EAVE Parachain Design

Emerging Asset Value Engine (EAVE)
Polkadot Parachain

John Whitton

April 2021

Abstract

As at Feb 21st, 2021 the Decentralized Exchange Market has a $3.42 Billion daily trading volume and is capturing market share from the Centralized Exchange Market which has a daily trading volume of $199 Billion. Polkadot's Valuation of $28 Billion has been steadily increasing, and growing more rapidly than Ethereum and other layer 1 platforms. Polkadot [1] is about to roll out it's Parachain [2] and Parathread offerings on Kusama.

EAVE is creating an EVM compatible decentralized finance platform for the custody, aggregation and exchange of digital assets across multiple disparate digital asset platforms including blockchains, centralized exchanges and financial institutions.

EAVE has completed the initial development of our Platform and testing is currently underway. Our development process is that of rapid deployment, testing and iteration. We combine this with an open, extensible architecture and strong focus on partnerships.

We have prototyped our initial liquidity, lending and staking offerings. The liquidity offerings are combined with cross platform bridging initially using Polkadot's Cross Chain Messaging Protocol (XCMP). We plan to deploy these offerings by initially partnering with other Polkadot parachains and moving forward with other blockchains to enhance their liquidity offerings.

Once we have a battle tested development environment available and liquidity on our chain, our Decentralized Financial Platform will be rolled out to the DeFi developer community as a whole. DeFi projects can build on or migrate to our platform which provides an open framework for cross platform DeFi projects. It will consist of development tools and standards, a liquidity pool framework, optimized custodial services and exchange functionality.

Contents

1 Overview

1.1 Opportunity

With the emergence of decentralized finance, a diverse financial ecosystem has been created on blockchain technology. Although these blockchains are feature rich, they have often been siloed from one another with many in need of access to additional liquidity options for the assets on their chain and the desire to interact more easily with other chains and the broader financial community.

Polkadot and specifically Substrate provides a framework for blockchain developers to build separate but connected blockchains. Polkadot [1] has been growing rapidly and is about to roll out it's Parachain [2] and Parathread offerings on Kusama.

This creates the following opportunities

1. **Digital Asset Marketplace (Exchange):** The exponential growth of value being secured by blockchains and specifically Polkadot provides an opportunity to provide much needed access to these Assets. A complete solution will include exchange, lending and yield earning from these digital assets.

2. **Marketplace Protocol for Settlement:** The growth of not only the Polkadot parachains but also blockchains in general has created multiple siloed asset holdings. An efficient cross platform settlement layer is needed to increase liquidity and unlock the true value of these assets. Moving forward this can also be integrated with Centralized Exchanges and traditional financial institutions.

3. **Liquidity Provisioning:** is needed both within parachains which have multiple digital assets and across parachains to enhance all parachain or blockchain liquidity capabilities.

4. **Decentralized Financial Platform:** The growing Polkadot ecosystem and developer community require platforms which offer robust tooling and a decentralized financial focus to build upon.

1.2 Solution

Detailed in this paper is EAVE's unique approach to capitalize on these opportunities.

1. **Digital Asset Marketplace (Exchange):** EAVE has completed the initial prototyping of it's digital asset marketplace. It provides the ability to hold, swap, lend and earn digital assets across multiple platforms. Moving forward this will be enhanced by additional DeFi Protocol offerings including the Protocol for Optimal United Custody Handling (POUCH). This flexible framework provides a robust settlement layer supporting multi-asset by supporting different bonding curves. Yield aggregation via the Yield engine, liquidity bands to optimize liquidity provisioning and utilization and an order book which combines off chain execution with on chain custody.

2. **Marketplace Protocol (POUCH):** is EAVE's Protocol for Optimal United Custody Handling. POUCH offers enhanced liquidity, better yields and gas efficiency via a custodial and settlement layer which provides multi-asset support by interacting with multiple liquidity pools and multi-platform support through the use of cross platform bridges. It also offers DeFi protocol developers a token management framework allowing them to focus on developing unique liquidity or yield functionality without worrying about the complexity of token management. Moving forward blockchain standards, such as Rosetta [3] developed by Coinbase, will enable interacting with multiple centralized exchanges via a standard interface.

3. **Decentralize Finance Platform:** in addition to POUCH EAVE plans to create and on-board multiple Liquidity Pool offerings to capitalize on this opportunity.

   (a) **Within a parachain or blockchain:** EAVE is creating Liquidity Pool offerings which can be deployed on the EAVE chain or standalone on existing parachains, such as Acala and Moonbeam, in the Polkadot Ecosystem.

   (b) **Across parachains:** POUCH provides the ability to combine liquidity from multiple liquidity pools and platforms and exchange them in a cost effective, gas efficient manner. It leverages XCMP to allow the transfer of assets between parachains.

   (c) **Across blockchains:** POUCH also allows the settlement of assets across multiple blockchains using Cross Platform Bridges.

   (d) **Multi-Asset support:** EAVE allows multiple Liquidity Pool Offering to cater for different asset classes including stable coins and semi stable coins using price oracles. EAVE Liquidity Pool Offerings [**?**] provide details of the different types of offerings including POUCH integration, different Bonding curves and approaches for stable coins and the leveraging of price oracles.

(e) **Yield Aggregation:** is provided by the Yield Engine which allows a unique opportunity for capital efficiency in liquidity pools and also allows Yield providers to increase the Yield for their farmers by adding additional yield from trading fees for managed assets.

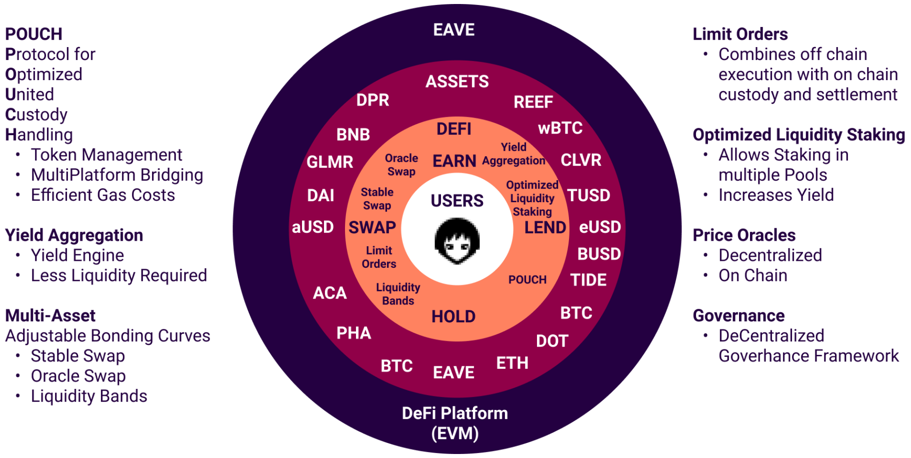
(f) **Price Oracles:** EAVE will implement both on chain and decentralized price oracles to facilitate trading of diverse real world assets.

4. **EAVE's Blockchain:** is built on top of Polkadot and is targeting being deployed as a Parachain on both Kusama and Polkadot. It can alternatively be deployed as a Parathread, Relaychain or Standalone Network. It provides EVM compatibility and robust developer tools including Solidity, Rust and Ink. It also includes standards such as the Polkadot's Open Runtime Module Library and Ethereum's ERC standards. The integration framework and a suite of standards enable scheduling of remittances, access to price oracles and assets from multiple chains.

Please note: Liquidity Pool Offerings, Digital Asset Exchange and Rewards Modules can and plan to be implemented as Decentralized Financial Protocol offerings not only on EAVE's Decentralized Financial Platform but also on alternate Parachains such as Acala or Moonbeam or Blockchains such as Ethereum, Binance Smart Chain or Serum.

1.3 Technology

To realize the opportunities EAVE is developing the following functionality.



