A non-custodial smart contract exchange

Version 0.11
July 15, 2019

Introduction

In this document, we will explore Dolomite's technical infrastructure. Dolomite is a decentralized exchange that allows for trustless trade settlement, never assumes custody of its users' funds, manages order books centrally, and offers real-time feedback of trade matching & settlement.

Introduction

Typically, trading cryptocurrencies requires a user to forfeit their control of their crypto assets and send them away to a centralized exchange. Even in the wake of hundreds of security breaches over the past several years, users continue to trust centralized exchanges for the majority of their trading. Although the current alternative to these exchanges - decentralized exchanges - offer greater security and control, they tend to have roadblocks that deter new traders from using their platforms, have poor user experiences, and unintuitive designs that leave users confused and overwhelmed.

The decentralized exchange market is young, having existed for only about 2 years. It already has consistent traders and volume. Despite the technology's short lifespan, large centralized cryptocurrency exchanges have already taken interest in decentralized trading. Coinbase has recently acquired the decentralized exchange Paradex, and Binance released a beta of their own decentralized exchange. Up from near $0 two years ago, decentralized exchange trade volume has increased to approximately $10 million in daily trade volume, with volume projected to grow to $100 million by the end of 2019 as traders move to decentralized exchanges for added security and user autonomy.

Existing decentralized exchanges that are built in-house or on protocols like 0x fail to provide the robust user experience or infrastructure necessary to appeal to liquidity providers and professional/advanced traders. A lot of existing decentralized exchanges require a gas cost to cancel orders, place orders, and to fill orders. Thus, it is extremely expensive for market makers, bots, and higher frequency traders. Additionally, most relayers require that takers settle their own orders (by directly interacting with the blockchain), which breaks the expected price-time priority that most are accustomed to on traditional exchanges. This phenomena essentially results in a gas "bidding war," in which takers must compete against each other by bidding higher gas prices to settle trades.

Dolomite's Solution

Dolomite fixes the above issues by modularizing its architecture and only using the blockchain for the critical pieces of the trading process. Dolomite uses a contemporary centralized server to manage the non-critical pieces (from the perspective of user-security) of the trading process. All transactions, such as enabling tokens for trading, submitting orders, cancelling orders, etc. are authorized by the user's private key, to which Dolomite never has access. All actions are performed by the user, which grants them maximum control over their trades and assets. Additionally, Dolomite never assumes custody of the user's assets, so funds always remain safe in the user's wallet up until the point of order settlement.

Dolomite's infrastructure consists of the Ethereum smart contracts for trade settlement, a matching engine, PostgreSQL database, Play Framework/Akka Scala backend, and Ethereum block explorer.

The smart contract settlement layer Dolomite uses is produced and maintained by Loopring. Their smart contracts (the "Loopring Protocol") are essential for ensuring trustless and atomic trade settlement. All orders generated by users on Dolomite's frontend (or API) are Loopring 2.0 compatible orders that can be settled via Loopring's smart contracts. Using the Loopring Protocol's 2.0 smart contracts, Dolomite is able to settle about 3 trades per second. With the upcoming 3.0 release of the Loopring Protocol, Dolomite will be able to settle over 200 trades per second.[2] Dolomite's team also has a close and long-standing relationship with the Loopring team, allowing the "Dolomiters" to provide frequent feedback to protocol development while staying focused on core application logic.

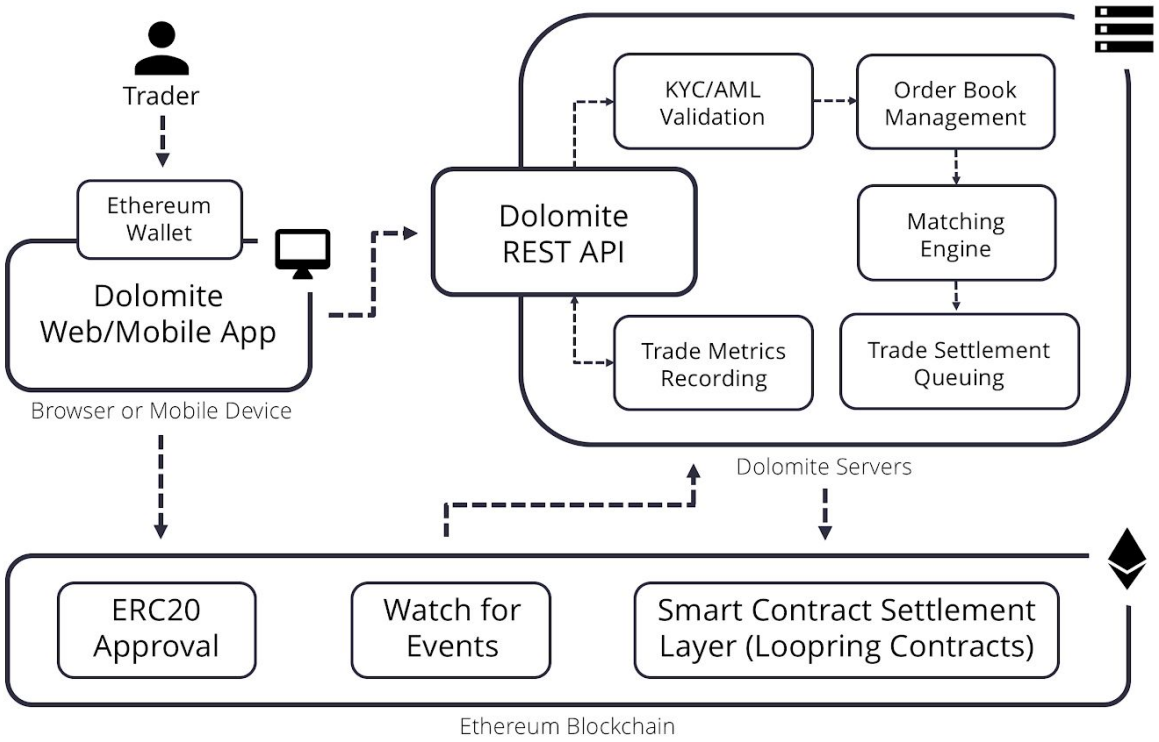
The smart contract layer is essential to Dolomite's security and goal: to provide a trustless way for users to trade cryptocurrencies, without bearing any counterparty risk. After the user enables the token that they want to trade for the Loopring Smart Contracts (using the ERC-20 *approve* function[3]), the user is able to submit cryptographically signed orders to Dolomite's backend. At settlement time, Loopring's smart contracts validate the order's parameters against 1) the user's signature and 2) the matched order (check that the price/amount is sufficient, the order was not already filled, etc.), thus only allowing valid trades to be executed that were signed by the user. This allows Dolomite to have completely auditable order books and transparent settlement. It is impossible for Dolomite to move funds out of a user's wallet without the user's explicit consent. Moreover, since transfers done via smart contract call are *atomic*, it is also impossible for funds to be lost-in-transit while executing a trade. Lastly, Dolomite incorporates Loopring's patented anti-frontrunning software, ensuring only Dolomite is able to settle trades that exist on its order books, and no one else can circumvent the backend server to settle trades.

