SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Comparison of transaction cost on different fair exchange protocols

Huan Zhang [*] Mehdi Tibouchi [†] Miguel Ambrona [‡] Masayuki Abe [§]

Keywords: fair exchange, optimistic fair exchange, transaction fee

Abstract

The fair exchange between two parties is when one exchanges digital goods for payment from another party. It is hard to achieve fairness without a third party. The smart contract acts as a self-executed trustful third party and is deployed to a decentralized blockchain. Therefore, fairness is guaranteed. We propose an optimistic fair exchange smart contract based on the untrust issues. In this smart contract, we use proof of misbehavior when they disagree to reduce the cost for optimistic cases where two parties are honest and compare the transaction cost among the proposed protocol and previous protocols (Fairswap[1], Optiswap[2], zk-contingent payment protocol[3]).

References

[1] Dziembowski, Stefan and Eckey, Lisa and Faust, Sebastian, "FairSwap: How To Fairly Exchange Digital Goods" *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*

[2] Eckey, Lisa and Faust, Sebastian and Schlosser, Benjamin, "OptiSwap: Fast Optimistic Fair Exchange",*Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*

[3] Fuchsbauer, Georg, "WI Is Not Enough: Zero-Knowledge Contingent (Service) Payments Revisited",*Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*

[*] Kyoto university, (zhang.huan.35w@st.kyoto-u.ac.jp)

[†] NTT Corporation, Kyoto university (mehdi.tibouchi@normalesup.org)

[‡] NTT Corporation(miguel.ambrona.fu@hco.ntt.co.jp)

[§] NTT Corporation, Kyoto university (abe.masayuki.914@gmail.com)