Jia-zhi XIA, Yu-hong ZHANG, Hui YE, Ying WANG, Guang JIANG, Ying ZHAO, Cong XIE, Xiao-yan KUI, Sheng-hui LIAO, Wei-ping WANG, 2020. SuPoolVisor: a visual analytics system for mining pool surveillance. *Frontiers of Information Technology & Electronic Engineering*, 21(4):507-523.
https://doi.org/10.1631/FITEE.1900532

SuPoolVisor: a visual analytics system for mining pool surveillance

Key words: Bitcoin mining pool; Visual analytics; Transaction data; Visual reasoning; FinTech

Corresponding author: Ying ZHAO
E-mail: zhaoying@csu.edu.cn
ORCID: Jia-zhi XIA, https://orcid.org/0000-0003-4629-6268; Ying ZHAO, https://orcid.org/0000-0002-4200-5200

Motivation

1. Mining pools play a critical role in cryptocurrency systems, and thus they are the focus of cryptocurrency surveillance. They may lead to the crisis of a mining monopoly if feasible regulation is not deployed. Mining pools also play a key role in the construction, development, and maintenance of the market infrastructure. In addition, the covert relationship between the pool and other roles will result in a crisis of confidence in the market.

2. Traditional de-anonymization relying on public identities cannot keep up with the changes in deceptive scenarios. Previous work cannot analyze the impacts of the Bitcoin flow in mining pools or determine the correlation between addresses and mining pools. In addition, there was a lack of comprehensive multi-aspect analysis capabilities and guidance in systems for mining pool.

Main idea

1. Based on the characteristics of Bitcoin transactions and mining pools, we propose a set of features for describing the behaviors and effects of mining pools.

2. The visual analytics can help users improve data perception, reveal hidden patterns, and interact with data. We propose a well-designed visual analytics system for supervising mining pools at the pool level and the address level.

3. The de-anonymization requires expert experience and reasoning capabilities. Our system supports an interactive address identification approach for disclosing miners.

Method

1. Recommend the internal address network of the mining pool to users based on a set of features: transaction network generation, feature abstraction, and internal address network recommendation

