Identification of Cross-Blockchain Transactions: A Feasibility Study

Patrick Nieves, 13.11.2017, Munich

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de
Outline

1. Motivation
2. Approach
3. Research Questions
4. Timeline
Rising Amount of Cryptocurrencies leads to rising Demand for Cryptocurrency Exchange

Trading Platforms

Instant Cryptocurrency Exchange
Motivation

Instant Cryptocurrency Exchange - Overview

- Small fee
- Simple process
- Fast
- Anonymous
Motivation

Instant Cryptocurrency Exchange - Overview

24 Hour Statistics

<table>
<thead>
<tr>
<th>Transactions</th>
<th>Bitcoin Volume Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>45,597</td>
<td>8,488.986 BTC</td>
</tr>
</tbody>
</table>

Average Processing Time

2101 seconds

Most Popular Trade

[Image of currency exchange]
Motivation

Instant Cryptocurrency Exchange Example - Changelly

Search on Trading Platforms (e.g. Poloniex, Bittrex)

Total Fee = Exchange Fee + Network Fee

Processing Time and volatile Currencies lead to different final Rates

1 BTC + Network Fee

14.6 ETH + Network Fee

Best Exchange Rate - Exchange Fee

EXCHANGE RATE: 1 BTC = 14.674 ETH
FEE INCLUDED (0.5%): 0.07337 ETH
ESTIMATED ARRIVAL: ≈5-30 minutes

YOU HAVE

1 BTC

YOU GET

14.60063 ETH
Motivation
Blockchain Data Analysis

Explorer for individual Blockchains

Trading Platforms

Instant Cryptocurrency Exchange

?
## Outline

1. Motivation
2. Approach
3. Research Questions
4. Timeline
Approach

Solution & Realization

Design of an Algorithm for Recognition of Instant Cryptocurrency Exchange Transactions and Implementation as an Explorer Platform

- **Analysis** of Cryptocurrency Exchange Processes and available APIs/Tools/Technologies
- **Design** of a Recognition Algorithm (starting with two currencies)
- **Implementation** of the designed Algorithm on an extendable Platform (e.g. possibility of adding more Currencies)
- **Testing** with real data
**Approach**

**Architecture**

- Blockchain 1
- Blockchain 2
- Blockchain API Service
- Exchange API Service
- Trading Data API Service

**System Frontend**

**External Services**

**Cross-Blockchain Transactions Identifier**

**Storage**

**Identification Algorithm using Parameters:**

- **Exchange Rate** based on extern Rate, Exchange Fee & Transaction Fee
- **Exchange Duration** based on Timestamps
- Known **Exchange Addresses**

<table>
<thead>
<tr>
<th>Age</th>
<th>From</th>
<th>To</th>
<th>Input</th>
<th>Outcome</th>
<th>Tx Fee</th>
<th>Tx Hash From</th>
<th>Tx Hash To</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 min</td>
<td>BTC</td>
<td>ETH</td>
<td>1 BTC</td>
<td>14.6 ETH</td>
<td>0.07 ETH</td>
<td>BwUj6Ex3ndo56lsi43N…</td>
<td>10x9029b388e83e2363f04…</td>
</tr>
<tr>
<td>2 min</td>
<td>LTC</td>
<td>BTC</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>
Approach

Data retrieval

Get last 50 Transactions
(shapeshift.io/recenttx/50)

```json
[{
  "curIn": "REP",
  "curOut": "BCH",
  "timestamp": 1510527712.046,
  "amount": 2.79353472,
  "txid": 318311
},
{
  "curIn": "LTC",
  "curOut": "BCH",
  "timestamp": 1510527706.291,
  "amount": 2.787439956,
  "txid": 777777
},
{
  "curIn": "ETH",
  "curOut": "BCH",
  "timestamp": 1510527706.225,
  "amount": 0.43348018,
  "txid": 589973
},
{
  "curIn": "SALT",
  "curOut": "BCH",
  "timestamp": 1510527705.528,
  "amount": 35.52130301,
  "txid": 407891
},
{
  "curIn": "ETH",
  "curOut": "LTC",
  "timestamp": 1510527684.702,
  "amount": 0.008,
  "txid": 998846
}]
```

Get Transaction by Hash
(shapeshift.io/txStat/0x0056d4165b1ba0b05ec334308db4b78d71299191)

```json
{
  "status": "complete",
  "address": "0x0056d4165b1ba0b05ec334308db4b78d71299191",
  "withdraw": "XotVm3i6mue9uhWxGbtsw7qmfPd8ms5aa",
  "incomingCoin": 1,
  "incomingType": "ETH",
  "outgoingCoin": "1.09433849",
  "outgoingType": "DASH",
  "transaction": "5a0101618c90dead9b0ab441733db9002ab4d4ade65427ab19ac77013990f38"
}
```
Approach
Gains & Problems

+ Transparency over Trading Behavior
+ Tracking of Cross-Currency Transactions
+ Potential Usage for other Projects

- Difficult Identification of Users
- Every Broker has different Fees & Rates
- Limited API's of Brokers
Outline

1. Motivation
2. Approach
3. Research Questions
4. Timeline
1. What is the current state of art regarding Cryptocurrency Exchange?

- Rise of Exchange Service Usage
- Exchange Services with different processes and different basic conditions (Fees, Time, Rates, Currencies…)
- Atomic Swaps (COMIT, Lightning)
Research Questions

2. How can Cross-chain Cryptocurrency Exchange Transactions be recognized?

• Available Analysis Tools and APIs
• Design of suitable Algorithms taking into account different Parameters

3. How accurate is the implemented Solution? What are the limits?

• Testing with real data (using Data retrieved from Shapeshift)
• Suggestion for future work
Outline

1. Motivation
2. Approach
3. Research Questions
4. Timeline
Timeline

<table>
<thead>
<tr>
<th>Literature/Research</th>
<th>October</th>
<th>November</th>
<th>December</th>
<th>January</th>
<th>February</th>
<th>March</th>
<th>April</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data retrieval &amp; Concept</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Writing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Official Start Date: 15.10.2017

Official End Date: 15.04.2018

Supervisors: Patrick Holl, Ulrich Gallersdörfer
B.Sc. Information Systems

Patrick Nieves

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel  +49.89.289.
Fax  +49.89.289.17136

patrick.nieves@tum.de
www.matthes.in.tum.de