dCustody

Infrastructure for Trustless Digital Asset Custody

Litepaper - June 2023

Mauricio Velez
Co-Founder
mvelez@dcustody.xyz

Franco Catena
Co-Founder
fcatena@dcustody.xyz

Nestor Coppi
Co-Founder
ncoppi@dcustody.xyz

Abstract

The inherent flaws of centralizing digital asset custody within a decentralized system stem from the fundamental principles underpinning these structures. In their essence, decentralized systems like blockchain are designed to eliminate the need for intermediaries, offering heightened security, privacy, and control to individual users through consensus algorithms and cryptographic proofs. These systems operate on a peer-to-peer basis and emphasize transparency and autonomy. Contrarily, centralized digital asset custody creates a 'single point of failure' by concentrating asset control within a single or limited number of entities. This centralization introduces significant risks - if the custodian is compromised via hacking, internal malfeasance, or regulatory intervention, users' assets are jeopardized. Additionally, it necessitates blind trust from users, both in the competency of the central entities and their commitment to user interests. These attributes starkly contrast with the principles of a decentralized system and reveal centralized custody as inherently flawed within such an ecosystem. The technology to fully implement decentralized custody has been unavailable until recently, which resulted in an initial reliance on centralized models. However, as technological advancements continue to unfold, the possibility of fully realizing the potential of a decentralized custody model is now within reach.

1 Technical problems: issues with centralized custody and the current state of organization onboarding in Web3

Between 2020 and 2023, the cryptocurrency domain witnessed the collapse of numerous centralized entities, leading to an extensive loss of user assets, collectively valued in billions of dollars. For example, Celsius declared bankruptcy[1] in July 2022 as its assets tumbled from over $25 billion to a paltry $167 million, resulting in a deficit of $1.2 billion on its balance sheet. At the same time, BlockFi declared its assets and liabilities in the range of $1 billion to $10 billion[2]. FTX confirmed the vanishing of nearly $9 billion of customers' assets[3], and Fireblocks experienced a $75 million Ether loss from Stakehound[4]. Coincidently, Genesis Earn collapsed, leaving a $900 million void on its balance sheet[5]. Such incidents underscore the inherent risks associated with centralized custody models, where the custodian functions as a single point of failure.

Notwithstanding these issues, an additional technical problem lies in the current state of organization onboarding to Web3. According to data from a16z[6], there are fewer than 20 million active addresses per month, and merely 2.5 million[7] multisig wallets in existence in May 2023. Compared with 4.6 billion Internet users, these figures illustrate the apparent deficiencies in onboarding organizations to the Web3 ecosystem, pointing to a sector in need of substantial improvement.

Furthermore, centralized custody models are associated with high transaction and maintenance costs, potentially excluding niche players. The majority of centralized custodians operate on an Assets under Custody (AuC) model, meaning smaller players might lack sufficient assets to justify the cost of custodial services. Coupled with the absence of transparency in centralized finance and custody operations, this leads to an inability for users to verify transactions on public ledgers, thereby generating a significant trust deficit.

Despite these challenges, solutions are emerging. Innovations such as dWallets and dCustody are introducing new possibilities. dWallets propose an innovative signing mechanism operating on-chain, constrained by trustless access control, granting users the ability to sign transactions for any network. dCustody provides users with stateful and programmable access control over their assets and data, introducing a viable alternative to centralized custodians.

Until the development of dCustody, no decentralized solutions allowed owners the flexibility of stateful and programmable decentralized access control. dCustody, built on top of the dWallet primitive, paves the way towards a trustless custody infra-layer. This new framework is designed to set a new standard for decentralized custodian infrastructure within the Web3 space.

Utilizing dCustody, users can engage a decentralized, trustless solution that eliminates the risks associated with centralized custodians. There is no single point of failure, and users can exert full control over their assets. dCustody provides an ideal solution for users prioritizing security, transparency and accessibility without sacrificing asset control. As such, dCustody is set to redefine the concept of digital asset custody, heralding the decentralized custodian infrastructure as the future of this sector.

2 Introduction “The dCustody Protocol: envisioning decentralized custody via a community-driven approach”

dCustody, a groundbreaking protocol, aims to bring universal access to digital asset custody by enabling any entity to become a decentralized custodian. The anticipated transformation is vast, forecasting a metamorphosis from the current centralized custody ecosystem to an open platform with limitless opportunities. dCustody acts as a trustless access enabler poised to cater to the next billion Web3 users.