POUCH
Protocol for
Optimized
United
Custody
Handling
- Token Management
- MultiPlatform Bridging
- Efficient Gas Costs

Yield Aggregation
- Yield Engine
- Less Liquidity Required

Multi-Asset
Adjustable Bonding Curves
- Stable Swap
- Oracle Swap
- Liquidity Bands

Limit Orders
- Combines off chain execution with on chain custody and settlement

Optimized Liquidity Staking
- Allows Staking in multiple Pools
- Increases Yield

Price Oracles
- Decentralized
- On Chain

Governance
- DeCentralized Goverhance Framework

Figure 1: EAVE Functionality

This functionality is being deployed on EAVE blockchain which was developed with the following architecture

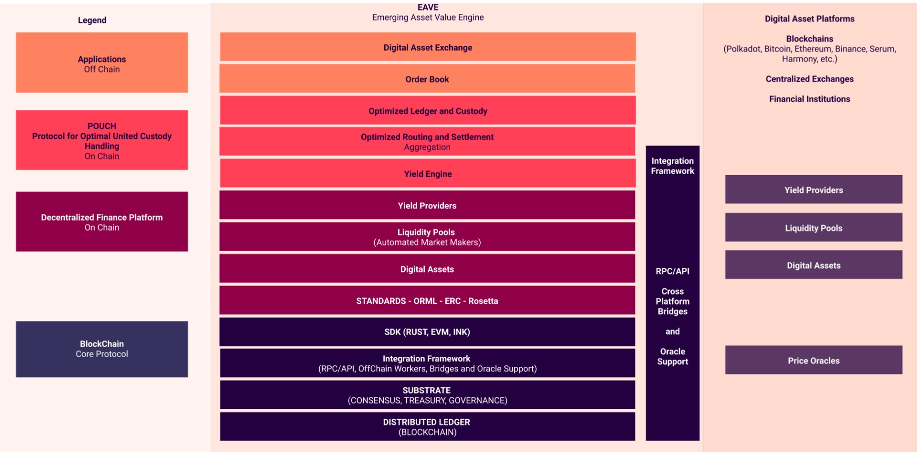


Figure 2: EAVE Architecture

- **Applications**
  Digital Asset Marketplace provides a cost cheap, fast solution for a broad range of digital assets. It will do this by leveraging an order book which combines off chain execution with on chain settlement. The optimized routing and settlement both minimizes gas fees and provides routing and settlement capabilities to liquidity pools from a variety of providers including other parachains, blockchains, centralized exchanges and financial institutions.

- **Protocol for Optimized United Custody Handling (POUCH)**

  1. **Secure:** The Optimized ledger keeps internal balances isolated among liquidity pools.
  2. **Simple:** All interactions will be done through one single access point: the vault.
  3. **Cost effective:** Trading against all liquidity pools will be on par with existing liquidity pools. Trades will cost even less if internal balances are used. Trading with many pools at the same time only marginally increases the gas costs. EAVE's gas costs will be significantly less than Ethereum's.
  4. **Higher Yield:** Liquidity pools have full control over the underlying tokens they add to the optimal ledger. This opens up vast design space to improve capital efficiency within and across multiple chains and can be combined with the Yield engines for greater returns and the EAVE Liquidity Protocol which allows assets to be leveraged for multiple staking scenarios, further increasing yields.

5. **Extensible:** EAVE will create a thriving cross chain ecosystem and will incentivize developers through it's comprehensive suite of developer tools and use of it's treasury funds for Grants and bounties.

- **Decentralized Financial Platform**
  Leveraging a robust IDE which includes the ability to develop natively in RUST, Solidity Vyper or Ink, the Defi Hub will allow for the rapid development of new Polkadot DeFi projects as well as enabling the porting of Solidity based projects to Polkadot. Finally, the Integration engine will enable exciting new cross-chain financial models based on composability of modular components through the use of bridging, price oracles and traditional fintech through off chain worker capabilities.

- **EAVE Chain**
  Built upon a robust, modular blockchain, the Core Protocol leverages Substrates modular extensible components to provide rich functionality including consensus, governance, RPC and API functionality and software development kits.

1.4 Use Cases

The following diagram gives an overview of the use cases that EAVE can support.

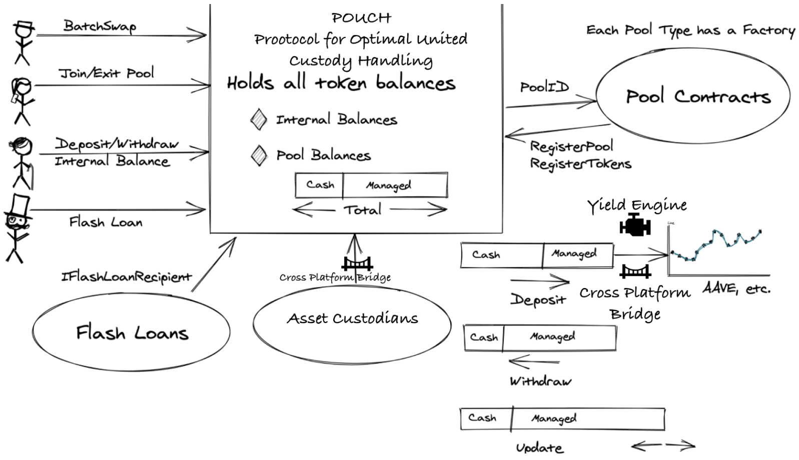


Figure 3: POUCH Functionality

1. **Token Holders/Traders and Arbitrages:** As well as holding and swapping tokens. Holders can combine multiple trades in a batch swap, provide liquidity by joining or exiting a pool, decide whether to leave there tokens in the POUCH as an internal balance or withdraw the assets back to the native token and create flash loans for arbitraging opportunities.

2. **Yield Providers:** Yield providers such as DeFi protocols like AAVE can use there managed assets to provide liquidity. Thus reducing the amount of assets needing to be held in pools and increasing their yield by augmenting there existing fees with trading fees from the liquidity pools.

3. **Asset Custodians:** Asset custodians are any entity which manages assets, these include Layer 1 blockchains, parachains, DeFi protocols, centralized exchanges and traditional financial institutions. All of these Custodians can increase liquidity for there assets (tokens). They can also increase liquidity for their platform, either by bridging to POUCH or moving forward implementing a POUCH light client on there platform.

2 Digital Asset Marketplace

EAVE has completed prototyping of it's digital asset marketplace. As a polkadot parachain or parathread it can provide liquidity for all parachain assets on Kusama or Polkadot.

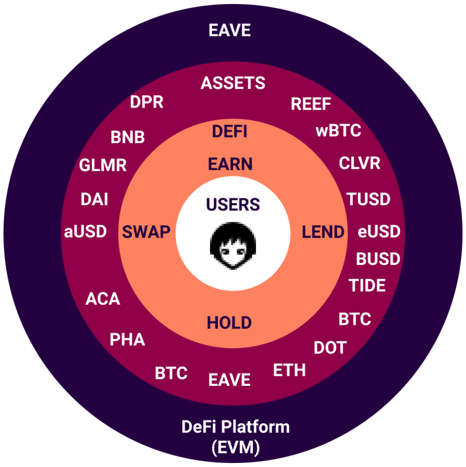


Figure 4: EAVE APP Functionality

Following is an overview of the functionality implemented currently through a combination of internal development and partnerships. The application runs on top of the EAVE Decentralized Financial Platform. The rest of the paper gives an overview of the additional functionality being built or migrated to the platform.

1. **HOLD:** EAVE's mobile app provides a secure digital wallet which holds all tokens stored natively on EAVE.

2. **SWAP:** functionality is provided by a simple UNISWAP v2 based exchange adapted by ACALA for the Polkadot ecosystem.

3. **LEND:** holders can collateralize loans for digital assets via a Collateral Debt Position Protocol called Honzon built by Acala and similar to MakerDao.

4. **EARN:** the first two earning opportunities on the EAVE Platform are liquidity provisioning and loan fees.

3 POUCH Marketplace Protocol

EAVE's Protocol for Optimal United Custody Handling (POUCH) provides enhanced liquidity, better yields and gas efficiency.

