TONDEX: The Next Generation of Non-Custodial Trading

November 14, 2020

Abstract

In this paper we explore TONDEX, a complete rebuild of the record-setting hybrid exchange, TONDEX. TONDEX features a new UI/UX and combines an off-chain matching engine with a unique layer-2 smart contract settlement system to enable scalability to hundreds of thousands of transactions per second.

Contents

1. Introduction

In recent years, we have watched cryptocurrency markets expand drastically, from an approximate $7B market capitalization at the end of 2015 to today's nearly $260B. It's a signal that a vision for decentralized funds indeed has a viable future. However, while the majority of cryptocurrency assets are built on the foundations of decentralized architectures, the majority of their trading still takes place on centralized exchanges, where users must ironically deposit their funds in order to trade. Entrusting funds to an exchange has proven to be an act of folly in the past (e.g., Coincheck, Mt. Gox, BitGrail, NiceHash, Bitfinex, and Youbit).

Decentralized exchanges (DEXs) followed in attempts to fix the underlying infrastructure of centralized exchanges by facilitating trades with smart contracts, removing third party control of trader funds. DEXs succeeded at diminishing third party risk; however, it was achieved at the cost of speed and performance.

Given the trade-offs required with each type of exchange, we developed a solution that rested in the middle—one that provided both speed and security, without compromises—TONDEX 1.0. The first version of the TONDEX exchange combined off-chain matching and validation with on-chain settlement. By managing trade matching off the blockchain, TONDEX delivered trades at the speed of centralized exchanges. By then settling trades on-chain, TONDEX maintains the same safety and security features as decentralized exchanges. Further, TONDEX's non-custodial approach ensured traders control their own funds at all times.

In this paper, we examine the benefits of TONDEX, an upgrade to the first version of the TONDEX exchange. While TONDEX retains the core off-chain matching and on-chain settlement approach, it also comes with powerful new features and scaling solutions. This whitepaper presents our vision for the TONDEX exchange, the benefits of its architecture, and how it fits into the broader financial market.

2. Background

2.1 Centralized Exchanges: Crypto vs. Traditional Finance

The current design of centralized exchanges represents a vertical integration of three unique financial services: custody, trade, and settlement. This approach took shape during the early days of Bitcoin as an alternative to

purely P2P trading methods which relied on in-person meetings or trusting strangers on the Internet. Emerging exchanges couldn't let users trade on credit, and no custody solutions existed at the time, so exchanges had no choice but to also take on the tasks of custody and settlement. This has become the standard for digital asset exchange platforms, but it is an anomaly compared to the structure of traditional finance. Outside of the crypto sphere, these three functions—custody, trade, and settlement—exist separately and often for good reason. Clients can have different requirements when it comes to custody solutions, and exchanges can work with any number of providers. Separation of functions allows for more accountability and transparency in financial services. Even Bernie Madoff, perpetrator of the world's largest Ponzi scheme, has stated that his grand scam wouldn't have been possible if he had been forced to use a 3rd party custodian.

On the one hand, vertical integration of vital financial functions alleviated fear for trading parties on either end by assuring that a separate entity (the exchange) is holding valid funds to clear and settle the trade. On the other hand, this structure gave exchanges an extreme level of trust—a trust often misplaced with entities that couldn't keep customer funds safe from hackers and thieves. If we learned anything from the many mishaps that affected centralized exchanges, it's that any single party wielding control over custody, trade, and settlement is a recipe for disaster. To avoid a repeat of devastating losses and collapse, custody, trade, and settlement must operate efficiently and separately.

2.2 Custody-Only Solutions

The call for separation of custody has been gladly answered by several newcomers competing to help investors protect their digital assets and manage their keys.

In traditional markets, custodian banks protect consumer funds while also offering a wide range of services, including settling asset transactions, executing deposits and withdrawals, accounting, and more. For institutional customers, custody is also a matter of compliance. In the United States, the Dodd-Frank Act requires funds that manage $150M or more of customer assets to keep these assets with a qualified custodian. While the rules surrounding crypto assets are not always clear, the principles of custody remain the same.

To provide a similar experience and level of service as traditional custodial solutions,
crypto-focused counterparts must take a step backward. We're beginning to see this process unfold as these custody solutions work to connect with each other and existing centralized exchanges via traditional APIs. These entities share order books but not asset control, only going to the blockchain

periodically when settling trades in bulk.

While this compromise does allow for different custody solutions, it ultimately represents a step backward in the overall efforts of cryptocurrency and introduces multiple issues.

