LiquiDAO: Bitcoin Enabled Finance

May 2021

liquidao.io

Abstract. Bitcoin is an instrument of global economic empowerment and a consolidated standard for individuals and organisations around the world to participate in a global monetary system, securing their financial future.

The rise of the Decentralised-Finance (DeFi) movement highlights the necessity for a permissionless alternative to today's heavily-centralised banking system.

LiquiDAO is the world's first Decentralised Anonymous Organisation designed to be the leader in accelerating Bitcoin enabled De-FI.

Relying on Bitcoin and Liquid Network, LiquiDAO aggregates and deploys financial liquidity into trust-minimised and non-custodial trading services, leveraging Discreet Log Contracts (DLC), Hashed Time-Locked Collateral Contracts, Multisignatures, and atomic swaps.

1. Vision and Introduction

We believe in a financial system that aligns incentives to further accelerate Bitcoin adoption as the world reserve currency, retaining as many properties and assurances of Bitcoin as possible—verifiable, pseudo-anonymous, borderless, and accessible by all.

Given the current uncertainty from a macroeconomic and monetary regime perspective that is leading to a hyper inflated economy and FIAT monetary debasement[1], and consequently, a rapidly evolving Bitcoin community, we believe now is the opportune time to join forces and launch this global common initiative.

Furthermore, recent events involving the censorship of some centralised exchanges — as shown by the arrest of the leadership team at BitMex, OKEx[2] and the ban of US users from the Binance platform — highlight the growing regulatory pressures on the crypto industry.

It is therefore vital to ensure an efficient, decentralized, and scalable financial system that can better manage regulatory capture while minimising trust in custodians third parties. For these reasons, LiquiDAO is established as a community-driven effort to accelerate the advent of Bitcoin-Enabled Finance.

LiquiDAO members can opt into a parallel, permissionless, and confidential financial infrastructure. Members benefit from the economic insights of a common liquidity pool while actively playing a key role in stewarding the development and adoption of Bitcoin-Enabled Finance.

---

1   https://bitcointalk.org/index.php?topic=3045707.0
2   https://www.financemagnates.com/cryptocurrency/news/okex-bitmex-more-are-btc-hodlers-losing-trust-in-crypto-exchanges/

LiquiDAO's design is optimised to achieve the following outcomes:

- Enable even greater Bitcoin adoption by concentrating more capital and development resources to Bitcoin-Enabled financial services;
- Empower every individual from anywhere in the world to opt into a parallel, permissionless, and confidential financial infrastructure that is independent from trusted parties;
- Accelerate the growth of Liquid Network — Bitcoin sidechain[3] — by creating an incentivised model designed to rapidly increase financial liquidity and energise Liquid Members for greater cooperation;
- Serve as a community-led guiding force to steward development, curation, and discovery of interoperable and non-custodial financial services;
- Bridge liquidity from other blockchain ecosystems onto the Liquid Network.

2. Design Overview

LiquidDAO enables a seamless and interoperable ecosystem of Bitcoin-Enabled financial applications. Its design relies on Liquid Network as a Settlement layer built on top of Bitcoin. It leverages primitives such as Asset Issuance, Discreet Log Contracts (DLC), Hashed Time-Locked Collateral Contracts, Multisignatures, and Atomic swaps.
LiquiDAO deploys liquidity on integrated non-custodial and trust minimised applications such as trading pools on top of

---

3   https://liquid.net/

atomic swaps platforms, derivatives, and over-collateralized
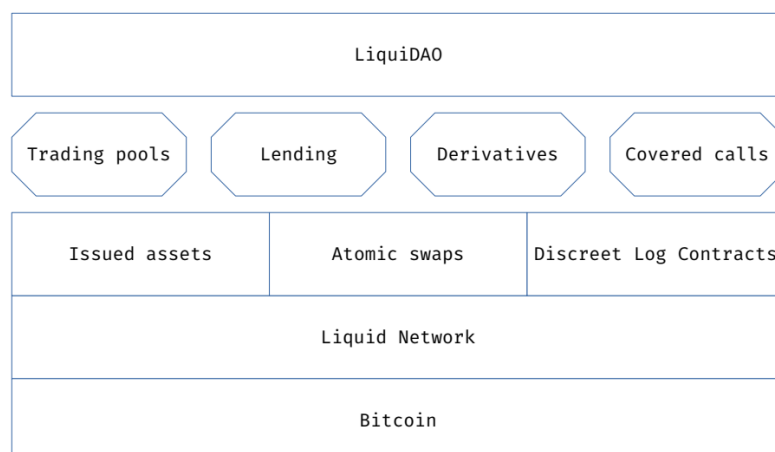
lending platforms.

