Version published on June, 18th 2023. This white paper is the basis for the finja.finance project.

Fully decentralized fiat to crypto exchange with PoS arbitration

Introduction

The rise of cryptocurrencies has led to the creation of numerous centralized exchanges. While these exchanges have provided a platform for users to trade cryptocurrencies, they have faced several problems. The most significant issue is the centralized nature of these exchanges, which requires users to trust their funds to a third party. Additionally, these exchanges allow users to exchange fiat to crypto directly through traditional payment/banking systems, which incurs fees and regulatory restrictions.

P2P exchanges as a version of decentralized exchanges appeared as a response to regulatory complexities and high fees. These exchanges evolved from a more centralized view and still use some centralized solutions, i.e. client registration in a central database (allows to block clients, potential exposure of personal data), arbitration done by employees of the exchange, exchange owned by central authority.

The solution proposed in this whitepaper is a fully decentralized exchange that allows for fiat to crypto transactions, supported by Proof of Stake arbitration. Third-party arbiters could step in to resolve conflicts between buyers and sellers by staking their tokens.

Solution overview

Problem definition

Centralized traditional exchanges are not designed for a new financial system that crypto is promising. Specifically:

1. Customers have to entrust their funds to the crypto exchanges. Furthermore, there have been several well-known bankruptcies connected either with poor management or misuse of customers' funds.
2. Customers have to go through traditional payments/banking systems to ramp up on crypto, which means they have to pay fees and abide by traditional restrictions and regulations that now try to discourage crypto use in many countries.
3. Some products in centralized crypto exchanges are being banned in certain jurisdictions (e.g. staking).

Solution proposed

A fully decentralized exchange that allows for fiat-to-crypto transactions, supported by Proof of Stake validation.

Principled mechanism of the solution:

1. The fiat-to-crypto exchange is essentially a P2P transaction where one customer is a buyer and another is a seller of crypto.
2. Crypto transfer will go through an escrow smart contract: the buyer deposits crypto to the smart contract and can't withdraw it. The seller can withdraw it when the buyer confirms the receipt of payment for crypto in fiat currency.
3. The seller sends fiat payment by any P2P method available in the traditional finance world, e.g. PayPal, Venmo, Alipay, card2card transaction.
4. Third-party arbiters can step in if there is a conflict between the buyer and the seller (i.e., the seller claims that they sent the funds, but the buyer claims that they didn't receive those). Arbiters are the holders of tokens issued by the exchange.
5. Resolution of the conflict is done by arbiters staking their tokens against supporting either the buyer's or seller's position. Buyers and sellers are allowed to post evidence of the transaction or absence of such to a forum where arbiters can study the evidence, ask questions, and make their decision. If the arbiters staked their tokens to support the side that loses arbitration, their tokens are transferred to those arbiters that supported the winner (proportionally to the staked amount of the winning arbiters). Thus, all arbiters are encouraged to support the side that has more chances to win (due to better evidence presented).
6. A small commission from successful transactions is also distributed among the arbiters, proportionally to their token holdings, to encourage buying and holding the token.
7. All parameters of the system (share of votes required to win, commission, penalty) can be decided by token holders in Governance protocol.
8. In order to prove the transaction in some of the cases, the seller and buyer can be asked to verify their identity, e.g. via Persona or Parallel Markets that attach NFTs to their wallet. NFTs that verify persona might be required for large transactions as well.
9. Buyers and sellers can start building their 'exchange credit score', e.g. by using NFTs. This will improve their trustworthiness long-term and can thus improve financial rewards for them through better exchange rates and higher liquidity.

Potential risks and ways to mitigate:

1. Not enough Arbiters in the beginning. This issue is solved by granting a share of tokens among first users of the protocol and its developers. Developers are encouraged to participate in voting to support the success of their protocol. Other users will see the 'missed rewards' and will eventually participate. In later stages, tokens will be distributed by selling these to investors who can value tokens based on volumes of the exchange.
2. Arbiters lose their interest if there are low volumes being disputed. This can be solved by balancing the commission and penalty components of the rewards system.