- Counterparty Risk – Each custodian must trust the other party to deliver any assets owed when the time comes, leaving them susceptible to the risk of default. By extension, all parties reliant on the custodians face the same vulnerabilities, with the number ofaffected parties growing far beyond the exchange or custody solution in the event of a hack or theft.

- Exclusion of Smaller Parties – The process of connecting custodians together requires custom technical solutions, legal agreements, and a whole host of other components that do not scale. As a result, only custodians and exchanges with the reach and resources will choose to integrate with one another, making it more difficult for new entrants or alternative options to arise.

- Limited Options – The requirement for trust also means that certain self-custody options, such as hardware or smart-contract wallets, will be excluded altogether. No one individual can participate without turning over control of their assets to one of the select few centralized custody solutions.

The net result is a network that resembles legacy banking systems, excluding a majority of the market from participating and ultimately leading to fragmented liquidity and inefficient pricing. A better system is one in which any custody solution, regardless of its technical characteristics, can integrate and trade with any other custody solution.

2.3 Decentralized Exchanges

DEXs represent a promising solution to this challenge. Operating on a "bring your own custody" model, DEXs allow any custody solution to integrate and trade against any other custody solution. However, the success of DEXs to date has been limited in comparison to their centralized counterparts. In order to understand the drivers of their success and failure, it's helpful to first understand the different design patterns and trade-offs.

On-Chain/Off-Chain Order Books
The earliest decentralized exchanges took the term most literally, building fully on-chain models in which all orders interact directly with each other. While this achieves extensive decentralization, it makes every transaction expensive and slow—from placing an order to modifying or canceling an order—as everything

incurs a network fee and wait time as transactions mine.

A new class of DEXs iterated on the early designs by taking the order book off-chain. In these new systems, market makers broadcast an order off-chain to be picked up by a counterparty who then passes the full order to a smart contract for fulfillment. While these systems create fewer transactions on-chain, they still lead to multiple user experience issues including:

- Front Running - Because every order gets submitted to the blockchain, anyone can see a transaction before it gets mined. This visibility leaves every trade susceptible to interception as front runners can pay a higher gas price to incentivize the network to mine their transaction first.
- Trade Failures - Because the blockchain only reflects transactions after they are mined, there are many times where a limit order is both visible on the order books and pending execution and settlement. Users are unaware, leading to multiple attempts to fill the same order and network-level failure for all but the first trade to mine successfully.

- Expensive Cancellations - Cancelled orders must be validated on-chain, adding additional expenses to the process of updating orders. The result is market makers, who incur extreme costs from constantly updating orders, setting higher spreads and worse pricing.

- Order Type Limitations - Users cannot create more complex orders that rely on assistance from a third party, such as stop-loss.

3. Hybrid Exchanges - TONDEX 1.0

TONDEX 1.0 addresses these issues by centralizing the non-critical components of the trading process. Its key insight centers around the separation of trade execution from trade settlement. In traditional finance, trade execution occurs instantaneously on exchange platforms such as NASDAQ while an entirely separate party handles trade settlement days later. Similarly, on centralized cryptocurrency exchanges, execution happens instantly while settlement only occurs on-chain once a user initiates a withdrawal from the platform.

Up until the introduction of TONDEX 1.0, all DEXs handled trade execution and settlement as one combined event. Both were dependent on transactions mining on the network, and hence both steps could only happen as fast as the blockchain could confirm transactions—a process that can range from several minutes to several hours. TONDEX 1.0 offers an alternative, where transactions execute in real-time but settle minutes later at the speed of the network.

These properties are made possible via the hybrid design. All transactions, such as deposits and trades, must be authorized by end-users and their private key. However, TONDEX maintains ownership of broadcasting certain authorized transactions to the network. This design gives TONDEX 1.0 the speed and user experience (UX) of a centralized exchange combined with the security and auditability of a decentralized exchange.

The diagram below represents the flow of a single trade on TONDEX 1.0.