At the core of dCustody's approach is community-driven governance. The protocol's economic model is built around a policy engine mechanism, transforming policies into the protocol's data engine. Community-created policy templates equip custodians with a plug-and-play set of workflows defined by the community. This model effectively substitutes manual, in-person, and challenging-to-enforce user permissions. Under the auspices of the Odsy network, where dCustody operates, users submit a Zero-Knowledge Proof of the state transition incurred by executing valid operations on the preceding state.

The dWallet only signs transactions when all workflow-defined criteria are met. The process necessitates to comply with the aforementioned rules before transaction execution, thereby enhancing security and minimizing fraud risk. The rules can be arbitrarily complex, from simple multi-signature requirements to complex trading schemes. With the dCustody protocol, organizations across the globe can adapt to local jurisdictional requirements as workflows are customizable to accommodate potentially any present and future need.

Additional policy samples such as Know Your Transaction (KYT) delineate asset types and operational code. This level of definition empowers custodians to enforce regulatory compliance without retaining customer assets. As a community-driven protocol, dCustody's evolution and the creation of new workflows rest upon the contributions of its community members who gain from the ecosystem itself.

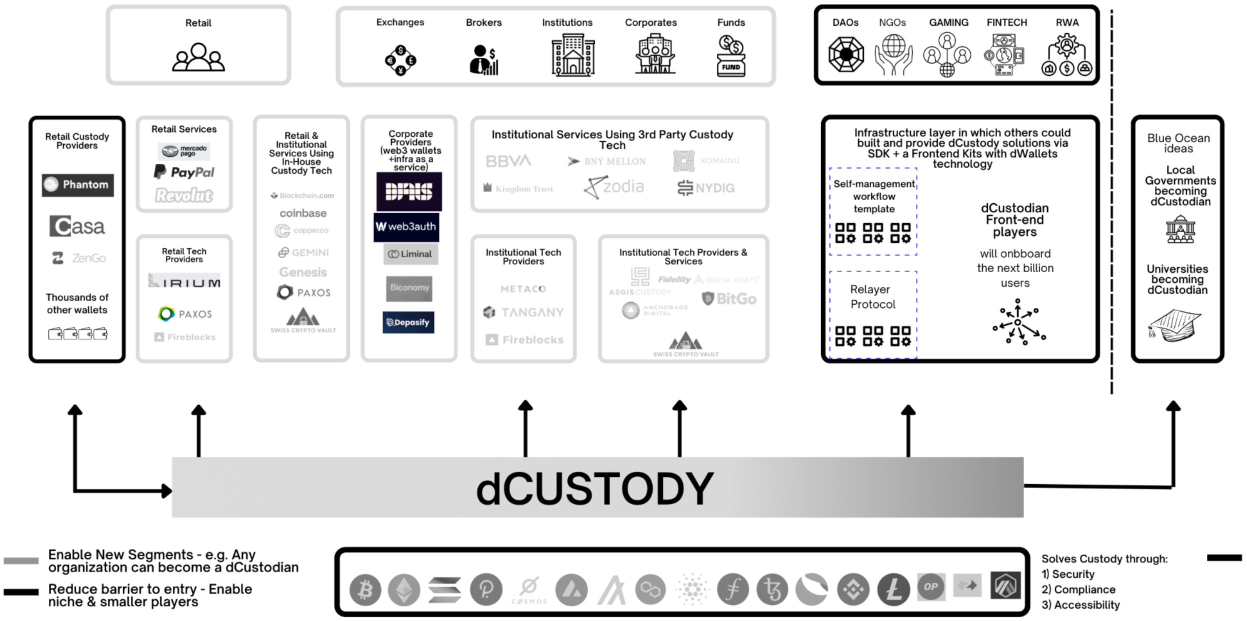
The dCustody protocol includes a Software Development Kit (SDK) and front-end kits to facilitate integration. These kits are designed to be initial and inspirational starter points while simplifying the adoption of the protocol by organizations, enabling seamless integration into existing infrastructure. The ongoing refinement of the SDK and front-end kits will be undertaken by the community, providing developers and stakeholders the opportunity to contribute to the protocol's development and improvements.