3. Arbiters are not willing to participate in the cases, where there are unclear outcomes and thus stalemate is reached (e.g. 50/50 split of votes when 2/3rd of votes are required in order for one party to win). This is solved by the version of ‘inactivity leak’ - the minority of Arbiters that already participated in the decision that didn’t reach consensus are penalized by taking a small part of their staked tokens and thus reducing their share of the votes until the consensus is eventually reached (this feature to be implemented in later versions of the protocol).
4. Arbiters can trade inside information or otherwise collude with the Seller or Buyer. This is solved by random selection of those Arbiters that can participate in the validation and thus Arbiters won’t know if they will be selected. The more the network grows, the smaller percentage of Arbiters will be selected. In the beginning of the network's existence, the tokens will be held mainly by protocol developers thus minimizing the possibility for colluders to win (this feature to be implemented in later versions of the protocol).

Expected outcomes

The proposed solution should result in a platform with the following characteristics:

- **Web3 Native.** No back-end, no databases, powered solely by smart contracts.
- **No Authority.** Fully decentralized fiat-crypto exchange, without any central authority that can control or block transactions.
- **Anonymous.** No personal data, emails, or phone numbers required.
- **Permissionless.** No registration or approval needed.
- **Immutable.** Non-upgradeable and unchangeable contracts, ensuring reliable use and predictable outcome.
- **Community-Governed.** PoS mechanism for voting and decentralized governance.
- **Game-theoretic incentives.** All parties have short-term and long-term incentives to behave ‘well’; collusion of parties to abuse the system is highly unlikely.

Novelty of the solution:

- The first-ever fully decentralized fiat-crypto exchange: there is no central authority, all disputes are decided in a decentralized way by the parties that are interested in the short-term (through staking) and long-term (through commission income) health of the platform.
- Buyers and sellers, particularly those with significant influence, are also incentivized to make good deals through their credit score, which leads to better exchange rates or more demand overall.
- The crypto segment of the exchange operates independently of traditional currency regulations, given that it's not owned by any entity and doesn't operate within a specific jurisdiction. Its governance is dictated by a smart contract that exists on the blockchain, which effectively separates crypto transactions from fiat transfers.
- Conversely, fiat transactions adhere strictly to regulations within their respective jurisdictions. These transactions are processed by established financial institutions or

banks, entities obligated to comply with all anti-money laundering, tax evasion, and other regulatory measures. This dual approach ensures that while the crypto exchange is innovatively autonomous, the handling of fiat currency remains fully compliant with prevailing laws.

Conclusion

In an era marked by the rapid adoption and evolution of cryptocurrency, the proposed solution responds directly to the challenges of traditional centralized exchanges. By offering a fully decentralized fiat-crypto exchange, this solution stands out as an innovative approach to address the trust and security issues inherent in centralized exchanges. By leveraging blockchain technology and Proof of Stake (PoS) arbitration, we strive to create an environment that promotes anonymity, incentivizes good behavior, and ensures the trustworthiness of transactions.

Moving beyond the limitations of centralized regulation, our solution taps into the strength of community-governance. This approach allows the network to grow organically, built on the faith of its participants. The solution offers an unparalleled level of financial freedom, thus contributing to the democratization of the financial system that cryptocurrencies promise. By integrating mechanisms like smart contracts, P2P payments, and novel arbitration, the platform brings an important contribution to the field of decentralized finance.

Appendices

Examples of financial incentives for all parties

Commission Distribution for Arbiters (long-term incentive)

- Let's assume that the exchange charges a 0.5% commission on successful transactions.
- If a transaction is worth $10,000, the commission earned by the exchange would be $50.
- Let's say there are 100 Arbiters who hold a total of 10,000 tokens issued by the exchange.
- The commission earned would be distributed among the Arbiters in proportion to their token holdings. So, if an Arbiter holds 100 tokens, they would receive $0.50 as commission for that transaction.
- The commission distribution formula can be expressed as follows:
- Commission earned by exchange * (Arbiter's token holdings / Total token holdings) = Commission earned by Arbiter

Staking for Arbiters (short-term incentive):

