Deepwaters version 2.0

Performant Trustless Trading Engine

Whitepaper DRAFT Rev 2.1.7

Zorrik Voldman
zorrik@deepwaters.xyz

Greg Barnes
greg@deepwaters.xyz

September 2022

Notice and Disclaimer

This document and the information contained herein constitutes **"Confidential Information"**, which strictly limits sharing and use. This document may not be further distributed or reproduced, in whole or in part, without the express written consent of VatnForn LLC (VatnForn).

The sole purpose of this document is to assist interested parties in deciding whether to proceed with further analysis of a potential strategic transaction involving VatnForn. No attempt has been made in this document to identify potential risk factors. In all cases, interested parties should conduct their own investigation and analysis of the company, its assets, financial condition and prospects, and the information set forth herein. The company makes no representation or warranty as to the accuracy or completeness of the information contained herein.

The information contained herein includes forward-looking statements regarding future strategy and plans, as well as commentary regarding future results of operations and prospects. These forward-looking statements are based on current information and expectations, and involve a number of risks and uncertainties. Actual plans implemented and actual results achieved may differ materially from those set forth in or implied by such statements due to a variety of factors.

This document is furnished for informational purposes only and does not constitute an offer or solicitation of an offer to subscribe for, purchase or sell any securities, business or assets of any entity.

Disclaimer **3**

Abstract **3**

Background **4**

Problems Affecting Trading Platforms **5**

- Overview 5
- Privileged Counterparties 5
- Order Flow Violations in Automatic Market Maker DEXs 5
- Order Flow Violations in CEXs and Orderbook DEXs 6
- Adverse effects of PFOF 6
- Bifurcation of Order Flow 7
- Information Asymmetry 7
- Margin Calls and Liquidations 7
- Custodial violations in DEXs 7
- Custodial violations in CEXs 8

Technological Limitation of Trading Platforms **8**

- Technological Limitations of CEXs 8
- Technological Limitations of DEXs 8

The Deepwaters Approach **9**

- Overview 9
- Deepwaters vs Competition Comparison Matrix 10
- Key Principles 11

Deepwaters Architecture **11**

- Overview 11
  - Major Components 12
- Deepwaters Trusted Execution Environment 14
- Auditors and Validators 15
  - Validator Compensation 16

Confidential Order Management **17**

Deepwaters Blockchain Services **18**

- Self-Custody 18
  - Deposits 18
  - Withdrawals 19
- Off-chain Operations 19
  - Trade Initiation 20
  - Balance Tracking and Settlement 20

Open Outcry **20**

Disclaimer

The majority of good data and research into the damaging effects of privileged information and control of order flow comes from traditional finance. While this paper uses some traditional market data and commentary to extrapolate the applicable effects into crypto trading, neither the initial data nor the latter are to be considered sacrosanct or 100% accurate. They do however, point to clear and obvious deleterious effects.

Abstract

Deepwaters is a performant trustless trading engine built on the intersection of centralized & decentralized methodologies. The Deepwaters platform resolves problems of loss and uncertainty that have been plaguing the latest evolutions of decentralized exchanges (DEXs) and centralized exchanges (CEXs) These challenges not only harm traders, but distort markets and magnify the impact of tail risk events. Such events occur most frequently in the digital asset space and we will focus our initial market and proof of concept therein.

This paper describes the philosophy, core designs and associated implementation methods of Deepwaters.

Background

Gary Gensler, Chairman of the SEC, recently tweeted:

> “Tech has transformed & continues to transform our equity markets. While this has led to good things, it also brings challenges […] There isn’t a level playing field […] **Markets have become increasingly hidden from view**. In '09, off-exchange trading accounted for 1/4 of US equity volume. Last year, that share peaked at 47%. 90 plus percent of retail marketable orders are routed to a small group of wholesalers that pay for this retail market order flow. It’s not clear, w/ such an uneven playing field, that our current national market system is as fair & competitive as possible for investors.”[1]

The selective blocking of order flow, which was revealed during the recent GameStop stock (NASDAQ:GME) and Terra Luna (LUNA) market events, is a dramatic expression of market flow monopolization, which has captured the public's imagination in recent years.

Privileged information results in unfair advantage for entities that possess it. The CEO of Virtu, one of the largest wholesalers, described the beneficial effects of expanding the order monopoly:

> “The reason the strategies are successful is because we have this enormous kind of cornucopia of orders that we’re getting from retail brokers, but we’re also getting from other broker-dealers, …and we are also acquiring on an exchange or a dark pool and all those get kind of thrown into our central risk book…It’s not a coincidence that when Knight and Virtu combined [...] we’ve seen improvements in our strategies and our performance.”[2]

Adam Cooper, who was Citadel’s general counsel in the early days of the company, argued in favor of banning Payment For Order Flow (PFOF) because the practice “distorts order routing decisions, is anti-competitive, and creates an obvious and substantial conflict of interest between broker-dealers and their customers.”[3]

While monopolization of order flow information and control increases volatility and causes well concealed damages over time, commingling and rehypothecating of customer assets is a problem that can have dramatic far reaching negative consequences for individual participants and entire markets. The discretionary nature of these decisions, combined with poor risk management, often results in significant loss of customer assets during tail risk events. Several recent high-profile incidents have revealed many companies that utilized customer-owned assets to cover their financial losses. If the fallout of such negligence spreads widely, it is often described as contagion.