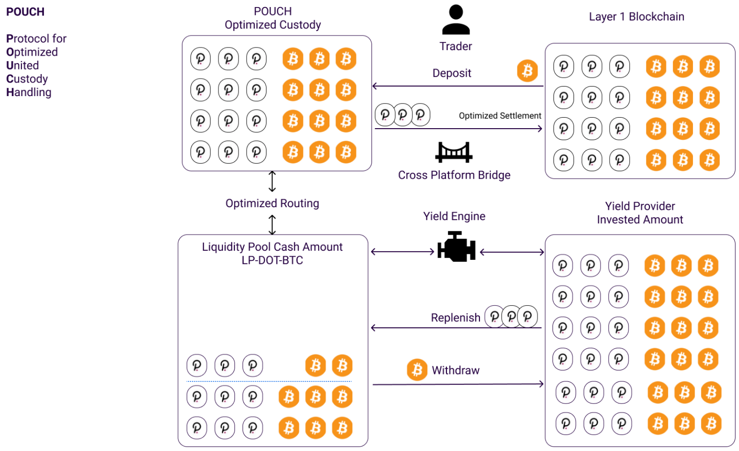


Figure 5: POUCH Yield Aggregation

3.1 Protocol for Optimal United Custody Handling (POUCH)

The POUCH holds all balances of the Liquidity Pools on the EAVE chain. It allows for a single interface point with all liquidity pools and abstracts away the underlying implementation of the liquidity pools thus allowing a gas efficient platform and agnostic interface for the exchange of tokens.

Routing and Settlement: off-chain swap routing enables the discovery of the best value for swaps via the Optimized Ledger. This includes all POUCH Protocol Liquidity Pools and may be augmented with on-chain components for realizing discovery fees.

A sample trade flow is as follows

1. Trader approves the Optimized Ledger to work as a proxy
2. Trader requests to swap one BTC for some DOT
3. The BTC is deposited into the Optimal Ledger (note: this optionally uses the Cross Platform Bridge if the assets come from another layer 1 platform)
4. Optimal Routing selects the most efficient swap route from multiple liquidity pools and executes the trade

5. The trader receives the DOT and then can either leave the DOT on the Optimal ledger or withdraw them using Optimal settlement (once again, if the funds are native to another layer 1 platform the Cross Platform Bridge will be used)

Yield Engine and Aggregation using Cross Platform Bridges

The Yield Engine connects Liquidity Providers to Yield Providers. Yield Providers *invest* in a liquidity pool. However, rather then sending all the invested tokens to the liquidity pool, only the minimum amount needed for transactions are sent. The role of the Yield engine is to monitor the balance of the liquidity pools and replenish and re-balance them as needed.

The Yield Engine flow is as follows

1. The Yield Provider (e.g. AAVE or Honza) ”invests” a number of tokens into a liquidity pool

2. The Liquidity Pool maintains a minimum threshold needed for trading, which is called the Optimal Liquidity Amount. The remaining ”investment” tokens remain in the Yield Provider enhancing the yield for the Liquidity Pool.

3. When the number of tokens for any token in the pool drops below the Optimal Liquidity Amount, a re-balance is triggered (optionally using the cross platform bridge if needed).
   Note: In the above scenario, BTC was traded for DOT thus triggering DOT to drop below its Optimal Liquidity Amount. Hence, DOT is replenished by the Yield Provider and BTC is withdrawn to balance the Liquidity Pool and continues to earn yield on the surplus BTC.

3.2 Cross Platform Bridge

Bridging will be combined with POUCH to provide access to Assets from currently siloed Asset Custodians. This will start with Polkadot Parachains and then other chains and in the future may include bridging with centralized exchanges and financial institutions.

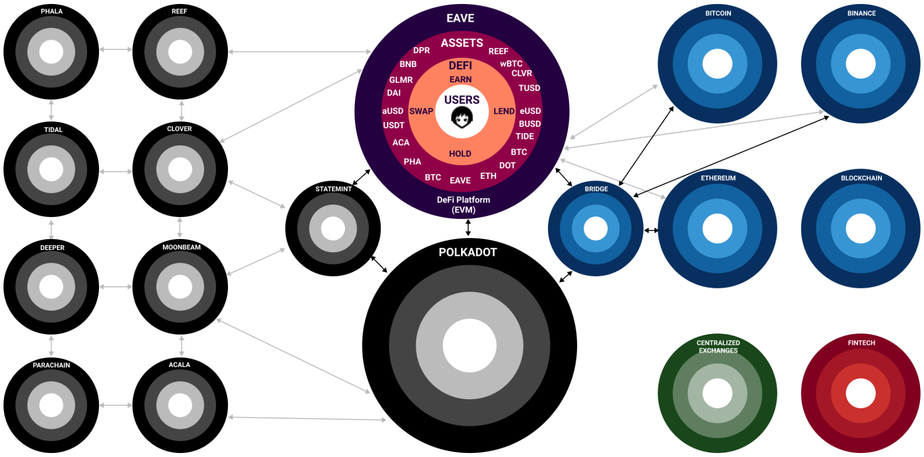


Figure 6: EAVE Bridging ECOSYSTEM

Polkadot Ethereum Bridge Overview

Polkadot has done extensive work on bridging parachains implementing Horizontal Relay Message Protocol[9] which is a pre-cursor to Cross Chain Messaging Protocol (XCMP) [10][11]. It has also partnered with other layer 1 platforms to build cross platform bridges [12][13].

Some notable bridge implementations include Snowfork (a Polkadot Ethereum Bridge), [14][15], the Ren Polkadot BTC Bridge [13], and Wormhole (a Polkadot Cosmos Bridge) [12].

Additional noteworthy work in this area includes Cosmos IBC Standards [16][17] as well as layer 1 bridges such as the NEAR Ethereum Rainbow Bridge [18] and the Harmony Horizon Bridge [20].

Multi Platform Build Strategy

EAVE plans to leverage these Bridges to create a multi-platform DEX. It will build a reusable bridging and locking framework for multiple platforms. It is planned to roll these out starting with Parachain and Ethereum Bridges and then adding additional platforms based on demand.

Note the bridging functionality will primarily be used when provisioning liquidity and once the liquidity has been provisioned to the pool. Then, the swaps will be executed on the EAVE Chain. Enabling traders able to unlock their tokens on the originating platforms as needed.

Centralized Exchange Integration

Blockchain standards can also be implemented to enable interacting with multiple chains via a standard interface. This is different from bridging where you are locking tokens across multiple platforms These standards can be used to orchestrate independent transactions into a logical transaction set across multiple blockchain platforms. A comprehensive set of blockchain platform standards has been developed by Coinbase called Rosetta [3], which could be leveraged by EAVE or further enhanced if needed.

3.3 Limit Orders - Order Book

An off-chain order book will be built to support Limit Orders.

The following key concepts and process overview are for EAVE Limit Orders. For background, we recommend also reading the following relevant Designs of off-chain order books integrated with on-chain DEX's: 0x [**?**], IDEX [4], HydraDX [5] and PolkaDex [6].

It is important to understand that Centralized exchanges offer three different financial services: custody, trade, and settlement. In traditional finance, these three functions—custody exist separately and often for good reason. Clients can have different requirements when it comes to custody solutions, and exchanges can work with any number of providers. Separation of functions allows for more accountability and transparency in financial services.

EAVE combines on chain trade settlement with an off-chain trade execution for an efficient solution.

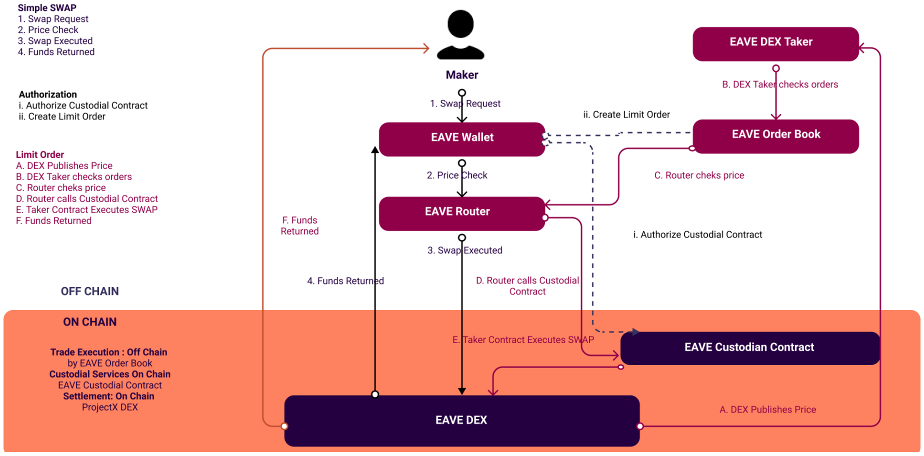


Figure 7: EAVE Order Book Functionality

Custodial services are provided by EAVE DEX Taker Contract which traders authorize to access there balances.

