Open Source Exchange Network

The Internet of Value Exchange

Problem Statement

Bitcoin solved the **trust problem for transfer of value**, and allows parties to make payments peer-to-peer, without a central trusted party.

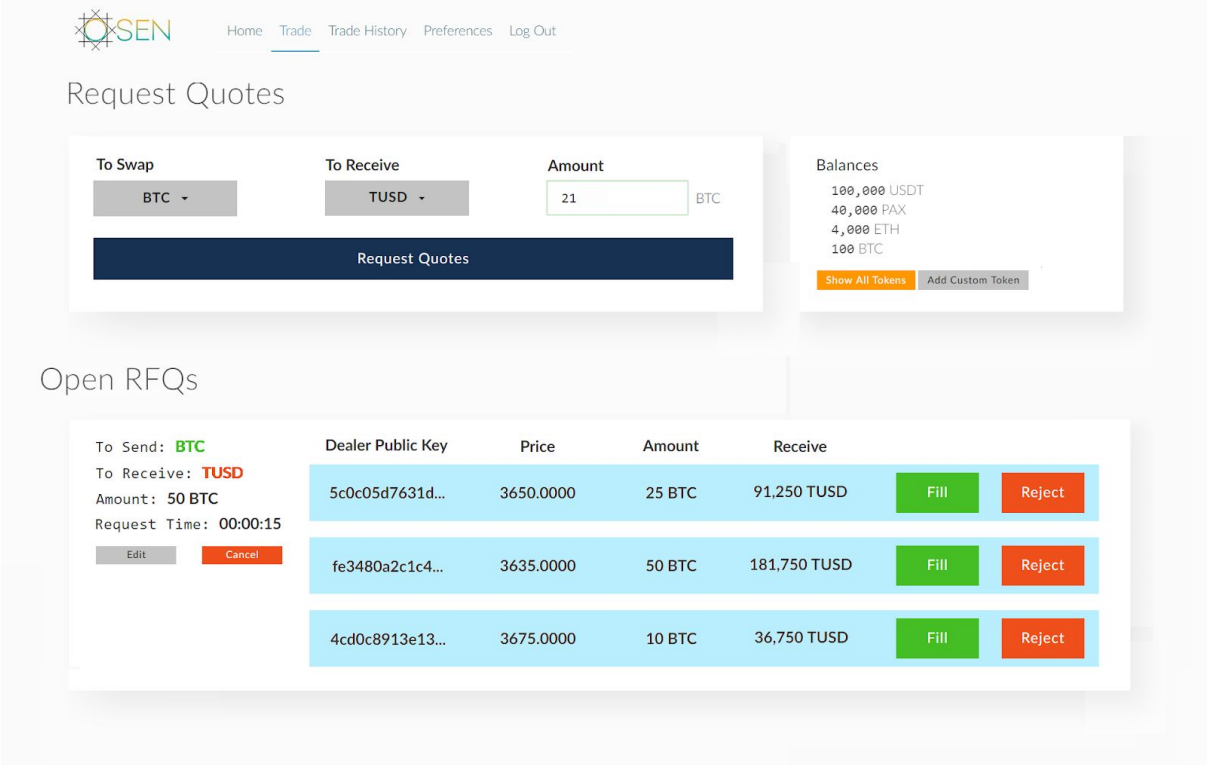
OSEN solves the **trust problem for exchange of value**, and allows parties to exchange value peer-to-peer, without a central trusted party.

Previous approaches, such as centralized exchanges and OTC groups, suffer from major flaws such as counterparty risk, limited, fragmented or ghost liquidity, and extended settlement times.

Existing decentralized exchanges resolve issues with counterparty risk but have even more limited liquidity, are inflexible in feature set, and can only trade assets on the same blockchain.

Only OSEN allows for peer-to-peer, cross-chain, decentralized exchange, solving the issues of risk, liquidity and flexibility and achieving a quantum leap in digital asset exchange.

Product



OSEN solves a core function of blockchains: value exchange. Through OSEN, two parties can swap assets, including Bitcoin, Tether, Ether, ERC20 tokens and many more, without a trusted third party or trusting the counterparty.

OSEN provides two main benefits:

- **Lower risk:** OSEN does not require trust, minimizing risk of loss of funds;
- **Higher liquidity:** As parties need not trust each other to trade, OSEN breaks down trust barriers and enables the entire market to trade with each other.

Instead of a single trusted platform, every OSEN node has its own order book, wallet addresses and matching engine. Peers connect using encrypted messaging and transmit orders directly, giving autonomy over data privacy.

