VaultCoin: Powering the Hybrid Custody Ecosystem

Abstract

VaultCoin is the utility token underpinning the Hybrid Custody Ecosystem, a decentralized cryptocurrency custody system addressing the vulnerabilities of traditional cryptocurrency custody solutions. With innovative Layer 2 Smart Vaults technology, the Hybrid Custody Ecosystem ensures Bitcoin and similar Altcoins are Unstealable, Unlosable, and Unconfiscatable, setting a new standard for secure crypto management.

VaultCoin combines cutting-edge technology from both open and closed ecosystems with quintessential real world services to create a decentralized and trust-minimized crypto custody management system on-chain.

---

1. Problem Statement

Individuals and institutions managing non-trivial crypto holdings face several challenges in the current cryptocurrency ecosystem that hinder broader acceptance and adoption by such entities. Crypto Custody is a 3 Trillion USD problem and below are the core issues plaguing this ecosystem:

1.1 Private-Key Dependency

Cryptocurrencies rely heavily on private keys for access and control. Losing or compromising a private key can result in the permanent loss of assets. Research estimates that approximately 3 to 4 million Bitcoin are lost due to lost private keys. [1] This represents a staggering $300 billion to $400 billion in lost assets. All this creates an immense psychological and financial burden for users, deterring newcomers from entering the ecosystem directly and prompting them to employ indirect methods to gain exposure to cryptocurrencies.

1.2 Limited Recovery Mechanisms

Unlike traditional financial systems, cryptocurrencies lack robust mechanisms to handle lost or stolen credentials. Existing solutions like hardware wallets and multi-signature setups fail to provide adequate protection when private keys are lost or stolen. Furthermore, multi-signature setups come with their own pitfalls and are often cumbersome for everyday users.

1.3 Inheritance and Custody Gaps

Inheritance planning is a critical gap in the cryptocurrency space. With no seamless method to transfer digital assets to heirs, many users resort to risky and inefficient workarounds. This lack of trustworthy and dependable inheritance mechanisms discourages long-term holding of cryptocurrencies and creates barriers for estate planning in an increasingly tokenized world.

These systemic challenges severely undermine the accessibility, security, and usability of cryptocurrencies, creating an urgent need for innovative solutions.

---

2. The Hybrid Custody Vaults

Hybrid Custody Vaults offer a groundbreaking approach to cryptocurrency custody by blending the best of self-custody and the best of managed custody solutions. They ensure user control while eliminating single points of failure.

2.1 Hybrid Custody Vault Design

Hybrid Custody Vaults are built on a dual-party dual-key architecture and cutting-edge Layer 2 protocols:

