Incentives and Governance Model for a Decentralised Crypto Asset Exchange

Final Project Presentation
First Internal Fund Call for Project Proposals on Distributed Ledger Technologies at the UCL Centre for Blockchain Technologies, 20 February 2020

Giacomo Livan, University College London
Francesco Pierangeli, King’s College London/National University of Singapore
Moritz Platt, King’s College London
Simone Righi, University College London
Agenda

1. Centralised and Decentralised Exchanges
2. Protocol
3. Outlook
### Cryptocurrency Market Capitalisation

<table>
<thead>
<tr>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Supply</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Bitcoin</td>
<td>$184,210,229,903</td>
<td>$10,116.92</td>
<td>$35,794,231,987</td>
<td>18,208,125 BTC</td>
</tr>
<tr>
<td>2  Ethereum</td>
<td>$25,093,191,977</td>
<td>$228.89</td>
<td>$14,936,061,883</td>
<td>109,628,359 ETH</td>
</tr>
<tr>
<td>3  XRP</td>
<td>$12,352,182,524</td>
<td>$0.282670</td>
<td>$2,268,819,803</td>
<td>43,698,224,662 XRP</td>
</tr>
<tr>
<td>4  Bitcoin Cash</td>
<td>$8,219,158,862</td>
<td>$449.89</td>
<td>$4,127,089,476</td>
<td>18,269,163 BCH</td>
</tr>
</tbody>
</table>

[CoinMarketCap2020]

- Bitcoin [Nakamoto2009] and the subsequent creation of “Altcoins” introduced the problem of exchanging cryptocurrencies.
- Exchanges are fundamental for the long-term development of a diverse and robust cryptocurrency ecosystem [Gandal2014, Wisniewska2016, Franke2019]
Centralised Cryptocurrency Exchanges by Trade Volume

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Adj. Vol (24h)</th>
<th>Volume (24h)</th>
<th>Volume (7d)</th>
<th>Volume (30d)</th>
<th>No. Markets</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BKEX</td>
<td>$3,125,835,625</td>
<td>$3,125,835,625</td>
<td>$18,384,841,662</td>
<td>$74,523,857,893</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>Fatbtc</td>
<td>$2,871,214,657</td>
<td>$2,871,214,657</td>
<td>$16,112,553,023</td>
<td>$66,644,916,873</td>
<td>114</td>
</tr>
<tr>
<td>3</td>
<td>BiKi</td>
<td>$2,411,115,558</td>
<td>$2,411,115,558</td>
<td>$13,565,814,043</td>
<td>$57,659,250,867</td>
<td>92</td>
</tr>
<tr>
<td>4</td>
<td>BitForex</td>
<td>$2,410,459,099</td>
<td>$2,410,459,099</td>
<td>$15,161,964,438</td>
<td>$60,694,131,095</td>
<td>153</td>
</tr>
</tbody>
</table>

- 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.
Centralised Cryptocurrency Exchanges

- 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 [Bundi2019]
Risk of Misappropriation of Funds in Transit

The recent past has provided several examples of the loss of assets in the exchange process, either due to theft or exchanges shutting down [Bolici2016, Chohan2018].
Exclusion of Participants

- Centralised Exchanges choose who they do business with
- Exclusions can be introduced for various reasons
  - Anti-Money Laundering legislation
  - “Know Your Customer” laws
  - Geoblocking [Wilmoth2018]
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
Transactional Cryptocurrency Transfers

- Atomic swaps between different cryptocurrencies are hard
- The prevalent paradigm utilised to enable them are “Hashed Time-Locked Contracts” (HTLC)
- Most commercially relevant cryptocurrencies can be connected via HTLC [Griffith2019]
Downsides of Atomic Swaps

- No exchange rate discovery mechanisms
- Manual matching of the buy and sell sides necessary (i.e., how can interested traders find each other)
- Protocols that lock collateral can incur opportunity costs for the participants in cases where trades that were previously agreed upon fall through
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
Optional first step of the protocol

Participants can query a price-reporting facility $P$ deployed in $\gamma$ for the exchange rate between two given currencies ($a$, and $b$) at the current time.

This facility can be used by both parties of an exchange, e.g., both $User_i$ holding $a$ and a potential counterparty holding $b$, to determine a fair exchange rate.

The price reporting facility utilises verified trade data to publish a rolling benchmark rate.
Order-driven market; a market in which heterogeneous agents trade via a central order-matching mechanism.