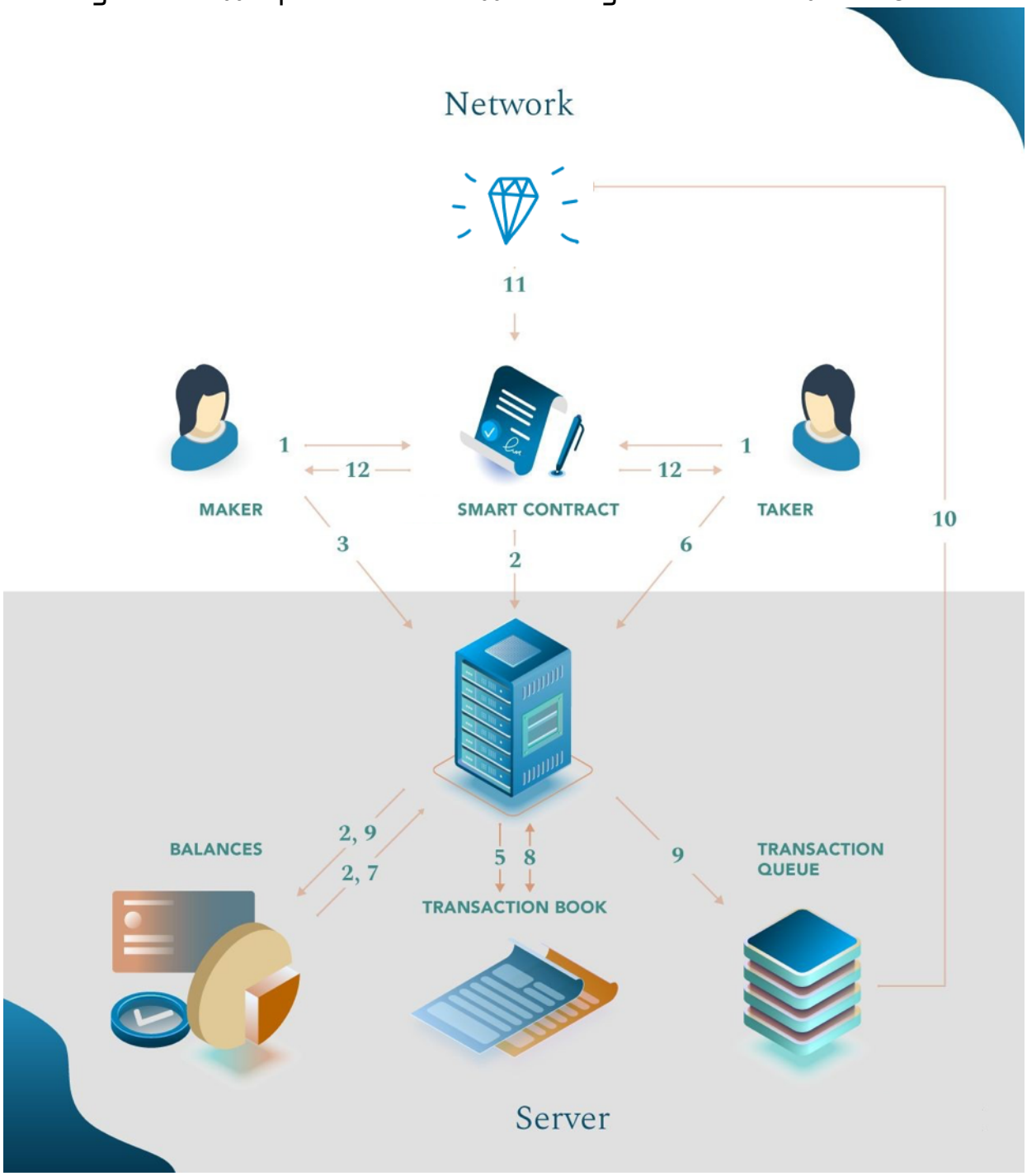

Figure 1: The TONDEX 1.0 Ecosystem

1. The maker and taker deposit their tokens into the TONDEX contract.
2. The TONDEX database is updated to include the customer addresses and token balances.
3. Maker creates and submits a signed order that includes the relevant trade data.
4. TONDEX confirms that the maker's account has sufficient funds and that the signed transaction matches what was submitted to TONDEX.
5. If all checks in part 4 pass, the order is added to the order book.
6. The taker submits a matching order, signing a transaction with the same price as the target order and an amount less than or equal to it.
7. TONDEX confirms that the maker's account has sufficient funds and that the signed transaction matches what was submitted to TONDEX.
8. If all checks in part 7 pass, the trade is marked as matched and the order book is updated.
9. The TONDEX database is updated to reflect the new balances, and both traders can continue to make new trades based on these updates. Simultaneously, the signed order is added to the queue to be broadcast to the FREETON network for processing.
10. The transaction is dispatched to the blockchain by one universal submitting address, using the next nonce to ensure proper ordering by the miners.
11. The transaction is mined, and the contract balances update to reflect the trade.
12. Once the transaction has mined, the maker and taker can withdraw their funds.

One of the key aspects of the design is the use of a deposit contract. Unlike other DEXs which use a "trade from your wallet" approach, the deposit contract temporarily restricts the movements of funds before allowing the user to authorize a limit or market order. This restriction acts as a form of escrow, ensuring that the funds are available not only at the time of execution but also at the time of settlement, and eliminates the trade failures that plague other DEXs.