[1] https://twitter.com/GaryGensler/status/1540033950244126720

[2] 2020 Quote from Virtu Financial CEO, Douglas Cifu, from the transcript of the Virtu Financial earnings call for Q4 2020.

[3] Release No. 34-49175; File No. S7-07-04 — Competitive Developments in the Options Markets https://www.sec.gov/rules/concept/s70704/citadel04132004.pdf

There is a problem in finance that extends across global markets and regulatory frameworks leading to the necessity for trusted and transparent systems.

Problems Affecting Trading Platforms

Overview

Current exchanges allow for unexpected outcomes resulting in excessive fees, undetermined expenses, and loss. Most of the **problems** affecting trading platforms can be separated into **two categories**.

1. No confidentiality and poor integrity of order flow before it is recorded in the publicly available order book, resulting in:
    a. Front-running
    b. Order flow reordering and blocking
    c. Spread deterioration
    d. Poor fill rates
    e. Privileged rent seeking

2. Violability of the custody of customer funds, resulting in rehypothecation and commingling. This causes customer funds loss, normally during tail risk events.

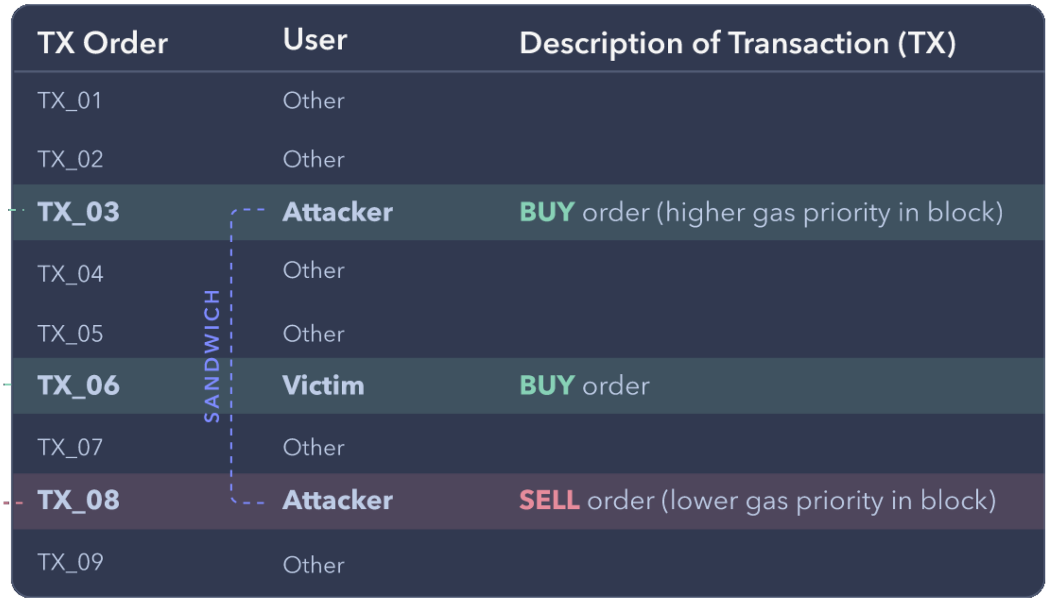
Privileged Counterparties

For the purposes of making this exposition generic, we will use the term “privileged counterparties” to designate actors other than good faith, non-extractive customers of the trading platform or wholesalers.

Order Flow Violations in Automatic Market Maker DEXs

In an invariant Automatic Market Maker (AMM) invariant-based DEX, swap orders are broadcast to the blockchain mempool, which acts as a queue for network transactions, allowing them to be executed during addition of future blocks. The mempool execution is typically ordered based on gas fees attached to the individual transactions (to maximize fee-based profits for miners). During the creation of a block, miners have authority to include transactions in ANY order, include transactions external to the mempool, and even omit [or censor] transactions entirely.

Consider a purchase transaction by a buyer, seeking to buy 100,000 USDC worth of ETH. The mempool can be observed by any market participant with access to a full node. Therefore, an attacker can insert a transaction prior to the buyer’s transaction, by simply using a higher gas fee. Such insertion, commonly known as front-running, creates an undesirable price increase (slippage). The attacker then uses the same gas fee ordering method, to send another transaction after the victim’s transaction, selling their ETH for a profit (see Table 1). This method of pre-pending and appending an attacking transaction to the buyer's transaction is known as a "sandwich attack".



TX Order	User	Description of Transaction (TX)
TX_01	Other	
TX_02	Other	
TX_03	**Attacker**	**BUY** order (higher gas priority in block)
TX_04	Other	
TX_05	Other	
TX_06	**Victim**	**BUY** order
TX_07	Other	
TX_08	**Attacker**	**SELL** order (lower gas priority in block)
TX_09	Other	

Table 1: Sandwich attack

Various solutions have been proposed, including transaction encryption. However, the solutions suffer from high gas costs and the potential for censorship.

Order Flow Violations in CEXs and Orderbook DEXs

While AMM DEXs suffer from mempool reordering that is opportunistic and subject to competitive interference, privileged players have a more certain path to exploiting the order flow in an orderbook approach. A privileged party may reorder, block the orders, or simply sell the order flow to another privileged counterparty. One such privileged action is called payment for order flow (PFOF).