Trade Execution combines an off chain order Book EAVE Order Book as well as a price determination mechanism used to calculate the swap price for Tokens, it combines this with virtual balances which are published.

Trade Settlement is carried out on chain using the EAVE DEX.

Sample Process Flows

SWAP Execution : Swap can be executed immediately

1. Maker places a swap for Token A to Token B
2. EAVE Wallet calls the EAVE Router to Determine the best route and Price
3. Order is executed on the EAVE DEX
4. Token B is returned

Limit Order Authorization : Swap price is higher then requested

1. Maker authorizes the EAVE Taker Contract to access their balance of Token A.
2. Maker places a signed limit order, including a duration the order is valid for, which is stored on the EAVE Order Book.

Limit Order Execution

1. The EAVE DEX Publishes the Token Price (based of virtual balances) at each Block to the EAVE DEX Taker.
2. The EAVE DEX Taker traverses the EAVE Order Book
3. For each order, it calls the EAVE Router to see if this price matches. (orders are sorted by swap price and chronologically based on submission time).
4. Matching Orders are sent to the EAVE Taker Contract to be executed. Note due to slippage as orders are queued router logic maintains an updated virtual balance and price.
5. EAVE DEX Taker Contract Executes the swap on behalf of the Maker on the EAVE DEX.
6. Once executed, EAVE Taker Contract sends the funds of Token B into the Makers wallet.

Future Direction

Optimized Optimistic Rollup [4] [7] [8] also offer an efficient way for combining batch settlements and layer two solutions. Effectively, EAVE could leverage this, either as a layer 2 solution for other blockchains combined with the EAVE Bridging Functionality or replacing a centralized order book above with a lightweight trading layer.

4 Decentralized Financial Platform

A successful DeFi platform needs the following key components which are layered upon each other.

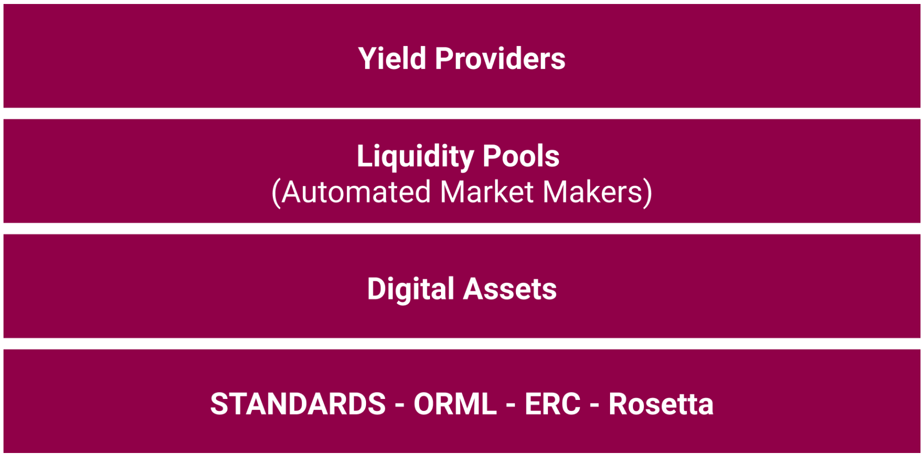


Figure 8: Decentralized financial platform key components

4.1 Standards

EAVE'S Decentralized Financial Platform provides EVM compatibility and robust developer tools including Solidity, Rust and Ink. It also includes standards such as the Polkadot's Open Runtime Module Library and Ethereum's ERC standards.

4.2 Digital Assets

A crucial component for developing a digital asset marketplace is the creation of Digital Assets. These digital assets include the following

- **Native Tokens:** such as BTC, ETH, BNB will be on-boarded via bridging or polkadot native tokens including parachains will be on-boarded automatically.
- **EAVE Tokens:** include any DeFi protocol tokens built by EAVE as well as EAVE's native tokens.
- **DeFi Tokens:** protocol developers bring enormous value to any DeFi ecosystem as such EAVE will combine comprehensive tooling as well as a strong partner focus to on-board DeFi protocols.
- **Stable Coins:** a subset of DeFi Tokens, play a critical role in both value storage and remittances. EAVE will on-board fiat backed, decentralized and algorithmic based stable coins.

4.3 Liquidity Pools

In addition to the support of standard tokens via EAVE's existing exchange and moving forward the POUCH protocol. POUCH provides support for multiple bonding curves. These curves are customized for individual use cases such as Stable Coin Swaps, Price Oracle based swaps and moving forward liquidity bands. For a comprehensive understanding of the various bonding curves that exist and how they may be customized please read our Liquidity Provisioning Paper [**?**].

4.4 Yield Providers

With the above foundational elements in place a Yield Providers can develop their own protocols on the platform allowing Token Holders to earn digital assets, otherwise known as yield farming. The yield engine provides the additional benefit of maximizing both utilization of managed assets as well as increasing the yield for token holders.

5 EAVE's Blockchain

EAVE's Blockchain: is built on top of Polkadot and is targeting being deployed as a Parachain on both Kusama and Polkadot. It can alternatively be deployed as a Parathread, Relaychain or Standalone Network. It provides EVM compatibility and robust developer tools including Solidity, Rust and Ink. It also includes standards such as the Polkadot's Open Runtime Module Library and Ethereum's ERC standards. The integration framework and a suite of standards enable scheduling of remittances, access to price oracles and assets from multiple chains.

5.1 EAVE on Polkadot

EAVE chose to build a dedicated trading chain on Polkadot for a number of reasons.

Liquidity: Polkadot is currently valued at 13% of Ethereum and is poised to have rapid growth in 2021 when it launches it's parachain capabilities.

Ecosystem: Polkadot is growing rapidly with over 386 projects up from 200 in early September of 2020 and a 90% increase in developers in the last 6 months.

Time to Market: Polkadot and Substrate provide a development platform to build blockchains, not just protocols and DApps. As such it is one of the quickest and cost effective ways to launch a dedicated blockchain.

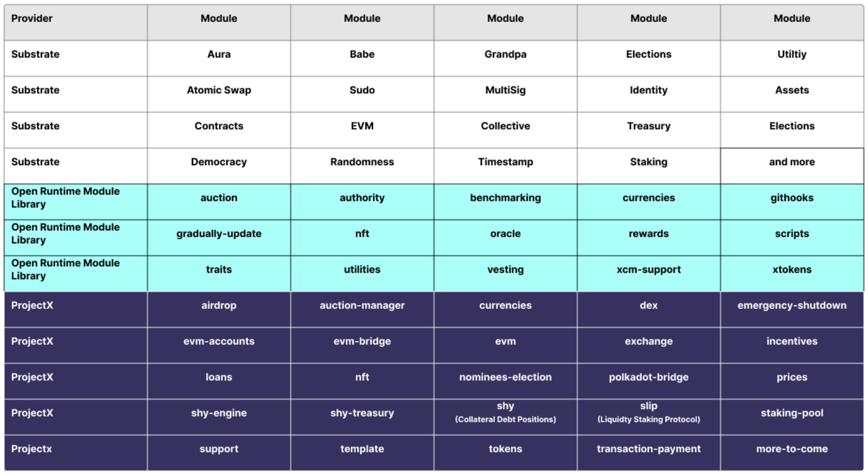
Speed and Cost: fast 5 second settlement time provided by Babe consensus and low gas fees make Polkadot an ideal platform for the EAVE.

FutureProof: Polkadot also allows pluggable consensus which allows upgrades without the need for hard forks. This is particularly important as EAVE moves forward as when it achieves a Network Value Token Value Ratio (NvTvR). Then, the large amount of value stored on the Protocol is secured by the large amount of DOT's for all the parachains and it allows upgrading to a more secure consensus model if needed.

Substrate's modular extensible framework, allows platform developers to pick and choose or modify the modules they implement. Upon this, the community has taken great lengths to create Decentralized Financial Primitives as a set of modules known as the Open Runtime Module Library. Using this as a foundation, at time of writing, EAVE has built upon this with the set of pallets in the diagram below.

5.2 EAVE extensible module overview

The functionality of the above modules can be logically grouped as follows:



Provider	Module	Module	Module	Module	Module
Substrate	Aura	Babe	Grandpa	Elections	Utiltiy
Substrate	Atomic Swap	Sudo	MultiSig	Identity	Assets
Substrate	Contracts	EVM	Collective	Treasury	Elections
Substrate	Democracy	Randomness	Timestamp	Staking	and more
Open Runtime Module Library	auction	authority	benchmarking	currencies	githooks
Open Runtime Module Library	gradually-update	nft	oracle	rewards	scripts
Open Runtime Module Library	traits	utilities	vesting	xcm-support	xtokens
ProjectX	airdrop	auction-manager	currencies	dex	emergency-shutdown
ProjectX	evm-accounts	evm-bridge	evm	exchange	incentives
ProjectX	loans	nft	nominees-election	polkadot-bridge	prices
ProjectX	shy-engine	shy-treasury	shy (Collateral Debt Positions)	slip (Liquidty Staking Protocol)	staking-pool
Projectx	support	template	tokens	transaction-payment	more-to-come

Figure 9: EAVE module overview

5.3 DeFi SDK

The core protocol offers a range of developer options. To deploy Decentralized Financial Applications on EAVE. They are as follows

Solidity and Vyper: EAVE is EVM compatible, allowing DeFi developers who are familiar with writing protocols for Ethereum or other EVM compatible blockchains to easily apply the same toolset to build or port DeFi projects to EAVE.

Rust: is the native development language for EAVE as such Rust Developers can either create *DeFi modules* or *RUST crates* which can be added to the EAVE codebase.

ink! : is a Rust-based embedded domain specific language (eDSL) for writing WebAssembly smart contracts specifically for the FRAME Contracts pallet. At the time of writing *ink!* is still under development and as it matures it will be offered as a DeFi development tool for the EAVE developer community.

5.4 Integration Framework

EAVE is built using an open architecture with a focus on integration and interaction with other platforms and applications.

Off-chain workers

Substrate offers the ability to query off chain data such as price oracles and include that data on chain. This is done via Substrate Off Chain Workers [23].

Price Oracles

As EAVE Trading Platform extends it's functionality to include more real world assets, the use of external price feeds becomes more relevant. The first use case we see for this is for international remittances using unpegged Stable Coins.

Substrate offers the ability to query off chain data such as price oracles and include that data on chain. This is done via Substrate Off Chain Workers [23].

EAVE will leverage this functionality and plans to partner with leading oracle providers such as Chainlink [24] and Band Protocol [25]. The Open Oracle Gateway project [26] [27] is already underway and has industry leaders such as Band Protocol and ACALA leading the initiative.

One risk factor for the use of price oracles is the ability for them to be exploited as happened in the recent Compound exploit where millions of dollars in funds were liquidated [28][29].

However, this was using a centralized price oracle whereas EAVE plans on leveraging a decentralized price oracle. The Open Oracle Gateway project [26] [27] is already underway and has industry leaders such as Band Protocol and ACALA leading the initiative.

EAVE plans to integrate decentralized oracles gradually and it is not targeted for the initial two releases of the EAVE Dex and EAVE Chain. Price oracles are planned to support unpegged Stable Coin Liquidity pools and international remittances and hence are targeted for the expansion release which is targeted for mid 2020.

This gradual rollout will give time for the Open Oracle gateway project to mature. It will also give time for EAVE to perform exhaustive testing and roll the functionality out incrementally targeting smaller trading pairs initially.

5.5 On Chain Features

EAVE On Chain Features lay the foundation for the applications and tooling that are built upon the EAVE chain. They are as follows

Virtual Balances

Decentralized Exchanges often have high slippage, especially when using a constant product model. Arbitragers quickly identify opportunities where the price on the DEX is different from the external market and hence will execute swaps to arbitrage these opportunities. Also, front-running attacks can be used by miners or traders to manipulate the price slippage and arbitrage from regular traders. To solve these issues, EAVE will use the following virtual balances.

Here, we adopt the idea from Vitalik[30] and implemented by Mooniswap[31] of using virtual balances to improve front running resistance.

Assuming at some moment, the balances of a token pair (T_1, T_2) is given by (x, y). We create virtual balance of this pair in two directions $T_1 \to T_2$ and $T_2 \to T_1$ as $(x, y)_{T_1 \to T_2}$ and $(x, y)_{T_2 \to T_1}$. Whenever a swap happens, it will only affect the virtual balance of the corresponding direction. This way, the arbitrager cannot easily gain an advantage by quickly doing a reverse swap. We can reset the values of virtual balances in the beginning of each block. Assuming in one pool, there are n tokens, it will create about $2n^2$ pairs of virtual balances. In practice, we will limit number of tokens in one pool to be capped by 4. This is based on the observation of the most popular pools in existing DEX's such as Balancer and Curve.

Another approach is to store the accumulated price in the block header, similar to Uniswap's approach[32]. This can also help to reduce transaction slippage.

Specifically, it accumulates this price by keeping track of the cumulative sum of prices at the beginning of each block in which someone interacts with the contract. Each price is weighted by the amount of time that has passed since the last block in which it was updated, according to the block timestamp.This means that the accumulator value at any given time (after being updated) should be the sum of the spot price at each second in the history of the contract.

$$a_t = \sum_{i=1}^{t} p_i \tag{1}$$

To estimate the time-weighted average price from time t1 to t2, an external caller can checkpoint the accumulator's value at t1 and then again at t2, subtract the first value from the second, and divide by the number of seconds elapsed. (Note that the contract itself does not store historical values for this accumulator—the caller has to call the contract at the beginning of the period to read and store this value.)

$$p_{t_1,t_2} = \frac{\sum_{i=t_1}^{t_2} p_i}{t_2 - t_1} = \frac{a_{t_2} - a_{t_1}}{t_2 - t_1} \tag{2}$$

Users of the oracle can choose when to start and end this period. Choosing a longer period makes it more expensive for an attacker to manipulate the TWAP, although it results in a less up-to-date price.

We are evaluating these two approaches and may implement features from both approaches to provide the optimal solution.

EAVE Chain provides low gas fees, fast finality and is built on Polkadot and initially planning to use the widely adopted grandpa and babe consensus models[**?**]. One of the great benefits of Polkadot and Substrate is pluggable consensus, which means that a chain can upgrade to a new consensus model if required without needing a hard fork.

There are two main concerns that may be solved by a consensus upgrade.

Front running: Currently, DEX's (which typically run on proof of work and proof of stake consensus) are susceptible to front running, transaction reordering and consensus instability [42][43]. These attacks occur when miners or incentivized parties gain visibility to a transaction and subsequently insert a transaction before the transaction to gain an economic advantage. Mitigation approaches include the randomization of transaction execution order and fixed gas fees. Both of these approaches will be evaluated further as EAVE Chain is implemented.

6 EAVE Token

EAVE's goal is to become a completely decentralized protocol.

6.1 EAVE Wealth Fund

Many Blockchain Protocols are solving the problem of both decentralized governance and long term sustainability using innovative approaches. One such approach is a EAVE's wealth fund. Using a surplus of network and protocol fees it will hold a mixture of digital assets in it's reserve. These funds will be used initially to achieve sustainability and long term can be used to accelerate development, partnerships and ecosystem growth.

6.2 Governance

To that end we are implementing governance capabilities for EAVE Token Holders leveraging Polkadot governance [37] [34] [35] [36]. This will allow the community to drive such things as bonding curve parameters, fee structures for stability fees, liquidation penalties and system (gas) fees. It will also allow the community to vote on the direction of the platform and prioritization of new functionality using a treasury[40]. Governance tools [36] [38] are being developed by the Polkadot community and governance is being used already on networks such as Kusama [39] and planned for implementations on networks such as ACALA [41].