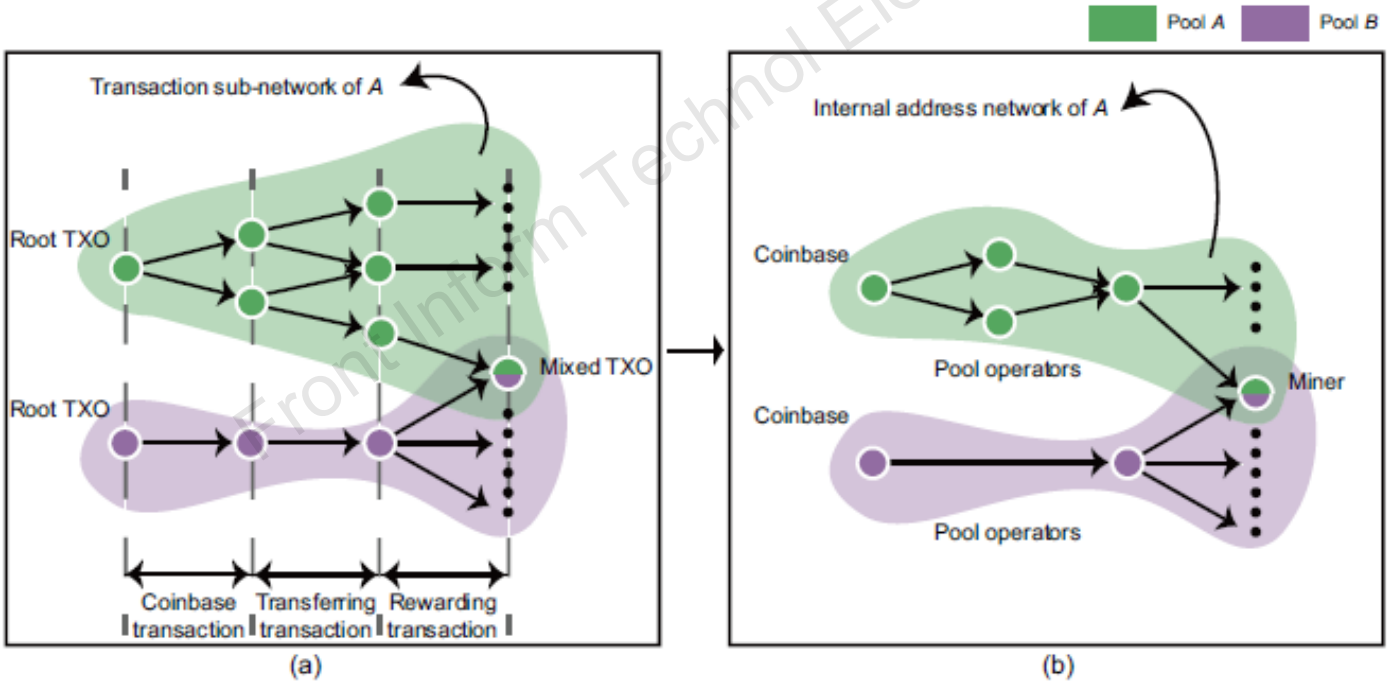

Fig. 3 Construction of the transaction sub-network (a) and the internal address network (b)
Unmixed TXOs are used to find the sub-network of mining pools and the recommended internal address network can be constructed based on the mapping from TXOs to addresses