- Arbiters can earn additional rewards by staking their tokens to support a particular side in case of a dispute.
- Let's say a pool of Arbiters stakes 800 tokens to support the Seller's position in a dispute and another pool of Arbiters stakes 200 tokens to support the Buyer's position.
- By the rules of the network it's designed that 75% of votes are required to prove one's position. And a 10% penalty is applied to the stakers that supported the losing position.
- In this case, the Seller is winning a position, since 80% of votes support his position.
- Thus, the Arbiters who supported the Buyer have to be penalized by 10% of their stakes (20 tokens), which are distributed among Arbiters who supported the Seller's position.
- The staking reward formula can be expressed as follows:
  - For those who supported the winning position: Staked tokens by Arbiter * Share of the Arbiters tokens in the pool that supported the winner * The penalty amount = Staking reward earned by Arbiter
  - For those who supported the losing position: Staked tokens by Arbiter * Penalty percentage = Penalty incurred by the Arbiter
- In the example above, if the one individual Arbiter supported the Seller with 100 tokens, such Arbiter should receive:
  - 100 tokens / 800 tokens * 20 tokens = 2.5 tokens

Better Exchange Rate for a Seller or Buyer (long-term incentive):

- Let's say a Seller wants to exchange 1 Bitcoin for fiat currency and the current market rate is $20,000 per Bitcoin.
- If the Seller has a high exchange credit score, they might be able to get a better exchange rate, say $20,200 per Bitcoin, which would result in $200 additional profit for the Seller.
- Similarly, a Buyer with a high exchange credit score might be able to get a better exchange rate when buying crypto, resulting in savings on the purchase.
- The exchange rate formula can be expressed as follows:
- Market exchange rate +/- Adjustment based on exchange credit score = Final exchange rate.

Solution architecture.

Proposed decentralized exchange will be implemented in 2 layers: front-end and smart contracts. The platform can work without any traditional back end to avoid any centralization.

Front-end functionality:

- Interface for users to deal with smart contracts
- Connection with EVM and wallets through libraries (web3.js, ethers.js) and nodes (Alchemy, Infura)

Smart contracts (core of the solution that handles of the important operations):

- Escrow and deals management smart contract (s) - This contract or the group of contracts will “register” users and store data on the deals they propose and payment instruments they would like to use in mappings, arrays and structs. The contracts will also manage basic deal flow like: registering proposals to buy, saving completed deals details. This contract will also hold the crypto deposited by the seller until the seller confirms the receipt of payment in fiat currency. Once the confirmation is made, the contract will release the crypto to the seller.
- ERC20 token smart contract - This contract will be used to issue tokens of the exchange that later can be used on Governance and Arbitration smart contracts
- Governance protocol smart contract - This contract will allow token holders to decide on the parameters of the system, such as the share of votes required to win, commission, and penalty.
- Arbitration smart contract - This contract will handle the resolution of conflicts between buyers and sellers. It will allow arbiters to stake their tokens and support either the buyer's or seller's position. The contract will also distribute commissions to the arbiters, proportionally to their token holdings.

External solutions:

- Identity verification smart contract via solutions like Persona or Parallel Markets that attach NFTs to the wallets of users. This might be encouraged or required for larger transactions and certain arbitrations.
- Infura/Alchemy nodes to interact with smart contracts.
- Wallet connection solution like WalletConnect to be able to connect to multiple wallets on desktop and mobile platforms.
- DAO governance site to do voting and Arbitrage (e.g. snapshot.org)

Back end

- No back end is planned to be used – fully decentralized architecture that allows anyone to write/copy front-end and continue using the protocol

Business rationale

- While there are several decentralized exchanges that allow for fiat-to-crypto transactions, these solutions have low levels of usage. E.g, at the time of wirting this White Paper, HodlHodl have 50k+ deals closed over 7 years, LocalCoinSwap has $2 mln equivalent in volume per day. These volumes suggest that even if the momentum is shifting from CEX to DEX, there is still no one big winner in the space.
- Current decentralized exchanges were built several years ago, before DeFi space and tools matured to the current level, thus they still use traditional solutions that are currently not appropriate in DeFi (e.g. email registration, central bases to store personal

data, central arbiters). While these solutions might not be critical, they still can be viewed as inadequate to the needs of DeFi users.

- Some of the current solutions are using either expensive in terms of transaction fees coins (like BTC in HodlHodl) or multiple coins which fragments the supply and demand (like LocalCoinswap). We propose to use one coin on a Layer2 chain like Polygon or Optimism. The coins can be easily exchanged and swapped by using existing liquid bridges and DeFi exchanges.
- The proposed solution is extremely low cost and durable to any regulatory actions. There are no servers, no personal data stored (and thus no breaches) and no company required to run this.