QUANTA

DESCENTRALIZED
EXCHANGE

WHITE PAPER

Lightning fast decentralized cryptocurrency exchange.

Quanta (noun, plural for quantum)

Any of the very small increments or parcels

into which many forms of energy are subdivided.

Introduction

Cryptocurrencies has exploded in the past few years, reaching its peak over $700 Billion dollars in valuation. Coupled with its growth are alt coins, which are intended to solve many other problems such as security, privacy, scalability, cost, or specific domains such as IoT, business, mobile, etc. As of this writing, Bitcoin makes up only 33% of a total $585 Bil market cap, wherein the rest are made up of hundreds of other alt coin cryptocurrencies. (1) There are dozens more ICO every month. It is clear that cryptocurrency has democratized investment, and more and more startups have chosen to raise money for their idea through cryptocurrency. We believe in the center of this new world economy, a cryptocurrency exchange will play a critical role.

Cryptocurrency exchange currently is dominated by legacy companies such as Bitfinex, Bittrex, Poloniex, GDAX, and Binance. Though security has gotten a lot better in the days of Mt Gox, it is not without its imperfection. Hacking incidents, whether it's from internal and external, are a constant threat. Just to name a few recent hacks, in 2016, $72m were stolen from Bitfinex, and in

2018, $400m were stolen from CoinCheck [7]. The inherent flaw, as many have observed is that traditional cryptocurrencies exchange are centralized, which are managed by transactional databases. Centralized databases are inherently weak, in that, if single person have access to it, can re-write the any user, trade, and balance records. In other words, records are mutable which makes auditing a challenging problem. Recently, decentralized exchange has been on the rise such as Waves, and 0x. The security problems go away in decentralized exchange (DEX), however most of them limits to trading its own tokens such as only ERC-20 tokens and have its own performance limitations. For this reason, many users still prefer centralized exchange for more cryptocurrency choices. We intend to introduce a solution that is both DEX, with all the security benefits, and still offer wide range of cryptocurrency choices.

Reliability is often an issue with centralized exchange. During heavy trading time, some exchanges become inaccessible for a period of time, causing trading loss. In centralized exchange, the configuration tends be much more complex, and the recovery time such as a database failure requires a lot of time to manually recover. Decentralized exchange benefit from the ability to deploy a new node with minimum amount of configuration, and it begins to synchronize and contribute to the network immediately. There's no central authority which means there is no central point of failure. A single node failure does not impact the accessibility of the network. Our decentralized solution will address the much needed reliability issue with cryptocurrency exchange.

Related Work

Ethereum provided a flexible and scalable support for token based (ERC20), and the next logical idea is to provide a way to exchange across them. 0x proposed a smart contract on Ethereum to facilitate an exchange, and create ERC20 tokens for those tokens that are not already an ERC20 token [2]. Performance issues of operating on a blockchain both in transaction cost, and delays in execution has been well documented in "The cost of decentralization in 0x and Etherdelta"[3]. A new approach has been proposed by Neon exchange [4], and 0x, to decrease cost, and delays by introducing a relay node to aggregate orders in an off-chain, and allow takers to pick out a matching order, and execute on the smart contract. Stellar provides an token system similar that of Ethereum, and an on-chain decentralized exchange with significant faster block time of 3s, compared to 15s on Ethereum [8]. However, Stellar on-chain limits itself at a 3s submit

order/cancel order/fill which can be limited for real-world trading. Trading data on Ethereum and Stellar are also exposed which may give an asymmetrical advantage.

Quanta Blockchain

In a decentralized cryptocurrency platform, user manage their own public/private keys, which are used to sign transactions such as trades, withdrawal, and etc. As a decentralized exchange (DEX), we would not retain any of this information, such that not even we can make or modify trades, withdrawal on your behalf. Trades are executed on a decentralized network, and agreed by consensus at a set quorum, and written into an immutable blockchain. Past trades can not be altered by any entity, thus ensuring the integrity of your trades, and balance for all the coins you store on our system.

Scalability, performance, security, and flexibility are the most important attributes of a decentralized exchange. We explored many major blockchain technologies and settled on forking Stellar as our base code. We have added significant features to the platform to facilitate lightning fast trade operations.

Below shows the important attributes of the Quanta blockchain:

1. **Distributed**
   All transactions, and trading data are recorded on a blockchain. Blockchain is synchronized across network, and globally distributed around the world.

2. **Token Model**
   The blockchain maintain the history of all your coin balances as a token model.

3. **Consensus**
   All trading decisions will be individually on each node, and recorded by consensus. As such, security can be assured even if there are few bad actors in the network. [8]

4. **Immutability**

   Like blockchain, once an order, or a trade has been recorded, it can never be changed. This assures your trading balance is correct at all times.

5. **Low Latency**

   Our network is based on Byzantine consensus (as opposed to PoW), and guaranteed to scale at low latency. Since our network is globally distributed, our API servers will transmit your trades to the closest server by proximity & latency

6. **Anonymity Features**

   Anonymous trading history is a must for an industry-grade platform.

7. **Scalability**

   The exchange scales up with more nodes added to the network.