2. The visual analytics system

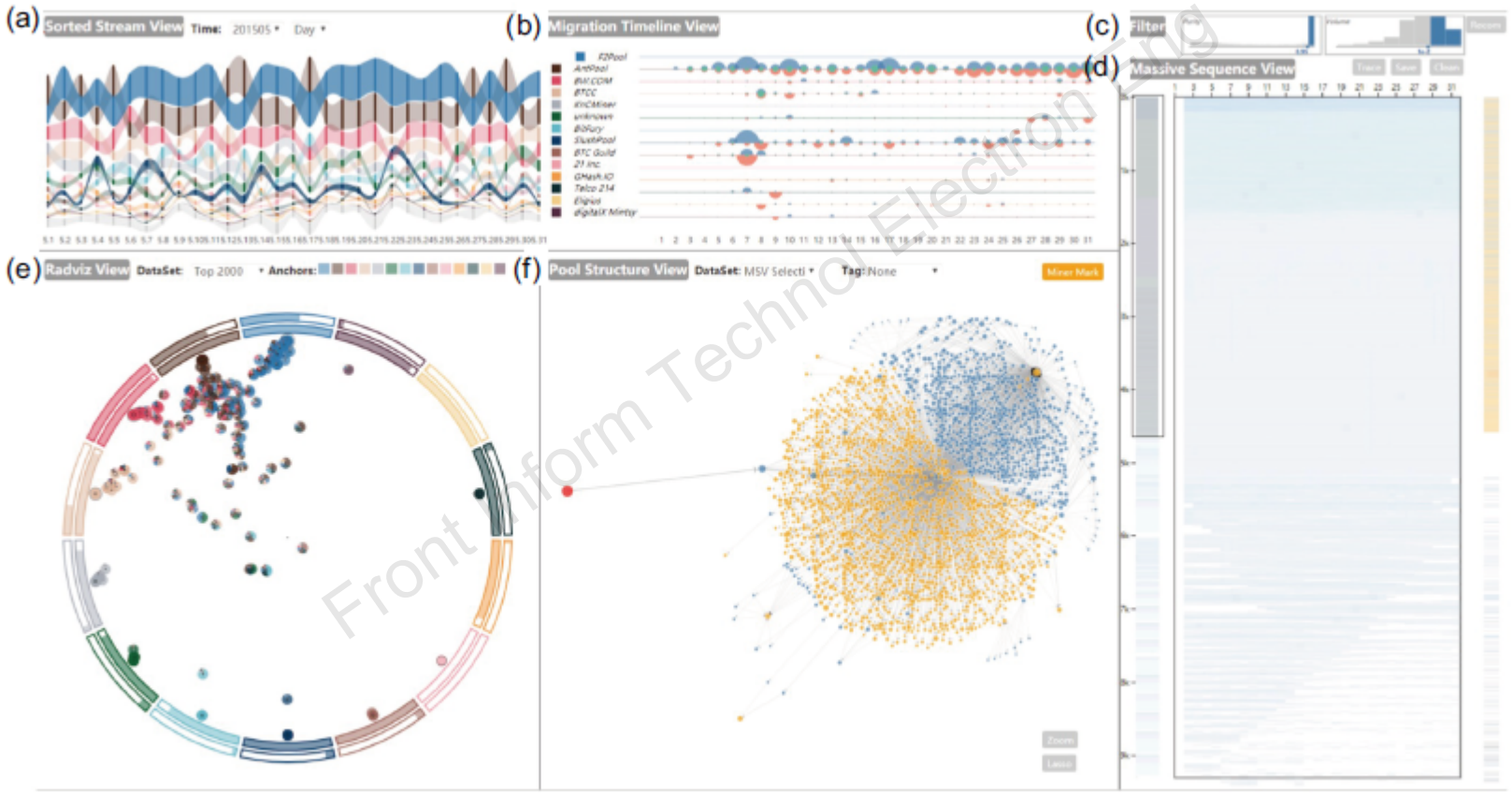

Fig. 4 Interfaces of SuPoolVisor: (a) sorted stream view; (b) migration timeline view; (c) threshold panel; (d) massive sequence view; (e) Radviz view; (f) pool structure view

3. Interactive visual reasoning

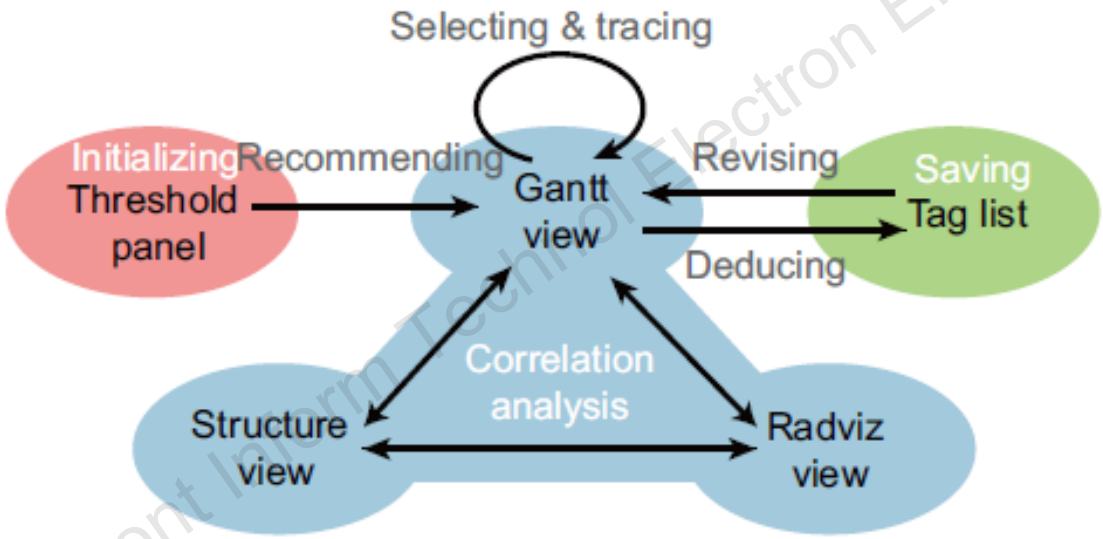

Fig. 6 Interactive reasoning process

Major results

Our expert iterated the visual reasoning processes until thousands of addresses in F2Pool were identified. The system can help users find key addresses and groups in mining pools and provide multi-aspect analysis. It can also significantly show reward destinations.

