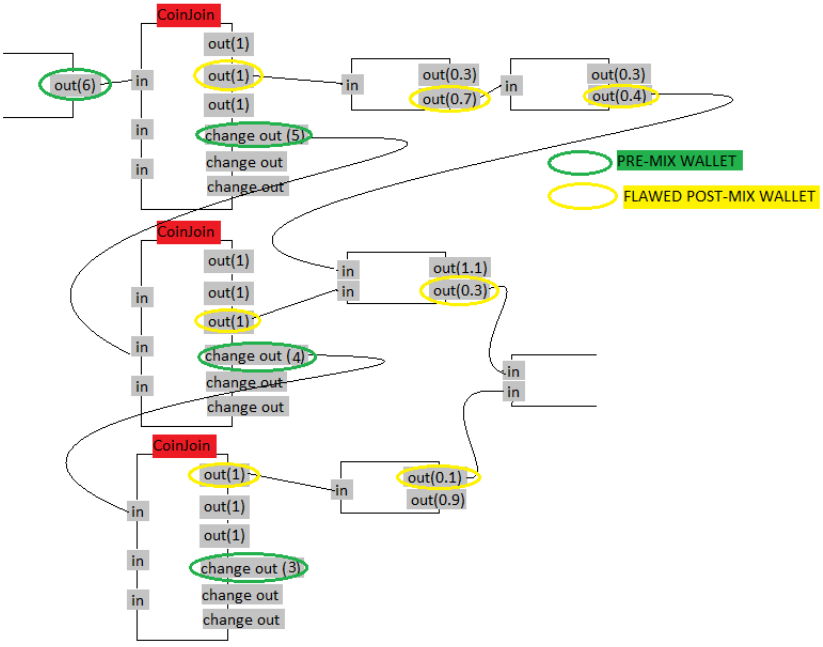
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Prof. R. Wattenhofer

Bitcoin Privacy from Chain Analysis

Bitcoin's blockchain is publicly visible. Chain analysis tools routinely go through the blockchain to unravel Bitcoin's transaction graph to associate real world identities with Bitcoin transactions. Real world identities are associated with transactions when KYC-enabled entities like exchanges or merchants are involved in them. These identities and their associations with some part of the transaction graph can be propagated to another part of the graph through heuristics like: 1) Re-using receiving addresses, 2) Common input ownership, 3) Change output characteristics, etc.



There are many ways of preventing analysis tools from associating one part of the transaction graph with another - through centralized or decentralized services. In this project, we investigate some of these privacy enabling tools, and see whether their own patterns are visible on the blockchain, and whether that makes it possible to split the Bitcoin UTXO set into "tainted" and "clean" coins. If that is the case, can we make these distinctions harder, or impossible? Do the latest developments in Bitcoin like Taproot, or Cross Input Signature Aggregation help such efforts?

Requirements: This project involves understanding Bitcoin's technical details, heuristics used in chain analysis, and the ability to apply "cryptographic tricks" to these problems.

Interested? Please contact us for more details!
Contact: Tejaswi Nadahalli: tejaswin@ethz.ch, ETZ G97