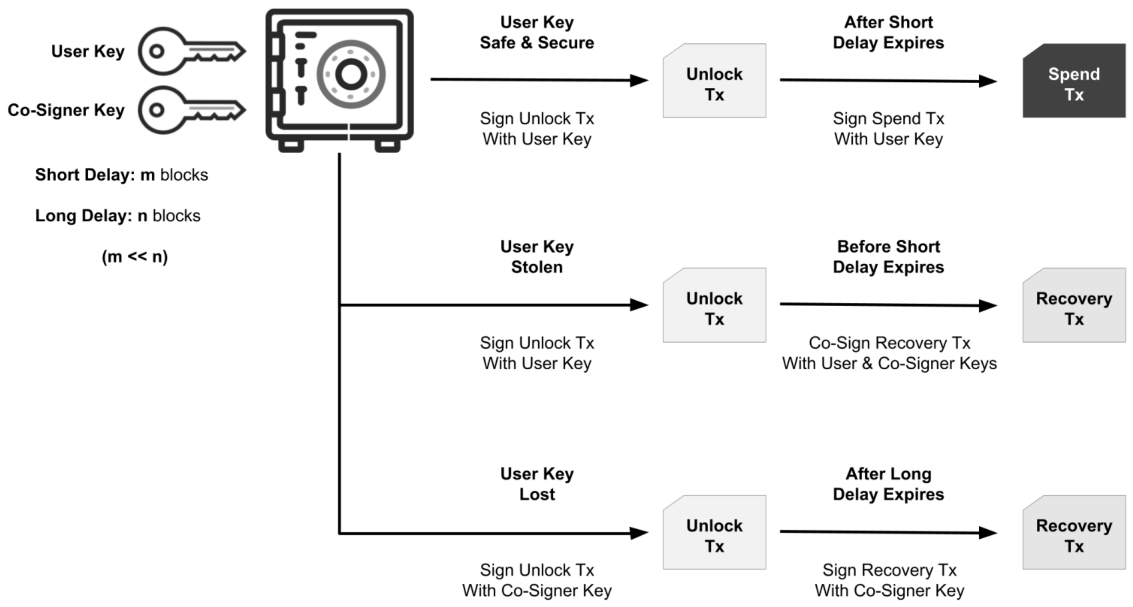
- **Dual Private-Key Architecture**: Each vault is secured using two private keys—one held by the user and the other by the user's Hybrid Custody Service Provider (co-signer). Under normal circumstances, users can transact using only their private key, similar to self-custody wallets. However, the second private key held by the user's Hybrid Custody Service Provider plays a vital role in enabling recovery mechanisms when the user's private-key is lost or stolen.

- **Zero-Knowledge Proofs and Smart Contracts**: The integration of interactive zero-knowledge proofs and smart contracts ensures that cryptocurrencies locked using Hybrid Custody Vaults can be recovered with no loss even when a user's private-key is lost or stolen.

- **Two Step Unlock and Spend Mechanism:** Unlike regular transactions spent using one or more private-keys (MultiSig), Hybrid Custody Vaults need to be unlocked with an on-chain Unlock Transaction before they can be spent using a Spend Transaction. There is also a configurable delay (1-to-n blocks) enforced between these Unlock and Spend transactions. This mandatory two step unlock and spend process with configurable delay helps the user and the Hybrid Custody Service Provider to initiate recovery mechanisms if the unlock is not initiated by them and when they suspect foul play.

For further details about Hybrid Custody Vaults and Layer 2 Smart Vaults protocol, please refer to the white paper - Hybrid Custody using Layer 2 Smart Vaults for Cold Storage. [2]

2.2 Recovery Mechanisms



Hybrid Custody Vaults provide robust solutions to address private key loss and theft:

- **Private-Key Loss**: In cases where users lose their private key, the system leverages the Hybrid Custody Service Provider's key in combination with zero-knowledge proofs and smart contracts to securely recover the tokens locked in the vault. This eliminates the risk of permanent loss due to user error, negligence and factors beyond user's control.

- **Private-Key Theft**: If a malicious actor gains access to the user's private-key and attempts unauthorized transactions, the Hybrid Custody Service Provider can help override such attempts by co-signing a recovery transaction with the user. This two-key approach combined with smart contracts and zero-knowledge proofs ensures that funds remain safe even in the event of key theft.

Note: Users can always override any unauthorized unlock and spend attempt by their Hybrid Custody Service Provider using just their private-key. So there is no counterparty risk when using Hybrid Custody Vaults.

2.3 Advanced Features

Hybrid Custody Vaults go beyond security and recovery, offering much needed additional functionality to users:

- **Crypto Inheritance**: Hybrid Custody Vaults simplify inheritance planning by enabling users to set up instructions with their Hybrid Custody Service Provider for transferring assets to designated beneficiaries after the event. This eliminates the need for risky manual private-key sharing arrangements and ensures that digital assets are

seamlessly passed on.

- **Insider Fraud Prevention**: The dual-key design and co-signing mechanisms make Hybrid Custody Vaults resistant to both internal and external threats. Insiders, even with access to the user's private-key, cannot steal the user’s coins, thereby removing the incentive to conspire in the first place.