Central order matching is provided by a matching engine deployed in $\gamma$.

To encode an order for exchanging a defined amount of one cryptocurrency for another, any account holder on $\gamma$ can post an order message using the matching engine (e.g. $A$).

The order posted using the matching engine includes the parameters relevant to the trade (units offered and units sought) and the technical parameters necessary for performing the trade via an HTLC.
II — Order Matching

- A will include a minimal performance rating \( t \) in the order
- This value is used as a threshold to exclude participants whose past performance was below expectations
- Buyers (e.g. \( B \)) can query the matching engine for orders that are of interest to them
- Should they qualify based on their performance rating, some aspects of the relevant orders are made available to them
- Once a buyer expresses their intention to engage in a particular trade—as referenced by its offer ID—this trade will no longer be visible to other potential buyers
The order book of the matching engine will be updated and the details of the trade (addresses and locking secret hash) will be made available to the buyer.

The buyer also needs to communicate their success address (where they seek to receive funds) to the seller.

The matching engine will be a witness to this transaction to allow for judging whether the transfer was executed as expected later on.

This message concludes the message flow necessary to establish a decentralised exchange.
A and B then engage in an exchange by following the respective HTLC protocol connecting blockchains $C_1$ and $C_2$. 
V — Execution Monitoring

- $\gamma$ offers key data in two dimensions to its users
  - a trustworthy exchange rate
  - a participant performance rating
- $\gamma$ observes transactions on $C_1$ and $C_2$
- A participant’s performance rating is computed using the total volume of their successfully fulfilled obligations in relation to the total volume of their failed trades
- Execution monitoring allows one to understand which of the two legs of a trade fell through, thus a positive score can be attributed to an honest counterparty of a failed trade
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.
- We identify economic trade-offs faced by users in both CEX and DEX.
- Taking the underlying conditions of an order-driven market into account, we show how a rolling benchmark rate of verifiable trades can establish a trustworthy exchange rate between cryptocurrencies.
Outlook

- Formal validation of the economics of the proposed protocol
- Decentralisation of more aspects of the system (i.e. credit scoring) through Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARK) with the ultimate goal of removing any central entity
Bibliography

WWW (CoinMarketCap2020)
CoinMarketCap
Top 100 Coins by Market Capitalization
2020
https://coinmarketcap.com/coins/

Misc (Nakamoto2009)
Nakamoto, S.
Bitcoin: A peer-to-peer electronic cash system
2008

TechReport (Gandal2014)
Gandal, N. & Halaburda, H.
Competition in the Cryptocurrency Market
NET Institute, NET Institute, 2014

TechReport (Wisniewska2016)
Wisniewska, A.
Altcoins
Institute of Economic Research, Institute of Economic Research, 2016

InBook (Franke2019)
Franke, J.; Härdle, W. K. & Hafner, C. M.
Financial Econometrics of Cryptocurrencies

InProceedings (Bolici2016)
Bolici, F. & Rosa, S. D.
Torre, T.; Braccini, A. M. & Spinelli, R. (Eds.)
Mt.Gox Is Dead, Long Live Bitcoin!

Article (Chohan2018)
Chohan, U.
The Problems of Cryptocurrency Thefts and Exchange Shutdowns
SSRN Electronic Journal, Elsevier BV, 2018

WWW (Harding2019)
Harding, R.
Bitpoint exchange says hackers stole $32m in cryptocurrency
2019
https://www.ft.com/content/c23930d4-a474-11e9-974c-ad1c6ab5efd1
WWW (Popper2016)
Popper, N.
Mt. Gox Creditors Seek Trillions Where There Are Only Millions
2016
https://www.nytimes.com/2016/05/26/business/dealbook/mt-gox-creditors-seek-trillions-where-there-are-only-millions.html

WWW (Wilmoth2018)
Wilmoth, J.
Decentralized Ethereum Exchange IDEX Waves Goodbye to New York Traders
2018

WWW (Griffith2019)
Griffith, T.
Atomic Swap Readiness
2019
https://swapready.net/

InProceedings (Lausen2019)
Lausen, J.
Regulating Initial Coin Offerings? A Taxonomy of Crypto-Assets
Proceedings of the 27th European Conference on Information Systems (ECIS), 2019
Assorted color shape and denomination
coin lot
Photo by Benjamin Lambert on Unsplash
https://unsplash.com/photos/KxdO8eLL5_c