The SDK offers developers the tools to build applications integrated with the dCustody protocol, and the front-end kits furnish a user-friendly interface for organizations to interact with the protocol. Consequently, organizations can establish their own decentralized custodian infrastructure, implement workflows of their choice, and afford their customers a secure and transparent digital asset management solution.

In a conventional setting, digital asset custody services have been administered by centralized intermediaries, imposing high service charges. These costs pose challenges for small to medium-sized organizations seeking to secure custody services for their digital assets. However, with dCustody eliminating the need for a centralized intermediary, those costs can be dramatically reduced.

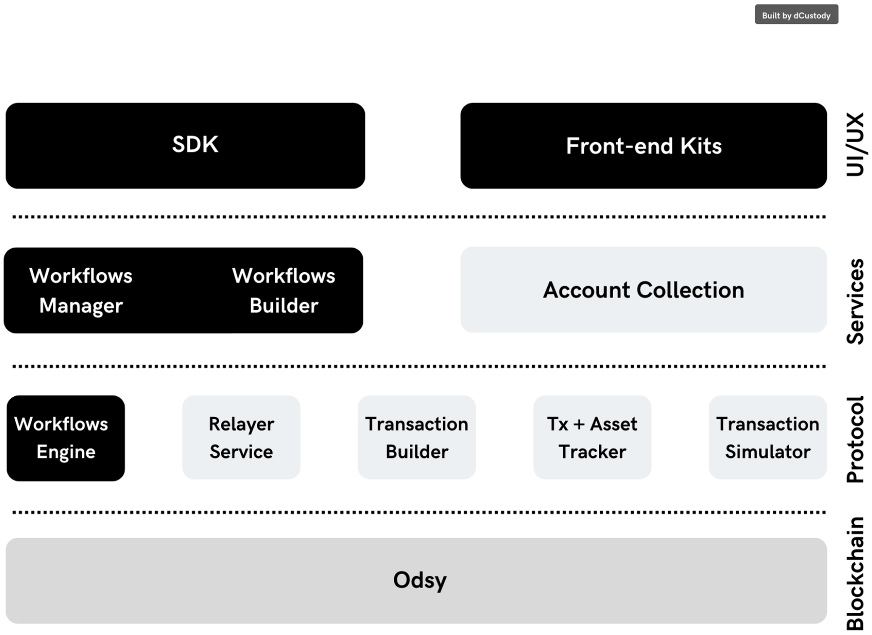
This cost reduction empowers even smaller financial institutions, such as local accountants, and even larger organizations, such as gaming applications, to build an embedded Web3 onboarding solution. Consequently, these organizations can augment their service offerings, grow their businesses, and offer their clients a more affordable and secure solution. Utilizing dCustody can also amplify transparency and auditability offered by blockchain technology, fostering trust with clients.

This will enhance the creation of a complete new paradigm shift in the Trustless Digital Asset Custody


Retail
Exchanges
Brokers
Institutions
Corporates
Funds
FUND
DAOs
NGOs
GAMING
FINTECH
RWA
Retail Custody Providers
Phantom
Casa
ZenGo
Thousands of other wallets
Retail Services
mercado pago
PayPal
Revolut
Retail Tech Providers
IRIUM
PAXOS
Fireblocks
Retail & Institutional Services Using In-House Custody Tech
Blockchain.com
coinbase
copper.co
GEMINI
Genesis
PAXOS
SWISS CRYPTO VAULT
Corporate Providers (web3 wallets +infra as a service)
DFNS
web3auth
Liminal
Biconomy
Depasify
Institutional Services Using 3rd Party Custody Tech
BBVA
BNY MELLON
KOMAINU
Kingdom Trust
zodia
NYDIG
Institutional Tech Providers
METACO
TANGANY
Fireblocks
Institutional Tech Providers & Services
Fidelity DIGITAL ASSETS
AEGIS CUSTODY
ANCHORAGE DIGITAL
BitGo
SWISS CRYPTO VAULT
Infrastructure layer in which others could built and provide dCustody solutions via SDK + a Frontend Kits with dWallets technology
Self-management workflow template
Relayer Protocol
dCustodian Front-end players
will onboard the next billion users
Blue Ocean ideas
Local Governments becoming dCustodian
Universities becoming dCustodian
dCUSTODY
Enable New Segments - e.g. Any organization can become a dCustodian
Reduce barrier to entry - Enable niche & smaller players
COSMOS
OP
Solves Custody through:
1) Security
2) Compliance
3) Accessibility