- **Hardware Tokens**: Hardware Tokens are just like Hardware Wallets but lack any seed phrase export mechanisms. Private-Keys are randomly generated inside Hardware Tokens and physical access to these devices is required to sign transactions using them. Hybrid Custody Vaults can leverage these Hardware Token based 2FA by requiring certain recovery pathways to need signatures from private-keys inside these Hardware Tokens.

- **Fallback Recovery Options:** Additional layers of protection can be added to the Hybrid Custody Vault by allowing private-keys from the Platform provider to be used in place of Hybrid Custody Service Providers private-key for signing recovery transactions. This allows the Platform provider to step in and manage recovery when the Hybrid Custody Service Provider is unreachable during the recovery window. Hybrid Custody Vaults are scalable and flexible enough to handle as many contingencies as needed.

By addressing the critical gaps in private key management, recovery, and inheritance, Hybrid Custody Vaults redefine how users interact with and secure their cryptocurrency holdings.

2.4 Comparison with MultiSig / MPC Vaults

2.4.1 Comparison with MultiSig:

MultiSig (m-of-n where m < n) Vaults can tolerate the loss and theft of a subset of private-keys used to create them and are often touted as a solution to the lost/stolen private-keys problem. But, MultiSig Vaults come with the burden of managing multiple private-keys when most crypto holders are shying away from setting up and managing a single private-key due to the complexities involved. More often than not, users store their Multi-Sig private-keys together or nearby for easy access, completely negating the benefits of the said scheme.

Some MultiSig setups, delegate the responsibility of additional private-keys to near and dear or third parties to simplify private-key management and to prevent users from becoming a single point of failure for their Vault setups, but these co-signers can then restrict users’ ability to spend and transfer their tokens as they see fit or can conspire and steal users’ coins!

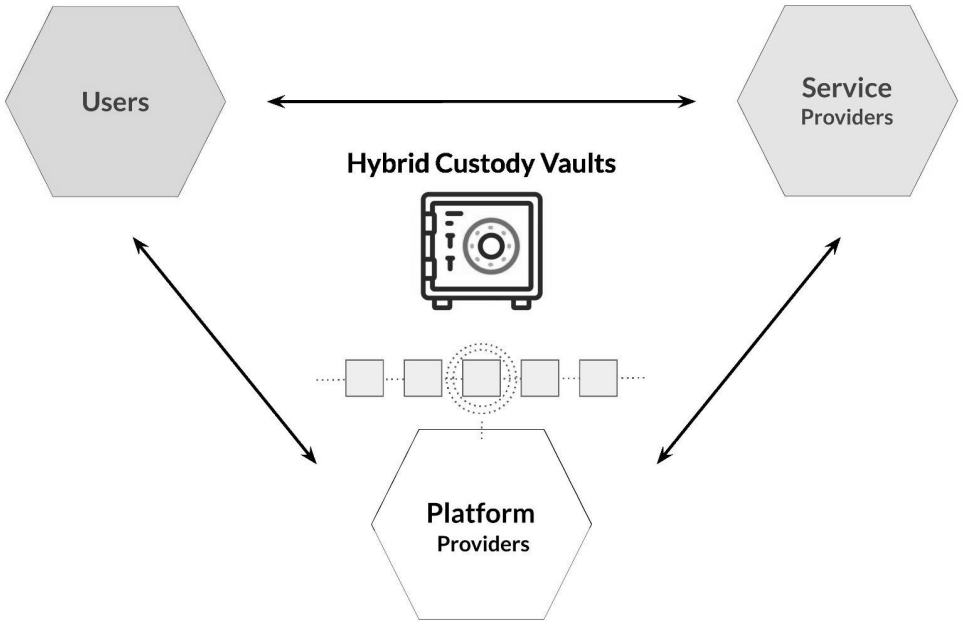
In the end, users either need to dilute their control over their crypto and risk insider fraud or accept themselves as a single point of failure for their crypto with MultiSig Vaults - which is a choice they don't need to make with Hybrid Custody Vaults. Moreover, there is no way to implement any kind of override, recovery, or clawback using MultiSig constructs making Hybrid Custody Vaults exponentially better than MultiSig.

