Proof-of-Balance-Sheet Whitepaper (2023) 1–24

Decentralized Proof-of-Balance-Sheet*

Abstract.

We introduce Proof-of-Balance-Sheet (**PofBS**), a mechanism where a network of validators (acting as *decentralized auditors*) verify and attest to the solvency of a financial platform. **PofBS** can be generalized and applied across a wide range of decentralized (Defi) and centralized (Cefi) applications where assets and liabilities are pooled — such as exchanges, banking, lending-borrowing, insurance, investment funds and prediction markets — to provide users with higher transparency of the financial state of their counterparties and reduce the risks of loss of funds from negligence or misconduct.

As an industry-first practical use case, we also present how **PoBS** is implemented in conjuction with robust risk management and zero-knowledge proofs (ZKP) at *everything*, a next-generation derivatives exchange that combines the transparency of Defi with the performance of Cefi platforms.

JEL Classification: G32, O32, M42

1. Introduction

The cumulative innovations in blockchain technologies have brought tremendous promises but also missed opportunities in financial applications. For example, the advance of automatic market makers (AMMs) allows for the creation of on-chain decentralized exchanges for the first time ever, while the adoption of perpetual futures contracts by Cefi derivatives platforms allows for the creation of off-chain markets for essentially any quantifiable indices. Nevertheless, perhaps for both technical and ideological reasons, these revolutionary innovations often re-

*Version 0.8, August 2023.

main segregated in their respective Defi/Cefi silos, resulting in what we believe to be sub-optimal trade-offs between security, scalability and decentralization — the **trilemma** — where users frequently find themselves trapped in the dichotomy between secure-transparent-but-slow Defi and fast-scalable-but-opaque Cefi applications.

Unsurprisingly, there have been increasing demand from the blockchain community for a more pragmatic, *hybrid* approach to building financial applications, one where the focus is on the *user experience* rather than purist philosophy. It is under this context that the Proof-of-Balance-Sheet (**PofBS**) concept is born. The goal of **PofBS** is not simply to introduce yet another blockchain protocol, but to maximize the usefulness of existing technologies by applying them *selectively* to solve the *appropriate* problems, thereby maximizing user utility with iron-clad security, blazing-fast performance and a high level of decentralization.

2. Design Principles

Financial systems are, ultimately, platforms where funds change hands between users. Before the invention of blockchain, operating a *secure and performant* financial platform was essentially exclusive to large regulated institutions where user assets are pooled together, maintained with centralized ledgers and periodically audited by independent (and costly) auditors. For centuries past, such monopolistic/oligopolistic setup persisted despite the deadweight loss associated with imperfect competition (not to mention countless private and public financial crisis, see Reinhart and Rogoff (2009)), due to the natural benefits of economy-of-scale (network effect), risk-sharing (insurance effect), and perhaps more cynically, the perceived reliability stemming from 'too big to fail' reasoning. Traditional (Tradfi) centralization and financial pooling were *second best*.

Satoshi Nakamoto's invention of Bitcoin (Nakamoto (2008)) and the subsequent advancement in decentralized computing ushered in the web3 era that promises the democratization of financial applications. Despite the limitation imposed by the trilemma, we strongly appreciate that the current generation of Defi and Cefi platforms — differing primarily in terms of the degree of on-chain decentralization of user

assets — already surpass Tradfi platforms in performance and user-friendliness by leaps and bounds.

That said, we also strongly believe that we have not yet reached the efficient frontier afforded by *currently available* technology, since web3 innovations had often been applied in a blanket manner to solve problems they are not designed for. One prominent example relates to the degree of decentralization of financial transactions (such as trading) *vs* financial custody. Despite being separable conceptually, in practice virtually all Defi and Cefi applications tend to bundle them together: On Defi, on-chain transactions are conducted on non-custodial on-chain wallets. On Cefi, off-chain transactions are conducted on off-chain centralized pools. Another example relates to the usage of zero-knowledge proofs (ZKP). ZKP is a promising tool to potentially scale a blockchain's throughput without sacrificing its security. Unfortunately, we fear that platforms that use ZKP *en masse* inadvertently risk over-emphasizing the importance of *user privacy* at the expense of *platform transparency*. It would be ironic for an on-chain platform to become so complex as to be perceived as an on-chain blackbox, especially to the layperson.

In designing **PofBS**, we attempt to stand on the shoulder of giants and learn from centuries of Tradfi financial crises and the latest web3 innovations. **PofBS** *separates financial transactions and financial custody* by decentralizing Tradfi financial pooling with web3 permissionless auditing technology. Special attention is also paid to *where* and *how* such innovations are applied to ensure that every incremental choice brings us closer to the trilemma efficient frontier. App developers can then utilize **PofBS** in combination with robust risk management and ZKP to build hybrid platforms with Cefi-caliber asset transaction capabilities (since user assets are pooled) and Defi-caliber asset protection (safeguarded by decentralized validators).

2.1 Components of **PofBS**

We envision **PofBS** to be a general framework and used as a plug-and-play module for financial applications/platforms with on-chain asset pools as their custody solution. There are otherwise no specific system requirements. Figure 1 outlines the four main **PofBS** components, their respective roles and interactions with each other.