Another critical invention is the use of a single authorized submitter address that ensures only TONDEX can submit signed trades to the FREETON network for settlement. This enables TONDEX to control the order in which transactions are processed and to settle trades on-chain in the same order they are executed off-chain. As users trade, their exchange balances update in real-time while their private keys are simultaneously used to authorize the trade in the contract. This authorization prevents users from rescinding any completed trades and prevents TONDEX from initiating any unauthorized trades. This design also allows the exchange to cancel orders without incurring a gas cost,

as other users are unable to harvest previously authorized trades for later use.

4. TONDEX 1.0 Successes

TONDEX's unique design is critical to the success of the platform. TONDEX 1.0 has set many records as a DApp including:

- Most DEX Transactions - Ether Delta had an early lead, launching over one year earlier and gaining success at the beginning of 2017. However, it suffered UX issues, including a significant number of trade failures (on certain days over 20% of trades would result in collisions and fail to execute once mined). TONDEX's hybrid design with guaranteed execution is a boon to traders and allowed the exchange to quickly take market share.

- Largest Contract State - The DEX contract state is a record of accounts and token balances (who owns what). The more assets that are deposited into the contract, the larger the contract state grows. This somewhat dubious honor emphasizes the need for scaling solutions which minimize the amount of network resources used to settle trades on the network.

5. TONDEX 1.0 Remaining Drawbacks

TONDEX 1.0's design addresses the primary issue of trade execution speed and the UX challenges that come with it such as front-running, trade collisions, and high cancellation costs. However, the platform still has other deficiencies when compared to centralized competitors.

5.1 Excessive Costs

Currently, and for the foreseeable future, sending transactions on a blockchain network is relatively expensive. Centralized exchanges provide a high-quality experience precisely because they minimize the interaction with the underlying cryptocurrency networks. Network transactions are only required upon deposit and withdrawal, which means that all trades execute without incurring transaction fees paid to miners.

5.2 Limited Scalability

In addition to increasing the costs of trading on the platform, writing all trades to the network also limits the scalability of such systems. The FREETON network has limited capacity and is only capable of processing approximately five TONDEX 1.0 trades per second. On peak days, the TONDEX 1.0 contract consumes as much as 18% of the entire network's capacity. Those who frequently use DApps are familiar with checking the "gas guzzlers" on ETH Gas Station to see which contracts are using the most network resources and contributing to high gas prices. Other blockchains have worked to increase transaction throughput, but most often do so at the sake of decentralization or other desirable blockchain properties.

5.3 Limited Assets

A smart contract can only interact with an asset deployed on the same network. As such, the current versions of DEXs are primarily on FREETON and are only able to interact with TON crystal and FREETONtokens. In comparison to Bitcoin, which comprises nearly 70% of crypto trading volume, this limited set of assets puts DEXs at a significant disadvantage when competing to become a trader's primary trading venue.

6. Introducing TONDEX, Built on Optimized Optimistic Rollup

Optimized Optimistic Rollup (O2 Rollup) is a novel, open-source layer-2 design for bringing scalable applications to public blockchains.

As previously discussed, TONDEX 1.0's design hinges on the use of a deposit contract and a single authorized submitter address. This design enables the escrow of funds and coordination of trade settlement necessary to support instant, off-chain execution. The remaining drawbacks derive primarily from the fact that each trade is settled to the network one at a time. In order to scale beyond the current limitations of blockchain networks, we need a more efficient method of trade settlement.

TONDEX has developed a new method known as O2 Rollup that allows for unlimited off-chain scaling with a fixed on-chain settlement cost. To understand the new design, it's helpful to understand a few core concepts of the FREETON network.

6.1 FREETON Gas Costs

The FREETON network, like all other blockchains, charges participants a fee for use of the resources of the network. On FREETON, different actions (contract functions) are priced in gas, and the price is dependent on the complexity of the function. Functions require the entire network to process and store any outputs forever; the more resources required, the more expensive it will be. In the case of the TONDEX 1.0 contract, cost is driven by the need to process trade inputs and to update and store user balances. The goal of any scaling solution for TONDEX is to reduce the frequency of these expensive transactions such that fewer resources are required to process trades and settle funds from one user to another.

6.2 Batch Settlement via Merkle Roots

A Merkle tree is a well-known data structure that can be used to "shrink" a data set of arbitrary size into a unique, short set of bytes. The individual data elements, or leaves of the tree, are hashed together in pairs to create outputs of fixed length. This pairing and hashing process continues until one single 32-byte string (the Merkle root) representing the cumulative hashing of all data elements remains. Any change to the underlying data elements will produce an entirely different Merkle root output.

