HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY, VNU-HCM
FACULTY OF COMPUTER SCIENCE & ENGINEERNG

MATHEMATICAL MODELING

Assignment

Mathematical model for UTXO selection

Tutor: Huỳnh Tường Nguyên (htnguyen@hcmut.edu.vn)
Class: HLMT1, Group: 4
Student members: Đặng Xuân Bình - 51100277
Lê Hoàng Bửu - 51100330

Ho Chi Minh, 04/2019

Contents

1 Introduction

Write context here ...

A decentralized cryptocurrency is a digital asset using cryptography systems collectively to secure the transactions and integrity without the third party's intervention. All the transactions in the system are registered on a ledger called blockchain that is constituted of a sequence of blocks. Each block contains an unfixed number of transactions and also a hash of the previous block so that all transactions in the blockchain are immutable and valid. A significant example of this kind cryptocurrency is Bitcoin introduced in 2008 which has currently over $141 billion in the coin market, with an average of 229K transactions daily and around 183.89 GB of storage[1].

In transaction-based blockchains, the selection strategy of UTXOs for the transaction plays an essential role in cryptocurrency balance management of any wallet. An optimized coin selection strategy should satisfy hard constraints and essential goals of three principal groups such as users, community and miners. Owing to consumers, they would like to create a transaction that minimizes the transaction fee and also reserves the privacy of their behaviors. By contrast, miners focus on mining transactions which have a higher fee as much as possible. To the community, the large UTXO pool size becomes a dramatic problem because it drops down the transaction processing performance and also produces a high cost of memory consumption. Like Bitcoin system, a snapshot of the current state required additional space in the memory to store objects for processing transactions [**?**].

In this work, we consider problem of strategy research in order to select a set of UTXOs for a given transaction which should cost a minimum fee for miners or gather as much as possible small UTXO in order to reduce the UTXO pool size. The remainder of this report is organized in the following. Section **??** presents short context and requirement of the considering problem. Then, we present our work in Section **??**. Section **??** summaries the performance evaluation and discussion on experimental results. Finally, we conclude our work in the last section.

2 Problem formulation

Describe clearly problem statement or requirement of the problem that needs to be modeled.

3 Proposed model

Variables:
Constraints:
Objective function:

4 Experimental evaluation

Input format:
Output format:
Implementation in GLPK/AMPL:
Experimental results

5 Conclusion

References

[1] wikipedia. "**link: http://en.wikipedia.org/**", , last access: 05/05/2015.

[2] Frey, D., Makkes, M. X., Roman, P.-L., Taiani, F., Voulgaris, S.: Bringing secure Bitcoin transactions to your smartphone. The 15th International Workshop on Adaptive and Reflective Middleware, (2016).

[3] Antonopoulos, A. M.: Mastering Bitcoin. 2nd edn. O'Reilly Media, CA 95472 (2014).

[4] Bitcoinjs: Open Source Organisation for Bitcoin JavaScript Libraries,https://github.com/bitcoinjs. Last accessed 15 August 2018.

[1] https://coinmarketcap.com

[5] Bitcoinj: Library for working with the Bitcoin protocol,https://bitcoinj.github.io. Last accessed 10 August 2018.

[6] Yanovich, Y., Mischenko, P., Ostrovskiy, A.: Shared Send Untangling in Bitcoin, White paper, Bitfury Group Limited (2016).

[7] Dai, P., Mahi, N., Earls, J., Norta, A.: Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform, https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3.pdf, (2016).

[8] Sergi, D.-S., Cristina, P.-S., Guillermo, N.-A., Jordi, H.-J.: Analysis of the Bitcoin UTXO set, IACR Cryptology ePrint Archive, (2017).

[9] Erhardt, M.: An Evaluation of Coin Selection Strategies, Master thesis, Karlsruhe Institute of Technology, URL: http://murch.one/wp-content/uploads/2016/11/erhardt2016coinselection.pdf, (2016).

[10] Zahnentferner, J.: Chimeric ledgers: Translating and unifying utxo-based and account-based cryptocurrencies, Cryptology ePrint Archive, Report 2018/262, 2018. https://epri nt. iacr. org/2018/262, (2018).

[11] Chepurnoy, A., Kharin, V., Meshkov, D.: A Systematic Approach To Cryptocurrency Fees. IACR Cryptology ePrint Archive, (2018).