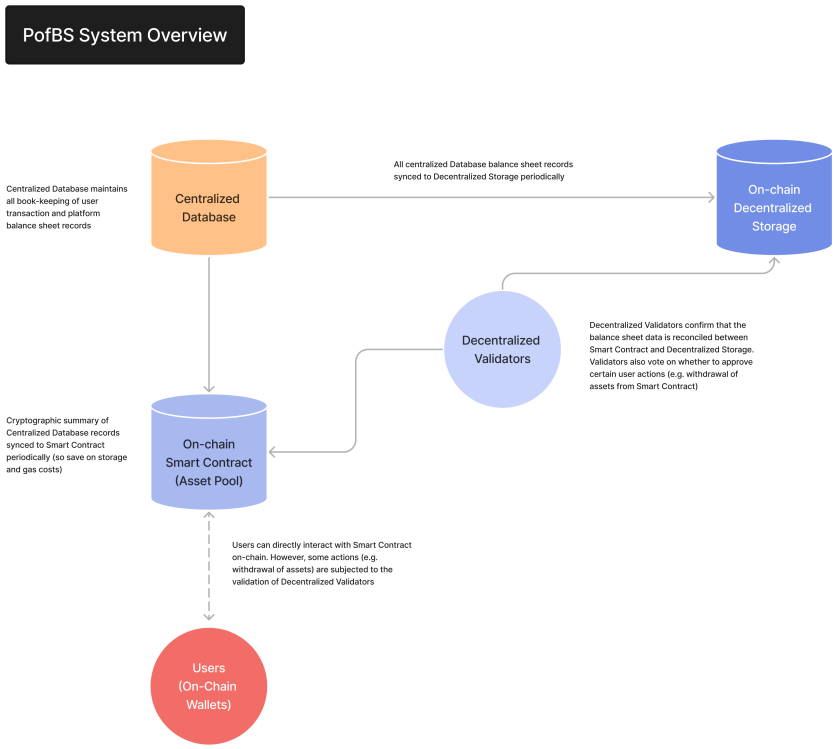

Fig. 1. **PofBS** Architecture

Custody Smart Contract

Under **PofBS**, user assets (platform liabilities) are stored in a on-chain Custody Smart Contract and pooled[1]. The Custody Smart Contract performs only basic functions such as user deposits and restricted withdrawals (e.g. subjected to decentralized validators' votes). All complex computations relating to the book-keeping of user assets are done in real-time by the Centralized Database (described next) and *periodically* synchronized on-chain in the same Custody Smart Contract and/or in separate Decentralized Storage (depending on storage costs and net-

[1] This is in contrast to non-custodial solutions where assets remain in a user's own on-chain wallet

work speed). For cross-chain applications, it is also possible to have multiple Custody Smart Contracts (one per network).

This design allows the separation of financial custody (handled by the smart contract) and financial transactions conducted on the platform (which determine the allocation of user asset and are recorded by the Centralized Database and then synchronized on-chain).

In the context of the trilemma, overall system throughput is dramatically improved over non-custodial setups because the most time-sensitive and computationally-intensive financial transactions are handled by the high-performance Centralized Engine instead of a decentralized network of nodes. The improvement in performance is not achieved through trade-offs in the overall *degree* of security and decentralization, but rather in the *frequency* of on-chain update of user asset balances which are relevant mainly during withdrawals. For most financial applications/platforms, user withdrawals are much less frequent and time-sensitive compared to regular transactions such as trading and staking. Moreover, since all user transactions (except deposits and withdrawals) are processed by the Centralized Engine, users do not need to pay gas fees or fear having their transactions front-run by MEV bots. As a result, we believe that the **PofBS** system flow results in substantial improvement in the overall user experience.

Centralized Database

The **PofBS** Centralized Engine is expected to have high throughput ($\geq$ 50,000 transactions-per-second), be easily upgradable and use a Centralized Database to maintain all user/system account balances and activities. Periodically[2], book-keeping information, user withdrawals and any information that are required by the decentralized validators (e.g. timestamps, cryptographic proofs) are also synchronized on-chain. Specifically, full user records are stored on Decentralized Storage, while only the summary (e.g. permalinks of network storage files, Merkle root hash of underlying data) and other necessary data (e.g. pending user withdrawals) are simultaneously stored in the memories of Custody Smart Contract.

[2] On the Ethereum mainnet, our goal is to complete one **PofBS** epoch in less than 10 minutes. On more scalable networks, the update frequency is expected to be in the order of seconds.

The **PofBS** Centralized Database stands out among centralized setups due to its high on-chain transparency and, in some cases, has higher transparency than DeFi platforms with blackbox-like smart contracts.

Decentralized Storage

A key component of the **PofBS** system flow is the *permanent* storage of user balances and activity records on-chain. Given the prohibitively high storage costs on the Ethereum mainnet and possible need to support cross-chain applications, the **PofBS** Decentralized Storage is expected to be deployed on storage-focused decentralized networks such as Arweave and IPFS. These permanent records are considered the source of truth when the Decentralized Validators verify and vote for/against the solvency of the platform (see below), which in turn dictates whether funds can be withdrawn from the Custody Smart Contract.

Since user records are stored permanently on-chain, great care must be taken to balance the trade-off between platform transparency and user privacy. Under **PofBS**:

- *User Balances* are anonymized and saved unencrypted (in plaintext) to maximize platform transparency and give clear evidence to the general public about the solvency of the platform. Since all blockchain wallets balance *and* transaction history are public, saving unencrypted user balances on-chain is at least on-par with existing Defi applications in terms of user privacy.