2.4.2: Comparison with MPC-TSS:

MPC-TSS Vaults are similar to MultiSig Vaults but execute the quorum logic off-chain and in our opinion are worse than MultiSig for most use cases. Importantly, MPC-TSS Vaults give plausible deniability to participants signing malicious transactions as we cannot trace which fragments were used to sign a spending transaction once fully signed.

---

3. Hybrid Custody Ecosystem



Hybrid Custody Ecosystem consists of:

- **Platform Providers:** Provide the hardware wallet devices, companion apps, and backend services.

  Note: Guardian is the flagship platform of this ecosystem and more platforms catering to different markets like institutional custody will be built to leverage this ecosystem as it matures.

  Guardian Hardware Wallet and companion apps seamlessly manage Hybrid Custody Vault setup, termination and recovery making all these steps as simple as signing any other transaction using Hardware Wallets like Ledger or Trezor. The dual-party dual-key Vault architecture is abstracted away by the platform to the point that it all appears like signing a simple transaction.

- **Hybrid Custody Service Providers**: Serve as local touch points for users across the world and coordinate vault setup and recovery when needed. They also manage

identity verification, recovery and inheritance in compliance with local laws and regulations for respective users.

- **Users**: Create Hybrid Custody Vaults to protect their coins using available Platforms and any of the Hybrid Custody Service Providers listed on those platforms.

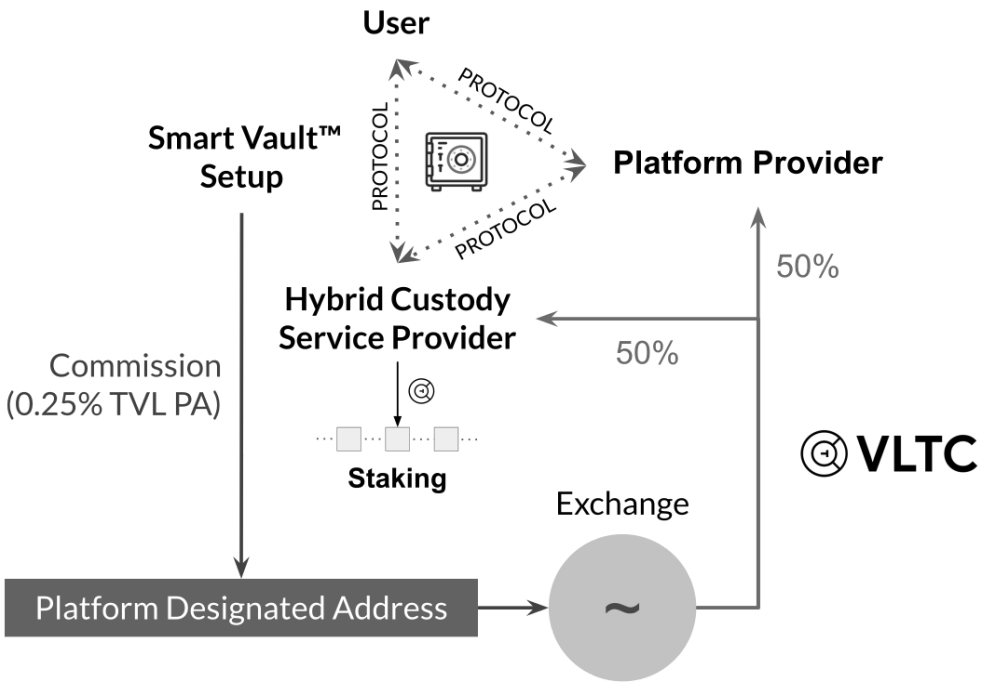
User's are free to choose their Hybrid Custody Service Provider on their chosen platform, depending on their needs and priorities, and the platform will enable a seamless experience for them.

