Cosmos Distributed Exchange

A major use-case for Cosmos is the Cosmos Distributed Exchange.

NOTE: This document assumes an understanding of the Cosmos hub and zone architecture. For clarity we refer to tokens like "bitcoin" and "ether", but in reality these tokens are referring not to actual bitcoins and ethers themselves, but 2-way pegged versions of these tokens, as issued by a Bitcoin peg or an Ethereum peg zone.

Distributed vs Decentralized

We make a distinction between a distributed exchange and a decentralized exchange.

A decentralized exchange refers to exchanges based on atom-cross-chain transactions, or similar techniques where the exchange of two tokens between two parties are each settled on their respective ledgers. For example, dogecoins on the Dogecoin blockchain, and litecoins on the Litecoin blockchain, as matched by some third-party off-chain trade-matching service. Another technique may rely on lightning networks, or linked payment channels. In general, decentralized exchanges require both parties to a trade to be online.

In contrast, a distributed exchange refers to exchanges based on distributed-ledger technology (aka blockchains). The orders of traders are signed and committed to a blockchain, where validators (or in the case of PoW chains, miners) agree on the order of order transactions and execute orders on the trader's behalf. In a distributed exchange, a trader can submit a limit order and go offline; the blockchain can execute these orders on behalf of the trader even if the trader's computer/client goes offline.

Distributed Custody

The biggest problem with centralized exchanges is that they take custody of the traders' funds. A long history of centralized cryptocurrency exchange hacks has shown that this is unacceptably insecure. And yet, traders continue to use centralized exchanges because they don't have a better option -- the convenience, speed, and volume of centralized exchanges has thus far been hard to beat.

This document is a blueprint for a more secure system that has the main advantages of a centralized exchange without the drawbacks of centralized (insecure) custody of trader funds.

The Naive Solution

Given the Cosmos architecture, a simple solution to the exchange problem can be created as follows: create a distributed exchange zone (the Cosmos Dex, or Dex for short) that attaches to the Cosmos Hub and let it accept any type of token from the Cosmos Hub. From the perspective of the Dex zone, the Hub zone is the "parent" custodian of funds, and the Hub is delegating limited control to the Dex such that the Dex can process trade orders however it wants.

To maximize security and Byzantine fault-tolerance, the Dex can share the same validator set as the Hub. How the Hub and Dex coordinate validator set changes and the details of the PoS system is beyond the scope of this document.

Problems with the Naive Solution

The problem with this solution is twofold. First, even if the DEX were powered by Tendermint (or any fork-accountable BFT middleware), a global distributed validator set will necessarily take some time to commit blocks. It is known that any BFT algorithm in the partially-synchronous or asynchronous context that can tolerate up to 1/3 of Byzantine voting power requires at least 2 rounds of signature communication to come to consensus (e.g. commit a block to finality). When the ledger's validators are distributed globally, and when there are many validators (both desirable qualities for a secure distributed exchange), the block-times will be significant, on the order of 1 second due to the limited speed of light.

What traders want, on the other hand, is "instant" trade matching akin to what centralized exchanges are already providing -- orders confirmed or matched on the order of milliseconds.

The other problem is that a distributed ledger allows for validators to "cheat" by determining the order of transactions. In the case of Tendermint, each round-robin block proposer has a chance to order transactions however it wishes within each proposed block. Although each validator may get a "fair" chance to "cheat", it doesn't change the fact that every validator gets to cheat.

Even "leaderless" consensus systems suffer from various forms of cheating. For some systems, such as Swirld's hash-graph system, the one who has more control over the network, or one who has more connections to peers, has greater power to determine the order of transactions. TODO: also mention other attemps.

Both problems are fundamental to the nature of distributed ledgers -- a global distributed ledger cannot make any final decisions (about the order of transactions) on the order of milliseconds.

The Hybrid Solution

Rather than letting round-robin block proposers, control over the network, or any other metric/heuristic determine the order of transactions, we let centralized exchanges (from here-on referred to as CEX's) be responsible for determining the order of transactions within their "subledger".

For a trader to trade on the DEX, first the trader must deposit funds to the CEX's subledger by submitting a signed transaction onto the DEX. Once the transaction is committed by the DEX, the trader has funds in "semi-custody" by the CEX.

Then, the trader can submit trade orders to the CEX. Orders submitted to the CEX are signed by the trader. The CEX responds with a receipt which is a signed message which includes the order, the current time T, an incrementing sequence number S, and hash H of the previous order (from potentially another trader with sequence number S-1).

All orders signed by the CEX should eventually (e.g. within 1 minute) get committed onto the underlying DEX ledger. The orders must be in incrementing sequence order, and all the hashes must match the previous order's hash.

Users can also withdraw funds from the CEX's subledger onto the the base DEX or another CEX's subledger by signing a withdrawal transaction and submitting it to the CEX for sequencing and signing, just like any order transaction. As we'll see in the next section, the CEX's cooperation is not necessary to withdraw funds from the subledger.

Security

We assume that both traders and CEX's have some collateral deposited on the DEX ledger. When evidence of malfeasance is detected (e.g. the CEX signing two conflicting orders with the same sequence number, or the CEX not committing transactions in a timely manner onto the DEX), these actors can be punished by slashing the collateral.

All validators of the DEX ledger must validate the orders of all subledgers. If a CEX is found to have submitted an invalid order (e.g. signed the market order of a trader even though the trader doesn't have any funds in the subledger), then the CEX can be punished as described above. In addition, subledger transactions that do not increment the subledger's last sequence number by 1 are considered invalid transactions.

If a trader is not satisfied with the performance or service of one CEX (e.g. it feels that it is not receiving a receipt in a timely manner), it can move its funds over to the "semi-custody" of another CEX, all via transactions that are posted onto the underlying DEX ledger. These "exit" transactions do not need to be signed by the corresponding CEX. Exit transactions do not take effect immediately, but rather take effect after some time limit (e.g. 10 minutes). This locktime prevents traders from withdrawing funds away from a CEX's subledger when in fact the trader's funds had been matched by some other order signed by the CEX with someone else. If after a trader submits an exit transaction, the CEX signs and submits a conflicting order by the same trader (e.g. a market/limit order) in timely fashion (e.g. within 1 minute), then the trader is considered to be malicious, and could be punished.

Most importantly, no CEX has custody of any trader's funds. No funds may be withdrawn (moved out of a subledger) or traded without the express permission of the trader (as evidenced by the trader's signature). The worst a CEX could do is match an order, which the trader wanted to do anyways. Recall that all validators of the DEX validate all the transactions of all subledgers, enforcing the rules of the system.

We incentivize third-party pen testers to hack into the validators and publish their success as soon as possible, as described in the Cosmos whitepaper. Since the DEX is a distributed/mass-replicated BFT ledger, a single CEX validator getting hacked does not affect the security of the overall system.

Conclusion

The distributed exchange system described here allows centralized exchanges to match orders centrally while keeping the custody of funds in a distributed ledger -- a hybrid that expresses the best of both worlds. Centralized exchanges can compete with each other for market volume, and yet the funds are not held in central custody by anyone, and thus is significantly more secure than any existing centralized exchanges today.