2019B010137002), National Key R&D Program of China (2018YFB1004804) and the Basic Research Program of Shenzhen (JCYJ20180302145731531).

Appendix. Impact of network

Our experiments are conducted under the ideal network conditions. Now we discuss the impact of the heterogeneous network environments on the protocol. We analyze the impact from two phases: the auction period and the asset exchange period. During the protocol working process, the communication volume is very small. This makes the bandwidth requirement very low. For the synchronous interaction feature of the protocol, there is a limit to the final communication time. Thus the most important issue is the packet arrival problem [40].

During the auction phase, a final deadline is designed for the buyer bid and seller broadcast bids. If data packet loss occurs during any period of the auction, the seller cannot receive the bid data and the bid cannot be reached eventually. During the asset exchange period, the packet loss will end the asset exchange transaction. Only when the data loss occurs after the seller receiving the payment and the buyer cannot get the auctioned-asset, the balance of the transaction will be

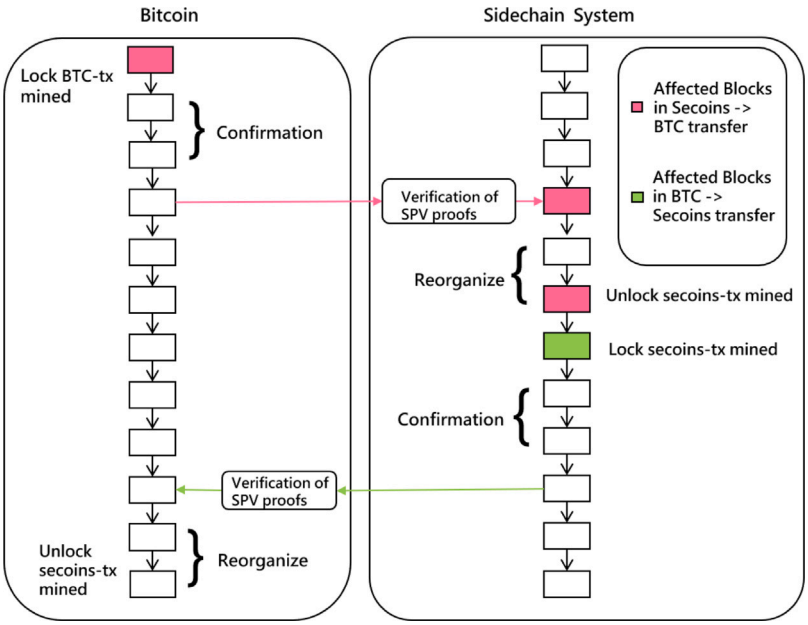

Fig. 9. The SPV process of BTC-Relay [32].

broken. This is a serious situation, but the possibility of this situation is extremely low. The buyer communicates with the seller correctly in the before bidding period. The buyer can avoid this situation by extending the trading deadline.

Thus, the network communication problems only affect the completion of the transaction, and only in some rare cases affect the security of the user assets, which can be avoided by extending the trading time.

References

[1] J. Wang, H. Wang, Monoxide: Scale out blockchains with asynchronous consensus zones, in: 16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19), 2019, pp. 95–112.

[2] Y. Jiao, P. Wang, D. Niyato, K. Suankaewmanee, Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks, IEEE Trans. Parallel Distrib. Syst. (2019).

[3] H. Jin, X. Dai, J. Xiao, Towards a novel architecture for enabling interoperability amongst multiple blockchains, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2018, pp. 1203–1211.

[4] C. Xu, K. Wang, P. Li, S. Guo, J. Luo, B. Ye, M. Guo, Making big data open in edges: A resource-efficient blockchain-based approach, IEEE Trans. Parallel Distrib. Syst. 30 (4) (2018) 870–882.

[5] A. Norta, B. Leiding, A. Lane, Lowering financial inclusion barriers with a blockchain-based capital transfer system, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2019, pp. 319–324.

[6] C. Egger, P. Moreno-Sanchez, M. Maffei, Atomic multi-channel updates with constant collateral in bitcoin-compatible payment-channel networks, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 801–815.

[7] A. Hari, M. Kodialam, T. Lakshman, Accel: Accelerating the bitcoin blockchain for high-throughput, low-latency applications, in: IEEE INFOCOM 2019-IEEE Conference on Computer Communications, IEEE, 2019, pp. 2368–2376.

[8] M. Rashid, H.H. Pajooh, A security framework for iot authentication and authorization based on blockchain technology, in: 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2019, pp. 264–271.

[9] S. Schulte, M. Sigwart, P. Frauenthaler, M. Borkowski, Towards blockchain interoperability, in: International Conference on Business Process Management, Springer, 2019, pp. 3–10.

[10] Ripple, Ripple, 2020, https://ripple.com/d, accessed December 26, 2020.

[11] Binance, Binance, 2020, https://www.binance.com/en, accessed December 26, 2020.