- *User Transactions* are encrypted and saved in the form of zero-knowledge proofs (e.g. ZK-STARK based on Ben-Sasson et al (2018)) on-chain to protect individual user's privacy and intellectual property (e.g. proprietary trading strategies), while providing cryptographic proofs that all user transactions are indeed valid.

Decentralized Validators

The **PofBS** Decentralized Validators are the crucial link between Custody Smart Contract and Decentralized Storage. As a group, they serve as a *decentralized auditors* that review platform solvency and approve

the processing of withdrawals from the Custody Smart Contract based solely on records on the Decentralized Storage.

During every synchronization **PofBS** epoch, Decentralized Validators first independently verify that on-chain data are valid and reconciled between the Custody Smart Contract and Decentralized Storage[3]. They then vote on the whether to approve (based on 2/3 majority) the Custody Smart Contract to trigger user withdrawals. In other words, *no fund can leave the Custody Smart Contract without a vote by the Decentralized Validators.*

Eligibility of Validators: Similar to Ethereum's Proof-of-Stake (PoS) consensus mechanism, ideally there would be a large number of small validators, each having staked interest in the long-term viability of the financial platform (instead of short-term profits just based on activities on the platform).

Validity of Data: While each financial application may have its own specific definition of data validity, the following necessary conditions should be jointly satisfied:

- Summary (e.g. permalink, Merkle root hash) on Custody Smart Contract consistent with data stored on Decentralized Storage
- Total assets on Custody Smart Contract $\geq$ Total liabilities (sum of user balances)
- All individual user balance ≥ 0
- All individual user withdrawal request $\leq$ user balance
- No duplication or other data error

Incentives of Validators: Decentralized Validators are incentivized to vote honestly by a consensus mechanism similar to Ethereum's Byzantine Fault Tolerance (BFT)-style PoS (Ethereum (2023)). Validators will be randomly assigned rewards if their votes are in line with the general vote outcome but risk losing their staked asset otherwise.

[3] The verification process occurs off-chain, and the platform is expected to provide a standard script for validators to run, similar to blockchain nodes running the respective blockchain clients.

2.2 Dissecting Security

We strongly believe adopting the **PofBS** framework describe above would significantly improve the overall security of financial platforms with pooled assets. In light of the diverse ways in which a financial platform may potentially fail — from outright theft of customer assets of Cefi platforms, to hacks of sophisticated Defi platforms, to *rug-pulls* of questionable platforms — we devote this section to discuss the four dimensions of platform security and how **PofBS** could contribute to improvements in each.

Balance Sheet Security

Balance sheet (state) security means an absence of solvency issues at all times, or simply put, 'funds are safe'. Specifically, both conditions below must hold true at all times:

- At the aggregate platform level, total assets $\geq$ total liabilities[4]
- At the individual user level, net equity balance ≥ 0[5]

What it requires: Platform operator eliminates solvency risks arising from both negligence (such as poor risk management and over-leverage) or misconduct (such as embezzlement and theft).

*How **PofBS** helps:* A platform can utilize **PofBS** to publicly and transparently prove its balance sheet security (the result of prudent risk-management, etc) on-chain without disclosing the workings of its internal systems, while also eliminating the possibility of off-chain/off-balance-sheet liabilities. Moreover, the on-chain transparency of **PofBS** also implies a strong deterrent force for bad actors to initiate invalid transactions, since any invalid state changes will likely be caught as well.

[4] Note that most Proof-of-Reserves (PoR) adopted by Cefi exchanges only attest to total platform assets without reference to total platform liabilities. Given the inherently off-chain (or even off-balance-sheet) nature of their platform liabilities, the current generation of Cefi platform will likely struggle to prove their balance sheet security.

[5] This condition is especially important for platforms with leverage (see Appendix A3), where the safety of any individual user account can only be guaranteed if *all* accounts are safe. This is because users with negative equity balances are *borrowers* of the platform. All remaining users suffer if these borrowers default on their obligations to the platform.

Transaction Security

Transaction (state transition) security means the absence of invalid transactions (such as double-spending, unfair ordering of transactions) that change the balance sheet (state) of the platform in ways that violate general-accepted principles of fairness.

What it requires: Platform operator has proper accounting/book-keeping capabilities, robust internal control and fair order management system that minimize the risks of invalid transactions happening and maximize the risks of catching invalid transactions that occurred due to unforeseen circumstances.

*How **PofBS** helps:* A platform can utilize **PofBS** and ZKP to publicly prove its transaction security (the result of proper internal control, etc) on-chain, without disclosing the actual transactions nor the workings of its internal systems.

Platform Security

Platform security means the absence or prohibitively high cost of *unauthorized* transactions.

What it requires: Pure Defi platforms use cryptographic techniques (requiring the signing of every transaction with private key) to solve this issue. That said, even Cefi platforms are incentivized to improve overall platform security due to the ease with which users can identify, report or even publicize unauthorized transactions, with high reputational damage to Cefi platform operators.

*How **PofBS** helps:* **PofBS** improves overall platform transparency, hence increasing the incentives for platform operators to enhance their platform security.

Systemic Security

Systemic security refers to the proper functioning of a platform as a fair and efficient *market*. It also concerns whether a platform produces positive *externalities* to the broader web3 economy (instead of negative externalities such as contagion risks). Considerations of systemic security may include:

- Is the market competitive, liquid and efficient?
- Is the market 'fair' with no asymmetric information nor bias against individual users?
- Does the market dis-incentivize 'wild west' behaviors such as front-running and wash-trading?
- Is the market prone to extreme boom-bust cycles?
- Is the market robust enough to withstand the contagion risks from the failure of individual platforms[6]?

Unfortunately, despite the incredible progress made so far, the nascent web3 markets still failed to satisfy many of the above criteria. We are hopeful that **PofBS** presents a positive step in the right direction, by incentivizing platforms to improve their market functions (e.g. proper risk management, robust internal control, prudent leverage) under public, decentralized scrutiny.

3. First Use Case: *everything* Exchange

We follow the conceptual discussion of the **PofBS** design principles with a showcase of how **PofBS** enables *everything*, a next-generation hybrid derivatives exchange, to combine the transparency of Defi with the performance of Cefi exchanges.

3.1 Current Problems

The current generation of web3 derivatives exchanges have made tremendous progress over Tradfi derivatives exchanges by breaking down participation barriers, reducing market frictions and introducing 24-7 trading. Nonetheless, Cefi and Defi exchange users are often left wanting for more because of, in our views, inefficiency in the *manner* with which web3 innovations are implemented.

Figure 2 illustrates the existing problems with Cefi and Defi exchanges. Interestingly, there seems to be a historical tendency for them to solve *each other's* problems, with highly complementary pros and cons:

[6] See Appendix A3 for an example of the financial risks to exchanges from leveraged trading

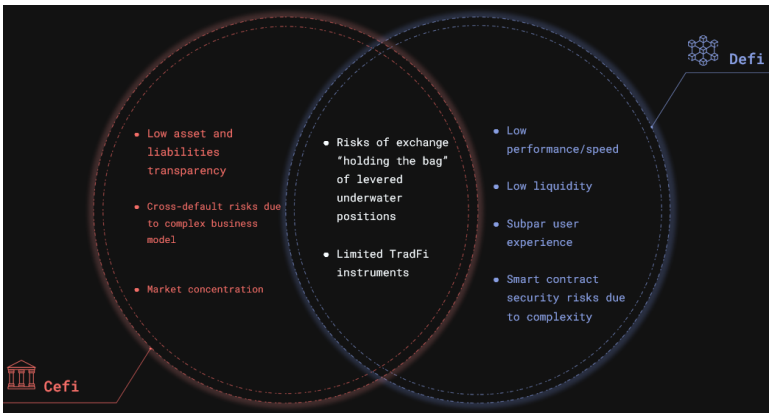

Fig. 2. Problems with Derivatives Exchanges

Cefi Exchanges

- *Pros:*
  - ⋆ Generally high-performance
  - ⋆ For most users, Cefi exchanges also serve as the 'on-ramp/off-ramp' gateways of the crypto world
- *Cons:*
  - ⋆ Low transparency in balance sheet, transaction, platform and systemic security

Defi Exchanges

- *Pros:*
  - ⋆ High transparency in transaction and platform security
- *Cons:*
  - ⋆ Generally low-performance
  - ⋆ Balance sheet security is low for Defi exchanges with complex smart contract designs
  - ⋆ Low systemic security (e.g. risks of front-running by MEV bots, contagion risks)

Last but not least, even though Cefi and Defi derivatives exchanges have widely adopted perpetual futures contracts[7] as the main trading instrument — and thus theoretically should support trading in virtually any quantifiable indices — they have mostly focused on crypto derivatives with limited offering on Tradfi and alternative assets.

3.2 The *everything* Solution

The contrasting pros and cons of Cefi and Defi exchanges described above are, in our view, a result of the indiscriminate application of centralization/decentralization techniques to *both* custody and trading. The *everything* approach is instead a hybrid one built on pragmatism: to maximize user utility by *separating* custody and trading.

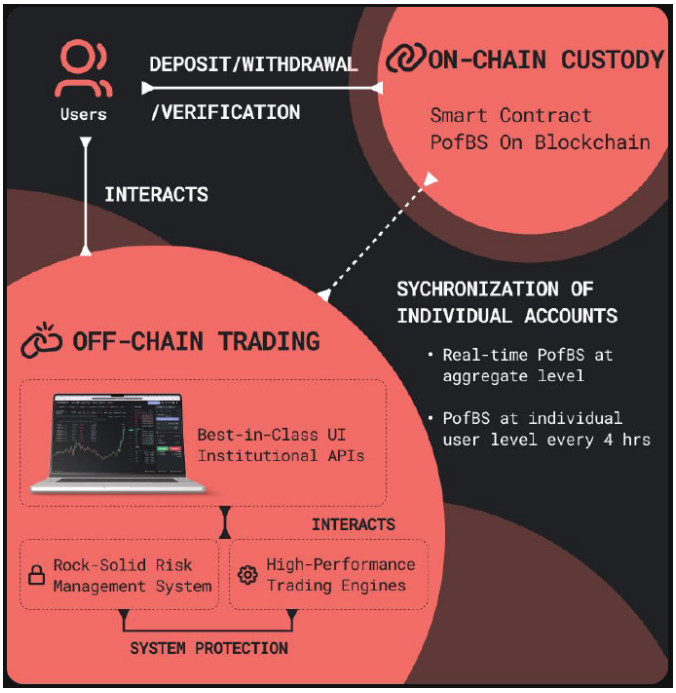

Fig. 3. The *everything* Solution

[7] See Appendix A1 for more background information.