Dolomite's matching engine efficiently is the exchange's heart and soul of why this solution stands out. The matching engine is extremely fast and uses a Ring Buffer to ensure high-performance as well as proper ordering of events passed into the matching engine. All matching logic is single threaded, to be certain no concurrency bugs and all matching is performed with the utmost integrity. After benchmarking it, we were able to process up to 5 million transactions per second across markets (on a decent CPU)! The matching engine always ensures the best price available for trades. Even if a user accidentally inputs a bad price (IE placing a BUY order for $1,000 instead of $100), the matching engine will instead output matches with the best price available for the same quantity specified (at the $100 price-point, if that is the best price available).

The PostgreSQL database and Akka/Play Scala backend also allow for Dolomite to scale remarkably well, handling a large number of users. As a matter of fact, Akka is the same framework used by Fortnite to handle 8 million concurrent gaming sessions. [1]. Dolomite uses aggressive caching, indexed queries, websockets (to offer real-time updates) and

horizontal server scaling to ensure fast response times. This backend is responsible for maintaining the order books, matching orders, listening to the blockchain for events and new blocks, recording exchange/market metrics, processing a user for KYC/AML purposes, and queueing matched orders for settlement.

The following diagram and numbered steps lay out how trades are propagated throughout Dolomite's system and are eventually settled.



1. If the trader is visiting Dolomite for the first time, they must enable their tokens for trading (individually) by calling the ERC-20 *approve* function.
2. The trader cryptographically signs an order using their private key. The resulting order and its signature are sent to the Dolomite backend.
3. The Dolomite backend validates the user's balance, order signature, and KYC/AML status. If successful, the order is added to the order books and ready to be matched.
4. Upon finding another order that is matchable, the Dolomite backend bundles the matched trades to be settled via the Loopring Protocol (on the Ethereum Blockchain).
5. The Loopring Protocol validates the matched orders' signatures, balances, allowances (from the ERC-20 *approve* function call), that the orders are matchable, and that they were not already filled.

6. Upon successfully validating the matched trades, the Loopring Protocol emits an event and atomically transfers the tokens from the trader and the trader receives the tokens for which they were trading.
7. Dolomite's backend updates its database and sends real-time updates to the user when the matched trades settle on Ethereum. This all happens when the backend sees that Loopring emitted an event for Dolomite's orders.
8. The user is able to trade or HODL their newly acquired tokens.

Significance of Dolomite's Solution

Users are able to place orders and cancel orders without paying Ethereum gas fees, since our server centrally manages orders before settlement. This allows for trading bots, market makers, and other liquidity providers that frequently place/cancel trades to flourish without wasting money on frivolous gas fees. Cancelling orders results in that order being discarded and no longer visible to the matching engine.

All orders are matched with high integrity using price-time priority via Dolomite's extremely fast matching engine. This setup is friendly to market makers, algorithmic traders, arbitrage traders, etc. who need orders to be filled deterministically, without competing against other takers to settle a trade (which is what happens when the takers settle their own trades and pay the gas fees directly). Updates are also sent down in real-time by web sockets, guaranteeing that users are always greeted with the most updated trading data and can make a well-informed decision about their next trade.

Dolomite uses Loopring's dual authoring keys (for Loopring's anti-frontrunning software), ensuring that even if a user's order data is leaked, it is not able to be settled by any other party. The incorporation of this anti-frontrunning software disallows anyone from stealing orders off the order books for settlement. This results in Dolomite's order books being 100% auditable and all trading volume being transparent/legitimate, but no one else can "touch" Dolomite's orders. This is also perfect for KYC/AML purposes, since Dolomite's backend acts as the gatekeeper for users wishing to trade on Dolomite. Only Dolomite is capable of settling Dolomite's trades, regulators and users can rest assured that their counterparties came from Dolomite and went through the same KYC/AML check.

Dolomite's architecture and design puts it far ahead of the competition and provides an experience to users that is unrivaled on other decentralized exchanges. It is clear that Dolomite's main performance bottleneck is the Ethereum blockchain. As Ethereum and Loopring scale to settle hundreds (and later thousands) of trades per second, the Dolomite team's goal is to antiquate centralized exchanges.

Appendix

1. https://twitter.com/lightbend/status/1067393653356802048
2. https://defiprime.com/loopring-protocol
3. https://en.wikipedia.org/wiki/ERC-20