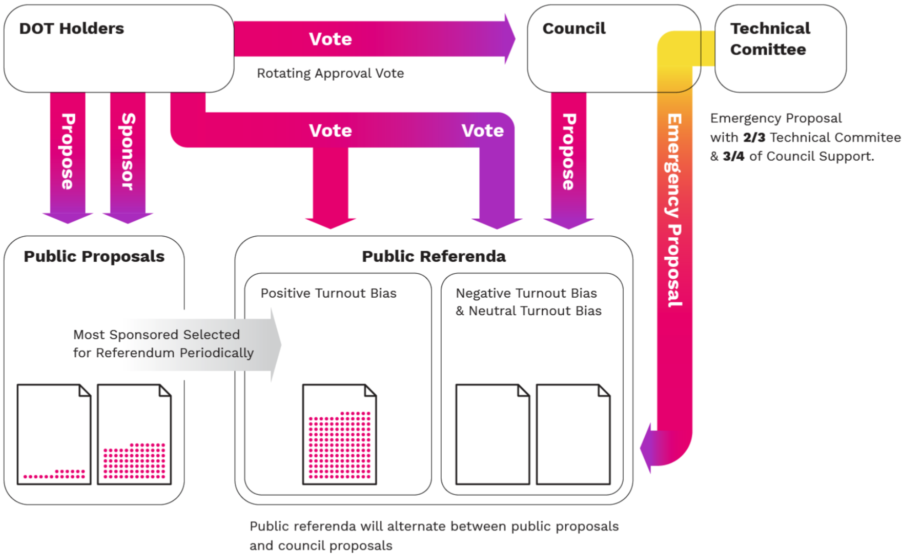


Figure 10: Polkadot Governance Process

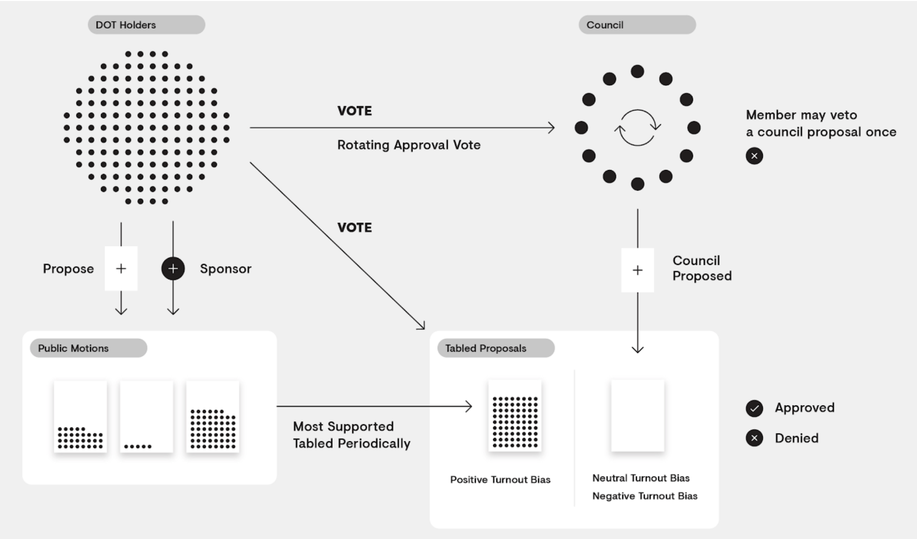
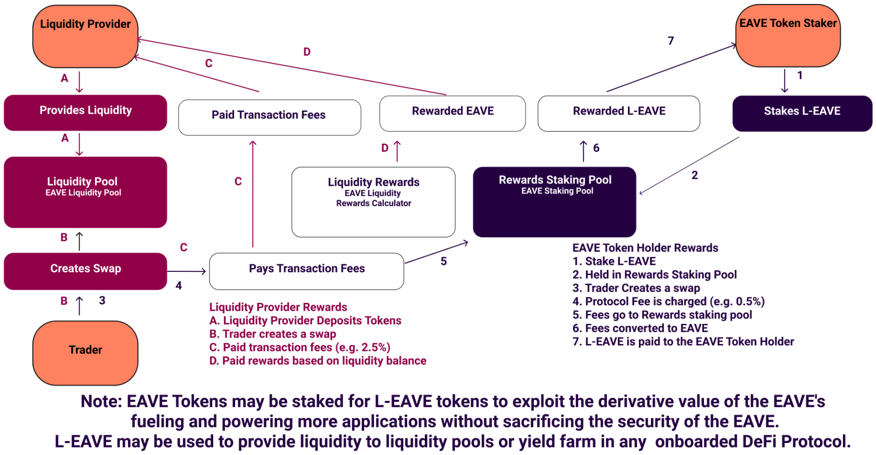


Figure 11: Polkadot Governance Council

6.3 Rewards Module



Liquidity Provider Rewards
A. Liquidity Provider Deposits Tokens
B. Trader creates a swap
C. Paid transaction fees (e.g. 2.5%)
D. Paid rewards based on liquidity balance

EAVE Token Holder Rewards
1. Stake L-EAVE
2. Held in Rewards Staking Pool
3. Trader Creates a swap
4. Protocol Fee is charged (e.g. 0.5%)
5. Fees go to Rewards staking pool
6. Fees converted to EAVE
7. L-EAVE is paid to the EAVE Token Holder

Note: EAVE Tokens may be staked for L-EAVE tokens to exploit the derivative value of the EAVE's fueling and powering more applications without sacrificing the security of the EAVE.
L-EAVE may be used to provide liquidity to liquidity pools or yield farm in any onboarded DeFi Protocol.

Figure 12: EAVE Rewards Capabilities

To ensure a robust set of high-value liquidity pools and growth of EAVE, we are building incentivization mechanisms into the EAVE. They include both transaction fees and liquidity rewards for liquidity providers as well as transaction and stability fees for the EAVE Token Holders. These rewards are targeted to be delivered in EAVE tokens wherever possible. Below is an overview of how each of the four rewards types are created and distributed.

Liquidity Provider Transaction Fees: A percentage trading fee will be charged on all transactions. These fees will be converted to EAVE and rewarded to the liquidity pool providers based on the % of liquidity they have provided relative to the pool and the total liquidity stored in EAVE. The fee structure will be refined but may be fixed at 0.3% similar to uniswap[51] or defined at the pool level with a valid range of 0.0001% to 10% similar to Balancer[52].

Liquidity Rewards: On top of transaction fees, Liquidity Providers will also based on the percentage of liquidity they have provided relative to the pool and the total liquidity stored in EAVE. Since liquidity in pools that have lower trading fees contribute more to the protocol usage than liquidity in pools with high fees, we propose to multiply the USD pool liquidity by a feeFactor that weighs down pools according to their fee (in %) $feeFactor = e^{-(k*fee)^2}$, this formula (inspiration from Balancer) is subject to change in the future.

EAVE Token Holder Transaction Fees: a percentage trading fee will be charged on all transactions. These fees will be converted to EAVE and rewarded to the EAVE Token holders based on the percentage of EAVE they hold relative to the circulating supply, similar to the sushi swap design[53]. When users make trades on the EAVE Exchange, a fee is charged. A percentage of this fee will be added to the EAVEBar pool in the form of Liquidity Pool (LP) tokens for the relative pool. When the rewards are calculated, all the LP tokens are sold for EAVE (on EAVE Exchange). The newly purchased EAVE is then divided up proportionally between the xEAVE holders in the pool, meaning their xEAVE is now worth more EAVE. It will start as 1 EAVE = 1 xEAVE, but just like Liquidity Pool (LP) tokens the price of xEAVE will change over time depending on how many EAVE rewards are in the pool. Further research on reward mechanisms for protocols such as uniswap[54] will be carried out as part of the implementation phase.

6.4 Staking Pool

In a Proof-of-Stake (PoS) network, there will be **natural competition** between assets being used in **staking (for yields)** and assets being **invested in DeFi (for returns)**. This results in a tension between security and liquidity. For example, Polkadot intends to have 50% of the DOTs staked, the rest in circulation would be used for bonding, paying transaction fees and other. **Can we have both security and liquidity at the same time?** The EAVE staking liquidity protocol solves this dilemma. Inspiration for this comes from ACALA[55].

Through the EAVE, staked DOTs become fungible and liquid L-DOTs that exploit the derivative value of the DOTs fueling and powering more applications without sacrificing the security of the whole network.

Users can essentially mint L-DOTs by supplying DOTs to the staking pool managed by the EAVE, and redeem L-DOTs for the underlying DOTs. The exchange rate between L-DOTs and the underlying DOTs are likely to increase over time, as staking rewards are accrued by validating and nominating, and is equal to

$$R_{ExchangeRate} = \frac{N_{sum} + N_{profit}}{N_{L-DOT}} \tag{3}$$

The effective profit/loss, however, is determined by various factors including but not limited to the inflation rate of DOTs[56], the chosen staking strategy and the performance of chosen validator nodes.

Liquid DOT

Users can stake DOTs **trustlessly** with EAVE staking pool, and in return you receive Liquid DOT (L-DOT), accounting for both the DOT amount and on-going staking reward earned. **L-DOT is fungible, can be traded, used for payment, in DeFi e.g. as collateral to generate eUSD stablecoin.** L-DOT as a derivative of DOT would extract residual value of it without compromising or competing for network security. Meanwhile it releases much liquidity for other use cases of a PoS network token.

EAVE is designed as a generic staking liquidity protocol, and firstly implemented for Polkadot and DOT as staking asset.

Note: user would transfer DOTs from Polkadot Relaychain account to EAVE via a bridge, this is being mocked until cross-chain message passing (HRMP) facility is ready.

Early Unbonding

Once DOTs are staked, there is a **28-day unbonding period** which in principle reduces liquidity and improves security and stability of assets at stake. Yet some users may want to have their DOTs back earlier. EAVE fills this need by providing **immediate withdrawn and early unbonding services** in addition to the standard 28-day bonding period. Users are required to pay a higher premium for a shorter wait time (or NO wait time!) to compensate the loss reward of free liquidity.

- **Immediate Withdraw**: A rather high premium is required, as it draws DOTs from the 'Free Pool' where liquidity is reserved by foregoing staking rewards. - **Targeted Unbonding**: user can specify when (in unit of Era) the DOTs need to be released, where a relatively lower fees are charge. The protocol maintains a targeted range of DOTs being unbonded to meet the demands.

Fees are paid in L-DOT and managed by the EAVE Treasury.

Staking Pool

The protocol uses the ‘Maximum Bond Ratio‘ and ‘Minimum Bond Ratio‘ to gauge how much of the deposited DOTs should be staked and how much should be kept in liquidity. The re-balance happens every Era. In addition it manages balances, rewards, slashes, unbonding claims on Relaychain via the bridge, this again will be mocked until cross-chain message passing facility is ready.

L-DOT Holder Voting for Validators

L-DOT holders have rights to vote for favorite validators using a selection mechanism similar to Phragmen election[**?**] to choose (for now) maximum of 16 validators. L-DOTs are required to lock their L-DOTs for voting rights and power.

L-EAVE Tokens

Similarly for the Rewards Staking Pool in the Rewards module, EAVE Tokens may be staked for L-EAVE tokens to exploit the derivative value of the EAVE’s fueling and powering more applications without sacrificing the security of the EAVE network.

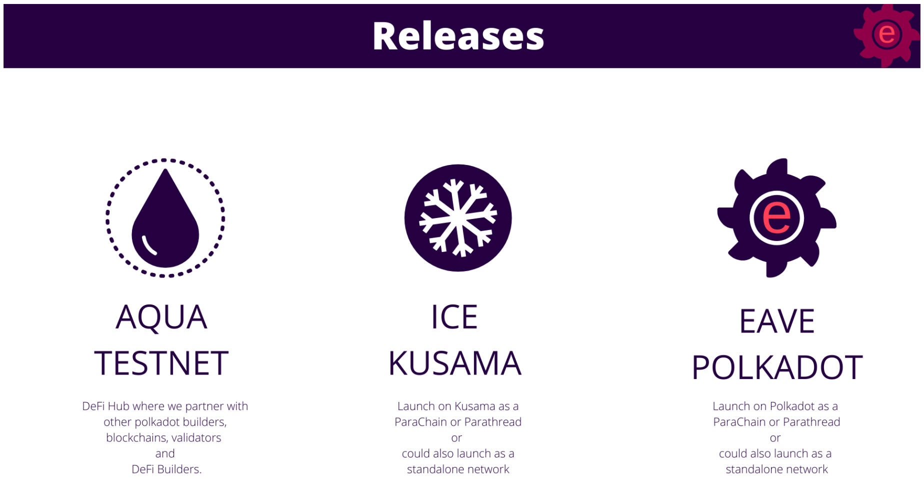
6.5 Economic Security:

One of the problems with securing a network with either Proof of Work or Proof of Stake is that the native token (e.g. Ethereum or DOT) is utilized for economic security. If the digital assets stored on the platform (e.g. ERC20 tokens or stable coins) have a value significantly higher than the value of the native token, then economic security is jeopardized. There have been a number of approaches to solve these. [44][45][46][47][48]. Further research will be done on this as we finalize the EAVE Chain Design.

7 Traction

7.1 EAVE Release Strategy

EAVE has deployed it’s AQUA Testnet and Steam Parachain which it is using to test cross chain settlement as well as it’s Digital Asset Marketplace. It’s planned launch on Kusama is next followed by it’s deployment on Polkadot.



DeFi Hub where we partner with other polkadot builders, blockchains, validators and DeFi Builders.

Launch on Kusama as a ParaChain or Parathread or could also launch as a standalone network

Launch on Polkadot as a ParaChain or Parathread or could also launch as a standalone network

Figure 13: EAVE Feature Roll out

Following are the next targeted features being worked on which will be rolled out incrementally.

- DeFi Protocol - POUCH
- Limit Orders (Order Book)
- Platform Bridges - Binance, Ethereum, Cosmos, Harmony
- Multi-Asset Support
- Protocol Onboarding - DeFi Protocols
- Optional - SuperChain on Polkadot

As you will notice above some of these features may depend upon partnerships. Partnerships and Ecosystem growth are a strong focus with a significant amount of Tokens being dedicated to Ecosystem Growth via grants. This is combined with EVM compatibility, a robust developer toolkit, integration framework and open standards to ensure a developer friendly platform.

EAVE has built an EVM compatible blockchain which has been deployed as a standalone IDE, a standalone Testnet and a parachain. This includes full support for development standards such as ORML and ERC to enable a rich, cost effective development environment as we become a DeFi Hub.

We are now dogfooding our own IDE and development tools as we create our liquidity pool framework. The result will be liquidity pools can be deployed

on other platforms and leveraged by other AMM developers. These liquidity pools can then integrate with yield engines to enhance return for liquidity providers and leverage EAVE Optimized Custodial and Settlement (OCS) to ensure greater liquidity.
https://www.overleaf.com/project/6088c67671e2d486c53c7497 As an aggregator and exchange of digital assets, we plan to work across the complete Polkadot ecosystem, blockchain community as a whole and centralized digital asset providers. Key focus areas include working with other blockchains to enhance their liquidity on their own chain via our liquidity pools and open up cross chain liquidity through our Integration Framework and Optimized Custodial Settlement. Working with DeFi projects to enable them to more easily build AMM's on multiple platforms using our liquidity pool standards.

List of Figures

References

[1] Gavin Wood. 2018. *POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK.* https://polkadot.network/PolkaDotPaper.pdf

[2] Polkadot Wiki. 2020. *Parachains.* https://wiki.polkadot.network/docs/en/learn-parachains

[3] Coinbase Inc, 2020. *Rosetta 1.4.8.* https://www.rosetta-api.org/docs/welcome.html

[4] IDEX, 2019. *The Next Generation of Non-Custodial Trading.* https://idex.io/document/IDEX-2-0-Whitepaper-2019-10-31.pdf

[5] HydraDX, 2020. *AMM combined with in-block order book style transaction clearing, proposing to become the AMM chain for Polkadot—Kusama ecosystem.* https://devpost.com/software/hack-hydra-dx-io

[6] Gauthamastro, 2020. *PolkaDex Light Paper.* https://github.com/Polkadex-Substrate/Documentation/blob/master/polkadex-lightpaper.md

[7] Alex Gluchowski, 2019. *Optimistic vs. ZK Rollup: Deep Dive.* https://medium.com/matter-labs/optimistic-vs-zk-rollup-deep-dive-ea141e71e075

[8] Mangata, 2020. *Mangata — a Polkadot's new hero Decentralized Exchange.* https://medium.com/coinmonks/mangata-a-polkadots-new-hero-decentralized-exchange-e17eb0105942

[9] Research at W3F, 2020 *HRMP Channels.* https://research.web3.foundation/en/latest/polkadot/XCMP/HRMP%20channels.html

