Facilitating the Decentralised Exchange of Cryptocurrencies in an Order-Driven Market

2nd conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 28-30 Sep 2020

Moritz Platt (Presenter)*, Francesco Pierangeli*, Giacomo Livan**, Simone Righi**

*King’s College London, **University College London
Agenda

1. Centralised Exchanges (CEX) vs. Decentralised Exchanges (DEX)—Two different paradigms creating different risk profiles for traders

2. Protocol—Combining centralised and decentralised elements and the need for performance scoring

3. Future Work—Addressing the trade-off between anonymity and reliability in a decentralised environment via a zero-knowledge protocol
### CEX by Trade Volume

<table>
<thead>
<tr>
<th>Name</th>
<th>Volume (24h)</th>
<th>Volume (7d)</th>
<th>Volume (30d)</th>
<th>No. Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>BKEX</td>
<td>$3bn</td>
<td>$18.3bn</td>
<td>$74bn</td>
<td>100</td>
</tr>
<tr>
<td>Fatbtc</td>
<td>$2.8bn</td>
<td>$16.1bn</td>
<td>$66bn</td>
<td>114</td>
</tr>
<tr>
<td>BiKi</td>
<td>$2.4bn</td>
<td>$13.5bn</td>
<td>$57bn</td>
<td>92</td>
</tr>
<tr>
<td>BitForex</td>
<td>$2.4bn</td>
<td>$15.1bn</td>
<td>$60bn</td>
<td>153</td>
</tr>
</tbody>
</table>

USD rounded, CoinMarketCap (2019)

- All commercially relevant exchanges on the market today operate in a centralised manner.
- Centralised exchanges provide market-making capabilities by holding a reserve of cryptocurrencies, standing ready to buy currency and to sell.
- Well understood model based on the same principles as foreign exchange spot trading of fiat currencies.
Anatomy of a *CEX*

- Participants deposit currency into exchange account
- Exchange pays out funds at agreed rate to recipient account
- Business model reliant on fees and bid-ask-spread (Bundi and Wildi, 2019)
## Risk of Misappropriation of Funds in Transit in CEX

Chohan (2018) outlines collates high-profile incidents:

<table>
<thead>
<tr>
<th>Year</th>
<th>Exchange</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>Mt. Gox</td>
<td>$8m</td>
</tr>
<tr>
<td></td>
<td>Bitomat</td>
<td>$220k</td>
</tr>
<tr>
<td></td>
<td>MyBitcoin</td>
<td>$800k</td>
</tr>
<tr>
<td>2012</td>
<td>Bitcoinica</td>
<td>$460k</td>
</tr>
<tr>
<td></td>
<td>Bitcoin Savings and Trust</td>
<td>$5.6m</td>
</tr>
<tr>
<td></td>
<td>Bitfloor</td>
<td>$250k</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Exchange</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Bitfloor</td>
<td>$250k</td>
</tr>
<tr>
<td>2013</td>
<td>Instawallet</td>
<td>$4.6m</td>
</tr>
<tr>
<td></td>
<td>Inputs.io</td>
<td>$730k</td>
</tr>
<tr>
<td></td>
<td>Global Bond Limited</td>
<td>$5m</td>
</tr>
<tr>
<td>2014</td>
<td>Mt. Gox</td>
<td>$390m</td>
</tr>
<tr>
<td>2015</td>
<td>Bitstamp</td>
<td>$5.1m</td>
</tr>
</tbody>
</table>

USD rounded
Naïve DEX

-Participant A transfers a previously agreed amount of $C_1$ to B who in turn transfers a previously agreed amount of $C_2$ back to A.
-Transactionality of transfers is key
The prevalent paradigm utilised to enable ‘atomic’ swaps between different cryptocurrencies are ‘Hashed Time-Locked Contracts’ (HTLC).

Most commercially relevant cryptocurrencies can be connected via HTLC (Griffith, 2019).
### Exchange Paradigms

Within paradigms, different aspects are beneficial to traders:

<table>
<thead>
<tr>
<th>Aspect</th>
<th>CEX</th>
<th>DEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk of misappropriation of funds in transit</td>
<td>High</td>
<td>None</td>
</tr>
<tr>
<td>Exclusion of participants</td>
<td>Feasible</td>
<td>Unfeasible</td>
</tr>
<tr>
<td>Direct trading costs</td>
<td>Prevalent</td>
<td>None</td>
</tr>
<tr>
<td>Trading partner discovery</td>
<td>Trivial</td>
<td>Complex</td>
</tr>
<tr>
<td>Exchange rate transparency</td>
<td>Transparent</td>
<td>Opaque</td>
</tr>
<tr>
<td>Opportunity costs due to tied capital</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>
Protocol Implementation

- Multi-stage protocol that facilitates HTLC-based decentralised exchanges
- Designed to alleviate the downsides of decentralised exchanges:
  - Complicated trading partner discovery
  - Opaque exchange rates
  - Opportunity costs incurred from failed trades
- Introduces a ‘supporting distributed ledger’ to facilitate trades
- Supporting ledger is not involved in the actual execution of trades, thus maintaining the advantages of decentralised exchanges
  - No risk of misappropriation of funds in transit
  - No direct trading costs
  - Censorship resistancy
System Design

Supporting DLT Network γ
- Market Services Operator O
- Matching Engine
- Rate Reporting Facility
- Score Reporting Facility
- Execution Monitoring Facility

Node I
- Order List
- Trading Engine

Node II
- Order List
- Trading Engine

Cryptocurrency α
- Address I₁
- Address I₂
- Address I₃

Cryptocurrency β
- Address I₁
- Address I₂

Uniqueness Consensus Component
Conclusion

- We show how combining centralised elements with decentralised technology can ease trading partner discovery, thus lowering the friction during the preliminary phase of a trade.
- We show how performance scoring can lower opportunity costs by reducing the risk of trades falling through.

Future Work

- Performance scoring is the main driver for centralisation.
- Can we do better, i.e. make performance scoring work in a decentralised fashion?
- Zero-knowledge proofs for successful/failed trade volumes?
Bibliography