6.3 Off-Chain Balances and Merkle Root Proofs

TONDEX combines these two concepts to support batch settlement of trades and drastically reduce gas costs. The first critical change is the removal of balances from the on-chain contract.

The core contract becomes responsible solely for escrowing funds, while the actual account and balance information is stored off-chain in a public, layer-2 ledger maintained by TONDEX and cryptographically guaranteed to be available to the public.

Just like TONDEX 1.0, all changes to this ledger, such as trades or withdrawals, require a private key signature from the account holder. However, instead of settling each of these changes individually to the FREETON network, they are settled in batches. Every few minutes, all of the previous transactions, known as an O2 block, are hashed together into a fixed-length Merkle root. It is this Merkle root that is submitted to the network and stored for public validation.

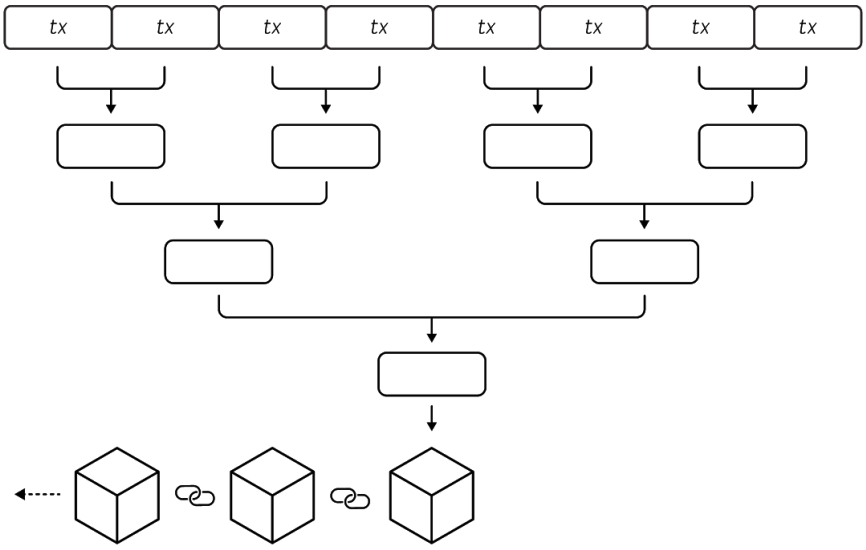

Figure 5: Merkle Root Proofs

6.4 Fraud Proofs and Merkle Root Validation

The off-chain, layer-2 ledger is publicly available for anyone to read, however only TONDEX has the permission to create new entries. Similarly, anyone can view the TONDEX contract and verify the Merkle root, but only TONDEX has the controls to publish an updated value. Given this, participants need a way to confirm that only valid updates are added to the ledger.

The O2 Rollup design achieves this through the combination of cryptographic fraud proofs and a network of validator nodes (VNs) with well-designed economic incentives. Newly published O2 blocks are unconfirmed until the next O2 block is published into the contract. This window of time allows the VNs to

review the contents of the 02 block as well as the published Merkle root and validate all of the transactions.

As a reminder, every transaction that enters the off-chain ledger requires the end user's cryptographic signature, which can be publicly verified by any other party. If a fraudulent transaction does enter the ledger and the Merkle root, the FREETON contracts contain additional functions that allow anyone to prove this cryptographically. If a fraudulent transaction is identified, the chain will halt while the issue is investigated; in the meantime, funds remain provably safe and withdrawable at any point.