2.1 Liquid Network: A Bitcoin sidechain-based settlement network for traders & exchanges.

Liquid enables faster, more confidential Bitcoin transactions, and the issuance of digital assets. Every Bitcoin on the Liquid Network are verifiably backed 1:1 on the Bitcoin main chain. Once a user transfers Bitcoins to Liquid, they can seamlessly make transactions, enjoying the network's speed, confidentiality, and asset issuance features.[4]

Liquid is operated by a federation of members which include exchanges, trading desks, and other cryptocurrency companies. Members collectively manage the network and guide its development. Every member has little to no power to halt a specific transaction thanks to the Confidential Transaction capabilities. End users of Liquid can fully

---

4   https://www.blockstream.com/sidechains.pdf

validate blocks that are signed by members running a full node Liquid implementation.

In the upcoming months, Liquid Network is evolving into a dynamic federation model[5], ensuring a higher degree of security and trust-minimised block verification.

Another essential building block is the upcoming rollout of Simplicity scripting language[6], which will allow more complex financial capabilities and self-enforcing covenants[7] in Multisignature contracts.

2.2 Financial primitives

Liquid inherits both the UTXO Model and the scripting language from Bitcoin, such as Multisignature[8], DLC[9], and HTLC[10]. Combined with its confidential transactions and asset issuance features, Liquid Network enables scalable and global atomic swaps, future contracts, derivatives, synthetic stocks, and over-collateralised lending.

2.3 Protocols, Applications, and Services

The following interoperable protocol applications guarantee a solid foundation to deploy capital and offer a wide range of financial services in a non-custodial fashion:

---

5   https://github.com/ElementsProject/elements/pull/642
6   https://blockstream.com/simplicity.pdf
7   https://fc17.ifca.ai/bitcoin/papers/bitcoin17-final28.pdf
8   https://github.com/bitcoin/bips/blob/master/bip-0010.mediawiki
9   https://adiabat.github.io/dlc.pdf
10   https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki

- Atomic-swap based, privacy-prioritised, Decentralised Exchange platforms built on the Liquid Network;
- Derivatives with trust-minimised forward contract transaction on the Liquid Network based on Discreet Log Contracts (DLC);
- P2P over-collateralised loan platforms based on Multisignature escrow and Hashed Time-Locked Collateral Contracts.

3. DAO: Decentralised Anonymous Organisation

To achieve its vision, LiquiDAO aims to serve as a catalyst for the growth of the above native protocols, applications, and services. The DAO will operate as a financial cooperative, offering added-value products and services for the benefit of all members.

3.1 Members

Key actors involved in the network:

- Liquidity Providers: Financial agents that lock liquidity into the DAO-owned trading pool;
- Traders: Financial actors that plug into the DAO-owned trading interfaces and markets;
- Liquid Federation Members: Individuals and organisations that are part of the Liquid Network and are proactively offering Liquid-based financial solutions.

3.2 Key Activities

- Running a trading pool infrastructure, collecting fees on each swap executed by the underlying market makers;
- Deploying liquidity on trading pairs, collecting swap fees gained by the market making activities;
- The DAO will trade liquidity-exploiting arbitrage opportunities between the spread of cryptocurrencies listed in various DEXs of other blockchains (Uniswap, Balancer, SushiSwap, PancakeSwap, etc);
- Facilitating over-collateralized lending of Liquid Bitcoin and stablecoins on p2p lending platforms;
- Earning yield on Bitcoin in a non-custodial, DLC-based covered call contract;
- Running an Oracle service for DLC-based derivatives, synthetic stocks, and futures;
- Wrapping existing digital assets from other blockchain ecosystems onto Liquid, providing additional liquidity to its trading pairs.

All proceeds generated from the above activities will be:

- Reinvested by the DAO's members to develop new products and solutions;
- Allocated as operative capital to buy back LDAO tokens.

3.3 Key Benefits for Members

- Increased liquidity in a non-custodial fashion, aggregated in a single interface, including ancillary services that streamline trading across assets;

- Increasing rewards and access to additional market volume and a broader set of traders by locking liquidity into a trading pool;
- Incentivise Liquid Partners to collaborate in a fully integrated financial ecosystem built on Liquid Network;
- Participating to the financial and economical insights granted by holding LiquiDAO tokens.