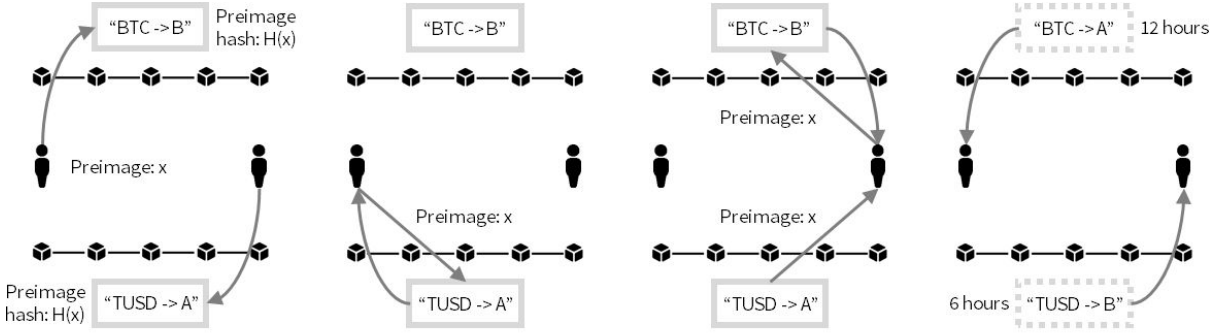
As a product targeted towards institutional users, regulatory compliance is a key aspect of OSEN. Each node stores KYC and other information locally, and regulatory requirements are generated dynamically based on the context of the trade. This allows for a high degree of both flexibility and privacy, and allows OSEN to adapt to local requirements while providing a regulated environment for institutional trading.

Crypto Settlement

Most existing OTC platforms settle through “second settle”, where the funds are sent to the liquidity provider first, or through a trusted 3rd party. This 3rd party can be the platform itself, an escrow or trust service, or a trusted individual. Regardless of the role, the high risk from giving them full custody of funds greatly increases the requirements for trust, while still leaving the opportunity for loss of funds.

Due to the unique programmable status of digital assets, various protocols allow counterparties to settle directly with each other, with minimal risk of loss of funds. For swaps on the same chain, an implementation of the 0x or Swap protocol enables atomic swaps.

For cross-chain swaps, we introduce the OSEN protocol, which uses Hashed Timelock Contracts (HTLCs), which are special transactions that guarantee one outcome when a specific hash is generated (such as sending a certain number and type of tokens to a specific address), and another after a certain period of time (such as returning those tokens to the initial sender). Essentially, both counterparties use the blockchain as escrow to set up each side of the trade, then use a shared secret to initiate the transfer of funds on both sides. Otherwise, both parties get their funds refunded after a certain amount of time.



#1: Issue HTLC
Both parties broadcast *hashed timelock contracts* to each other’s addresses, locked with the same hash.

#2: Redeem 1st HTLC
The liquidity taker redeems their side of the trade by broadcasting the preimage on-chain.

#3: Redeem 2nd HTLC
The liquidity provider picks up the preimage from the blockchain and redeems their side of the trade.

Recovery
If the preimage is never broadcast, either party refunds their transaction after the timelock runs out.

A full specification of this protocol is available in the appendix.

By using HTLCs, which are the foundation for layer 2 networks like Lightning and Celer, OSEN is drawing upon shared research within the blockchain space to improve security.

Transaction fees are taken from both sides of the trade directly from each HTLC, ensuring payment for OSEN, and also allowing guaranteed commissions for OTC brokers, thereby incentivizing them to bring order flow to the network.

Market Size

OSEN has a simple business model. We charge a 0.1% transaction fee, and provide custom cloud services to enterprise users. We primarily target the OTC market (especially BTC-USDT and BTC-TUSD), which is an established market with steadily increasing volume.

We estimate the total market to be **$650 billion in annual transaction volume in 2018,** and to grow to **$17.5 trillion in annual volume by 2021.** This is based on the following:

- OTC trading volume is difficult to estimate. Some statistics include:
    - Cumberland traded more than $20 billion in 2017[1]
    - As of June 2018, Circle trades around $4 billion per month, adding up to $48 billion per year, while Genesis Trading trades around $1.5 - $2 billion a month, adding up to around $20 billion a year[2]
    - Octagon Strategy traded around $1.5 billion a month in December 2017, adding up to $18 billion a year[3]
    - If we assume Cumberland, Circle, Genesis Trading and Octagon's trading volumes increased in 2018, and assume these four trading desks account for 50% of the market, we get a total addressable market of $275 billion in trading volume.
- On-exchange volume totaled around $7.3 trillion in 2018[4]
    - The users that trade on exchange and withdraw their tokens are the addressable market for OSEN. If we assume 5% of all trading volume is with delivery, that implies an addressable market of around $375 billion.
- Adding the two markets together, we estimate the **total addressable trading volume** as **$650 billion** in 2018.
- Based on 0.1% transaction fees (market rates range from 0.5% to 3%), the **total potential revenue** in 2018 is **$650 million**.
- Assuming **3x growth per year** from 2018 to 2021 (in line with comparisons between 2017-2018, and significantly lower than average growth between 2009-2018, which is over 10x per year), trading volumes in 2021 would be **$17.5 trillion.**

