A Payment Channel Based Hybrid Decentralized Ethereum Token Exchange

Xuan Luo[1], Wei Cai[2], Zehua Wang[1], Xiuhua Li[1], and Victor C. M. Leung[1]
[1]Dept. Electrical and Computer Engineering, The University of British Columbia, Vancouver, Canada
[2]School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, China
Email: {xuanluo2,zwang,lixiuhua,vleung}@ece.ubc.ca, caiwei@cuhk.edu.cn

***Abstract*—Traditional centralized token exchange (CEX) is criticized for its security and privacy issues, since cryptocurrency users are required to surrender their private keys to the exchange. In contrast, decentralized token exchange (DEX) solves this issue by introducing additional trading gas fee and latency to the system. Hybrid decentralized token exchange (HEX) has been proposed to combine the advantages of CEX and DEX. However, existing HEX is still suffering from two issues. The first issue is that it is unfriendly for a trader who needs to exchange tokens frequently within a certain period of time, due to the fact that it is time-consuming and expensive. The second issue is the potential network congestion in Ethereum caused by excessive simultaneous transactions from the exchange. In this paper, we propose a payment channel based HEX, which extends existing solutions by adding a new payment channel layer to benefit frequent traders and alleviate network congestion.**

***Index Terms*—Blockchain, Payment Channel, Ethereum, Smart Contract, Token Exchange, Decentralized Application**

I. Introduction

As the killer decentralized application [1] hosted by blockchain [2], cryptocurrencies [3] have been accepted as digital cash by many investors and consumers nowadays [4]. Due to the popularity of Ethereum-based tokens, the most sophisticated token exchanges are implemented over Ethereum platforms as well. Therefore, we focus on the studies on Ethereum token exchange in this work. In general, we classify current token exchange into three categories, i.e., centralized token exchange (CEX), decentralized token exchange (DEX), and hybrid decentralized token exchange (HEX).

CEX is the most common practice in the current coin market. In a typical CEX, users need to transfer their tokens to a CEX-provided address, which can be accessed through a user-defined ID and password. Hence, CEX is able to provide a rapid transaction speed for user trading. Moreover, the centralized nature of CEX requires all users to trust CEX as their middleman. As a matter of fact, a CEX is intrinsically vulnerable to hacking and denial of service attacks, which makes it a single-point-of-failure. Potential systematic risks include exchange hacks, financial mismanagement from the exchange operators that results in bankruptcy, operational errors by CEX employees, and unexpected account freezes.

DEX leverages smart contracts [5] executed on a blockchain to mitigate above risks. Different from CEX's centralized management on trading operations, DEX implements all trading procedure as smart contracts. These trading smart contracts are transparent and immutable programs that are guaranteed to be executed as predefined. With DEX, token traders need not transfer their digital assets to a centralized exchange. Instead, they invoke smart contracts to conduct their trades. The automatic execution of smart contracts can eliminate the human intervention to the trade, which minimizes the potential risks in security and privacy. Nonetheless, there are two critical issues introduced by DEX. First, traders may find it difficult in discovering appropriate counterparts, due to the lack of order matching service available to the public. Second, smart contract invocations for token transactions imply the trading operations are on-chain processes, which are constrained by the burden of Proof-of-Work [6].

HEX is a hybrid approach that combines the advantages of CEX and DEX, in order to address the trade discovery issue discussed above. A HEX maintains a centralized database to provide matching services for the traders, while all transactions are still executed by smart contracts hosted in a blockchain. However, this approach still cannot solve the second issue introduced by on-chain transactions. In particular, it is unfriendly for a trader who needs to exchange tokens frequently within a certain period of time, due to the fact that it is time-consuming and expensive. On the other hand, there will be potential network congestion in Ethereum due to excessive simultaneous transactions from the token exchange.

In this paper, we extend existing HEX solutions by adding a new payment channel[1] layer, so that frequent traders utilize a payment channel to avoid causing a traffic congestion. The payment channel is a technique allowing for off-chain transactions with an on-chain settlement [7]. A trader opens a payment channel with HEX with a deposit, continue to sign and verify transactions off-chain and close the channel with one final transaction on-chain. The major contribution of the work is to design and implement the very first payment channel based HEX to benefit frequent traders and ease potential traffic congestion on Ethereum.

II. Proposed Approach

The proposed system framework consists of two layers: *on-chain layer* and *off-chain layer*.

The on-chain layer is the key to securing users' assets. In order to implement the bi-directional payment channel, both

[1] https://en.bitcoin.it/wiki/Payment_channels

978-1-7281-1328-9/19/$31.00 ©2019 IEEE

the HEX user and the HEX system need to deposit a certain number of tokens into the smart contract. The deposit initiated by a user will trigger to create a new payment channel between the user and the HEX, or to add fund to the existing payment channel between the user and the HEX. Afterward, the HEX user can sign off-chain trading transactions with the HEX. When a user wants to withdraw his/her fund, both the user and the HEX sign an agreement to close the payment channel and send the close transaction to the smart contract. Settlement can then be done on-chain with smart contracts that cannot be altered or interfered with. The smart contracts act as a verifiable, open source trust engine.