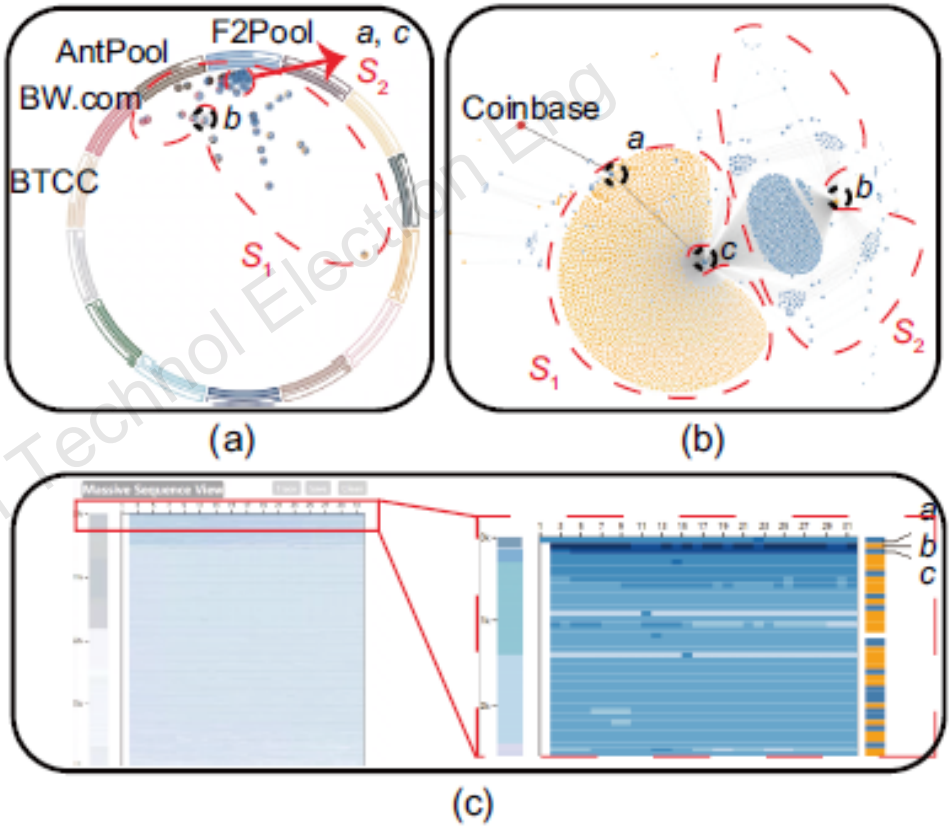

Fig. 7 multi-aspect analysis of special groups and addresses in F2Pool: (a) special groups and addresses in Radviz; (b) special groups and addresses in PSV; (c) three special addresses in MSV

Major results

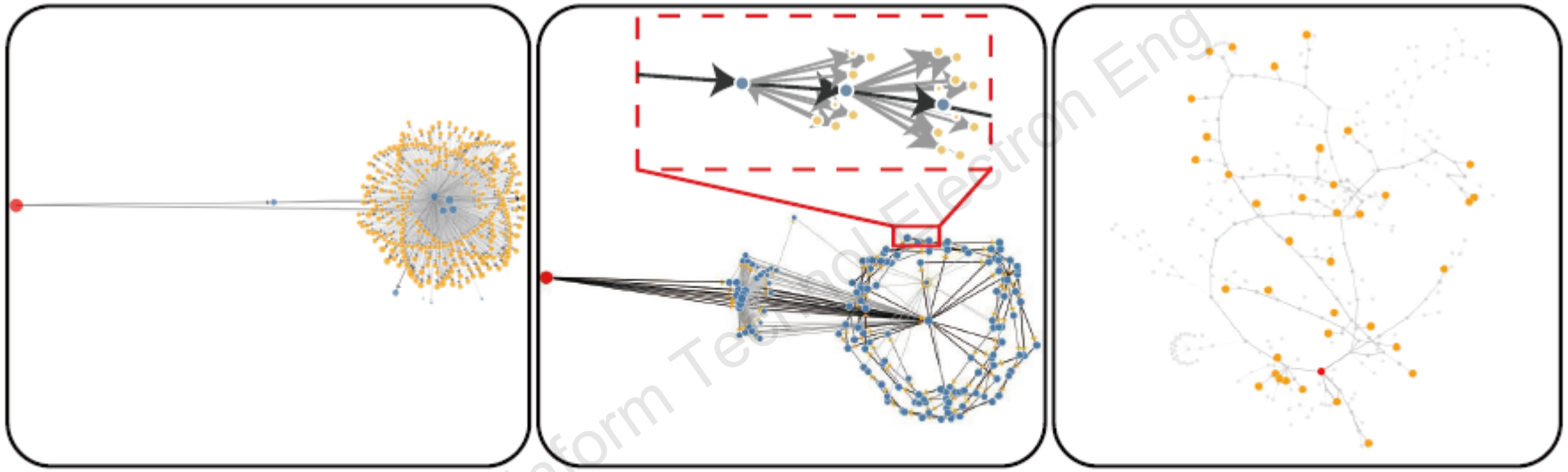

Fig. 8 Three typical internal structures of mining pools: (a) one-to-many payment; (b) iterative payment; (c) linear transferring

Major results

Analyzing the effect of hard forks

At the pool level, in July 2017, the overall block production was stable, and it did not fluctuate when the fork happened. The pool ranking fluctuated sharply, and the number of blocks decreased significantly on August 20–25, 2017. The distribution of these addresses was more concentrated after the fork. At the address level, the planner of the fork, i.e., ViaBTC, ultimately benefited, and F2Pool inevitably received a negative impact.