---

[1] https://www.wsj.com/articles/bitcoins-trading-star-is-chicago-high-speed-firm-that-nods-to-the-grateful-dead-1511787600

[2] https://www.newsbtc.com/2018/04/03/over-the-counter-cryptocurrency-exchanges-see-increased-volume-following-high-profile-attacks-on-online-exchanges/

[3] https://www.prnewswire.com/news-releases/asia-pacifics-largest-cryptocurrency-brokerage-octagon-strategy-appoints-wayne-trench-ceo-julia-pang-coo-founder-and-md-dave-chapman-named-chairman-300602458.html

[4] https://www.ccn.com/cryptocurrency-trading-volume-to-see-50-growth-in-2019-research/

Market Strategy

Connecting to OSEN is as easy as integrating an API, allowing the user base to be grown rapidly while maintaining low marginal cost and rapidly establishing network effects. The result is an Uberfication of exchange, where OSEN becomes the largest network for exchanging digital assets without itself being an exchange.

Based on market feedback, we have identified the following use cases for OSEN:

Bitcoin OTC

BTC trading pairs continue to be the most highly traded on the OTC market. OSEN addresses the following user profiles:

- **Buy-side Market Participants:** For funds, family offices and trading groups, OSEN allows them to transact large volumes of cryptocurrency at optimal prices while minimizing counterparty risk.
- **OTC Desks:** Settling through OSEN removes the trust barrier for counterparties, thus levelling the playing field with more established desks. Additionally, for desks that need to source additional liquidity, OSEN connects multiple desks together to settle large trades.
- **Miners:** OSEN simplifies mining OTC operations, while helping miners realize price premiums on newly mined coins without having to find buyers individually.
- **Exchanges:** OSEN allows exchanges to approach the institutional market by creating private non-custodial pools of liquidity.

Non-Bitcoin OTC

Altcoin ownership is often highly concentrated, with limited liquidity on spot exchanges. This can be addressed through OTC trades with large holders, such as funds or the project team. However, the settlement process for these trades can be expensive and complicated, requiring either a trusted 3rd party or to divide settlement into ten or more tranches to settle in increments. OSEN helps these trades settle in minutes with minimal counterparty risk, providing significant improvements in efficiency, cost and safety.

New decentralized financial instruments that are issued on-chain are emerging, such as Market Protocol (https://marketprotocol.io/), UMA (https://umaproject.org/) and dYdX (https://dydx.exchange/). These products can face challenges with finding exchanges and market makers. OSEN provides a robust network of sophisticated market participants, as well as a permissionless medium for exchanging on-chain assets, making it a default choice for these emerging instruments.

Dapps

Decentralized applications, especially gaming dapps, are seeing increasing volume as user experience improves and infrastructure becomes more robust. By integrating with wallets, OSEN allows dapp interaction and payment to occur cross-chain, without requiring trust in 3rd parties like block header relayers.

Market Validation

OSEN has received support from key customer segments in the market:

- **OTC Dealers:** A core stumbling block for any trading venue is the chicken and egg issue of aggregating liquidity. Liquidity providers prefer markets with high volume, while volume congregates where there is liquidity. OSEN has received verbal agreement from **four market makers** to provide liquidity to the network. The result is that any user in the network can receive up to 1,000 BTC of liquidity for any given digital asset from day one.
- **Exchanges:** The centralized exchange market has become increasingly commodified, and exchanges must compete on differentiators or unique access to communities in order to gain liquidity. OSEN has a strategic partnership with a Chinese exchange to launch an OTC dark pool, to resolve the issue of block trades for institutional customers, while providing fiat liquidity for OSEN.
- **Wallets:** Capital flows wherever risk is lowest, making wallets a key channel for OSEN. OSEN has a partnership with a hardware wallet provider, which allows users to exchange digital assets directly from their wallet.
- **Brokers:** Most digital asset brokers either work with a designated market maker, or build their own exchange connectivity to access the market. OSEN is partnering with a white-label brokerage solution to integrate OSEN as a liquidity source for large orders into their solution.

Based off this market validation, we are projecting **$200 million in monthly trade volume** in the network with 1,000 nodes (users in the network) by end of 2019, with revenues of **$200,000 monthly**.

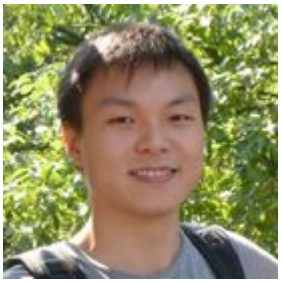
Team

OSEN brings together an experienced group of operators and developers to approach this opportunity.

Maomao Hu, **Chief Executive Officer**: Maomao has extensive experience leading teams to build and deploy fintech products, including Morgan Stanley's money movement and roboadvisor products, using AI to detect market manipulation at Neurensic, capital markets back-office at MiddleLink, and cross-border payments to 80 Nigerian farmers via the blockchain at Kora. Currently, he manages business operations for cryptocurrency market maker Eigen Capital.

Daniel Tsui and **Matt Slipper, Protocol Engineers:** Daniel and Matt are key protocol engineers for OSEN. They previously founded the blockchain software development firm Kyokan and executed deeply technical projects for groups including Ethereum Foundation, Tendermint, Dfinity, and Handshake.

Tim Geannopulos, Business Development: Tim has a storied career in fintech, starting as the fifth founding partner and general counsel for Trading Technologies ("TT"), the premiere professional futures software trading platform. He later transitioned to Global Head of Sales and grew TT to be the leading product among futures trading platforms. After leaving TT in 2013, Tim served as President at Neurensic, which was acquired in 2017, and drove growth for several fintech startups including MiddleLink and Vertex Analytics.



Wenyu Wang, Quantitative Trading: Wenyu has led several teams for capital markets activity. After earning a Ph.D in Operations Research from Purdue University, he gained experience as a Quantitative Researcher at Merrill Lynch and JP Morgan, before returning to China to lead a team of fintech developers in Beijing, allowing for cost-efficient and high quality software development.

Brian Kaye, Cloud Services: Brian has industry-leading experience with high-availability, low-latency networking solutions for capital markets. He led the development and operations for TTNET, the most widely used hosted futures trading solution.

Appendix

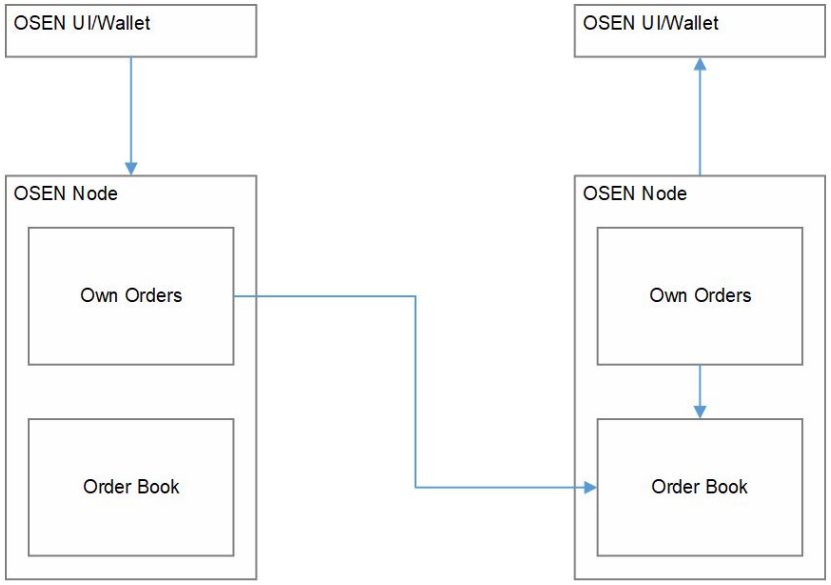
Exchange Protocols

The OSEN exchange protocols are a suite of protocols for exchanging digital assets in a trustless manner, with various tradeoffs between risk, privacy and convenience.

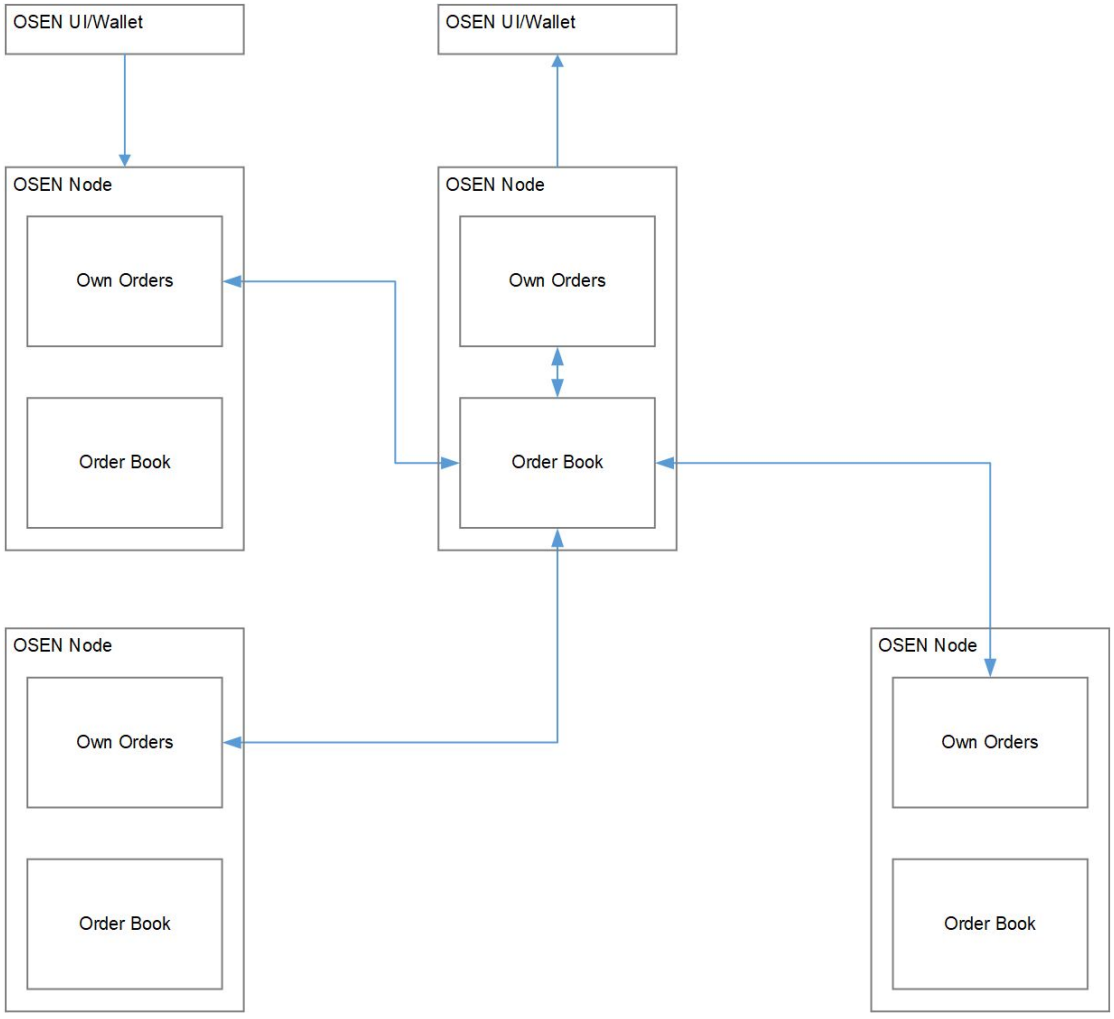
There are two main execution protocols for sending, sharing and filling orders:

Peer to Peer Execution (P2PE)

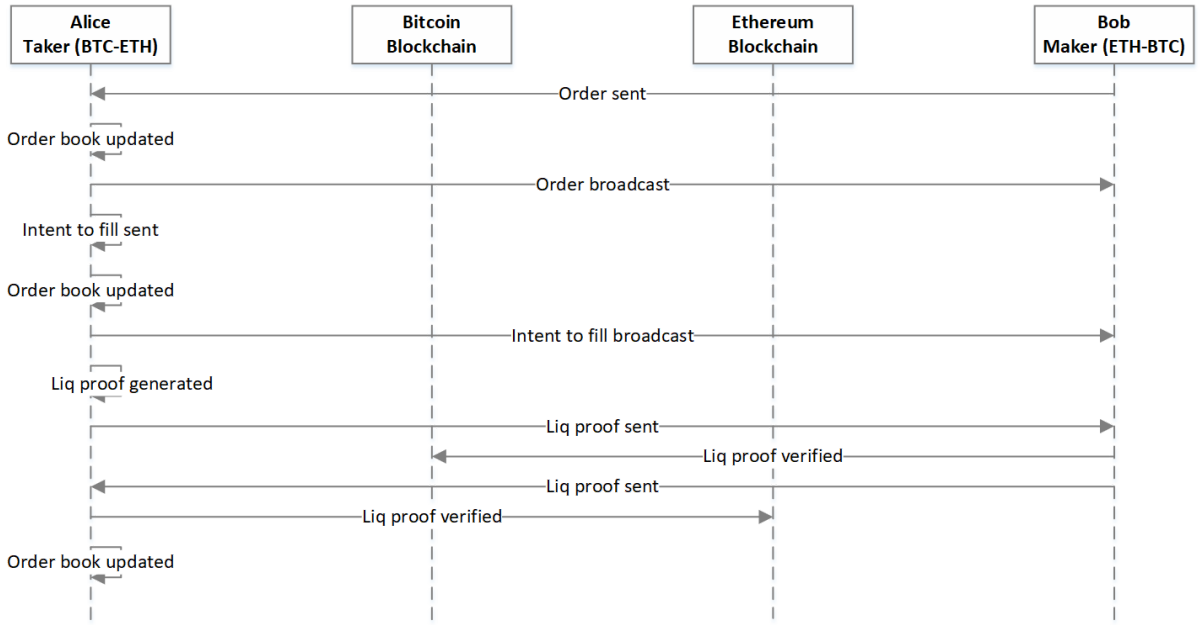
In this mode, peers connect directly with each other. Orders and fills are sent directly.



Relayers can be created by having multiple peers connect to a single peer who aggregates an order book.



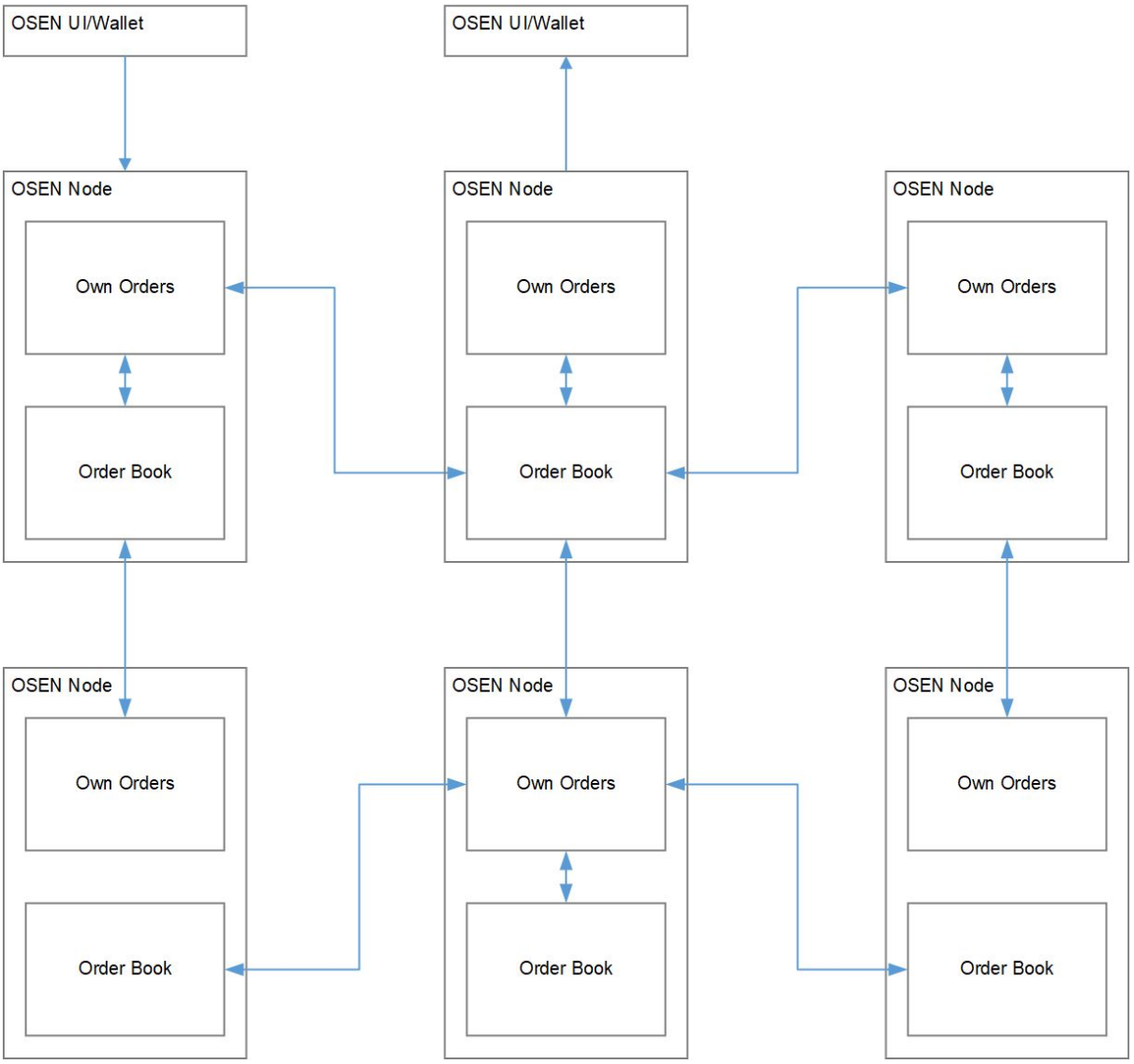
The OSEN P2PE protocol is as follows:



1. *Order Book Construction*. One of the peers sends an order to the node with *NewOrderRequest*. The node receives the order, sends *NewOrderResponse*, and updates their order book by adding the new order. The node sends the new order to all other peers they are connected to, except the peer that sent the order.
2. *Intent to Fill*. Since fills cannot be guaranteed in a peer-to-peer environment, an intermediary step must take place known as intent to fill. In this step, a peer, which can be the node itself if it is filling an order it holds sent to it by another node, sends *IntentToFillRequest* to the node. The node receives the message, sends *IntentToFillResponse*, and updates the order book so that the intent to fill is reflected in the order book. The order will stay in the order book during this process. The intent to fill should be taken to mean the sender of the intent is willing to send the HTLC first.
3. *Proof of funds*. Before the orders are filled and settlement begins, the peers who are completing the trade need to verify that their counterparty has sufficient funds to settle. The node generates a liquidity proof for a given address and sends this to the counterparty with *NewLiqProofRequest*. The counterparty verifies the liquidity proof on-chain, then sends their own proof, which is verified by the node. This step can have a timeout. If liquidity proofs aren't received on both sides in the duration of the timeout, the intent to fill is canceled. If they are received, the intent to fill is accepted and the order is filled. At this point the order is removed from the order book, the updated order book is broadcast, and the peers enter the settlement phase.

