Non-custodial Bank

Joe Blau

6a6f65626c6175@proton.me

v1.0

July 26, 2023

Abstract

The services of a bank, backed 100% by smart contracts, operating without reliance on financial institutions and centralized counter-parties. Trusted and vetted onchain hyperstructures[1] replace the existing banking infrastructure by providing banking services. Protocols are abstracted as services, and public/private key pairs are abstracted as accounts. The two largest challenges to onboarding the next billion users are the risks of losing money and losing keys. The non-custodial bank addresses both of these challenges with Services and Accounts.

1 Introduction

Modern economics relies on financial institutions to facilitate actions such as trading, borrowing, lending, and yield generation. While this system works well for some, it can be predatory and may prevent individuals from truly having freedom and access to their money. It also suffers from misaligned incentives where financial institutions can make substantial bets, privatize gains and socialize losses.

A non-custodial bank is a bank that offers all of the same services as a traditional bank, but relies 100% on protocols on the blockchain to provide these services. Many protocols have proven resilient to coercion and socializing losses, by enforcing strict rules in the smart contracts that can't be overturned.

2 Services

The sole aim of Service construction is capital preservation. Each service is backed by a set of cryptographic protocols that meet the non-custodial bank's risk threshold. Services include, but are not limited to, products for Trading, Lending, Borrowing, and Yield. Each corresponding service will have a protocol or set of protocols that empowers the bank owner to interact with the protocol in a trustless way. These services are a representation of what a non-custodial bank could offer. It would be incumbent upon the architect of the bank software to operate within the regulatory and legal framework of their jurisdiction.

Services					
Trade	Lend	Borrow	Yield	Derivatives	Privacy
Uniswap	Compound	Compound	Uniswap	DyDx	Tornado
Solidty	AAVE	AAVE	Curve	GMX	
Balancer			Liquity		

2.1 Risk Criteria

In assessing protocols supporting various services, the most crucial consideration is the potential risk of failure. The established risk criteria aims to safeguard capital and reduce the likelihood of scams, deceitful liquidations, market manipulations, fraudulent activities, and security breaches. From a conservative standpoint, any protocol affirming two or more of these risk factors is deemed excessively risky for inclusion in a non-custodial bank.

- Lack of auditing
- Administrative keys with comprehensive control over functionality
- Economic centralization exceeding 51%
- Age of protocol is less than 18 months
- Previous history of a security breach
- Total Value Locked TVL is under \$50 million
- Transaction volume is below \$5 million
- Presence of an anonymous founder
- Protocol operating on fewer than four blockchain networks
- Utilization of offchain oracle data feeds
- Capability of the protocol to undergo upgrades

3 Accounts

The sole aim of Account management is access control preservation. Accounts are an abstraction built on top of public and private keys. Accounts should have the ability to engage in any operation that can be performed by an Externally Owned Address EOA without the use of a smart contract or custom software.

3.1 Vault

Account vaults are used to aggregate and manage public and private keys. Each individual should have full access to their vault with the ability to verify and sign transactions with any keys in the vault.

3.2 Forgot Password

The ”Forgot Password” feature is designed to preserve accounts and mitigate issues such as losing private keys, forgetting private keys, and ensuring any user can restore their accounts in a trusted, decentralized way. Shamir’s Secret Sharing[4] can be used to back up the user’s vault, preventing access to the vault unless a quorum of a group acts together to pool their knowledge. The owner must have a method to send and request pieces of the vault from the quorum in order to back up and reconstruct their Vault.

4 Conclusion

We propose the strategy of implementing Services and Accounts. Services are designed to mitigate capital loss and Accounts are designed to mitigate key loss. These two factors account for more than 90% of the capital being lost in crypto. By addressing these two challenges, we pave the way to onboard the next one billion users onto crypto.

References

[1] Jacob Horne (2022) Hyperstructures: Crypto protocols that can run for free and forever, without maintenance, interruption or intermediaries.

[2] Hayden Adams, Noah Zinsmeister, Dan Robinson (2020) Uniswap Core V2:

[3] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, Dan Robinson (2021) Uniswap Core V3:

[4] Adi Shamir (1979) How to Share a Secret: In this paper we show how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces