PintSwap: A fully p2p solution to hybrid DEX

Adrien Vlădescu

2023/09/01

Abstract

PintSwap is a purely decentralized exchange supporting private OTC offers, which can optionally be published via a p2p channel to a fully decentralized and distributed orderbook. The PintSwap orderbook does not rely on a centralized relayer and does not involve management and execution of offline signatures. Execution against the set of orders hosted by a single node is aggregated into a O(1) on-chain operation, instead of classic limit order DEX which relied on O(n) ECDSA signature recovery for on-chain settlement. Cryptographic operations are performed entirely offchain when a trade is negotiated over the protocol, using 2p-ecdsa to generate a 2-of-2 offchain multisig between traders, for each trade execution.

The PintSwap p2p stack, codenamed pintp2p, is built from the same libraries that make IPFS work, but configured to use webRTC as its sole transport and thus capable of running entirely in the browser. By these mechanisms, PintSwap is the first of its kind in a new class of p2p hybrid DEX applications.

1 Introduction

The evolution of the decentralized exchange has featured rapid paradigm shifts in response to regulatory challenges, market conditions, and general sentiment around design patterns. Only briefly did mainstream DEX include the limit order as a primitive in a given trade mechanic. Instead, it was the AMM which dominated and laid out the battlefield for what can only be referred to as DEX warfare, when you consider the adversarial environment a trader is met with when he attempts to execute a market order. With AMMs we saw a new domain of research and products designed to capture MEV, which is a blanket term for any value that can be captured with frontrunning programs, often designed for the purpose of executing economic attacks against traders with great stealth and precision. Still, the AMM is the most common tool for trading assets on networks supporting DEX programs or smart contracts.

On the Ethereum network, the interest in MEV brought about the centralization of block production largely to entities which offer block building as a service. These block builders provide an RPC interface with a consistent standard which gives all Ethereum users the ability to bundle transactions to be executed in a single block at the desired execution layout. Block builders include bundles such that they can maximize profit from producing a single block, and it is also true that submitting trades through a block builder RPC directly will obscure trade transactions from visibility to adversaries.

This creates the opportunity for a DEX architecture which actually can make use of these block builders to optimize execution for the traders themselves, instead of the MEV bots, a complete reversal of the threat model.

With PintSwap, we propose a solution to hybrid DEX architecture which can make use of these block builders on behalf of the traders, as described, but also can provide a limit order interface in a way that is truly decentralized, unlike the first generation of limit order DEX which relied on centralized relay servers.

2 PintSwap Protocol

2.1 Addresses

PintSwap addresses are a `pint1` prefixed sequence of base32 characters, encoded using bech32 (similar to a Segwit address on the Bitcoin network is encoded with a bc1 prefix). The `pint1` address is simply an encoding of the underlying libp2p PeerId multihash. A PeerId is a libp2p compatible key and maps to a peer `pint1` public address, similar to how an Ethereum address can be computed from a secp256k1 private key. The bytes that make up the address, once decoded, act as the lookup key in the pintp2p DHT, which is queried for connection information when connecting to a remote peer.

A node on pintp2p must have a unique pint1 address to be able to transmit data to the network successfully.

2.2 Nameservers

The PintSwap protocol supports static nameserver instances which can be set per top level domain internal to pintp2p. By default, a public nameserver exists for .drip names, which can be queried to lookup a pint1 address associated with the name. This provides facilities similar to DNS, but simplified for the needs of pintp2p, which is strictly a 1-to-1 mapping between a pint1 address and a more memorable and human-readable name.

The protocol built into pintp2p to query a nameserver is

/pintswap/0.1.0/ns/query

For name registration, the required protocol is:

/pintswap/0.1.0/ns/register

2.3 Orderbook

The public orderbook is made available to the global pintp2p network via broadcasts over GossipSub. The PintSwap SDK library automatically manages repeated publishing on a customizable interval, and it also handles decoding incoming broadcasts and aggregating a complete view of the orderbook in an in-memory mapping.

The GossipSub topic on which orders are broadcast is:

/pintswap/0.1.2/publish-orders

By default, publishes occur within the SDK at a 30s interval.

2.4 Query Peer Data

A node on pintp2p must respond with a local view of its outstanding limit orders when dialed on the following protocol:

/pintswap/0.1.2/userdata

The response can optionally include a PNG graphic or NFT tuple for use as a profile image, as well as a message which can be rendered for a user profile.

2.5 Trade

Transmission as it relates to a complete 2p-ecdsa key generation and offline signatures compatible with Permit/Permit2 for trade execution, ETH addresses of either party must occur with the following protocol:

/pintswap/0.1.0/create-trade

Once a 2p-ecdsa public key is computed, the contract address for the transaction script to be signed can be computed by both parties, and signatures can be exchanged which authorize the atomic exchange of ERC20, ERC721, or ERC1155 tokens by the contract to be deployed. The transaction script is assembled and validated to be identical and expresses the exact exchange to take place agreed upon by both parties, and once consensus is achieved and gas cost is predicted, the complete Ethereum transaction is signed using 2p-ecdsa, and the taker is given the opportunity to submit the complete payload to the network via any preferred RPC.

2.6 Data Structures

The pintp2p wire protocol uses binary serialization via the protobuf schema. A complete schema of the data structures used in the protocol is reproduced below:

```
syntax = "proto3";
package pintswap;

message ERC20Transfer {
  bytes token = 1;
  bytes amount = 2;
}

message ERC721Transfer {
  bytes token = 1;
  bytes token_id = 2;
}

message ERC1155Transfer {
  bytes token = 1;
  bytes token_id = 2;
  bytes amount = 3;
}

message Transfer {
  oneof data {
    ERC20Transfer erc20 = 1;
    ERC721Transfer erc721 = 2;
    ERC1155Transfer erc1155 = 3;
  }
}

message Offer {
  Transfer gives = 1;
  Transfer gets = 2;
}

message OfferList {
  repeated Offer offers = 1;
}

message MakerBroadcast {
  repeated Offer offers = 1;
  string bio = 2;
  ERC721Transfer pfp = 3;
}

message UserData {
  string bio = 1;
  repeated Offer offers = 3;
  oneof pfp {
    bytes file = 4;
    ERC721Transfer nft = 5;
  }
}


message Fill {
  bytes offer_hash = 1;
  bytes amount = 2;
}

message BatchFill {
  repeated Fill fills = 1;
}

message Transmission {
  bytes data = 1;
}

message NameQuery {
  oneof data {
    bytes multiaddr = 1;
    string name = 2;
  }
}

message NameQueryResponse {
  enum NameQueryResponseStatus {
    NAMEREG_QUERY_ERR = 0;
    NAMEREG_QUERY_OK = 1;
  }
  NameQueryResponseStatus status = 1;
  string result = 2;
}


```

```
message NameRegisterResponse {
  enum NameRegisterResponseStatus {
    NAMEREG_OK = 0;
    NAMEREG_NO = 1;
    NAMEREG_ERR = 2;
  }
  NameRegisterResponseStatus status = 1;
}

message Permit1Data {
  bytes v = 1;
  bytes r = 2;
  bytes s = 3;
  bytes expiry = 4;
}

message Permit2Data {
  bytes nonce = 1;
  bytes deadline = 2;
  bytes signature = 3;
}

message PermitData {
  oneof data {
    Permit1Data permit1_data = 1;
    Permit2Data permit2_data = 2;
  }
}
```

3 Trade Engine

PintSwap itself delegates permissions to run order matching and arbitrage strategies against the public orderbook via the OPPS NFT. Wallets (or smart contracts) holding the OPPS NFT are able to borrow liquidity from vault contracts constructed for every ERC20 traded on the network. These sipERC20 vaults lend capital to OPPS as part of an MEV bundle, such that they are are repaid with profits within the same block.

The OPPS will actively react to orderbook publishes and attempt to find matches within the PintSwap orderbook itself, or otherwise fall back to DEX aggregators, in order to capture the desired execution price. In the event that a PintSwap order is to be matched to another order on the platform, the trade negotiation protocol is initiated with two peers at the same time, and the entire transaction bundle is reorganized and packed for maximum efficiency for execution. Profits from all strategies are fed back to the vaults in terms of the input asset, but a configurable portion is always used to buy PINT, which is transferred to the core sipPINT vault.

Combined, these mechanisms create a realtime clearinghouse for any EVM asset, immune to the usual threat of economic attack from adversarial MEV bots. At the same time, trade execution can always capture the exact value desired by the end-user, but also drive value back to the protocol itself at no consequence.

4 Token Economics

The PINT token is the network token of the PintSwap protocol. The token has two purposes. First, it will function as a governance token by which the protocol can make decisions or upgrades to the system via vote. Second, it will act as a value accrual token for value captured by the PintSwap protocol.

4.1 Revenue Streams

4.1.1 Market Making

The PintSwap protocol will act as a market maker on specific pairs. The profits from this activity will flow back to the ecosystem.

4.1.2 Taxes

The PINT token bears a buy/sell tax when used on classic AMM DEXes. Of course, trading PINT on PintSwap itself will be immune from these taxes, as is the case with any other asset that applies a buy/sell tax in its usual trade.

4.1.3 Arbitrage/MEV Strategies

Inefficiencies will exist between PintSwap and other DEXes, and these inefficiencies will be captured by the PintSwap protocol via the OPPS, described in an earlier section. The captured value will flow back to holders of the token.

4.1.4 Trading Fees

The trades executed via PintSwap will incur a 1% fee. As of writing, this fee is not in place, but will be activated by governance vote at a later date.

4.2 PINT Ecosystem Tokens

The PINT protocol allows for single-sided staking on any ERC20 traded by the network. The framework is designed such that all vaults grow in terms of their underlying asset, but a portion of growth across all vaults is always driven to the vault for PINT itself.

sipERC20 is the contract from which all single sided staking vaults are derived. The OPPS are permissioned to perform an atomic borrow from the vaults in order to execute strategies via MEV endpoints on block builder RPCs. Part of the profit that results from each execution is returned to the vault that was borrowed from, in terms of the underlying asset. The remainder of profit is swapped to PINT, which is then transferred to the core sipPINT vault.

sipPINT can be minted by staking PINT. Value accrual from all activity on the protocol is driven to sipPINT in proportions configurable by governance. Revenue is generated by the protocol via the following mechanisms:

1) The OPPS actively borrow from vaults to run various strategies, and profit in surplus of what is atomically returned to the vaults is always swapped to PINT and transferred back to sipPINT.

2) A 5% tax is applied to PINT trade on AMM exchanges which accumulates in the form of PINT. A portion of PINT is swapped back to ETH on the same AMM, similar to the usual mechanism by which taxes function on the latest generation of tokens. A portion of the ETH output from taxes is transferred directly to the PINT/ETH LP pair, after which the `sync()` or equivalent API is called to apply a direct upward price effect on the PINT token. The remaining ETH from tax output is transferred to the PintDAO treasury to fund initiatives by governance. Finally, the PINT tokens that were not swapped to ETH as part of the tax callback are transferred to the sipPINT vault, in order to provide the greatest upside to active PINT stakers.

3) Trading fees on PintSwap trades themselves are used to buy and transfer PINT to the sipPINT vaults.

4.3 Contract

PINT is an ERC20 asset with 18 decimals.

The PINT contract is available at the following address:

`TBD`

4.4 Token Distribution

Max Supply	1,000,000,000
Team (3mo cliff, 12mo linear vest)	20%
Advisors (3mo cliff, 12mo linear vest)	3%
Seed (25% TGE, 12mo linear vest)	5.2%
Public Sale / TRIS NFT (100% unlock at TGE)	10%
Treasury (25% TGE, 12mo linear vest)	10%
Liquidity TGE	2%
PintDAO (Locked until governance release)	49.8%

5 Governance

PintSwap protocol authority retained by Cold Water Labs Ltd, a British Virgin Isles corporation, will be transferred to the PINT token, upon network token launch. The initial token supply is capped at 1,000,000,000.

A pivotal transition will occur upon the completion and thorough review of the alpha platform. Cold Water Labs Ltd (BVI) will undertake a liquidation process, transferring all company assets to the DAO, a fully decentralized entity. This transition signifies an unwavering dedication to decentralization and community-driven decision-making.

Central to the success of the DAO is an inclusive voting mechanism that empowers each token holder. With the DAO's launch, every token holder gains the right to actively participate in shaping the future of the PintSwap protocol. The DAO will autonomously determine quorums and voting protocols through a dynamic voting system, ensuring a fair and effective decision-making process.

Furthermore, the holders of the tokens will collectively determine the individuals granted access to the executive multi-signature wallet, permissioned within PintSwap to set parameters within the protocol or otherwise consume any administrative functions within the PintSwap smart contract API. This democratized approach to wallet access reinforces our commitment to transparency and user-driven management.

The genesis of PintDAO represents a paradigm shift in governance and decentralization. By uniting token holders under a sophisticated voting system and entrusting them with executive control of the protocol, we join a larger saga of delegation to a free and collective intelligence, driven by an immutable structure for decentralized decision-making.