Custody: Decentralized PofBS

All user and exchange assets are held and pooled in the on-chain Custody Smart Contract, with account allocation maintained by the Centralized Engine on a real-time basis. While deposits can be made at any time, withdrawals are gated by the **PofBS** process: periodically (every 30 minutes initially), a snapshot of the complete *everything* balance sheet — containing plain-text representation of anonymized user balance and withdrawal requests[8] — is uploaded to the Decentralized Storage, with summary uploaded to the Custody Smart Contract. Withdrawals are only processed after the Decentralized Validators verify and approve the **PofBS** snapshot.

Trading: High-Performance Centralized Engine

All computationally-intensive and time-sensitive tasks such as user trades, internal transfers, accounting and risk management are processed by a high throughput, high availability Centralized Engine, in a private and anonymous manner that protects users' intellectual properties. Positions and account balances are updated and reflected on a real-time basis, so are any liquidations. Since all user transactions are handled off-chain, there are no gas fees involved nor opportunities for MEV bots to front-run user transactions. Last but not least, the trading of all perpetual futures contracts on *everything* are 24-7, even for Tradfi assets with periodic market closure[9].

Underpinning Security: Risk Management

everything, as a derivatives exchanges, supports leveraged trading through collateralized perpetual futures contracts. To ensure the solvency and operational continuity of *everything* under system-wide leverage and even the most extreme market conditions, we design a multi-prong risk management system based on battle-tested principles learnt from centuries of financial crises.

---

[8] We plan to add ZKP of the validity of all user transactions in future versions.

[9] See Appendix A2 for a discussion on the sources of market liquidity during after-hour or for new markets.

3.3 **PofBS** and Custody Solutions of *everything*

In line with the specification in Section 2., the *everything* Custody Smart Contract's two main functions are accepting deposits and processing withdrawals subjected to the Decentralized Validators' votes and approval. Computationally-intensive and time-sensitive functions such as book-keeping and trading are delegated to the Centralized Engine. The simplicity of the smart contract makes it easily auditable and, from a platform security perspective, gives it a small attack surface.

Deposit Flow

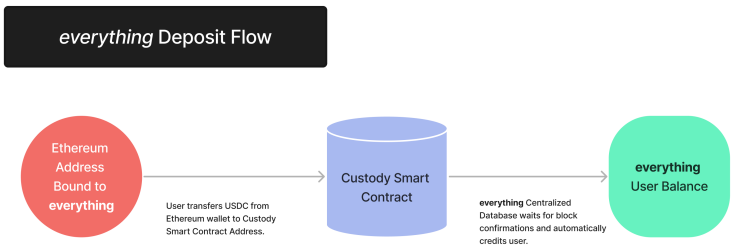

Fig. 4. *everything* Deposit Flow

Users deposit into *everything* by directly transferring funds to the Custody Smart Contract from the on-chain wallet bound to their accounts (Fig. 4). The Centralized Engine would then detect and recognize the on-chain deposit transaction and credit the users' accounts in the Centralized Database accordingly. A significant security advantage comes from the fact that users are *pushing* funds into *everything* and retain complete control over their wallets during the entire deposit process. In contrast, many Defi exchanges have designs that request users to approve the exchange smart contracts to *pull* funds (in some cases unlimited funds) from their wallets, implicitly asking users to surrender the control of their wallets.

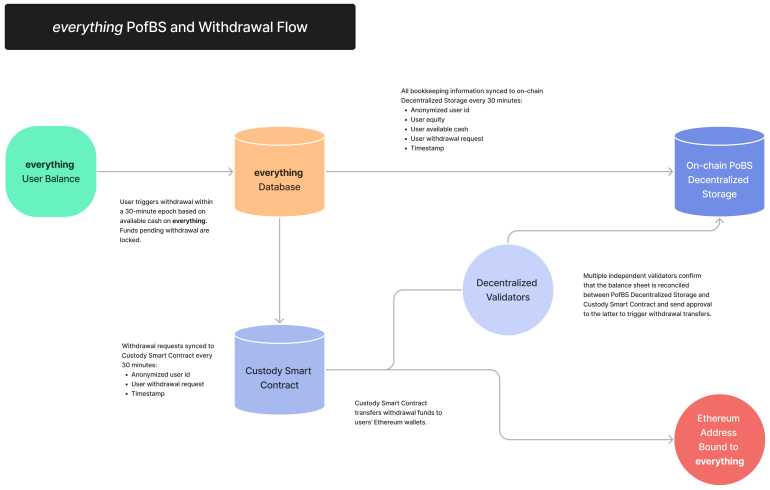

Fig. 5. everything **PofBS** and Withdrawal Flow

***PofBS** and Withdrawal Flow*

Periodically[10], *everything* conducts a complete **PofBS** cycle. Users can submit withdrawal requests between these cycle epochs based on their real-time withdrawable balances in the Centralized Database. All funds pending withdrawal are immediately set aside and deducted from the withdrawable balance. Fig. 5 summarizes the following:

1. Centralized Engine generates *plain-text* snapshot containing:
   - ⋆ User anonymized ID
   - ⋆ User wallet address
   - ⋆ User total balance
   - ⋆ User withdrawable balance
   - ⋆ User withdrawal request

[10] At the initial phase, a **PofBS** cycle happens every 30 minutes to give enough buffer for unforeseen delays. Going forward, we hope to complete a cycle in less than 10 minutes and improve transaction security further by supplementing plain-text balance sheet information with ZKP of user/system transactions between epochs.

- ⋆ Timestamp of the snapshot

2. Centralized Engine uploads snapshot (*without* user wallet addresses) to Decentralized Storage and publishes on *everything* website the corresponding file permalink (CID)

3. Centralized Engine generates the **Global PofBS Merkle Proof (GPMP)** from the complete snapshot file, which include a joint test that all the following conditions are TRUE:

- ⋆ For all users:
  - ⋆ User total balance ≥ 0
  - ⋆ User withdrawable balance ≥ 0
  - ⋆ User withdrawal request ≥ 0
  - ⋆ User withdrawable balance $\geq$ withdrawal request
- ⋆ Total assets on Custody Smart Contract $\geq$ total liabilities (sum of user total balances)
- ⋆ No duplicated records
- ⋆ Timestamp and CID consistent with each other

4. Centralized Engine uploads snapshot summary to Custody Smart Contract:

- ⋆ **GPMP**
- ⋆ User (by wallet address) withdrawal request
- ⋆ Timestamp and CID of the snapshot

5. Decentralized Validators receive the mapping file linking anonymized user ID and wallet address[11]

6. Decentralized Validators merge on-chain snapshot and mapping file and generates **GPMP** from scratch

7. Decentralized Validators verify that:

- ⋆ All conditions in Step 3 are TRUE

[11] Note that the general public can access *anonymized* balance sheet data on Decentralized Storage permalink. Mapping file is only accessible by Decentralized Validators.

⋆ All data (including **GPMP**) saved in Custody Smart Contract are identical to/consistent with those generated from data stored in Decentralized Storage

8. Decentralized Validators vote on the validity of the snapshot

9. Custody Smart Contract executes and distributes the withdrawal requests stored in memory subjected to approval vote by 2/3 majority of Decentralized Validators

3.4 Centralized Engine of *everything*

The *everything* Centralized Engine is built on a state-of-the-art architecture (Fig. 6) with high availability/disaster recovery (HA/DR) and supports unique trade features that cater to a wide range of traders.

Life-Cycle of Trade Orders

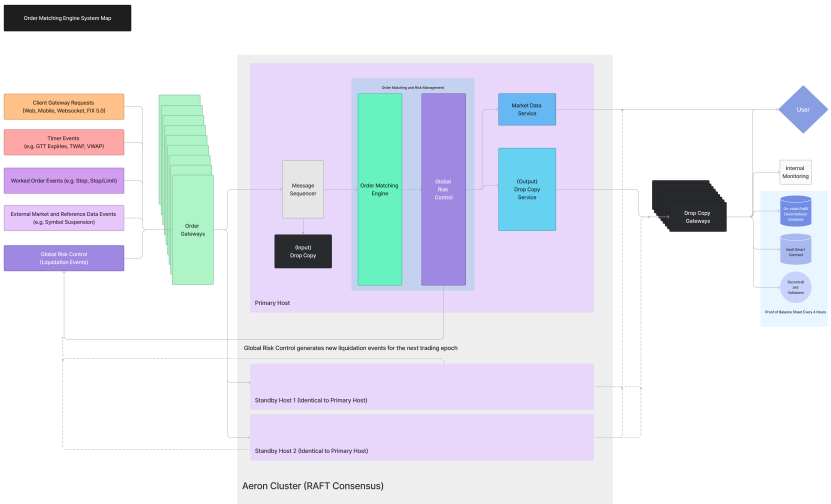

Fig. 6. Order Matching Engine Flow

1. Multiple user and system (liquidation) orders fed to the Order Matching Engine

2. Orders matched and executed with a *deterministic* algorithm

3. Upon completion of order execution, updated system states (limit order book, user positions and account balances) fed to the Global Risk Control

4. Global Risk Control simultaneously:

   a. Generates new potential liquidation orders based on the updated system states

   b. Feed updated system states to downstream modules including Market Data Service, HA/DR, and Drop Copy Service (which feeds external users, Internal Monitoring, and **PofBS**)

Unique User Features

- *FIX 5.0 Support:* industry standard for professional Tradfi traders
- *Auto-roll:* automatically re-strike open positions (at discounted fees) when the unrealized profit-and-loss (PnL) exceeds predefined thresholds to take profit or reduce the risks of liquidation
- *Novation:* migrate open positions between accounts.
- *Batch Order:* upload batch order via UI, API or CSV files. Can be used in combination with TWAP/VWAP orders
- *Transaction Cost Analysis (TCA):* powered by AI and big data
- *Volume-Weighted-Average-Price (VWAP) Order*
- *Time-Weighted-Average-Price (TWAP) Order*
- *Visual Trading:* one-click on-screen trading tool
- *Social Trading*
- *Real-time News Feeds*
- *Flexible Register/Login:* with wallet address or email/password combination
- *Quantzone:* complimentary trading toolkits such as arbitrage/market-making bots, exploratory data analysis (EDA) tools and algo/backtesting environment

3.5 Risk Management of *everything*

everything supports leveraged trading in perpetual futures contracts. To minimize the solvency risks arising from system leverage[12], we designed a two-tier liquidation system (Fig 7) to protect all users from extreme market conditions, in addition to measures that encourage users to reduce their leverage in the first place.