Peer to Gossip Execution (P2GE)

In this mode, peers connect to a decentralized gossip network which shares order books. Privacy is weaker in this mode, as IP addresses can be shared and aggregated.

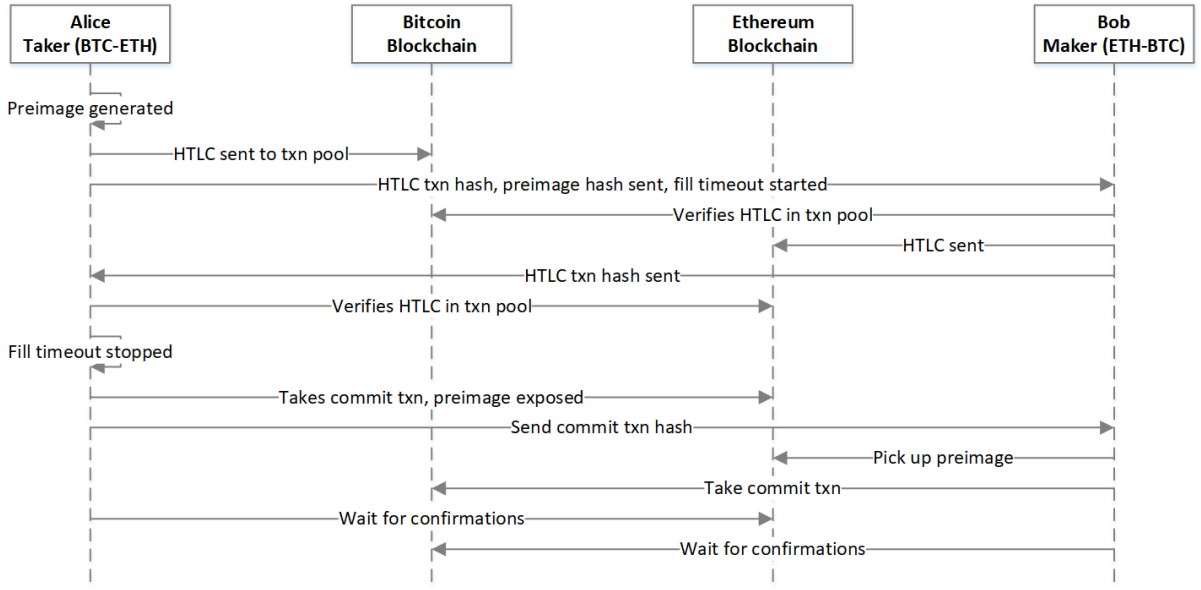


The OSEN P2GE protocol uses a variant of the SWIM protocol, where a membership list of everyone in each gossip network is created, with each node declaring which currency pairs they're subscribing to. The nodes randomly sync on the pairs they're interested in, which should be a subset of the membership list.

Peer to Peer Settlement (P2PS)

In this mode, after peers fill an order, they send fill information to each other directly and broadcast HTLCs on-chain. This mode maximizes privacy, at the cost of increased counterparty risk.

The OSEN P2PS protocol is as follows:

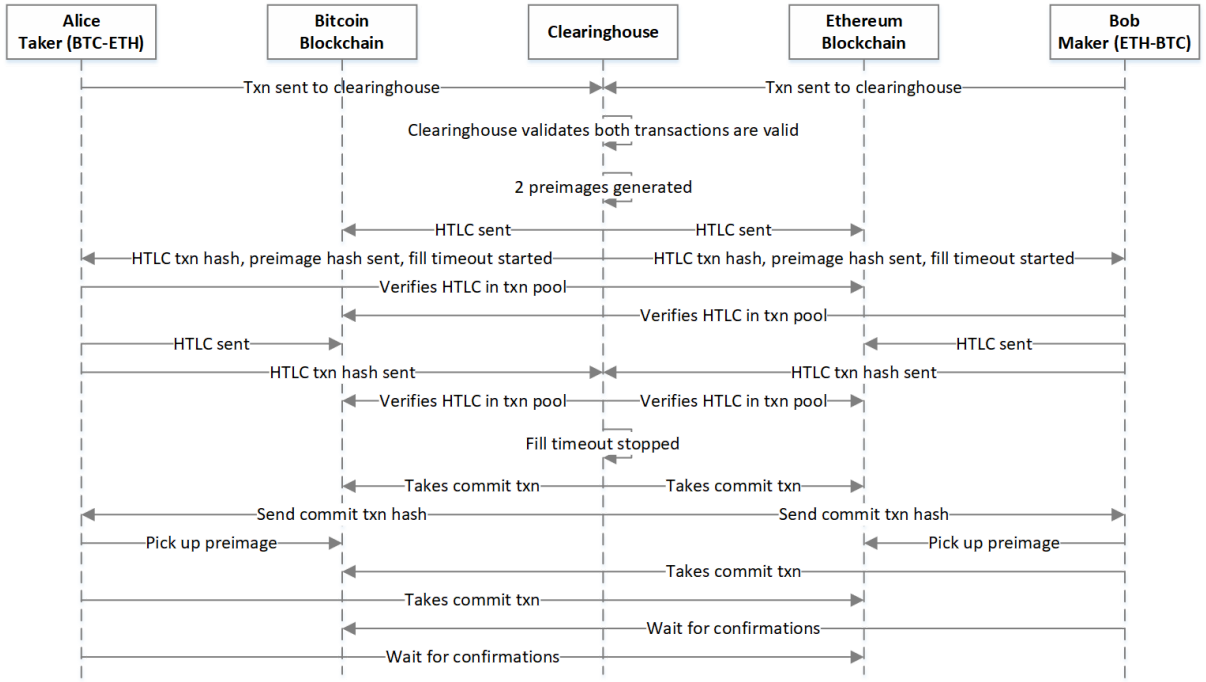


1. *Staging*. Both sides settle by issuing HTLCs for the respective amounts they are transacting using *FillRequest.* The liquidity taker, defined as the sender of the intent to fill, generates the preimage, issues the initial HTLC on-chain and sends the HTLC txn hash to their counterparty. This starts the fill timeout process, where the counterparty must submit their own HTLC within the specified timeframe. The counterparty verifies the HTLC in the transaction pool, sends their own HTLC, and sends the HTLC hash to the taker. The taker verifies the HTLC in the transaction pool and upon successful verification, stops the fill timeout.
2. *Commit.* At this point the taker initiates the commit transaction by broadcasting the transaction with the preimage. When this occurs, the counterparty can pick up the preimage from the blockchain and initiate their own commit transaction.
3. *Confirmations.* After the commit transactions from both sides are included in blocks and enough confirmations are reached, the transaction is considered complete.

Peer to Clearinghouse Settlement (P2CS)

In this mode, after peers fill an order, they send the fill to a clearing node, which becomes the counterparty to both trades and broadcasts the HTLC first. This mode minimizes risk, at the cost of some privacy.

The OSEN P2CS protocol is as follows:



1. *Initialization*. Both sides begin the clearing process by sending clearing requests to the clearinghouse using *CHFillRequest.* The clearinghouse validates that it has received the same information from both parties.
2. *Staging.* If the clearinghouse validates both transactions, it begins the staging of settlement by generating two preimages. For each asset that is being settled, it uses one to send an HTLC on the respective chain, sends the HTLC transaction hash to the counterparty, and starts the fill timeout process. The liquidity taker, defined as the sender of the intent to fill, generates the preimage and issues the initial HTLC on-chain. The counterparty verifies the HTLC in the transaction pool, and sends their own HTLC. The counterparty verifies the HTLC in the transaction pool, sends their own HTLC, and sends the HTLC hash to the clearinghouse. The clearinghouse verifies the HTLC in the transaction pool and upon successful verification, stops the fill timeout.
3. *Commit.* At this point the clearinghouse initiates the commit transaction by broadcasting the transaction with the preimage. When this occurs, the counterparty can pick up the preimage from the blockchain and initiate their own commit transaction.
4. *Confirmations.* After the commit transactions from both sides are included in blocks and enough confirmations are reached, the transaction is considered complete.

Attack Vectors

There are various ways to attack the OSEN protocols.

Stuffing

After both parties have broadcast their HTLCs, the party that generated the preimage can redeem their commit transaction, then “stuff” the blockchain their counterparty is settling on by spamming it with transactions until the timelock on their refund transaction runs out. In this way they can both receive funds from their counterparty and recover their side of the trade.

This attack only creates economic gain for the attacker when the cost to stuff the blockchain is lower than the amount that would be gained. An adversary may still choose to attack even when losing funds. It can be mitigated with careful float management and sufficiently long timelocks for HTLCs.

Counterparty DOS

As a variant of the stuffing attack, the party that generated the preimage can attack the counterparty’s OSEN node instead, causing it to go offline until the refund period runs out.

This attack can be mitigated with conventional methods for defending against DOS attacks, such as instance replication and IP blacklisting.

Preimage Theft

After one HTLC has been broadcast, the party that didn’t generate the preimage can redeem their counterparty’s commit transaction without broadcasting their own HTLC by stealing the preimage.

This attack can be mitigated with conventional methods for defending against data theft, such as firewalls and further encryption for the preimage.

Trade Reneging

After one HTLC has been broadcast, the counterparty can cause the first party to lock up funds fruitlessly by refusing to broadcast their HTLC.

This attack can be mitigated with a reputation and/or staking layer for the network.

Garbage Orders

An entity can grief the network by broadcasting large volumes of orders or intents to fill that is does not intent to settle.

This attack can be mitigated with a reputation and/or staking layer for the network.