4. VaultCoin

VaultCoin powers the Hybrid Custody ecosystem, ensuring smooth operation and incentivizing ecosystem participants.

Key utilities include:

4.1 Fee Payments by Users



A small percentage fee is deducted from assets protected by Hybrid Custody Vaults during setup and the respective coins are pooled and swapped for VaultCoin in open markets asynchronously. This mechanism makes vault setup and recovery gasless and friction free. The VaultCoin thus earned is then distributed among the stakeholders - the Platform Provider and the respective Hybrid Custody Service Provider, ensuring long term sustainability of the ecosystem and a continued demand for VaultCoin.

4.2 Staking by Hybrid Custody Service Providers

Hybrid Custody Service Providers must acquire VaultCoin from open markets and stake the same on the platform to come onboard as co-signers and earn VaultCoin as compensation for their services such as providing recovery and inheritance support.

4.2.1 Staking Pools

Hybrid Custody Service Providers can create staking pools, allowing other VaultCoin holders to stake their holdings alongside the providers' own holdings to earn a piece of the fee revenue earned by the Service Provider. These combined stakes serve as a guarantee for users creating Hybrid Custody Vaults with the respective Service Provider. It should be noted here that any lapses by the Service Provider could affect the staked coins of staking pool participants too. However, Service Provider's stake will be slashed first and pool participants' stake will be slashed only when Service Providers stake is not sufficient to cover the penalties levied on it.

4.3 Staking Rewards

VaultCoin staking by service providers and holders via service provider pools ensures and promotes active ecosystem participation. They are in turn compensated by fees paid by users during vault setup and other rewards distributed to incentivize growth and participation in the ecosystem.

4.4 Governance

VaultCoin holders can vote on ecosystem upgrades, fee structures, and new feature implementations.

---

5. Technical Architecture

The Hybrid Custody system is built on:

5.1 Hybrid Custody Vaults

- Enable recovery using advanced Layer 2 Smart Vaults protocol under the hood.
- Simple but powerful smart-contracts that are portable across blockchains set up interactive zero-knowledge proofs on-chain to determine which private-keys and combinations get priority and so on, enabling highly configurable and programmable vault mechanisms.

Please refer to the white paper about Hybrid Custody using Layer 2 Smart Vaults for Cold Storage for more in depth details. [2]

5.2 Hardware Wallet & Companion Apps

- Affordable, State-of-the-art hardware wallets secure private keys for everyone using the flagship Guardian Platform. Moreover, Guardian Hardware Wallet devices already have Hardware Token functionality built into them to harden certain recovery pathways for high value Hybrid Custody Vaults.
- Companion apps (iOS/Android) provide a seamless experience to users and Hybrid Custody Service Providers using the Guardian Platform.
- Every Platform Provider in the ecosystem will have its own set of hardware wallet devices and companion apps enabling similar functionality for their target audience.

5.3 Backend Infrastructure

- Platform Providers manage the backend infrastructure necessary to enable all the functions and services on the said platform.

5.4 Security Validation

- Independent peer-reviewed research paper by Dr. Maram et al. from Cornell University, USA. proves Smart Vaults as the best available technology for crypto custody. Accepted to ACM CCS 2024. [3]
- Hardware Wallet firmware and companion apps' source code will be published on GitHub for scrutiny and the same will be audited by renowned crypto security agencies such as KeyLabs after the Alpha Testnet launch.
- White Hat Hacker Challenges and Bug Bounties will be organized after the Alpha Testnet launch to further harden the entire ecosystem and build confidence in the wider community.