Two-Tier Liquidation System

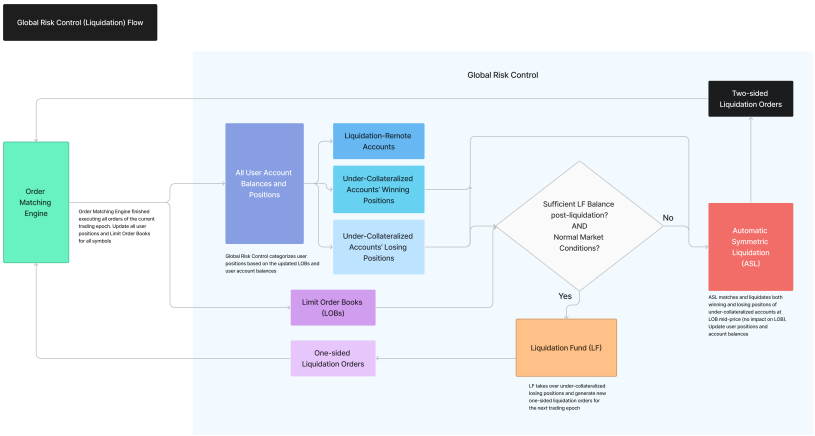

Fig. 7. *everything* Two-Tier Liquidation Flow

Under normal market conditions, the Liquidation Fund (LF) is used to facilitate one-sided liquidation of under-collateralized losing positions. The Liquidation Fund is funded with a portion of the trading fees and will absorb all PnL associated with the one-sided liquidation process.

Under extreme market conditions and/or when the Liquidation Fund is depleted (or close to being depleted), the liquidation of under-collateralized losing positions will be under the Automatic Symmetric Liquidation (ASL) mechanism, where they are matched with the corresponding most under-collateralized winning positions i.e. both losing- and winning- positions are simultaneously liquidated at the market

[12] See Appendix A3 for a more in-depth discussion.

mid-price. This eliminates potential market impact (in a likely volatile market) and PnL from the liquidation process, shielding the Liquidation Fund and *everything* from potential losses and ultimately protecting all users[13]

ASL, once activated, will remain active until market conditions stabilize and the Liquidation Fund balance recovers to a normal level.

Incentivize Responsible Trading Behaviors

Ultimately, the best way to reduce financial risks to *everything* stakeholders is to encourage all users to trade responsibly i.e. by incentivizing users to reduce their leverage.

To that end, excess capital in the Liquidation Fund (above a pre-defined ratio vs Open Interest) will be periodically distributed to users who are the most over-collateralized. Moreover, when the ASL mechanism is active, users who post more collateral relative to those with opposite positions are in effect subsidizing the other side's risk-taking. Therefore, during those times, such relatively-over-collateralized (ROC) users are compensated with a periodic interest, paid by users who are relative-under-collateralized (RUC).

4. Future Roadmap

Given the modular architecture of **PofBS**, there are various potential ways to improve each components and apply **PofBS** in conjunction of other promising technologies. For example:

- Equip Decentralized Validators with AI-powered tools for the detection of fraudulent transactions or suspicious accounts
- Give higher priority to Decentralized Validators who submit Proof-of-Human-Identity to further democratize the decentralized auditing process and reduce the risks of Sybil attacks
- Create a generalized L1 blockchain network based on **PofBS** and promote **PofBS-as-a-Service**, enabling cross-chain asset management and fund administration (e.g. mark-to-market services).

[13] Note that users with winning positions can avoid being liquidated under ASL by opting to auto-roll their positions.

A Appendix

A1 Perpetual Futures Contracts

A futures contract is a binding bilateral financial contract between two parties (buyer and seller). Both parties agree and are obligated to exchange an underlying asset at a set price on a predetermined future date (settlement date). On the settlement date, the two parties fulfill their obligation to buy/sell the underlying asset and incur profit/loss. In practice, most futures contracts are not signed bilaterally but through a trusted middleman such as an exchange i.e.

- Buyer enters a long position against the exchange and
- Seller enters the mirroring short position against the exchange

This allows both the buyer and seller to later transfer their open positions to other parties at the prevailing futures price. In the presence of market arbitrageurs, futures price eventually converges to the spot price of the underlying asset on the settlement date. Furthermore, futures contract are often deployed with leverage: both buyer and seller can enter the full position by posting partial margin/collateral upfront. Should the loss exceed the maintenance margin requirement, a "margin call" occur and the losing position holder is required to post additional collateral, failure to do so would result in position liquidation.

A perpetual futures contract, invented by Robert Shiller (Shiller (1993)) and popularized by crypto derivatives exchanges, is a futures contract with no settlement date i.e. the buyer and seller cannot realize their PnL based on contract settlement, but only through the transfer of their open positions to other parties (at the prevailing perpetual futures price). The lack of a settlement date means that perpetual futures price need to be anchored to the underlying spot price with a special mechanism, the funding rate mechanism:

When the perpetual futures price is above the spot price, traders holding long positions would pay a funding fee (= notional of position x funding rate, a rate proportional to the difference between perpetual futures price and spot price) to those holding short positions. This increases the costs of holding long positions and benefits of holding short

positions. Conversely, when the perpetual futures price is below the spot price, traders holding short positions would pay a funding fee to those holding long positions, hence incentivizing traders to hold long positions instead of short positions.