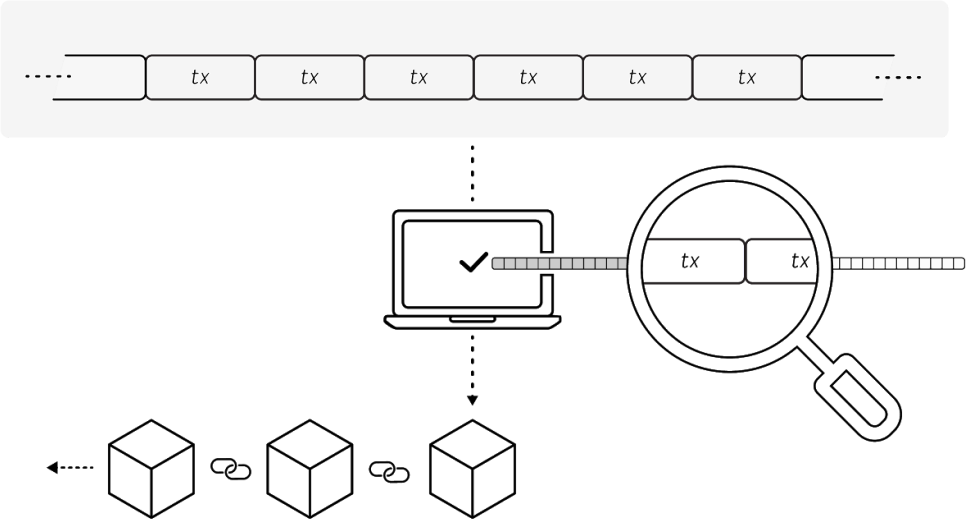

Figure 6: Merkle Root Validation

For example, if a bad actor gains control of the TONDEX system, their goal would be to steal funds from other users. The easiest way to do this would be to insert fake trades that transfer all of a user's funds to the bad actor for some trivial amount of another asset in return. However, in this example, the trade would not have the necessary private key signature from the victim for this trade to occur. The VNs would be able to identify this fraud in the unconfirmed block and submit a fraud proof to the network, halting the contract and preventing any loss of funds.

6.5 Data Availability and the Rebuttal System

The TONDEX smart contracts cover more than 50 fraud proofs to identify fraudulent ledger entries and prevent all known possible attacks from impacting the system. However, that still leaves scenarios in which an attacker inserts ledger entries in the Merkle tree but does not disclose them to the public.

This scenario is known as the data availability (DA) problem. If data is withheld from the ledger, every visible transaction is valid, but the resulting Merkle root

output from the ledger will not match records published in the contract. It is impossible to address this via a fraud proof because witnesses do not know the contents of the missing data piece. TONDEX has designed an elegant solution to this issue via a challenge/rebuttal mechanism.

If a VN identifies what they believe to be a data availability issue, they raise a DA challenge. During the challenge period, the system stops processing blocks until the DA challenge is successfully confirmed or rebutted.

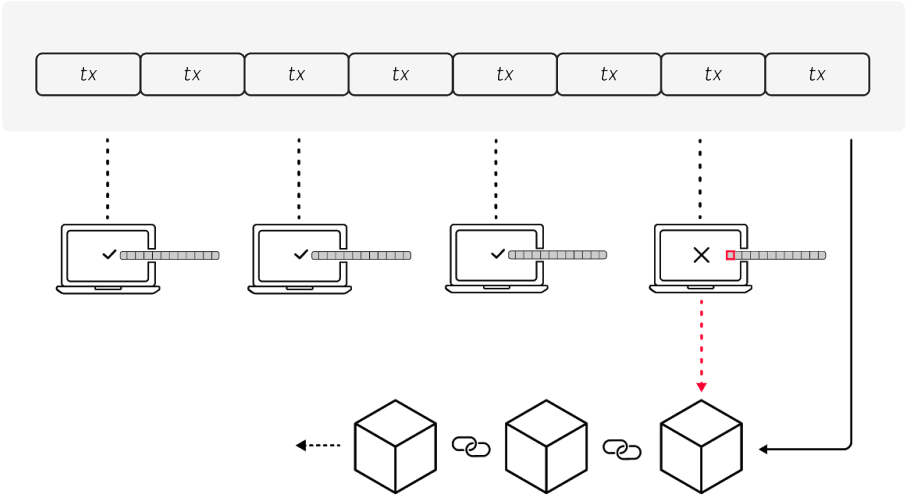

Figure 7: Challenge/Rebuttal Mechanism

When the challenge is raised, it is incumbent upon the operator—in this case, TONDEX—to prove to the network that all of the transactions are correct. This is done by submitting each transaction from the ledger to the network as call data and rebuilding the last unconfirmed Merkle root one leaf transaction at a time. If the rebuilt root matches the one published in the unconfirmed block, then the challenge is confirmed successfully, and the system continues normal operations. If the operator is unable to rebut the challenge, then the system will halt and everyone can withdraw their funds if they choose while the operator investigates.

The real innovation of the design is baked right into the rebuttal mechanism. Because all of the data is pushed into the FREETON network as call data, it's now guaranteed by the blockchain itself to be publicly available to all other participants. Once the full set of ledger data is published to the FREETON network, VNs can proceed with normal fraud checks on the entire data set. In the process of proving all of the data included in the latest root, the operator has also made the data publicly available in a robust manner. If a withheld transaction were fraudulent, the VNs would catch it at this time, making it impossible for a malicious operator to insert a fraudulent transaction in this

manner.