---

6. Market Potential

6.1 Target Markets

- **Assisted Custody Market**: The Assisted Custody Market represents a 500M USD PA Target Addressable Market, comprising Bitcoin holders managing 1 to 10 BTC directly on-chain. This cohort collectively holds over 2M BTC, valued at more than 200B USD. [4]

  Projections estimate that this group's holdings will exceed 1 trillion USD over the next decade, driven by increasing Bitcoin adoption and value appreciation (Projected CAGR: 31% - Past 5 yr CAGR: 62%). Despite this, no current custody solution specifically caters to this market due to complexities in private key management and limited recovery options, making it a significant opportunity for the Hybrid Custody Ecosystem. Hybrid Custody Vaults address these gaps with user-friendly recovery mechanisms and robust security features, uniquely positioning Hybrid Custody

Ecosystem and VaultCoin to capture this untapped market.

- **Institutional Custody Market**: The Institutional Custody Market, currently valued at over 1 Billion USD, comprises 550 Billion USD in managed assets growing at 24% CAGR as of 2024. [5][6]

  This segment includes High Networth Individuals, financial institutions, asset managers, and enterprises seeking secure and compliant crypto custody solutions. Hybrid Custody Vaults provide advanced features like multi-party multi-key arrangements and customizable recovery options, addressing both security and regulatory needs. Key industries driving this growth include banking, investment management, and DeFi projects, making this an essential market for VaultCoin's expansion strategy.

- **Hybrid Custody Enabled Cryptocurrency Exchanges:** Centralized Cryptocurrency Exchanges can also become non-custodial using Hybrid Custody Escrow Vaults, a variant of Hybrid Custody Vaults, and greatly reduce their burden of managing all their users' assets while still enforcing settlement as if they have full custody of user assets using deferred custody mechanisms. More details about Hybrid Custody Escrow Vaults can be found in the whitepaper - Hybrid Custody using Smart Vaults for Hot Wallets. [7]

  Just the Top 5 Cryptocurrency Exchanges manage more than 200 Billion USD worth user assets. [CoinMarketCap]

6.2 Revenue Streams

- Percentage-based fees on Total Value Locked/Protected (TVL) through Hybrid Custody Vaults on available Platforms.

  People holding and managing 1-10 BTC on-chain collectively hold more than >2M BTC (worth >200B USD) and a conservative 0.25% TVL PA fees for securing their holdings using Hybrid Custody Vaults on available platforms can bring in >500M USD in revenue just from this cohort.

  Note: Digital Asset custodians like CoinBase Custody, Gemini Custody, BitGo, Cactus, etc. offering primitive MultiSig/MPC vaults charge between 0.35% to 0.5% of AUM PA. [8]

---

7. Tokenomics

7.1 Supply and Distribution

VaultCoin will have a capped supply of 10 billion tokens, distributed as follows:

- **Ecosystem Growth and Rewards - 20%**
  Incentives for staking and ecosystem development, released over 2 years.