Adverse effects of PFOF

PFOF has been a hotly debated topic. Several studies make a convincing case against PFOF. Sviatoslav Rosov, the director of capital markets policy at the CFA Institute, examined the effect of the PFOF ban on UK markets. He states: "We observe an increase in the proportion of retail-sized trades executing at best quoted prices between 2010 and 2014 from 65% to more than 90%...We believe this change is a positive one for market integrity because it implies that displayed liquidity providers are rewarded with executions at the price they quote. This reward mechanism upholds market integrity by supporting the incentive to post the displayed limit orders on which price discovery is based and should lead to more aggressive quoting and competitive pricing. By contrast, this outcome may be jeopardized in markets with PFOF arrangements where internalisers are able to step ahead of the quoted price on the order book by offering price improvement. It appears that the current best execution regime in the United

Kingdom appears to be working well, despite the lack of a US-style trade-through rule that explicitly prevents executions away from the best quoted price.*"*[4]
Preserving confidentiality of orders and the order flow would result in 25% improvement in NBBO[5] spread[6]

Bifurcation of Order Flow

As privileged counterparties make decisions on order routing based on profitability, market orders and limit orders are segregated in a way that prevents traders from trading against market orders directly, which are absorbed by privileged counterparties. This means larger exposure to toxic flow[7] for traders. The net result is an increase in adverse selection[8] and decrease in fill rates, both detrimental to traders.

Information Asymmetry

Having early access to order flow information creates a significant information asymmetry between privileged and non-privileged counterparties. This information allows privileged counterparties to react before non-privileged traders and significantly increase the adverse selection effect. This situation damages organic price discovery and results in a monopoly for privileged counterparties, e.g. right of first refusal. Average adverse selection on exchanges is 61% of the spread, while adverse selection for wholesalers, resulting from servicing non-privileged counterparties, is only 15% of the spread. The information asymmetry has clear advantages for privileged counterparties, resulting in poor fill rates for customers.

Margin Calls and Liquidations

Conflict of interest violations damage execution of margin calls and liquidations as well. This increases implicit trading costs, as limit orders fail to fill and market orders experience significant price fade. Algorithmic trading in particular is suffering from excess execution risks as back-tested strategies fail to live up to expectations predicated on a “fair” trading environment.

Custodial violations in DEXs

Custodial violations in DEXs are normally due to discretionary actions by insiders with access to fund storage or exploits.

[4] Payment for Order Flow in the United Kingdom Internalization, Retail Trading, Trade-Through Protection, and Implications for Market Structure. Sviatoslav RosovPhD, CFA https://www.cfainstitute.org/en/advocacy/policy-positions/payment-for-order-flow-in-the-united-kingdom
[5] National Best Bid and Offer
[6] The good, the bad & the ugly of payment for order flow. Hitesh Mittal & Kathryn Berkow
[7] Toxic flow is order flow from parties that have advantage in information or speed.
[8] Adverse selection refers to prices going up after a sell and going down after a buy.

Custodial violations in CEXs

Custodial violations in CEXs are due to discretionary actions by insiders affecting rehypothecation and commingling of customer assets, sometimes in violation of contract. As such, loss of customer funds outside the scope of exploits and security breaches is more common in CEXs, often the result of poor risk management.

Technological Limitation of Trading Platforms

Technological Limitations of CEXs

CEXs are, as the name suggests, centralized in nature. This means that they can be highly performant and very efficient. However, they require a high degree of trust, as the technology does not openly enforce confidentiality of order flow or sanctity of customer's deposits. Users are at the mercy of discretionary decisions and actions of an organization, subject to various conflicts of interest and misaligned incentives. Exposing customer-owned assets to risk is commonplace, often without adequate compensation for the customer.

Technological Limitations of DEXs

DEXs can be inherently trustless *if* implemented according to the best industry practices. Assuming trustlessness, a primary issue is performance. Underlying blockchain technology sacrifices efficiency for resiliency. Blockchain is using a significant amount of computational resources to make itself trustworthy, but not performant. As such, trading on DEXs is both slow and expensive. Various scaling solutions (optimistic and zero knowledge rollup strategies) can be employed to improve the situation; however, they introduce new tradeoffs and additional points of failure.

Public blockchain-based solutions also face another significant challenge: lack of confidentiality. Using a public validation system makes protecting the order flow and order book problematic, as the execution environment initial load, ongoing integrity and privacy of data, as well as purity of the operating environment can be difficult to control, even if strong encryption is used. At any point, discretionary actions of individuals may compromise the confidentiality and/or integrity of the data flow. Private validation system compromises the trustless elements and ultimately leads to the same problems. Blockchain normally exposes data to public consumption, which violates the confidentiality requirements of order flow.

The Deepwaters Approach

Overview

Conceptually, Deepwaters is a ‘hybrid’ approach leveraging both centralized and decentralized components to create a platform that is compliant, highly performant and effectively trustless. It introduces enforceable integrity, accountability, and transparency; all of which are *provable* without significantly affecting the speed, efficiency, and low cost that users have come to expect from well-designed centralized trading platforms.

Deepwaters combines the concepts of confidential computing- which utilizes Trusted Execution Environment (TEE) enclaves - with blockchain custody and consensus-based validation to audit the deployment and maintenance of TEE enclaves. As such, it is capable of high transactional throughput, complex operations, and crash fault tolerance, while maintaining a high level of integrity and non-interference assurance, as well as immutability of custody.

