2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS) | 978-1-7281-7002-2/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICDCS47774.2020.00148

An Inter-blockchain Escrow Approach for Fast Bitcoin Payment

Xinyu Lei, Tian Xie, Guan-Hua Tu
Dept. of Computer Science and Engineering
Michigan State University
East Lansing,
Email: {leixinyu, xietian1, ghtu}@msu.edu

Alex X. Liu
Ant Financial Services Group
Hangzhou, China
Email: xiangyangalex.lxy@antfin.com

***Abstract*—In recent years, the Bitcoin (BTC) payment is increasingly popular in retailers and service providers. A BTC transaction (tx) needs six confirmations (one hour) to be validated, making it not suitable for fast-pay scenarios. Theoretically, a shorter waiting time period increases the success possibility of a double-spending attack. To address this problem, we propose BTCFast scheme to support fast BTC tx. BTCFast is a novel, decentralized, escrow-based scheme on top of the programmable smart contract (PSC)-enabled blockchains (e.g. Ethereum, EOS). We develop a smart contract (PayJudger) to work as a trusted payment judger, which guarantees the tx fairness. In addition, we devise a proof-of-work (PoW)-based payment judgment mechanism for PayJudger to resolve a BTC payment dispute. Our theoretical and experimental results show that BTCFast can reduce the waiting time to be less than 1 second with comparable security as the current approach (i.e., waiting for six confirmations) with no extra operation fee.**

***Keywords*-Bitcoin; fast payment; double-spending attack; Ethereum; smart contract.**

I. Introduction

Nowadays, BTC is the most popular cryptocurrency. It supports txs between payers and payees via BTC public peer-to-peer network. The most prominent feature of BTC is decentralization which allows users to perform txs without using trusted parties (e.g., banks). In practice, BTC has been used as a payment option by many famous retailers and service providers (e.g., OverStock). A recent study [1] shows that the number of active Bitcoin wallet users is about 2.9 million in 2017 and will reach 200 million by 2024, which represents a compound annual growth rate of 83.09%. However, the BTC payment service does not come without issues or limitations. For example, to defend against the double-spending attack launched by payers, the current approach for the payees is to wait for six block confirmations before accepting a BTC tx. Nevertheless, the one-hour waiting time hinders the adoption of BTC in real-world applications. To address the issue, this paper aims to develop a new fast BTC payment technique, which meets the following four requirements. (1) Fast tx. The time required for the payee to validate a BTC tx should be short while still being able to resist double-spending attacks. (2) Mainly use BTC. In most use scenarios, BTC is the used payment cryptocurrency. It should not require users to give up using BTC and adopt other cryptocurrencies for payment. (3) Decentralization. It should preserve the decentralization feature of BTC: no trusted third parties are needed. (4) Cost-efficient. The extra operation fee should be as low as possible.

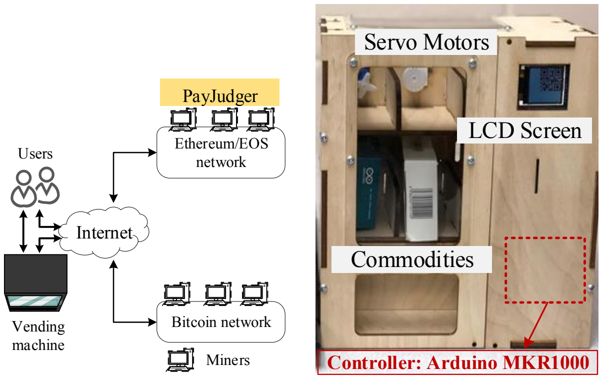
II. Proposed Approach: BTCFast

To support fast BTC txs, we propose an inter-blockchain escrow approach (BTCFast). There are two key ideas in BTCFast. First, BTCFast employs a smart contract (PayJudger) to hold the payer's security deposit and work as a trusted BTC tx judger, who guarantees the BTC payment tx fairness. Second, BTCFast can achieve fast BTC tx validation by harnessing the fast tx validation property of the emerging PSC-enabled blockchains. For instance, EOS blockchain requires less than 1 second to validate a tx [2]. Note that BTCFast can be deployed on any PSC-enabled blockchain platforms. In detail, BTCFast is composed of four steps. (1) A payer adds security deposit into PayJudger. (2) While the payer broadcasts a BTC tx to the BTC network, she also broadcasts a BTC fast payment request message to PayJudger. The request message contains all information that PayJudger needs to make the BTC payment judgment if a payment dispute arises later. (3) Once the escrow request message tx is successfully validated in the PSC-enabled blockchain, the payee can deliver the purchased commodities to the payer. As a result, the waiting time is reduced to the time for validating a tx on the PSC-enabled blockchain. (4) If a payment dispute arises later, BTCFast allows both parties to submit proof to show that they are the honest parties. If the payee successfully proves that she does not receive the BTC payment, PayJudger pays the payee using the security deposit fund. Otherwise, the payer still owns the security deposit fund. The key challenge in BTCFast is that it is not easy for PayJudger to recognize the dishonest party in a payment dispute since the BTC blockchain information is inaccessible for PayJudger that is deployed on another blockchain. To tackle this challenge, we devise a PoW-based payment judgment mechanism for PayJudger to recognize the dishonest party, thereby ensuring BTC payment fairness.