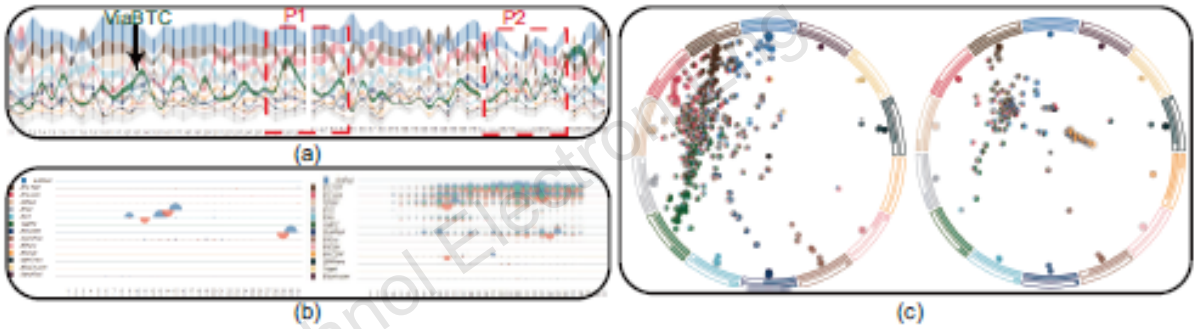

Fig. 9 Overview of Bitcoin market before and after the fork: (a) comparison of SSV in July and August 2017; (b) comparison of MTV in July and August 2017; (c) comparison of Radviz in July and August 2017

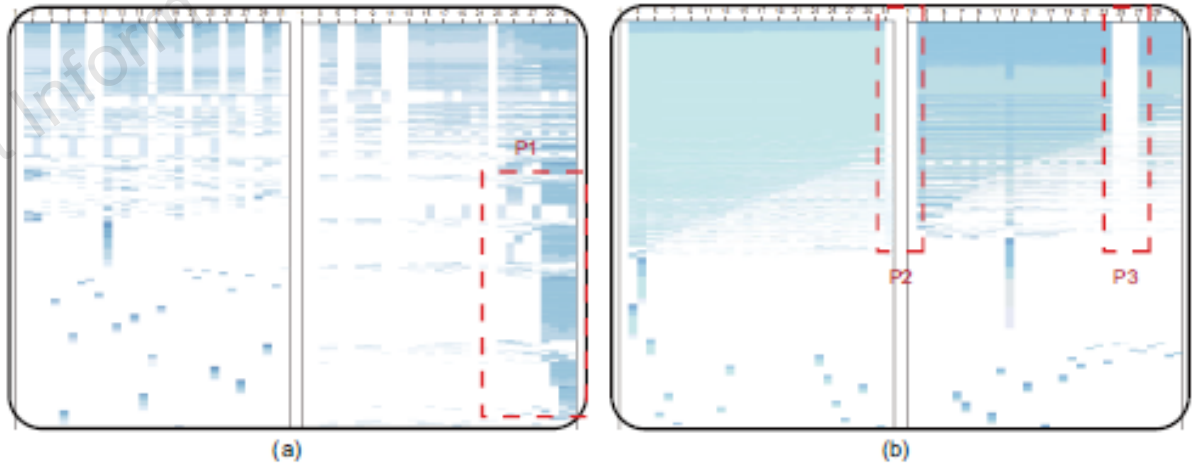

Fig. 10 Comparison of miners' behavior before and after the fork: (a) MTV of ViaBTC; (b) MTV of F2Pool

Conclusions

1. We proposed a visual analytics system, SuPoolVisor, to facilitate regulators and researchers in surveillance and de-anonymization in Bitcoin. Multi-level and multi-faceted interactive analysis was implemented in the system. In particular, we proposed a set of features to identify miners, and the initial internal address network was recommended based on them.

2. Further research will focus on two aspects. The first task is to improve graph representation and visualization. We plan to express large-scale dynamic graphs in a vectorized form. Another useful improvement in the future is to use deep learning in de-anonymization and recommendation to reduce repetitive interactions and provide guidance.