Deepwaters vs Competition Comparison Matrix

Deepwaters solves the following problems that are present in conventional centralized and decentralized order books and automatic market makers (AMMs) (see *Table 1*).

Problem	Order Book	Invariant AMM	Deepwaters
Compromised Price	PFOF[9] widens spreads. Adverse selection. Price Fade.	Local scarcity micro economic price discovery anchored in arbitrage (invariant-based slippage + MEV-based slippage)	PFOF is *provably* impossible
Order Flow Disruption	Privileged parties can change and block order flow.	MEV[10] players change and block order flow	Order flow Immutability
Poor Order Execution	Front-running and sandwiching by privileged parties. Bifurcation of orders.	MEV players sandwich and front-run traders	Front-running and sandwiching is *provably* impossible
Opacity	Bid/Ask pyramid may not reflect reality (order flashing) Informational Asymmetry.	Just-in-time liquidity and other MEV-based attack vectors	WYSIWYG[11]
Custodial Violations	Undisclosed and unagreed asset rehypothecation and commingling	Immutable custody, but smart contract risk.	Immutable custody, but smart contract risk.

Table 2: Solving the problems of conventional trading platforms
Mechanics of ***Deepwaters*** *vs. conventional order book & invariant AMM*

Note: Hybrid DEXs share some advantages and disadvantages with traditional CEXs but also introduce their own idiosyncrasies, such as Request For Quote (RFQ) pricing determined by market makers (MM).

[9] PFOF: payment for order flow
[10] MEV: miner extracted value
[11] WYSIWYG: what you see is what you get

Key Principles

Confidentiality.
Even the host cannot see what is going on inside the business logic. Therefore, there are no privileged parties that can use trading data prior to it being available to all market participants. This ensures the premise of fair execution by preventing various trading evils:

- Front-Running
- Order Flow Reordering
- Order Flow Blocking
- Spread Deterioration
- Privileged Rent Seeking.

Integrity
The code that is executing is guaranteed to be the one we intended to execute.

Third Party Attestation.
Computation is reflected to third parties outside the platform for validation. Third parties outside the platform can verify and validate the function of trade execution in real-time, and validate individual trades after a delay.

Immutable Custody
Clients are in control of their assets. No possibility of asset rehypothecation or commingling by platform operators.

Deepwaters Architecture

Overview

Deepwaters uses on-chain technology to support self-custody: deposits and withdrawals are done using smart contracts. Business logic and critical data are encapsulated in a TEE enclave. Independent validators are compensated to verify integrity of the system as a whole. Market participants interact with Deepwaters through technology that they're used to: the Deepwaters Trading API and trading terminal. All business logic is open-sourced. Validators can subscribe to log replication and *native* TEE cryptographic attestation to verify that behavior is as intended. These validators are compensated to verify behavior and dispute against bad actors.