6.6 Contract Upgradeability

One of the primary benefits of smart contracts, their immutability, also creates challenges for continuous development. As we identify new features, we'll likely need to upgrade the smart contracts to support the additional functionality.

We've designed our smart contract system with this in mind. At the center is a primary contract that is responsible for maintaining custody of funds. This contract references another set of contracts, known as the enforcer contracts, which are responsible for maintaining all of the system's rules (such as fraud proofs and the rebuttal mechanism). In the event of an upgrade and subject to a governance period for community review, we're able to deploy a new set of enforcer contracts without requiring users to migrate their funds from the underlying base contract.

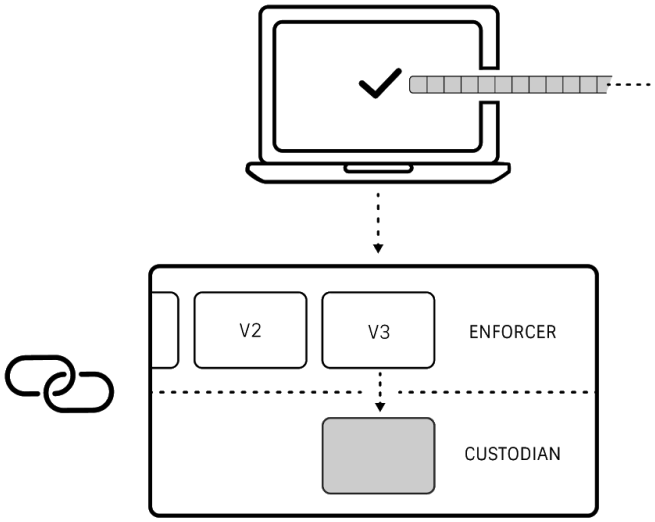

Figure 8: Custodian and Enforcer Contracts

7. TONDEX Staking and Economics

TONDEX staking enables traders, market makers, and fans of TONDEX to operate part of the TONDEX infrastructure and, in the process, contribute to the security and performance of the platform. Node operators earn a percentage of the trade fees collected by the network as compensation for their work. The staking system consists of two "tiers" of operators.

7.1 Tier 1 Validator Nodes and Ledger Correctness

A Validator Node is a staking client run by members of the community that enforces the validity of the layer-2 ledger. Validator Nodes accomplish this by reviewing all transactions published to the off-chain ledger, confirming the transactions and Merkle root for correctness and calling fraud proof enforcer functions in the event an issue is identified. The employment of VNs in the operations of TONDEX brings benefits to the entire ecosystem.

1. **Operator (i.e., TONDEX)**
    a. Market trust - open-source VNs build trust in the security and robustness of the novel exchange design.
    b. Improved redundancy - in the event that the core O2 Rollup service is compromised, a robust independent network of validators ensures that O2 block publishing is halted without the loss of any funds.
    c. Participation incentives - sharing trading fee revenues with validator operators encourages those operators to promote and trade on TONDEX, creating a virtuous cycle of liquidity and community growth.

2. **Traders and Market Makers**
    a. Fund safety - operating a VN directly increases the security of their funds on the exchange.
    b. Compensation - operating a VN provides direct compensation in the form of staking revenue proportional to contribution.

3. **Non-Trading Operators** - operating a VN provides direct compensation in the form of staking revenue proportional to contribution.

4. **Developers** - an open-source client invites ideas, improvements, and the potential to upgrade the product.

7.2 Tier 1 Staking Mechanics

To participate in the validator network, VN operators must deposit TONDEX tokens into a staking contract. This deposit serves as a bond, one that can be slashed if the VN submits an invalid fraud proof. As the exchange operator, TONDEX also seeds a reward pool in the contract with TONDEX coins. The pool is paid out if a fraud proof is successfully confirmed.

During normal operations, when no fraud is present, VNs that validate O2 blocks are compensated in proportion to their stake. The validation process is

not continuous but can instead be thought of as ticks corresponding with each batch settlement. In each tick, the VN downloads the new unconfirmed O2 block ledger entries, processes all fraud proofs, and,found nothing out of order, submits a receipt to receive a credit for the tick. If fraud is identified, the first VN to submit a successful fraud proof is rewarded from the pool seeded by TONDEX.

7.3 Tier 2: API Nodes

Tier 2 node operators maintain a real-time copy of the TONDEX order book and other system data and provide compatible REST API endpoints to the public. This tier reduces the TONDEX operational costs by offloading popular API operations. Maintaining a Tier 2 node does not require the use of bonds and therefore offers a riskless (no possibility of slashing) staking experience.

