

btctrackr : **Finding and Displaying** **Clusters in Bitcoin**

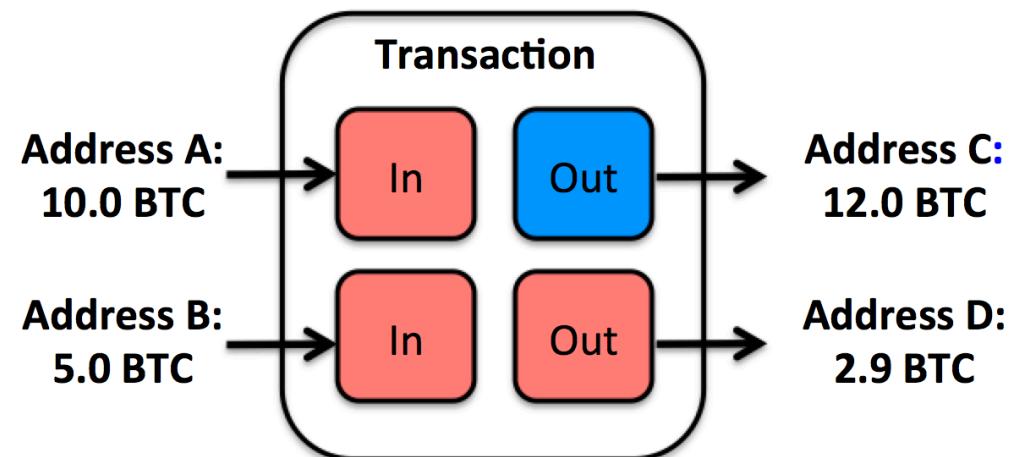
Aaron Doll, Shaheed Chagani,
Michael Kranch, and Vaidhyanath Murti

Overview

- Motivation (Fistful of Bitcoins)
- Challenges and Goals
- btctrackr System
 - Parser
 - Database
 - Website
- Demonstration
- Evaluation
- Future Work

Motivation (Fistful of Bitcoins)

- Improve upon Existing Address Clustering
 - Heuristic 1 – All inputs
 - Heuristic 2 – Change Addresses
- Current Implementation
 - Need significant by hand cleaning
 - Not in real-time
- Znort Parser