High Performance Matching Engine

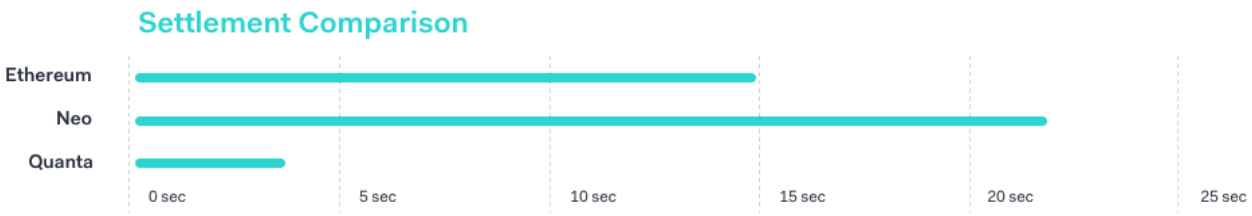
We implement an on-chain FIFO matching engine in C++, capable of handling 1M+ trade operations per pair. Designated Quanta Node is responsible for running an order book & matching engine for a specific pair. Other designated nodes are responsible for running replication node which provides redundancy, and safety for the order book.

Quanta blockchain maintains security end-to-end is to encapsulate the original matching trades, and the user's ed25519 signature. The buyer, the seller, and the exchange signatures are verified on the blockchain before the transactions can commit into the ledger.

Settlement Comparison

Settlement is referred to the time it takes write to ledger and reach consensus, also known as a block confirmation. For on-chain matching, the settlement time would be the time it takes to make one trade request, including modify and cancel request. Typical decentralized exchange built on Ethereum network suffer from a 15 sec block time. It is becoming more popular to

process trades on off-chain matching, the settlement time is still the greatest common denominator. We opted to use a modified fork of Stellar, which achieves 3 second block time. Our modification includes support for a new transaction to validate buy, seller, and matching engine ed25519 signature, record the trade on the blockchain.

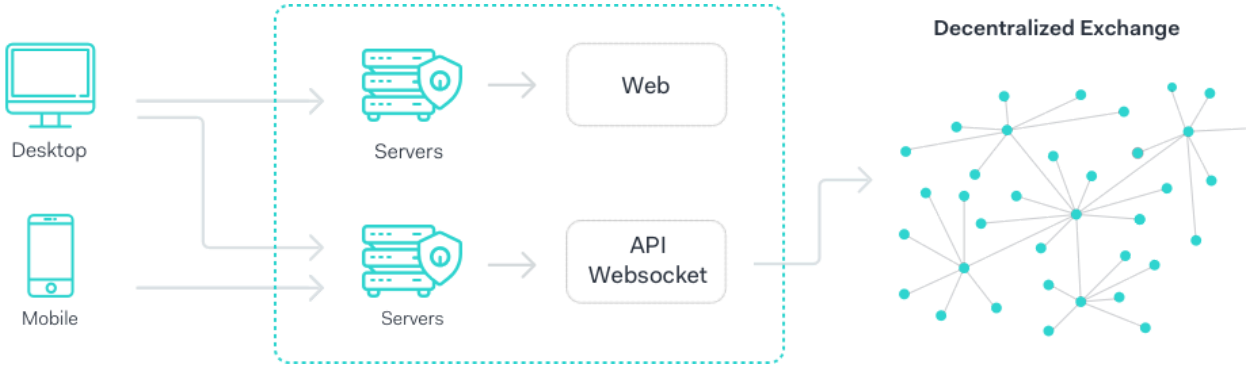


Funding Model

All trade-able assets are represented as a token on the Quanta Blockchain. An account will have pre-generated receiving addresses where the user will send their coins. The exchange trust wallet acts as a Trust which holds on the money, then issue the credit onto the Quanta blockchain. When the Quanta tokens are deposited back to the exchange, signed by the user, containing the memo of the receiving external account, the exchange trust wallet will transmit the money back.

Components

The frontend client is built on React and Quanta JS client. The server component systems are written in Play/Scala [5]. The WS server is powered by Akka [6], a concurrent distributed framework, capable of handling massive amount of connections. The exchange and blockchain are written in C++.



User Interface

Community Driven

We intend to build a community driven decentralized exchange, and eventually achieve full autonomy. We will establish Quanta Foundation, which will be a non-profit organization with the goal to nurture, and promote the decentralize exchange. While limited in resources, we will be

launching a beta under a private blockchain for simplicity and security. Following the ICO, we will work toward making public blockchain, allowing anyone to participate in the network, and strengthen the network. Those who run the network will be incentivized.

Network Operator

Earn % of trading fee based on the volume & the latency of trades executed on their server.