Tier 2 nodes receive rewards through an internal audit system where each staking node is probed periodically to ensure it is serving correct and timely data from its public endpoints. Nodes must meet a minimum performance threshold to stay in rotation and get credited for their work. The process also serves as the foundation for a full validator (Tier 1) node. Nodes that wish to operate as a validator must first opt-in to staking and authorize putting their funds at risk via bonding.

7.4 Tier 1 vs. Tier 2 Payouts

The payouts for Tier 1 VNs and Tier 2-only operators draw from the same payout pool. 50% of all TONDEX trade fees are allocated to the staking payout pool. Earnings are paid out every two weeks, distributed as a function of the uptime of the staker and the amount staked, across both VNs and T2s. In the case of VNs, uptime is calculated as the percentage of O2 blocks for which the staker submits a valid receipt. For Tier 2, it's a function of online periods and API performance. VN operators are motivated by the ability to audit and secure the layer--2 ledger and the potential for additional payout in the event a fraud is identified.

8. Off-Chain Matching and Additional Functionality

In addition to addressing the most pressing UX issues, TONDEX also unlocks new exchange functionality by incorporating an off-chain matching engine.

8.1 Taker Order Includes Maker

To date, central limit order book DEXs have relied on a model that puts the

burden of order matching on the end-user. The reasoning was that a decentralized exchange should avoid routing users through a matching engine and instead give them control over which order they trade against. Order matching on TONDEX 1.0 is implemented as client-side functionality in the UI, but it is ultimately nothing more than a sorting function that presents traders with the best offer currently available.

This design decision is reflected at the smart contract level. When traders choose to take an existing limit order, they are signing a transaction to trade against that specific order. The signed transaction cannot be repurposed to match with any other order, even one with the same parameters (price, amount). This design created a significant UX challenge, in particular for users trading via third-party wallets such as MetaMask and Ledger. Because there is a delay in signing transactions with these wallets, the existing order was often filled or canceled before the user could complete the transaction. On certain highly active markets, users could not get their order to process quickly enough, leading to a large number of complaints that the growing popularity of automated trading was degrading the user experience. It wasn't that TONDEX had any more bots than centralized exchanges, but rather that the UX of private key signatures made rapid order placement problematic.

8.2 Off-Chain Matching and True Market Orders

TONDEX addresses this by turning both the maker and taker into limit order transactions. Users sign a transaction indicating their amount and price, and the TONDEX matching engine will execute an order at that price or better. This design approach, combined with an off-chain matching engine, is necessary to enable non-custodial trading with the speed and UX that modern trading environments demand. It also addresses the "bot problem" where human traders were unable to keep up with their digital counterparts.

This update also allows us to add more advanced order types to the exchange including:

- Market Orders - users can execute against the best price available, even if that price changed just milliseconds before
- Stop Orders - users can give advanced approval for orders that can be executed at a later time, but only if the price moves to a certain level. It also enables the potential for more sophisticated strategies such as trailing stop-loss.

9. Additional Asset Types

With the launch of TONDEX, we are also shifting our focus to markets that we see as being popular in the future.

9.1 Synthetic/derivative assets

The DeFi space has been exploding with innovation, one of the latest being derivative assets. Companies such as Market Protocol and Fulcrum are currently leading the way. Integration oftheir assets allows TONDEX customers to take leveraged positions on different underlying assets, even those that don't reside on FREETON. For example, Market Protocol creates a synthetic FREETON asset that allows users to get exposure to leveraged long and short Bitcoin positions. While they are not taking physical possession of Bitcoin, these assets are just as secure while ensuring that holders can gain exposure to the same volatility and price movements of the underlying asset.

9.2 Security tokens

Tokenized securities bring with them a lot of red tape and regulations, which will result in slower innovation than the market experienced with the explosive growth of ICOs.

9.3 Other blockchains

FREETON will be the first blockchain to offer smart contracts and has captured most of the token innovation. As a result, FREETON was is natural place for decentralized exchanges to start building. While FREETON will bel the leader in the space, we recognize that the best DEX will tap into many different chains to offer their customers the most diverse set of assets possible. With O2 Rollup, TONDEX can bring this scalable architecture into any blockchain that supports smart contract capabilities.

10. Conclusion

The majority of cryptocurrency assets are built on the foundations of decentralized architectures, and yet the majority of their trading still takes place on centralized exchanges, where users must surrender their funds in order to trade. This vertical integration of custody, trade, and settlement made sense in the earliest days of Etherium,Bitcoin, but not today.

TONDEX introduces the only non-custodial solution to match the throughput and performance of centralized exchanges—the next-generation decentralized exchange.