3.4 Founding Team

The founding team acts as a guiding force to coordinate the successful launch of the DAO. The aim is to gradually delegate both the direction and control of funds and activities to its community. The anonymous nature of LiquiDAO is instrumental in fulfilling its vision to preserve the original Bitcoin ethos and overcome rent-seeking government policy standards such as KYC/AML.

4. LDAO Token

LDAO serves as the governance token and as an incentive to bring liquidity onto LiquiDAO's network. Furthermore, it enables LiquiDAO to secure the resources necessary to develop its vision.

The following benefits apply to LDAO members — token holders that lock their tokens in a verifiable timelock script.[11]

- Influence the allocation of DAO resources;
- Fund initiatives that support the development, integration, and adoption of additional financial services;

---

11 https://github.com/bitcoin/bips/blob/master/bip-0112.mediawiki

- Benefit from discounted trading fees on LiquiDAO's pools;
- LDAO tokens grant its users a portion of the Pool fees.

4.1 Static Rewards

To achieve the goal of constant increased liquidity, LDAO token features a Static reward model.

The reward amount is conditional upon the volume of the token being traded in order to alleviate the downward selling pressure of early adopters and incentivize liquidity.

Moreover, the reward mechanism encourages holders to hold their tokens to access higher bonus rewards which are based upon percentages carried out and dependent upon the total tokens held by the owner.

4.2 Liquidity Mining

The Liquidity Mining program incentivises users to become a Liquidity Provider (LP) in the LiquiDAO trading pool.

By providing liquidity in the LiquiDAO protocol, LPs are eligible to receive a daily LDAO reward on a pro-rata basis to the assets provided, as well as a higher portion of pool fees.

4.3 Manual Burn

Having burns controlled by the team and promoted based on achievements helps keep the community rewarded and

informed. The conditions of the manual burn and the amounts can be advertised, tracked, and verified.

LiquiDAO aims to implement a burn strategy that is beneficial and rewarding for those engaged for the long term. Furthermore, the total number of LDAO burned is featured on our readout located on the website which allows for further transparency in identifying the current circulating supply at any given point.

Over time, the burn mechanism will be decentralised and fully controlled by the token-holder community.

5. Governance

The DAO is a financial cooperative operated by its members. The founding team is committed to delegate control of the treasury and its core infrastructure to the members over time.

5.1 Governance Roles

LiquiDAO's governance model is fulfilled through the following key roles, assuring different degrees of control and responsibilities:
- **Directors** are trusted community members that oversee the DAO's infrastructure, secure revenues and treasury, and publish rules and proposal results.
- **Members** hold an average balance of LDAO tokens above the voting threshold defined by the community and are eligible to issue new proposals and cast votes.
- **Witnesses** are members willing to supervise the off-chain voting infrastructure, running a node and

verifying the replica log correctness against the recurrent timestamp[12] published by the directors.

5.2 Treasury

The treasury is a time-locked multi-signature that holds rewards and contributions in Liquid asset and is responsible for issuing and burning LDAO.

The majority of the signers are the directors with a minority of keys retained by members that are chosen randomly after each time-lock period. In the rare case of time-lock expiration, all funds could be spent by the minority. This serves as a sort of dead man switch to ensure business continuity, forcing the directors to move funds to a new Multisignature in a timely manner.

All Members can view the treasury's list of transactions. With the advent of Simplicity, we will deploy more granular covenants that can limit the spending power of the directors, adding an additional security layer.

5.3 Infrastructure

To coordinate operations across pseudo-anonymous members, directors will deploy a set of web apps published as Onion services.

All proposals are submitted to a public git repository. Everyone can view the proposals and add comments.

---

12   https://petertodd.org/2016/opentimestamps-announcement

Votes, consisting of messages signed with members' private key, will be submitted to an interface that verifies the corresponding locked average balance.

Anyone can run a read-only node voting infrastructure, independently hashing the replica log and verifying it against the timestamp published by the directors.

6. Conclusion

LiquiDAO is a financial system that enables scalable, non-custodial, and trust-minimised trading services. The system relies on Bitcoin and Liquid Network core functionalities, therefore inheriting its key properties and assurances — verifiable, pseudo-anonymous, borderless, and accessible by all. Designed as an anonymous community-led financial cooperative, the system incentivises users to play an active role in fueling its core activities and to steward governance of the common pool of liquidity.