[12] N. Dashkevich, S. Counsell, G. Destefanis, Blockchain application for central banks: A systematic mapping study, IEEE Access 8 (2020) 139918–139952, http://dx.doi.org/10.1109/ACCESS.2020.3012295.

[13] M. Borkowski, P. Frauenthaler, M. Sigwart, T. Hukkinen, O. Hladkỳ, S. Schulte, Cross-blockchain technologies: Review, state of the art, and outlook, 2019.

[14] Cosmos, Cosmos, 2020, https://cosmos.network/, accessed December 26, 2020.

[15] Polkadot, Polkadot, 2020, https://polkadot.network/, accessed December 26, 2020.

[16] P. Gaži, A. Kiayias, D. Zindros, Proof-of-stake sidechains, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 139–156.

[17] S. Johnson, P. Robinson, J. Brainard, Sidechains and interoperability, 2019, arXiv preprint arXiv:1903.04077.

[18] M. Herlihy, Atomic cross-chain swaps, in: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, ACM, 2018, pp. 245–254.

[19] S. Thomas, E. Schwartz, A protocol for interledger payments, 2015, URL https://interledger.org/interledger.pdf.

[20] M. Dorofeyev, M. Ksov, V. Ponkratov, A. Masterov, A. Karaev, M. Vasyunina, Trends and prospects for the development of blockchain and cryptocurrencies in the digital economy, Eur. Res. Stud. J. XXI (3) (2018) 429–445.

[21] I. Jovović, S. Husnjak, I. Forenbacher, S. Maček, 5g, blockchain and ipfs: A general survey with possible innovative applications in industry 4.0. EAI, 2018, http://dx.doi.org/10.4108/eai.6-11-2018.2279695.

[22] C. Noussair, S. Robin, B. Ruffieux, Revealing consumers' willingness-to-pay: A comparison of the bdm mechanism and the vickrey auction, J. Econ. Psychol. 25 (6) (2004) 725–741.

[23] W. Vickrey, Counterspeculation, auctions, and competitive sealed tenders, J. Financ. 16 (1) (1961) 8–37.

[24] L.M. Ausubel, P. Milgrom, et al., The lovely but lonely vickrey auction, Comb. Auction. 17 (2006) 22–26.

[25] D. Harz, L. Gudgeon, A. Gervais, W.J. Knottenbelt, Balance: Dynamic adjustment of cryptocurrency deposits, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 1485–1502.

[26] Z. Liu, Y. Xiang, J. Shi, P. Gao, H. Wang, X. Xiao, B. Wen, Y.C. Hu, Hyperservice: Interoperability and programmability across heterogeneous blockchains, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2019, pp. 549–566.

[27] T.W. Sandholm, Limitations of the vickrey auction in computational multiagent systems, in: Proceedings of the Second International Conference on Multiagent Systems (ICMAS-96), 1996, pp. 299–306.

[28] S. Dziembowski, L. Eckey, S. Faust, D. Malinowski, Perun: Virtual payment hubs over cryptocurrencies, in: 2019 IEEE Symposium on Security and Privacy (SP), IEEE, 2019, pp. 106–123.

[29] T. Chen, Y. Zhang, Z. Li, X. Luo, T. Wang, R. Cao, X. Xiao, X. Zhang, Tokenscope: Automatically detecting inconsistent behaviors of cryptocurrency tokens in ethereum, in: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 1503–1520.

[30] T. Roughgarden, Twenty Lectures on Algorithmic Game Theory, Cambridge University Press, 2016, http://dx.doi.org/10.1017/CBO9781316779309.

[31] Binance, Binance exchange libbinacpp, 2020, https://github.com/binance-exchange/binacpp/ accessed December 26, 2020.

[32] BTC-Relay, Btc-relay, 2020, http://btcrelay.org/, accessed December 26, 2020.

[33] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Tech. rep., Manubot, 2019.

[34] G. Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum Proj. Yellow Pap. 151 (2014) (2014) 1–32.
[35] J. Poon, T. Dryja, The bitcoin lightning network: Scalable off-chain instant payments, 2016.
[36] L. Shapley, H. Scarf, On cores and indivisibility, J. Math. Econom. 1 (1) (1974) 23–37.
[37] R.M. Kaplan, An improved algorithm for multi-way trading for exchange and barter, Electron. Commer. Res. Appl. 10 (1) (2011) 67–74.
[38] C. Decker, R. Wattenhofer, A fast and scalable payment network with bitcoin duplex micropayment channels, in: Symposium on Self-Stabilizing Systems, Springer, 2015, pp. 3–18.
[39] V.A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, G.C. Polyzos, Interledger approaches, IEEE Access 7 (2019) 89948–89966.
[40] B. Rodrigues, B. Stiller, Cooperative signaling of ddos attacks in a blockchain-based network, in: Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos, 2019, pp. 39–41.