In short, the funding rate mechanism rewards users who help the futures market to converge to the underlying and penalizes those who do the opposite. Funding fees are usually calculated and transferred periodically (e.g. every hour) to ensure ongoing anchoring of the perpetual futures price to spot price. It is worth pointing out that a perpetual futures exchange's role in the funding rate mechanism is merely as a neutral calculating agent.

A2 Liquidity Sources of After-Hour/New Markets on *everything*

Conceptually, after-hour trading of Tradfi assets is similar to trading of new alternative assets (e.g. NFT index) – in both cases, *everything* becomes essentially the *only* trading venue. Even though *everything* being the lone one trading venue may present challenges for some high-frequency market markets (which are generally strictly market-neutral and hedge their directional exposures on multiple venues), the act of creating a new venue for under-served markets would likely attract liquidity supply from natural hedgers and speculators (profit-takers). For example, in commodities there are natural hedgers on both long (e.g. commodity consumers) and short (e.g. commodity producer) sides. Similar natural hedgers can be identified in equities, FX, and even alternative asset classes like NFTs. Speculators also have incentives to leave limit/stop orders to protect their PnL during after-hours.

Large hedgers in each market could be solicited to supply their respective *one-sided* liquidity (i.e. long hedgers to submit bids, short hedgers to submit offers) which would be matched against each other or speculators. Bootstrapping from these anchor liquidity positions (which tend to be less dynamic), *everything* may become the *de facto* benchmark for after-hour markets and move closer to the 'liquidity begets liquidity' positive feedback loop.

Admittedly, liquidity during after-market hours will likely be worse compared to market-hours. To incentivize market participation and

encourage price discovery, we could potentially relax trading requirements for market makers, adjust funding rate calculation parameters, or reduce trading fees during after-market hours. Higher funding rate volatility would also be a likely result of lower market liquidity during after-market hours. That said, funding rate also serves as a tool to *attract* investors to participate in the market (in the opposite direction of the index premium), while at the same time making it more costly for malicious players to manipulate the market.

From a risk-management perspective, users should also be alerted to the heightened risks of liquidation before the end of market-hours.

A3 Risks to an Exchange that Supports Leveraged Trading

An exchange that does not allow leveraged trading is conceptually identical to the betting pool in parimutuel betting (zero-sum game) and is fully immune from market price movements, since all market risks are shared between the exchange users only.

An exchange that supports leveraged trading deviates from the parimutuel betting model, since the bets users place against each other are not fully collateralized i.e. any user account may potentially incur losses beyond the posted collateral. Exchange usually employ one-sided liquidation to manage their financial risks: losing (but not winning) leveraged positions would normally be liquidated before the users' collateral are exhausted. Under normal market conditions, one-sided liquidations are generally lucrative for the liquidators, because they are able to acquire the losing positions at a favorable price (i.e. buy low, sell high) and subsequently offload the position to the market. Liquidators are compensated for temporarily holding the liquidated positions.

Under extreme market conditions, a sudden and extreme market price "gap" move could overwhelm even the most deep-pocketed liquidators e.g. they may not be able to offload their rapidly building positions without losing money. In such scenarios, it may be possible for users' losing positions to not get liquidated in time, and their balances become negative. If these users fail to make up for the negative balances, the exchange will suffer a financial loss since it is still responsible for paying the full balance owed to users on the winning side. Such *mar-*

gin breaches occur frequently on even regulated Tradfi exchanges[14]. To make matters worse, some crypto exchanges engage with related parties as liquidators, and losses borne by the liquidators will further erode the financial integrity of the exchanges themselves.

In short, for any exchange (Tradfi or crypto) with *system leverage*, there is always a non-zero probability of an adverse market event so extreme that it causes the exchange to exhaust all available financial resources and go bankrupt. While system leverage has already wrecked havoc in the Tradfi world for centuries, the risks to the crypto world is even more worrisome due to the lack of "buyers of last resort". If a crypto exchange goes bankrupt, all exchange users are impacted and losses are socialized.

In our view, *everything*'s decentralized **PofBS**, built on a robust and multi-prong risk management system, represents the first quintessential web3 solution to the centuries-old system leverage problem.

References

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf

Reinhart, C. M. and Rogoff, K. S. (2009) *This Time is Different: Eight Centuries of Financial Folly.* Princeton University Press

ethereum.org (2023) *Ethereum Proof-of-Stake Documentation.* https://ethereum.org/en/developers/docs/consensus-mechanisms/pos

Ben-Sasson, E., Bentov, I., Horesh, Y. and Riabzev, M. (2018) *Scalable, Transparent, and Post-Quantum Secure Computational Integrity.* Cryptology ePrint Archive

Shiller, R. J. (1993) *Measuring Asset Values for Cash Settlement in Derivative Markets: Hedonic Repeated Measures Indices and Perpetual Futures.* The Journal of Finance, 48(3), 911-931

[14] See https://www.fia.org/margin-breaches for recent statistics.