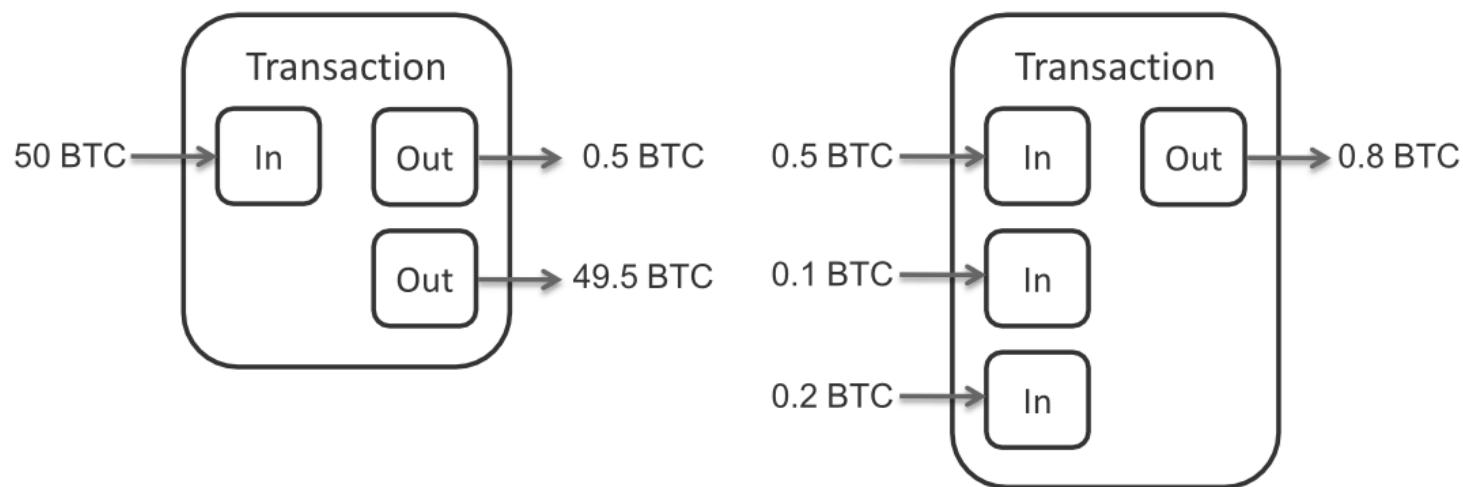


Goals / Challenges

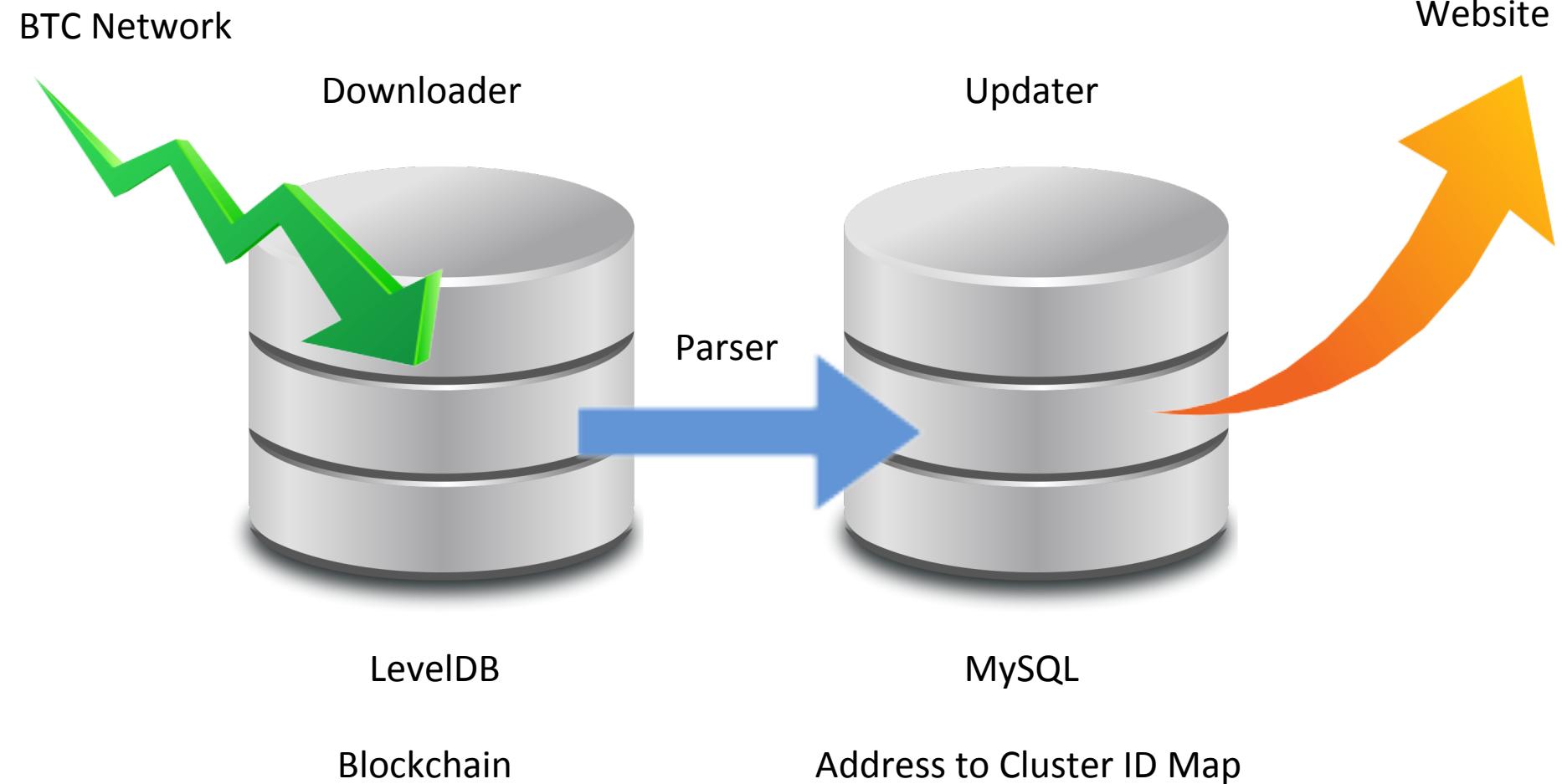
- Challenges
 - Resource management
 - Continually updating information
 - Legacy block chain information
 - Integration of systems
- System Goals
 - Real-time responses
 - Accurate
 - Expandable

btctrackr: Parser

- Libbitcoin
- Three Steps
 - Find clustering transactions
 - Find input addresses of transaction
 - Keep track of connected components



btctrackr: Database



btctracker - Website

Track



Enter an address to find out which other addresses likely belong to the same person.