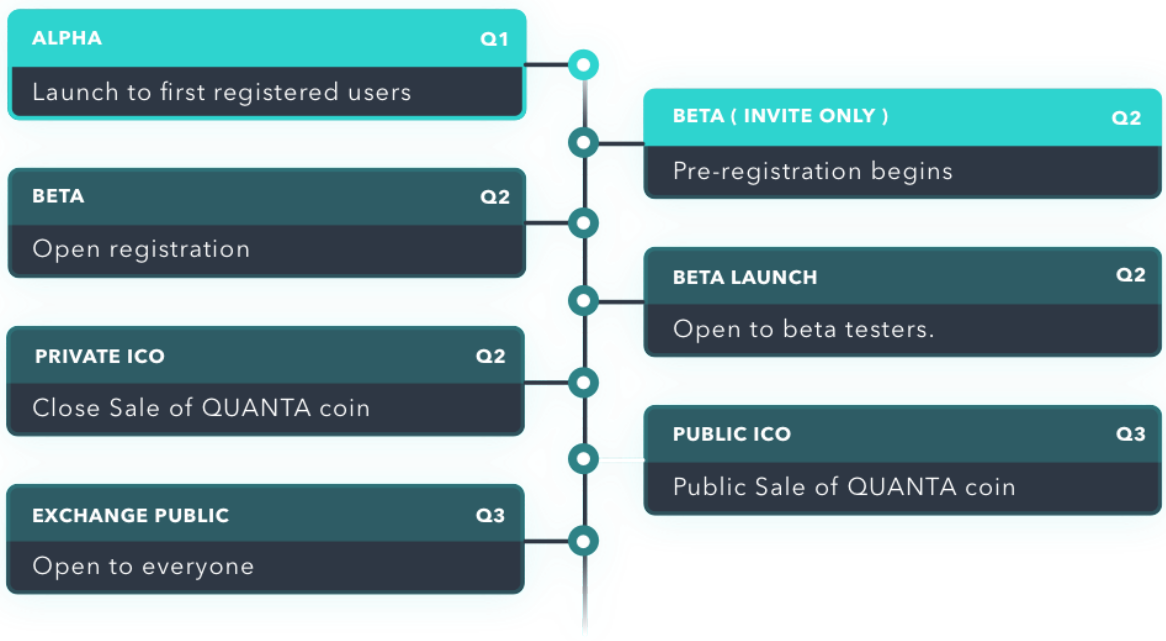
Voters

Listing and delisting will be driven by the community voting process.

Coin holders

Trading fees are distributed back to the network. Fees will accumulate to a minimum threshold in a holding account, and re-distributed at approximately 12-24 hrs interval.

ROADMAP



TECHNOLOGY

We have implemented a fork of Stellar as described in this paper, and will release these publicly in Q3 2018 before our ICO. We have also begun work on prototypes for the trading interface and matching engine. We strongly believe in a transparent development process where possible, and will be open sourcing much of our early work to benefit the Quanta community. See our Github account for updates and more information: https://github.com/quantadex.

Formation

We will establish the Quanta Foundation in Singapore. We are currently working with a law firm in Singapore to ensure full compliance.

QUANTA Coin (QNT)

We will issue our own coin called Quanta Coin (QNT). There will be a strict total of 200M QNT tokens that ever will be created.

- Use it to pay for fees
- Holding it reduces the fees
- We incentivize for signing up.
- We incentivize for referrals
- We incentivize for marketing our platform

Allocation

Founding Team	40,000,000	20%
Advisors & Investors	10,000,000	5%
QUANTA Foundation	50,000,000	25%
ICO	100,000,000	50%

All vesting period for founding, advisors, and investors extend for 4 years, with 1 year cliff period.

Funds Usage

- **55%** of the funds will be used to build the QUANTA platform and perform upgrades to the system, which includes team recruiting, training, and the development budget.

- **25%** will be used for QUANTA branding, marketing and legal, including continuous promotion and education of QUANTA and blockchain innovations in industry mediums. A sufficient budget for various advertisement activities, to help QUANTA become popular among investors, and to attract active users to the platform.

- **20%** will be kept in reserve to cope with any emergency or unexpected situation that might come up.

References

1. **Coinmarketcap**
   https://coinmarketcap.com/charts/#dominance-percentage

2. **0x whitepaper**
   https://0xproject.com/pdfs/0x_white_paper.pdf

3. **The Cost of Decentralization in 0x and EtherDelta**
   http://hackingdistributed.com/2017/08/13/cost-of-decent/

4. **Neon Exchange White Paper**
   neonexchange.org/pdfs/whitepaper_v1.1.pdf

5. **Play Framework**
   https://www.playframework.com/

6. **Akka**
   https://akka.io

7. **Coincheck confirms Crypto hack...**
   https://www.coindesk.com/coincheck-confirms-crypto-hack-loss-larger-than-mt-gox/

8. **Stellar Consensus Protocol**
   https://www.stellar.org/papers/stellar-consensus-protocol.pdf

Follow us on

- **TWITTER >** https://twitter.com/QuantaDex
- **LINKEDIN >** https://www.linkedin.com/company/quantadex
- **FACEBOOK PAGE >** https://www.facebook.com/quantadex
- **FACEBOOK GROUP >** https://www.facebook.com/groups/780414542153157/
- **MEDIUM >** https://medium.com/@quantadex
- **CRUNCHBASE >** https://www.crunchbase.com/organization/quanta
- **ANGELLIST >** https://angel.co/quanta-2
- **TELEGRAM >** https://t.me/QuantaDex