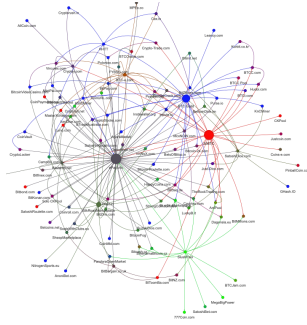


Pattern Analysis of Money Flows in the Bitcoin Blockchain

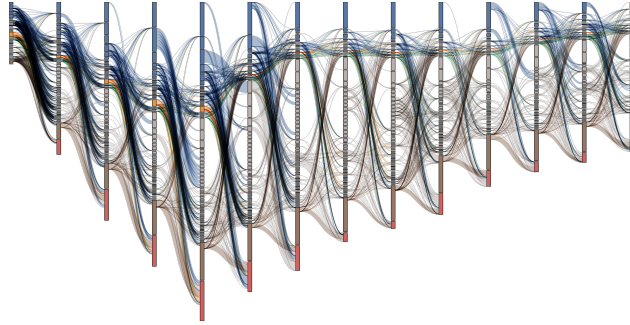
Natkamon Tovanich,¹ and Rémy Cazabet²

1. Blockchain & B2B Platforms Chair, École Polytechnique, CREST, IP Paris, Palaiseau, France

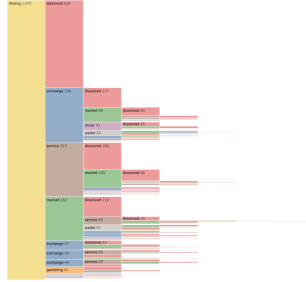
2. Univ de Lyon, CNRS, Université Lyon 1, LIRIS, UMR5205, Villeurbanne, France



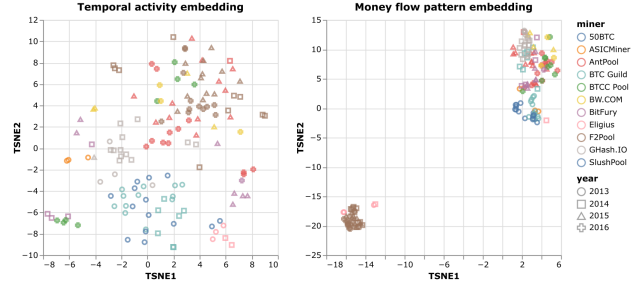
(a) Static network



(b) Dynamic network



(c) Money flow pattern



(d) Network features projections

Bitcoin is a cryptocurrency that stores transaction records in a public distributed ledger called the blockchain. All transactions that occurred since the beginning of Bitcoin in 2009 can therefore be consulted by anyone. This unique dataset allows us to study financial transaction networks among pseudonymous participants. Several works analyzed static transaction networks but did not consider the flow of money over the time^{1,2}. In this work, we focus on the analysis of flows, a challenging task given the scale of the data (hundreds of millions of transactions).

We propose a method based on taint analysis³ to track Bitcoin money flow from initial starting points to the dissolution of the taint. The algorithm derives the dynamics subgraphs passing through known entities in the transaction network. We study the pattern of money flowing from different starting points: we taint coins minted by different mining pools in one day period between 2013 and 2016, and use graph embeddings from three representations of the data: (1) static network, (2) dynamic network, and (3) money flow pattern tree. Both qualitative and quantitative analysis show that mining pools have different diffusion patterns and that those patterns evolve over time. Based on this initial result, we are developing a method to select critical entities and expand our unsupervised approach to characterize other money flow patterns, in particular, related to illegal and cybercrime activities.

¹Akcora, C. G., Li, Y., Gel, Y. R., & Kantarcioglu, M. BitcoinHeist: Topological data analysis for ransomware prediction on the Bitcoin blockchain. In *Proc. IJCAI* (2020).

²Kondor, D., Pósfai, M., Csabai, I., & Vattay, G. Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PloS one*, 9(2), e86197 (2014).

³Di Battista, G., Di Donato, V., Patrignani, M., Pizzonia, M., Roselli, V., & Tamassia, R. BitConeView: Visualization of flows in the Bitcoin transaction graph. In *Proc. IEEE VizSec* (2015).