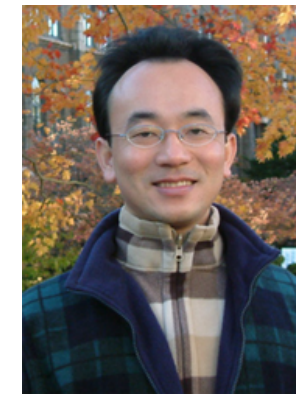Software engineering midtrem report

A STUDY ON TRANSACTION FEE MINIMIZATION STRATEGIES BASED ON THE UTXO MODEL IN CRYPTOCURRENCIES

Zhong-Rui Tsai (Jerry)
Institute of Information Management

Professor: Min-Yuh Day
Institute of Information Management

DATE:APR.9,2025

OUTLINE

1.1 RESEARCH BACKGROUND

- Blockchain is developing fast, with many new chains and cryptocurrencies emerging.

- In UTXO-based systems, fees are based on data size, not amount.

1.2 RESEARCH MOTIVATION

- Dust problems in the UTXO model increase fees and reduce transaction efficiency.

- User behavior studies highlight an urgent need for effective UTXO management.

1.3 RESEARCH OBJECTIVES

Proposes a **comprehensive algorithm** that focuses on three key strategies:

- Dynamic chain selection

  Automatically choosing the lowest-fee blockchain when multiple cryptocurrencies are available.

- Dust UTXO consolidation

  Merging small UTXOs during low-fee rate to reduce future costs.

- UTXO selection for payments

  Selecting optimal UTXO combinations to minimize fees and maintain usable change.

These methods aim to offer users more flexible and reduce transactions fee across multiple blockchains.

1.4 EXPECTED RESULTS

- Goal 1. Minimize transaction costs

- Goal 2.Reduce dust UTXOs
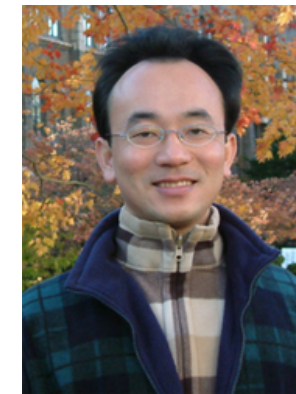
- Goal 3. Improve transaction efficiency

REFERENCE

- S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- S. Delgado-Segura, C. Pérez-Sola, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Analysis of the bitcoin utxo set," in Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22, 2019: Springer, pp. 78-91.
- C. Pérez-Solà, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Another coin bites the dust: an analysis of dust in UTXO-based cryptocurrencies," Royal Society open science, vol. 6, no. 1, p. 180817, 2019.
- G. Ramezan, M. Schneider, and M. McCann, "MACS: A Multi-Asset Coin Selection Algorithm for UTXO-based Blockchains," in 2023 IEEE International Conference on Blockchain (Blockchain), 2023: IEEE, pp. 121-126.
- M. H. Tabatabaei, T. Garrett, and R. Vitenberg, "Analysis of Input/Output Count and Transaction Size in Bitcoin," in 2024 IEEE International Conference on Blockchain (Blockchain), 2024: IEEE, pp. 386-391.
- X. Wei, C. Wu, H. Yu, S. Liu, and Y. Yuan, "A coin selection strategy based on the greedy and genetic algorithm," Complex & Intelligent Systems, vol. 9, no. 1, pp. 421-434, 2023.
- D. Mohanty, D. Anand, H. M. Aljahdali, and S. G. Villar, "Blockchain interoperability: Towards a sustainable payment system," Sustainability, vol. 14, no. 2, p. 913, 2022.
- H. Mao, T. Nie, H. Sun, D. Shen, and G. Yu, "A survey on cross-chain technology: Challenges, development, and prospect," Ieee Access, vol. 11, pp. 45527-45546, 2022.
- G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," White paper, vol. 21, no. 2327, p. 4662, 2016.
- J. Ma and E. Mahmoudinia, "Comprehensive Modeling Approaches for Forecasting Bitcoin Transaction Fees: A Comparative Study," arXiv preprint arXiv:2502.01029, 2025.
- G. E. Box and G. C. Tiao, "Intervention analysis with applications to economic and environmental problems," Journal of the American Statistical association, vol. 70, no. 349, pp. 70-79, 1975.