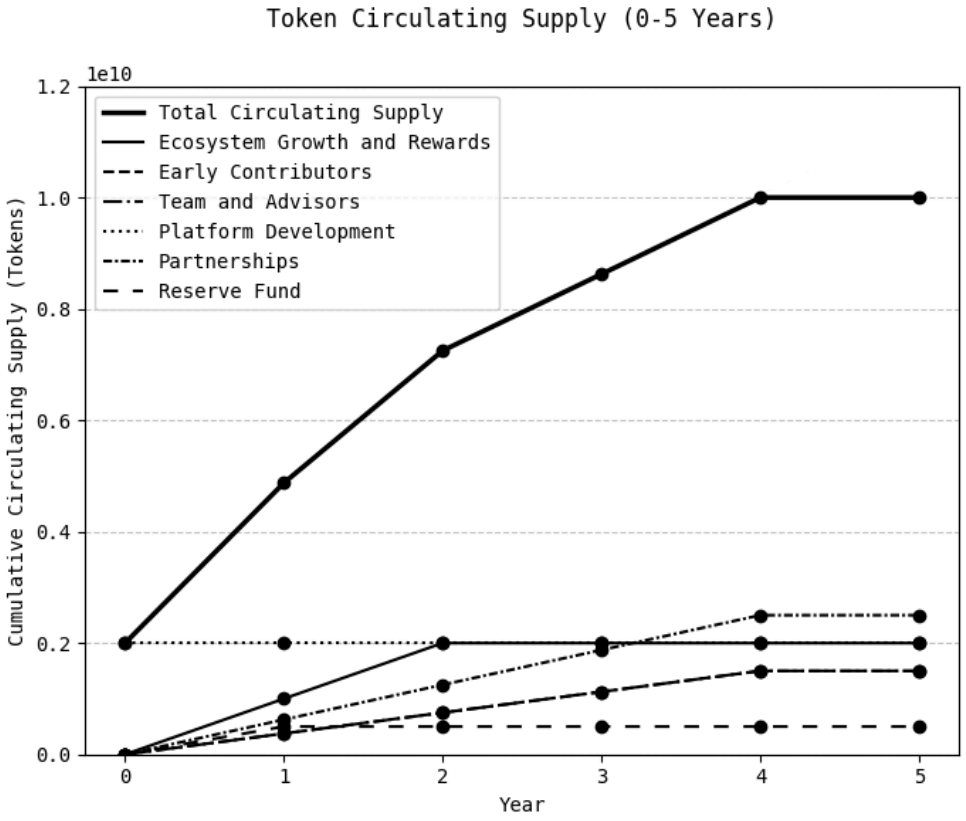
- **Early Contributors - 15%**
  Will be allocated to those who have committed time, effort and/or resources to bring the whole thing to fruition with vesting and unlocking schedules from 1 to 4 years

- **Team and Advisors - 15%**
  Will be allocated to core contributors, employees and advisors, with vesting and unlocking schedules from 1 to 4 years.

- **Platform Development - 20%**
  Development, Audits and Maintenance.

- **Partnerships - 25%**
  Licensing and royalties for key enabling technologies like Layer 2 SmartVaults protocol and other proprietary technologies. Vesting and unlocking in 4 tranches over 4 years.

- **Reserve Fund - 5%**
  Reserved for unforeseen requirements and partnerships. Unlocked after 1 year.



7.2 Token Utility Lifecycle

- **Phase 1**: Ecosystem growth by onboarding and incentivizing prospective Service Providers & other allied participants.
- **Phase 2**: Introduction of fee-based revenue streams and governance mechanisms.
- **Phase 3**: Expansion into institutional and DeFi markets with advanced custody features such as escrow vaults, NFT storage, and decentralized asset management tools. VaultCoin will become the backbone of enterprise-grade custody solutions, scaling Hybrid Custody Vaults to meet the demands of the global crypto ecosystem.

7.3 Demand Analysis & Projections

1. **AUM by Target Audience:**

    - **Current AUM by Target Audience: ~200 Billion USD** (People holding 1-10 BTC)

    - **Projected AUM in 5 years by Target Audience: ~1 Trillion USD**

        i. **845 Billion USD** - 200 Billion USD in AUM currently by people holding 1-10 BTC appreciating to 845 Billion USD over 5 years with BTC appreciating @ >31% CAGR (Past 5 years CAGR 62%)
        ii. **160 Billion USD** - 10% of 1.6 Trillion USD managed by Institutional Custodians (currently 550B - growing @ 23% CAGR) [5][6]
        iii. Not counting Altcoin holdings by Target Audience for lack of data.
        iv. Not counting Hybrid Custody Enabled Cryptocurrency Exchange market for lack of reliable data.

2. **Market Share after 5 years: 10%** (100 Billion USD of ~1 Trillion USD AUM by Target Audience[#])

    The Guardian Hardware Wallet and Companion Apps deliver cutting-edge security and user experience at a fraction of the cost (~$20) compared to competitors like Ledger or Trezor, driving rapid adoption in the self-custody ecosystem. This momentum can be leveraged to guide users toward Hybrid Custody Vaults, which provide superior safety, enhanced security, and seamless continuity through recovery solutions for lost or stolen keys, along with robust inheritance planning.