2575-8411/20/$31.00 ©2020 IEEE
DOI 10.1109/ICDCS47774.2020.00148

III. Demonstration Setup

We instantiate BTCFast based on two PSC-enabled blockchains: Ethereum and EOS. Both Ethereum-based and EOS-based BTCFast are used to support a vending machine prototype to demonstrate its practicability. The system model of the BTCFast-enabled vending machine is depicted in Figure 1(a). The vending machine server connects to both the BTC network and the Ethereum/EOS network to access the real-time BTC blockchain and Ethereum/EOS information. The vending machine works as follows. (1) The customer selects the commodity to buy. (2) The vending machine controller generates a BTC address in the form of the Quick Response (QR) code on the display screen. (3) The customer scans the BTC address, initiates the BTC tx, and simultaneously triggers an Ethereum/EOS tx to send the required message to PayJudger. (4) Once the Ethereum/EOS tx is validated, the controller delivers the commodity. The vending machine prototype is exhibited in Figure 1(b). The ARDUINO MKR1000 WIFI module is adopted as the vending machine controller. The monitor is a 2.2-inch SPI TFT LCD Display Module which is used for the user interaction (e.g., displaying the QR code). Two FS90R rotation robotic servos are applied to rotate the connected mechanical spring and push out the vending commodities. For the vending machine with the Ethereum-based BTCFast, our experimental result shows that the average waiting time for the users is about 3 mins. For the vending machine with the EOS-based BTCFast, the waiting time for the users is less than 3 seconds (take the mechanical delay into consideration).



(a) The system model. (b) The prototype.

Figure 1. The BTCFast-enabled vending machine system model and prototype.

IV. Related Work

The related solutions for fast BTC tx have different limitations. (1) Prevention-based solution. The prevention-based solutions [3–5] deploy observers in the BTC network to detect the conflicting BTC txs (two or more txs that spending the same BTC). However, these solutions are not very reliable because it cannot ensure 100% detection. (2) Escrow-based solution. The escrow-based solutions (e.g, [6]) only support micropayments. (3) Secure wallet-based solution. Secure wallet-based solutions [7, 8] need a trusted secure wallet, so they cannot ensure decentralization. (4) Non-BTC-based solution. This solution enforces users to use other cryptocurrencies (with accelerated tx validation time), but it is not practical to enforce users to adopt this solution. (5) BTC Relay solution. BTC Relay solution [9] lets relayers to relay BTC blockchain headers to the Ethereum blockchain to enable Ethereum smart contracts to validate BTC txs. However, BTC Relay lacks relayers. (2) Summa solution. The Summa solution [10] validates a BTC tx in an Ethereum smart contract by only checking total PoW carried by a proof. However, this solution is not secure because an adversary with a small portion of hash power can still fabricate a valid proof by extending the mining time.

V. Conclusion

In this paper, we present an inter-blockchain escrow approach (BTCFast) to enable BTC fast payment. Unlike Lightning Network (an intra-blockchain escrow approach), BTCFast can support relatively large BTC txs. We show that BTCFast can support fast BTC txs without sacrificing security and increasing the operation cost. We hope that our initial study can attract more research on this important topic in the future.

References

[1] "Exponential growth: Number of bitcoin users to reach 200 million by 2024," https://bit.ly/2HaBj29.

[2] "Eos.io white paper," https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

[3] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *CCS*, 2012, pp. 906–917.

[4] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, "Have a snack, pay with bitcoins," in *P2P*, 2013, pp. 1–5.

[5] C. Pérez-Solà, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Double-spending prevention for bitcoin zero-confirmation transactions." *IACR Cryptology ePrint Archive*, 2017.

[6] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," *https://lightning.network/lightning-network-paper.pdf*, 2016.

[7] A. Dmitrienko, D. Noack, and M. Yung, "Secure wallet-assisted offline bitcoin payments with double-spender revocation," in *AsiaCCS*, 2017, pp. 520–531.

[8] Takahashi and A. Otsuka, "Secure offline payments in bitcoin," in *FC*, 2019.

[9] "Btc relay," http://btcrelay.org/.

[10] "summa project," https://bit.ly/2QBMML9.