Major Components

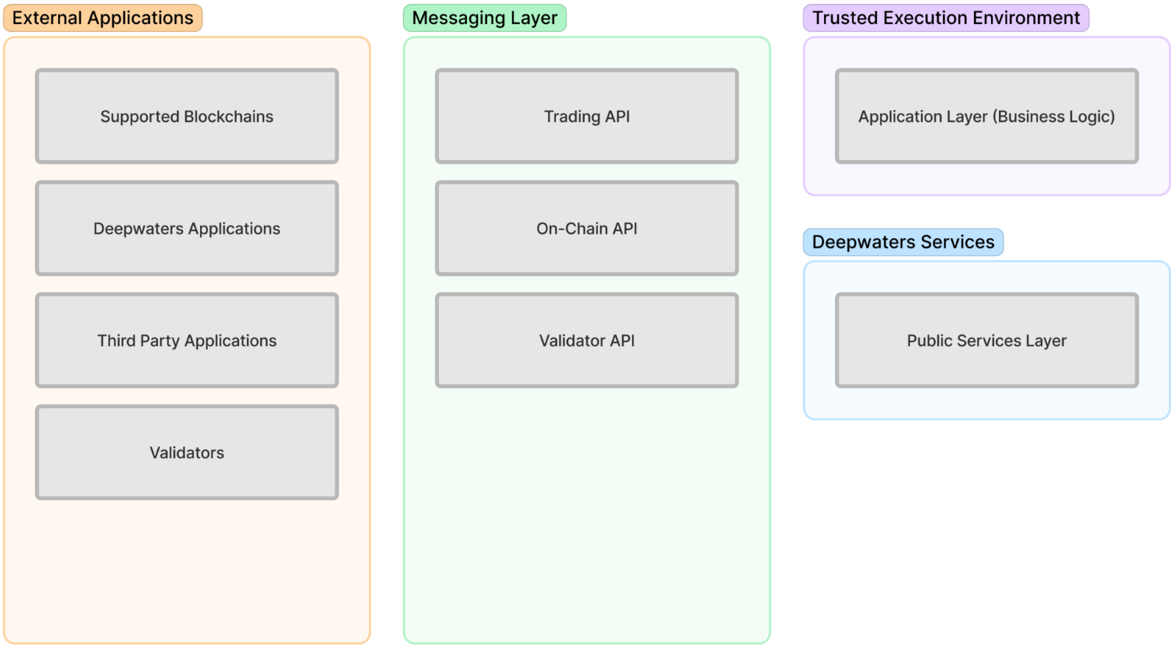


Figure 1: Deepwaters Major Components

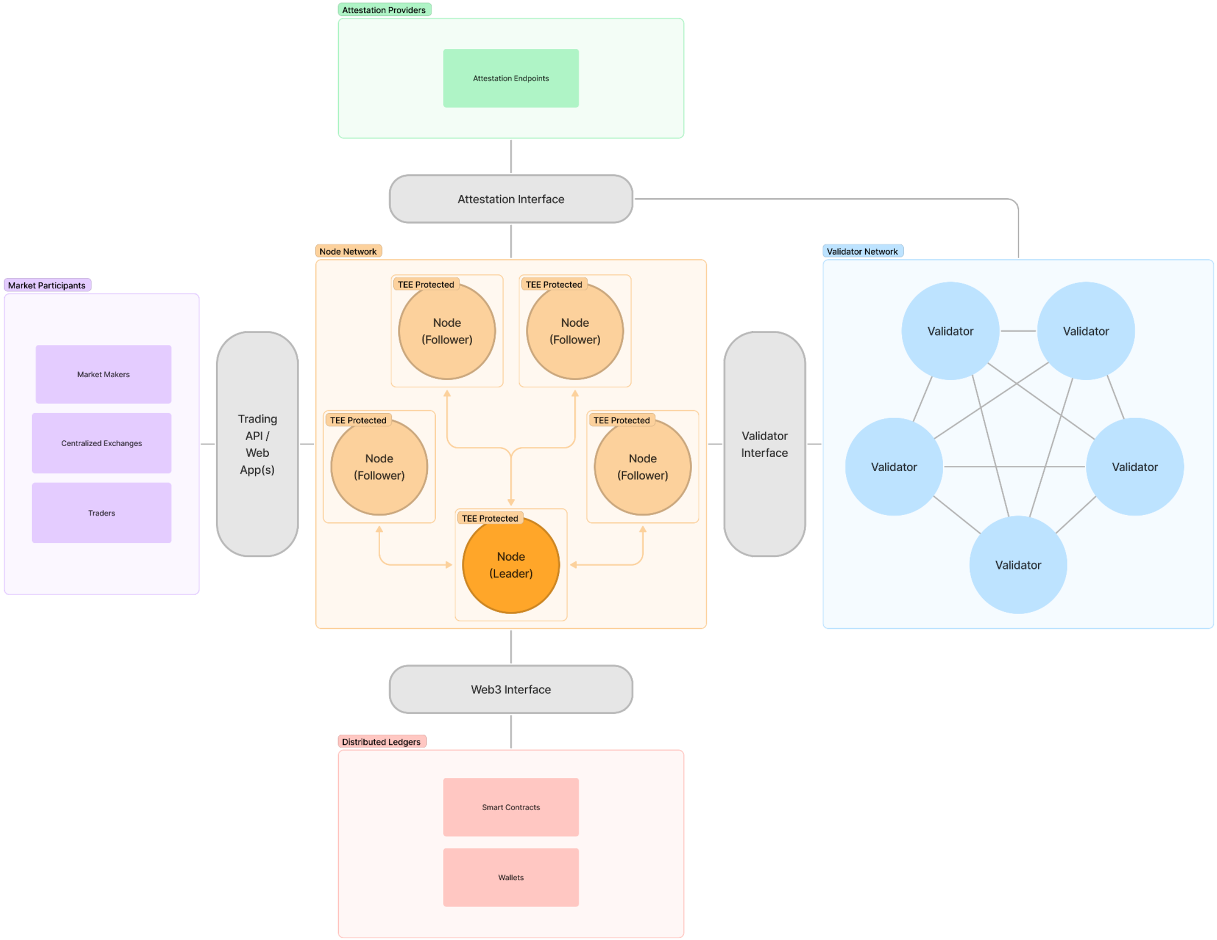


Figure 2: Deepwaters in Detail

Deepwaters Trusted Execution Environment

The Deepwaters application is deployed into a Trustless Execution Environment (TEE). This ensures that the kernel, application, and data is protected from outside users' viewing and tampering (including Deepwaters). Inside of the TEE, the application will run exactly as expected. All interactions with the application are explicitly restricted to the Deepwaters Trading API; communication is end-to-end encrypted. The result of this setup establishes privacy, fair execution, and unbiased sequencing. Additionally, the application [business logic] is open-sourced for any individual to audit.

Nodes running the Deepwaters application and TEE are distributed across varied regions and participate in RAFT[12]-based consensus. In this way, the system exhibits crash fault tolerance and replication of data while maintaining high throughput and allowance for complex operations.

