

ODIN Protocol: A Bitcoin-based Decentralized Exchange

Introduction:

The rapid growth of Bitcoin-native digital assets, such as inscriptions and runes, has created a need for efficient trading platforms that are secure, decentralized, and cost-effective. Traditional centralized exchanges have limitations in terms of security, while on-chain solutions suffer from high transaction fees and slow confirmation times. The Odin Protocol addresses these challenges by implementing a P2P trading mechanism based on light pools, which enables direct asset trading between users.

Our system combines the power of Runes a Bitcoin token standard, with the custom Runes Dex protocol (ODIN) on the ODIN Lightning node to create a unique P2P trading platform with low fees and lightning-fast speeds.

System Players:

- **Maker:** A user offering to buy and or sell Runes in exchange for Bitcoin and or other Runes.
- **Taker:** A user who accetps the offers, sells and or buys the Runes from the maker in exchange for Bitcoin and or other Runes.
- **Odin:** The DEX node acts as a middleman and guarantor by signing the final transaction.

How Trading Works on the DEX: (Example case where Maker sells Runes and Taker buys them with Bitcoin)

1. Opening Channels:

- **Maker:** Opens a Lightning channel (ch1) to bring their Runes into the system.
- **Taker:** Opens a channel (ch2) to contribute Bitcoin for the upcoming trade.

2. Publishing an Offer:

- The Taker signs an exchange offer and publishes it to the P2P network using the gossip protocol.

3. Creating and Signing the PSBT:

- The Maker accepts the offer and drafts a partially signed Bitcoin transaction (PSBT) that includes inputs from both ch1 and ch2.
- The Maker signs this PSBT and sends it to the Taker.

4. Signing and Verification:

- The Taker signs the PSBT and sends it to Odin.
- Odin signs the transaction, and the fully signed transaction is returned to both the Maker and Taker.

5. Closing the Deal or Further Trading:

- At this point, the transaction can be broadcast to the Bitcoin network to finalize it. Alternatively, the system can open a few more virtual Lightning channels, allowing further trading by grouping or expanding the number of participants.

The Odin Protocol Architecture

The Odin Protocol is built on the Lightning Network, a layer-2 scaling solution for Bitcoin that enables fast and low-cost transactions. The protocol leverages the Lightning Network's infrastructure to facilitate the exchange of Bitcoin-native digital assets through light pools.

A light pool is a decentralized network of nodes that quote prices for swaps between Bitcoin-native digital assets. Each node maintains a quote for a specific asset pair and broadcasts it to other nodes in the network using a gossip protocol.

When a user wants to accept a quote from a maker, they use the information in the quote to construct a PSBT (Partially Signed Bitcoin Transaction) that includes their signatures. The PSBT is then broadcast to the network, and the maker signs the transaction, confirming the trade.

Architecture Advantages:

- **Security:** Runes leverages OP_RETURN metadata for token tracking, while smart contracts ensure secure exchanges.
- **Flexibility:** PSBTs let participants pre-agree to terms, giving them full control over trades.
- **Efficiency:** Lightning Network offers instant transactions with low fees, easing the load on Bitcoin's main chain.
- **Privacy:** The gossip protocol and custom channels distribute offers without exposing transaction details.

Conclusion:

Odin protocol, using Runes and Lightning Network, brings a new model for P2P trading into the Bitcoin ecosystem. It combines smart contract security, Lightning Network speed, and custom protocols to offer users a flexible, fast, and decentralized solution.

ODEX Trading Process