15iGN5CAkTarcoY85XxwTYWajJyz5hxbYv

Track

Shortest Path



Enter two addresses to find their shortest connecting path.

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy



15iGN5CAkTarcoY85XxwTYWajJyz5hxbYv

Shortest Path

Cluster Balances



The address 1KCszN2rch9SMPagTS1r2QeGt7h9P7ehne (0 ₿) likely belongs to an entity controlling 59 other addresses and 0 ₿.

1112cfXejap7ph4eJyGMxdKV63dMqAGJA (0 ₿)
115kBURFyLpoHYaHkHaR53Dah2Au4oMPcD (0 ₿)
12jn5UKnA393WnPcEQzT2VQavDz2RaDFis (0 ₿)
12S5HaA2KqHqxjsgCxQZafuefWSsNcVKs3 (0 ₿)
139XRbcUerNFDud6nmW7354GGjc9K4d41p (0 ₿)
14pbaDjFKxjcJCBDyqMK3jMgjwH5Pzw9A (0 ₿)
14T6tX5w2dvvq54FRX9gKdgUpXX43Huhow (0 ₿)
154eBsTnVRLLkRYPdz88cMvAKPXPJcx5ME (0 ₿)
156SgGubQC44UvkuA6fPfzWxJWVncEjno7 (0 ₿)
158t3VzjRFyXQvcSydmzAv5KBbVtagm8Pe (0 ₿)
15BTysPZA57Qyj5gzFyroXYNGRRbNu8n96 (0 ₿)
15GznXHKRkwLz3D9BcVUcFLqYzdJqyoqq6 (0 ₿)
15HDdWRJ9zYZxGdCes1gicNURLBuJiuVES (0 ₿)
16LSQHMwrSW1M54QLpTXEPk49CMorSGCza (0 ₿)
171Y4B13xLvoEHisr34FeFSwoC2aBciekC (0 ₿)
17FhZZJ7ZziaQC5kYUTHikBnnZdRb182k (0 ₿)
17gd6BJpBSt36fKj14fRJts6oYYiKyMK4 (0 ₿)
17JLFY9KjPS8dkMy33RJ5yiGN1P6K68JZZ (0 ₿)
181j7x6SraKRrK2KEwP5W3Szrd417BERxf (0 ₿)
18Fzbd1bdn5Qe3b5wP8F4Tb2zYxvAtMwRC (0 ₿)

DEMO

Evaluation

The screenshot shows the Bitlodine web application interface. At the top, there's a navigation bar with links for 'Home', 'Find paths', 'See clusters', 'Get insights', and a dropdown for 'Country' (set to 'US'). Below the navigation is a large circular network visualization composed of numerous small yellow dots, with a prominent yellow 'B' in the center. To the left of the visualization, text reads: 'With Bitlodine you can find connecting paths between two addresses, visualize clusters controlled by the same user or entity, and get insights about activity on the network.' Below this, there are several input fields containing Bitcoin addresses: '1AA2MkdGEv7kQzq2XXCSHdQcvvac58QcGE', '1A1zPleP5QGefi2DMPtTlLSSunv7DivaN', '1Shremdr9tVop1gxMzj7bhsp6XXzWWRW', and 'Cluster'. There are also buttons labeled '→ B →' and 'B →'. At the bottom of the page, a copyright notice states: '© 2014 - a project by Michele Spagnuolo (Github). Blockchain data delayed ~6h. 35637573 nodes. 214132686 J.'

VS

The screenshot shows the btctrackr web application interface. The main heading is 'btctrackr'. Below it, a sub-header says 'Enter an address to find out which other addresses likely belong to the same person.' A text input field contains the Bitcoin address '15iGN5CAkTarcoY85XwTYWajJyz5hxbYv'. To the right of the input field is a yellow 'Track' button. At the bottom of the page, a link reads 'Track - Shortest Path - Github'.

	False Negative %
btctrackr*	35.8
Bitlodine	54.2

- at the time of this evaluation btctrackr only had 200,000 blocks parsed

Future Work

- Increased speed for balances
- Increased accuracy for 1-hop paths
- Cluster labeling
- Advanced Features:
 - Implementation of the change heuristic
 - Labeling and Identifying well-known cluster
 - Tracking IP addresses