    [#]10% of the AUM by BTC holders with 1-10 BTC and 1% of AUM by Institutional Custodians.

3. **Staking Requirements:**

    - **At Launch: 0.1%**
    - **After 5 years: 0.6%** (Platform mandated increase of 0.1% every year) - **600 Million USD** worth VaultCoin needs to be staked to manage 100 Billion USD TVL in Hybrid Custody Vaults

    - Hybrid Custody Service Providers can and will stake more than the minimum required amounts by the platform to show their commitment and compete with other Hybrid Custody Service Providers on the platform.
    - Staking requirements will be managed through voting by VaultCoin holders as the ecosystem matures.

4. **Fees:**

    - **At Launch:** Stakers are compensated through rewards from the Ecosystem Growth Pool. Reward rate will be ~100% PA at launch to promote more people to sign up as Hybrid Custody Service Providers. These rewards will then be weaned off as fee revenues kick in.
    - **In 5 years: 250 Million USD** (0.25% of 100 Billion USD TVL) worth VaultCoin is needed to pay as fees every year for the projected TVL in Hybrid Custody Vaults.
    - Fees will be managed through voting by VaultCoin holders as the ecosystem matures.

---

8. Roadmap

8.1 Short-Term (0–12 months)

1. **Community Engagement**: Start airdrops, staking rewards, and early access campaigns to onboard users and prospective service providers.
2. **Security Audits**: Get the entire Guardian Platform audited by renowned security agencies.
3. **Public Beta Launch**: Launch the Guardian Platform with Hybrid Custody Vaults for Bitcoin.
4. **Expand Hybrid Custody Vaults Coverage:** Roll out Hybrid Custody Vault support for Ether, ERC-20 Tokens, Solana, etc.

8.2 Medium-Term (1–3 years)

1. **Global Partner Integration**: Onboard service providers in key geographic regions to expand the ecosystem and provide local touch points for users across the globe.
2. **Enterprise Custody Features**: Introduce specialized vault services for institutions, such as Multi-Key Multi-Party Vaults and Escrow Vaults.
3. **Governance Activation**: Enable VaultCoin holders to propose and vote on platform changes, ensuring decentralized decision-making.

8.3 Long-Term (3+ years)

1. **Institutional Custody Markets**: Scale Hybrid Custody Vaults to manage trillions in institutional crypto assets, integrating with legacy financial systems.

2. **Decentralized Ecosystem**: Transition control of Hybrid Custody ecosystem to a decentralized autonomous organization (DAO) governed by VaultCoin holders.
3. **Advanced Use Cases**: Expand support for NFTs, decentralized identity systems, and cross-chain asset management, establishing VaultCoin as a cornerstone of Web3 infrastructure.

---

9. Conclusion

VaultCoin and the Hybrid Custody ecosystem redefine how cryptocurrencies are secured, managed, and inherited. By solving critical challenges such as private key dependency, recovery mechanisms, and inheritance planning, the platform fosters confidence in the larger cryptocurrency ecosystem. VaultCoin's staking-based model incentivizes service providers and holders to stay committed to the ethos of the ecosystem while providing unmatched safety and security to everyone's crypto assets.

Join us in building the future of cryptocurrency security with VaultCoin.

Ref:

1. 20% of All BTC is Lost, Unrecoverable, Study Shows
2. Hybrid Custody using Smart Vaults for Cold Storage - CoinVault
3. Interactive Multi-Credential Authentication by Dr. Maram et al.
4. Who Owns the Most Bitcoin in 2024? | River
5. Digital Asset Custody Market Size | Global Report -2032
6. Crypto Asset Management Market Size & Share Report, 2030
7. Hybrid Custody using Smart Vaults for Hot Wallets
8. Crypto Custody Providers Comparison - MooLoo