[12] The Raft Consensus Algorithm
https://raft.github.io/

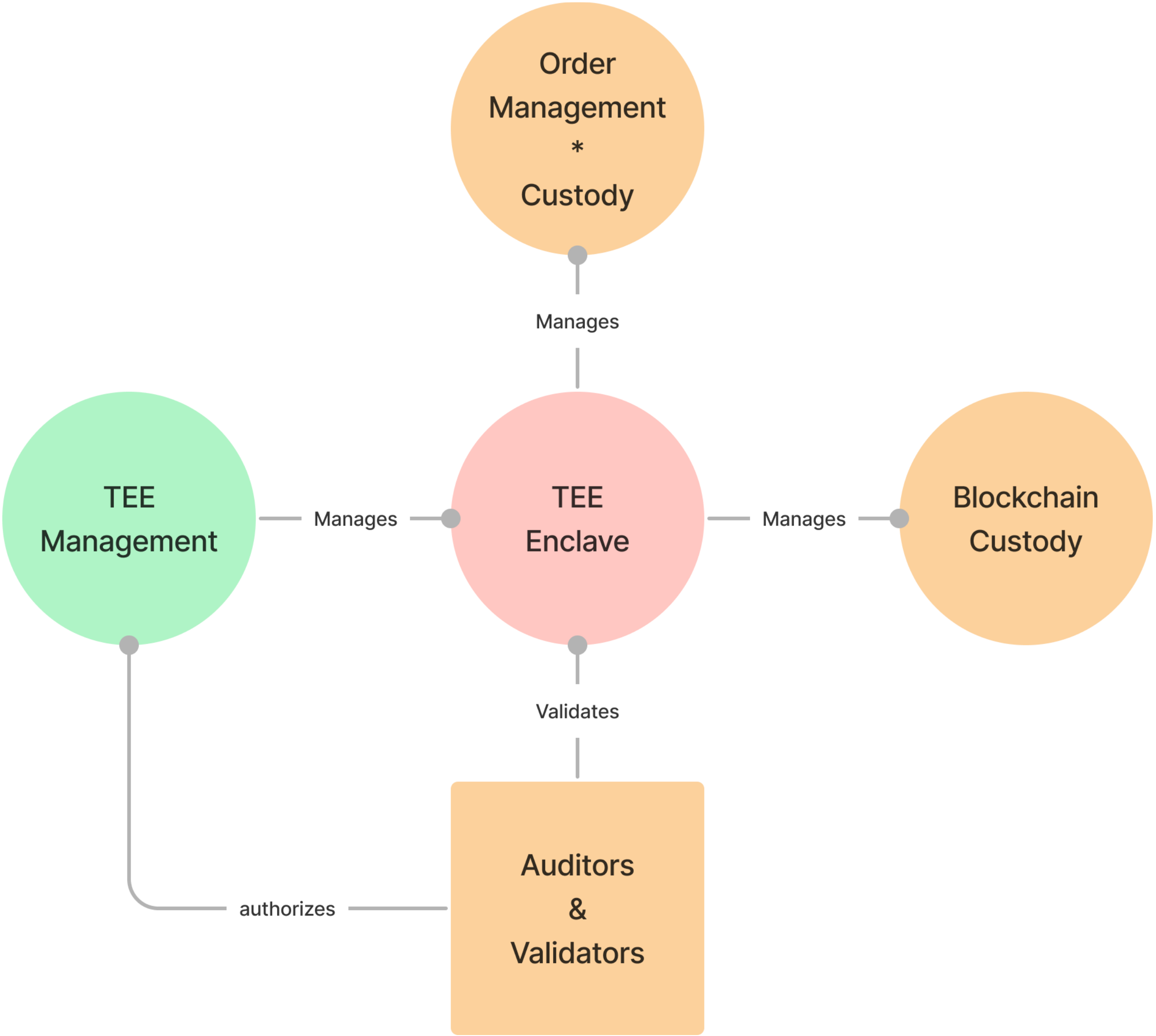


Figure 3a: Protecting TEE with Blockchain

Auditors and Validators

Business logic is encapsulated in Deepwaters TEE Enclaves and audited by Deepwaters Validators.

Roles of Deepwaters Validators:

- Check native TEE cryptographic attestation
  - Verify enclave image
  - Verify linux kernel
  - Verify application
- Consensus-based deployment
- Consensus-based updates

- Subscribe to log replication
    - Listen to order flow and recreate results in local build of application

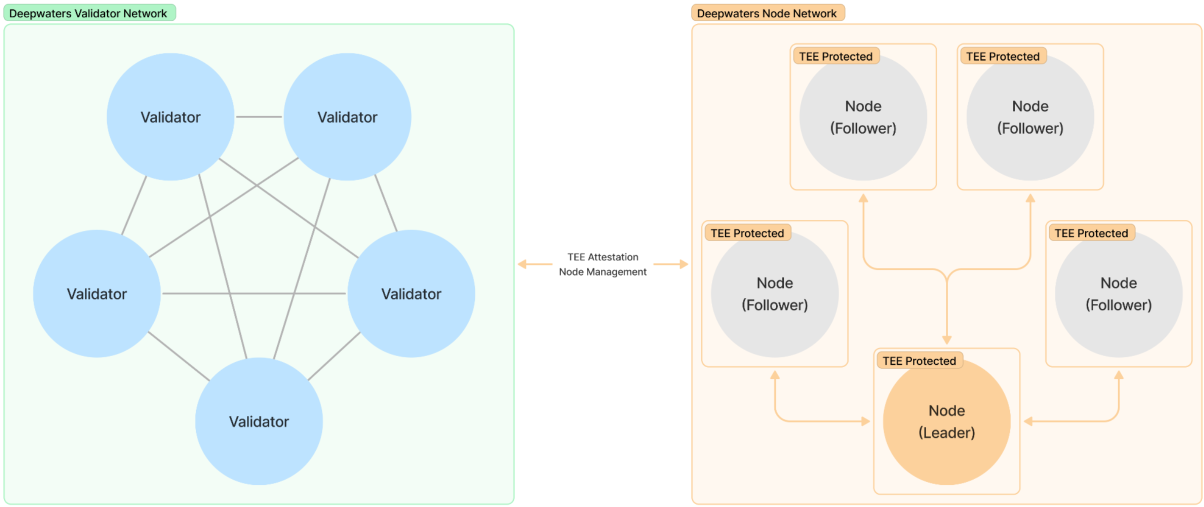


Figure 3b: TEE-Protected Node Network and Validator Network

Validator Compensation

Users who have gone through KYC can be compensated for running the Deepwaters Validator client. Payment is based upon number of validations (fixed rate) with bonuses for reliability (uptime) and length of validation.

Confidential Order Management

Incoming orders can be divided into two major categories:

- Post orders (maker orders)
- Take orders (taker orders)

Post orders are limit orders that do not cross the market: that cannot be matched immediately against the existing order book. Take orders are market orders or limit orders that can be matched immediately against the existing order book.

The resulting order book is public, however the integration of a TEE ensures that incoming order flow is confidential until after it is posted or matched against the existing order book, as illustrated in Figure 3. Sequencing and execution of orders is the same for *all* parties, including the host of the engine**.**

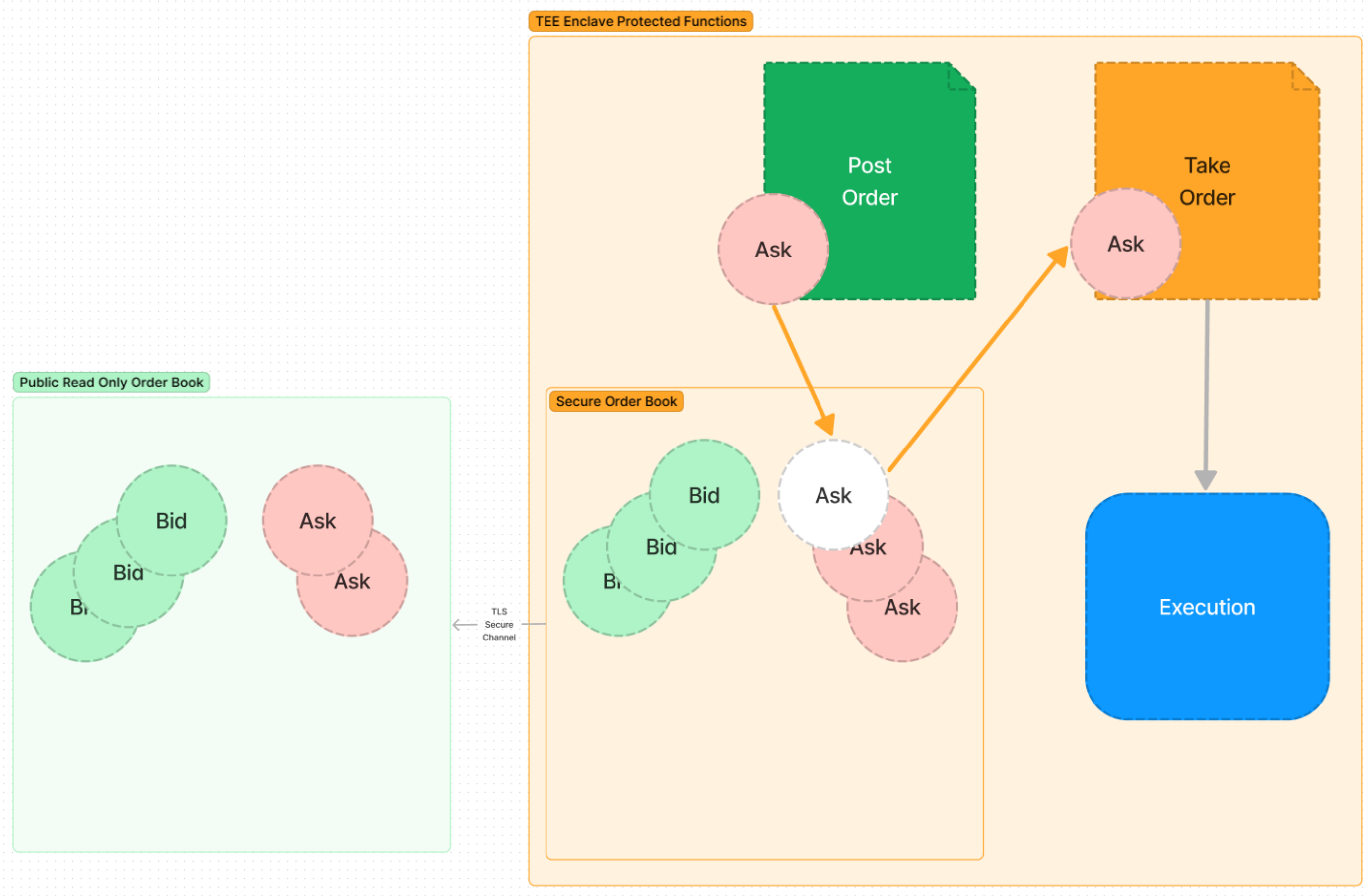


Figure 4: Confidential Order Flow Management

Deepwaters Blockchain Services

Self-Custody

The Deepwaters (DW) application leverages the trust and decentralization of existing blockchains to facilitate self-custody. Deposits and withdrawals are performed ‘on-chain’ in smart contracts, in conjunction with the Deepwaters application. Beyond the initial set of blockchains, Deepwaters is capable of upgrades to support any smart-contract-enabled blockchain. All deposits and withdrawals can be audited on-chain in their respective ecosystem in real time.