[10] Polkadot Wiki, 2020. *Cross-chain Message Passing (XCMP).* https://wiki.polkadot.network/docs/en/learn-crosschain

[11] Research at W3F, 2020. *XCMP Overview.* https://research.web3.foundation/en/latest/polkadot/XCMP/index.html

[12] ChorusOne, 2020. *ormhole: A Cosmos-Substrate bridge.* https://github.com/ChorusOne/wormhole-bridge)

[13] Ruitao Su, 2020. *Bringing BTC to Polkadot: Acala x Ren.* https://medium.com/acalanetwork/bringing-btc-to-polkadot-acala-x-ren-e7959855d5aa

[14] Polkadot Wiki, 2020. *Bridges* https://wiki.polkadot.network/docs/en/learn-bridges

[15] Parity Technologies, 2020. *Parity Bridges Common.* https://github.com/paritytech/parity-bridges-common

[16] IBC Specification Team, 2020. *The InterBlockchain Communication Protocol url:* https://github.com/cosmos/ics/blob/master/spec.pdf

[17] Cosmos 2020. *Interchain Standards.* https://github.com/cosmos/ics

[18] Maksym Zavershynskyi, 2019. *ETH-NEAR Rainbow Bridge* https://near.org/blog/eth-near-rainbow-bridge/

[19] Ganesha Upadhyaya, 2020. *ethhmy-bridge* https://github.com/harmony-one/ethhmy-bridge

[20] Rongjian Lan, Ganesha Upadhyaya, Stephen Tse and Mahdi Zamani, 2020. *Horizon: A Gas-Efficient Trustless Bridge for Cross-Chain Transactions.* https://github.com/harmony-one/papers/blob/master/horizon.pdf

[21] Snowfork 2020. *polkadot-ethereum.* https://github.com/Snowfork/polkadot-ethereum

[22] Alistair Stewart, Fatemeh Shirazi, Leon Groot Bruinderink, 2020. *XCMP - Relay chain light client design.* https://w3f-research.readthedocs.io/en/latest/polkadot/XCMP/index.html

[23] Substrate Developer Hub, 2020. *Off-Chain Workers.* https://substrate.dev/docs/en/knowledgebase/learn-substrate/off-chain-workers

[24] Steve Ellis, Ari Juels and Sergey Nazarov, 2017. *ChainLink A Decentralized Oracle Network.* https://link.smartcontract.com/whitepaper

[25] Sawit Trisirisatayawong, 2020. *Band Protocol White Paper.* https://github.com/bandprotocol/bandchain/wiki/Terminology

[26] Bryan Chen, 2020. *Introducing the Open Oracle Gateway for Polkadot.* https://medium.com/polkadot-network/introducing-the-open-oracle-gateway-for-polkadot-1cf2e1b71c92

[27] ACALA, 2020. *Open Oracle Gateway.* https://wiki.acala.network/learn/basics/oracle

[28] Chris Williams, 2020. *Compound User Liquidated for $49 Million, Price Oracle Blamed.* https://cryptobriefing.com/compound-user-liquidated-49-million-price-oracle-blamed/

[29] Scott Chipolina, 2020. *Oracle Exploit Sees $89 Million Liquidated on Compound.* https://decrypt.co/49657/oracle-exploit-sees-100-million-liquidated-on-compound

[30] Vitalik Buterin, 2018. *Improving front running resistance of x*y=k market makers.* https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281

[31] Anton Bukov, Mikhail Melnik, 2020. *Mooniswap white paper.* https://mooniswap.exchange/docs/MooniswapWhitePaper-v1.0.pdf

[32] Uniswap org docs, 2020. *Core Concepts: Oracle.* ttps://uniswap.org/docs/v2/core-concepts/oracles/

[33] Joe Petrowski, 2020. *Polkadot Governance* https://polkadot.network/polkadot-governance/

[34] Sunshine Protocol, 2020. *Sunshine Governance* https://sunshine-protocol.github.io/sunshine-bounty/intro.html

[35] NucleiStudio, 2020. *Governance OS* https://github.com/NucleiStudio/governance-os

[36] Sunshine Protocol, 2020. *Sunshine Governance* https://sunshine-protocol.github.io/sunshine-bounty/intro.html

[37] Polkadot, 2019. *A Walkthrough of Polkadot's Governance.* https://medium.com/polkadot-network/a-walkthrough-of-polkadots-governance-486555a056e0

[38] Polkadot Wiki, 2020. *Governance.* https://wiki.polkadot.network/docs/en/learn-governance

[39] Gavin Wood, 2019. *Kusama Rollout and Governance, 2019.* https://polkadot.network/kusama-rollout-and-governance/

[40] Polkadot Wiki, 2020. *Treasury* https://wiki.polkadot.network/docs/en/learn-treasury

[41] ACALA Wiki, 2020, *Governance Overview.* https://wiki.acala.network/maintain/governance-guides/governance-overview

[42] thegostep, 2020. *Flashbots: Frontrunning the MEV crisis* https://ethresear.ch/t/flashbots-frontrunning-the-mev-crisis/8251

[43] Philip Daian, Steven Goldfeder,Tyler Kell, Yunqi Li,Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, Ari Juels, 2019. *Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges* https://arxiv.org/pdf/1904.05234.pdf

[44] M. Lokhava et al. 2019. *Fast and Secure Global Payments with Stellar.* https://www.scs.stanford.edu/~dm/home/papers/lokhava:stellar-core.pdf

[45] E. MacBrough 2018. *Cobalt: BFT Governance in Open Networks.* http://arxiv.org/abs/1802.07240

[46] D. Mazieres. *The stellar consensus protocol: A federated model for internet-level consensus". In: StellarDevelopment Foundation 32 (2015).* http://www.scs.stanford.edu/~dm/20160606-scp-talk.pdf

[47] T. Rocket, 2020. *Snowflake to avalanche: A novel metastable consensus protocol family for cryptocurrencies.* https://ipfs.io/ipfs/QmUy4jh5mGNZvLkjies1RWM4YuvJh5o2FYopNPVYwrRVGV

[48] Anatoly Yakovenko, Feb 2018. *Solana: A new architecture for a high performance blockchain v0.8.13* https://solana.com/solana-whitepaper.pdf

[49] Hayden Adams, Noah Zinsmeister, Dan Robinson. 2020. *Uniswap v2 Core.* https://uniswap.org/whitepaper.pdf

[50] Fernando Martinelli, Nikolai Mushegian. 2019. *A non-custodial portfolio manager, liquidity provider, and price sensor.* https://balancer.finance/whitepaper/

[51] Uniswap Org, 2020. *Advanced Topic Fees.* https://uniswap.org/docs/v2/advanced-topics/fees/

[52] Balancer Finance, 2020. *Are there constraints for setting up a Balancer Pool?* https://docs.balancer.finance/getting-started/faq#are-there-constraints-for-setting-up-a-balancer-pool

[53] SushiSwap, 2020. *SushiSwap Staking SushiBar (xSushi).* https://help.sushidocs.com/products/sushiswap-staking-sushibar-xsushi

[54] Uniswap Org 2020. *Introducing UNI.* https://uniswap.org/blog/uni/

[55] Bette Chen, 2020 *Homa Liquid DOT.* https://github.com/AcalaNetwork/Acala/wiki/7.-Homa-Liquid-DOT

[56] Alfonso Cevallos, Jonas Gehrlein, 2020. *W3F Token Economics.* https://w3f-research.readthedocs.io/en/latest/polkadot/economics/1-token-economics.html

[57] Fernando Martinelli, 2021 *Introducing Balancer V2: Generalized AMMs* https://medium.com/balancer-protocol/balancer-v2-generalizing-amms-16343c4563ff

[58] Fernando Martinelli, 2021 *Aave Balancer Partner to Build The First Asset Manager for Balancer V2* https://medium.com/balancer-protocol/balancer-partners-with-aave-to-build-the-first-v2-asset-manager-d9c173330151

[59] Mike McDonald, 2021 *Developers: Balancer V2 Smart Contracts Are Now Live* https://medium.com/balancer-protocol/developers-balancer-v2-smart-contracts-are-now-live-e97002ee0310

[60] Balancer Team *Balancer V2* https://github.com/balancer-labs/balancer-core-v2