The off-chain layer is responsible for order placement and order matching. After a user creates a payment channel with the HEX, a user is eligible to make trades continuously with the HEX off-chain. The user would be able to place buying/selling orders in the HEX, along with sending related signed transactions to the HEX via the payment channel. If the HEX can find a matching order for the user, the HEX would fulfill both orders by signing both transactions from both users.

To help readers better understand the working mechanism of our proposed HEX system, Figure 1 and Figure 2 illustrate the key components and continuous trading flow of the conventional HEX and the proposed payment channel based HEX, respectively.

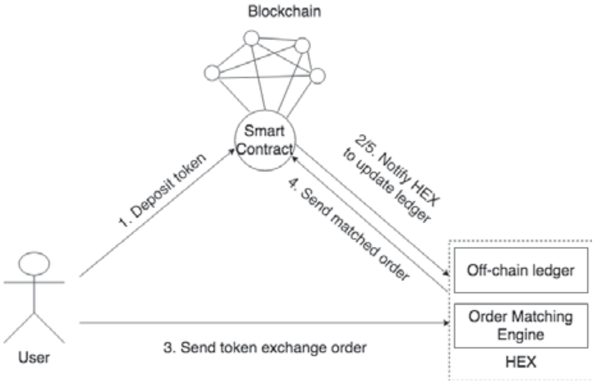

Fig. 1. An example for how a trader exchanges tokens with the HEX without payment channel. For continuous trade, a user will need to repeat step 3, 4 and 5.

To compare Figure 1 and 2, it is obvious that the proposed HEX adds a payment channel to alter the workflow of one trading transaction. In the proposed system, a user will need to deposit tokens into the smart contract to open a payment channel with the HEX, before he/she can sign off-chain transactions with the HEX for continuous token exchanges. Similarly, when the user needs to withdraw tokens from the smart contract, he/she will be required to sign a final close transaction with HEX. By sending this transaction to the smart contract, the user can close the payment channel and withdraw the funds he/she possesses after the sequence of deals.

According to the workflow of continuous trade, step 4 and 5 in Figure 1 are on-chain transaction, while step 4, 5, 6 in Figure 2 are completely off-chain. Apparently, the proposed payment channel based HEX eliminates the transaction fees and transaction delays introduced by the blockchain, thus, achieve better performance over conventional HEX.

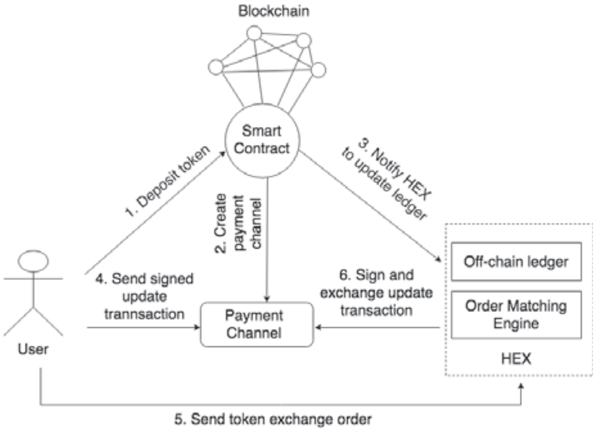
Blockchain
Smart Contract
1. Deposit token
2. Create payment channel
3. Notify HEX to update ledger
Off-chain ledger
Order Matching Engine
HEX
4. Send signed update trannsaction
Payment Channel
6. Sign and exchange update transaction
User
5. Send token exchange order

Fig. 2. An example for how a trader exchanges tokens with the payment channel based HEX. For continuous trade, user will need to repeat step 4, 5 and 6.

While the proposed platform is promising, this paper reveals several limitations that we intend to address in our future work to refine this platform: 1) More sophisticated token allocation models should be designed to maximize the profit of the HEX. The more tokens the HEX allocates to one user, the less number of users the HEX can serve and the higher quality of service is received by individual users. 2) Due to the nature of token locks in creating payment channel, malicious HEX users may initiate attacks to HEX by creating a large number of channels with a huge amount of deposit. Therefore, an effective incentive-and-punishment mechanism should be designed to prevent these attacks. 3) More efficient algorithms should be designed to decrease the gas fee of creating and closing a payment channel. A possibility is to let the trader choose the target exchange tokens when creating a payment channel.

REFERENCES

[1] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized applications: The blockchain-empowered software system," *IEEE Access*, no. 99, 2018.

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, Jun 2017. [Online]. Available: https://doi.org/10.1007/s12599-017-0467-3

[3] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016, pp. 745–752.

[4] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*. Boston, MA: Springer US, 1983, pp. 199–203.

[5] N. Álvarez Díaz, J. Herrera-Joancomartí, and P. Caballero-Gil, "Smart contracts based on blockchain for logistics management," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, ser. IML '17. New York, NY, USA: ACM, 2017, pp. 73:1–73:8. [Online]. Available: http://doi.acm.org/10.1145/3109761.3158384

[6] A. Back, "Hashcash - a denial of service counter-measure," 09 2002.

[7] B. Xiao, X. Fan, S. Gao, and W. Cai, "EdgeToll: a blockchain-based toll collection system for public sharing of heterogeneous edges," in *2019 IEEE Conference on Computer Communications Workshops (INFOCOM 2019 WKSHPS), Paris, France, 29 April - 2 May*, Paris, France, Apr. 2019.