Deposits

After a user has registered with Deepwaters and completed KYC requirements, they are ready to deposit assets.

Functionally, a deposit executes as follows:

1. The depositor requests permission for the deposit to DW using the Deepwaters Trading API
2. DW responds with a signature corresponding to the depositor and the parameters of the deposit
3. The depositor executes an on-chain deposit transaction (including the signature and deposit parameters). The smart contract verifies that the correct user is depositing and the parameters of the function call are correct
4. DW consumes the on-chain event. After sufficient block confirmations, assets are available for trading in the Deepwaters platform (this is necessary to prevent double-spend attacks)

After an asset has been deposited into a Deepwaters smart contract and sufficient block confirmations are completed, the user is able to execute actions quickly and efficiently (without gas costs) off-chain, using the Deepwaters Trading API (API).

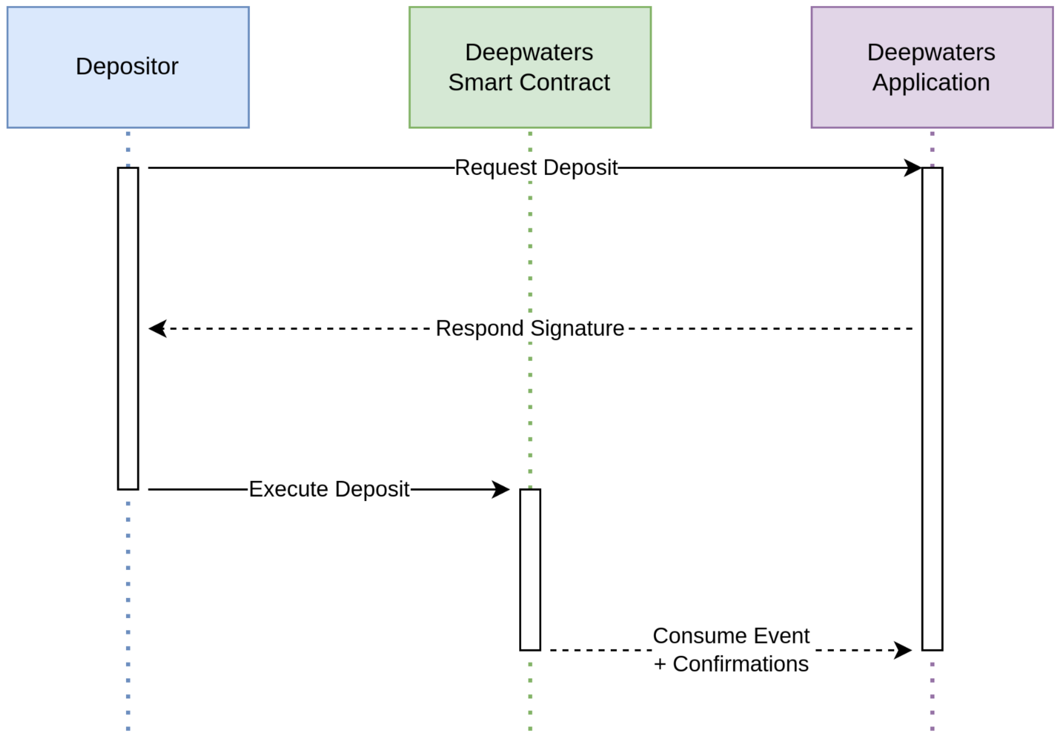


Figure 5: Deposit Sequence Diagram

Withdrawals

A user is able to withdraw their assets through a process similar to deposits, described below.

1. The withdrawing user requests a withdrawal to DW using the Deepwaters Trading API
2. DW responds with a signature corresponding to the user and the parameters of the withdrawal
3. The user executes an on-chain withdrawal transaction (including the signature and withdrawal parameters). The smart contract verifies that the correct user is withdrawing and the parameters of the function call are correct

The Deepwaters system ensures that business logic is not violated and attempts to withdraw assets are valid.

Off-chain Operations

The majority of actions initiated by users will occur off-chain, utilizing the Deepwaters Trading API. A combined cross-chain state of user balances and other information is held in a secure computing environment. Actions can *only* be created by a user, who cryptographically proves they own the address associated with the action they are initiating.

Trade Initiation

The following will describe a typical off-chain operation, a trade, using the Deepwaters web application or API.

1. The user signs a message (proving ownership of a wallet associated with their account) and sends this to DW
2. The user submits a trade request to DW using the API
3. DW verifies the signature to check for ownership, executes the trade, and returns a response that the trade was successful

Balance Tracking and Settlement

On-chain settlement is only required during withdrawals. Tracking of balances and other information is maintained off-chain in a secure computing environment. Deepwaters data is replicated across multiple node operators in varying jurisdictions to ensure data is replicated and stored safely.

Open Outcry

Deepwaters uses an ‘Open Outcry’ system to broadcast select trading opportunities to subscribed participants. This acts as a push notification system for external takers and serves to improve the fill rate of orders.