Overall, the dCustody protocol offers secure, compliant, and accessible services built on a decentralized MPC, a community-defined compliant workflow, and an SDK with front-end kits, respectively. It sets the stage for an array of possible applications, making it a vital component in the widespread adoption of digital asset custody.

dCustody Protocol Architecture:



2.1 A comprehensive technical overview of the dCustody Protocol

The dCustody protocol announces a new era in trustless infrastructures for digital asset custody. Building upon the foundational technology of dWallets and integrating it with the Odsy Network, this innovative protocol forges a secure and cohesive solution for managing digital assets. The dCustody protocol acts as a decentralized infrastructure layer, facilitating collaboration between workflow makers and individual contributors within the protocol. Embedded within the core of the protocol are specific incentive mechanisms aimed at coordinating activities for common good, which would otherwise pose significant challenges for individual participants to execute efficiently and economically.

A fundamental cornerstone of the protocol is its underlying security, built upon a t-out-of-n Multi-Party Computation (MPC) wallet implementation. This system is meticulously designed by Odsy to maximize security, reduce single points of failure, and ensure the integrity of the digital assets under custody.

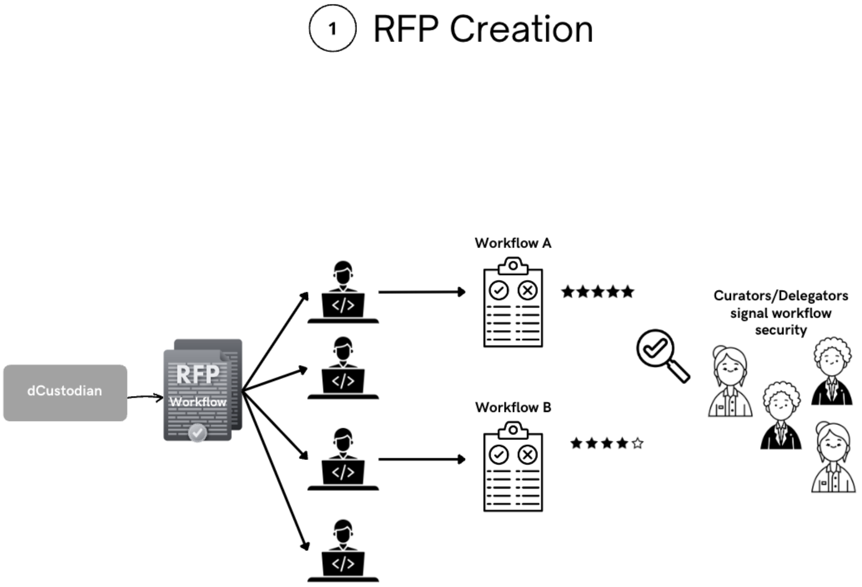
The protocol acknowledges the pivotal role of workflows in customizing each dCustodian framework and is committed to establishing an internal economic system around the workflow engine. To this end, each workflow is developed using Rust and compiled to WebAssembly (WASM) for deployment on the Odsy Network. The smart contracts that form part of this system are thoroughly curated by the community, ensuring the integrity and consistency of the protocol.

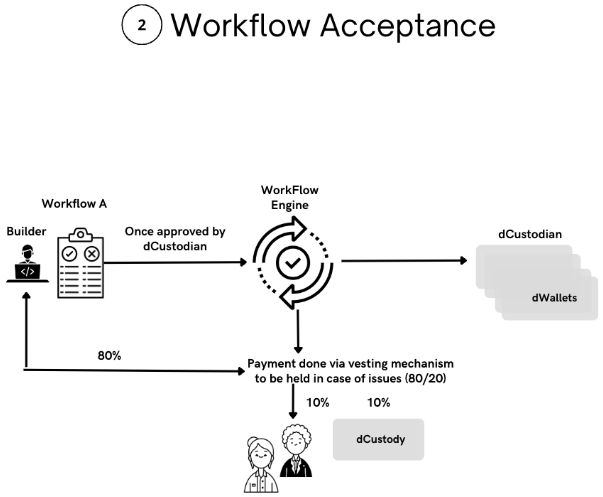
The economic model underpinning the dCustody protocol is designed around a Workflow Marketplace. This platform allows entities to select the rules most suitable for their use cases, enables builders to enhance existing rules or create new ones, and permits curators and delegates to endorse and maintain optimally designed workflows.

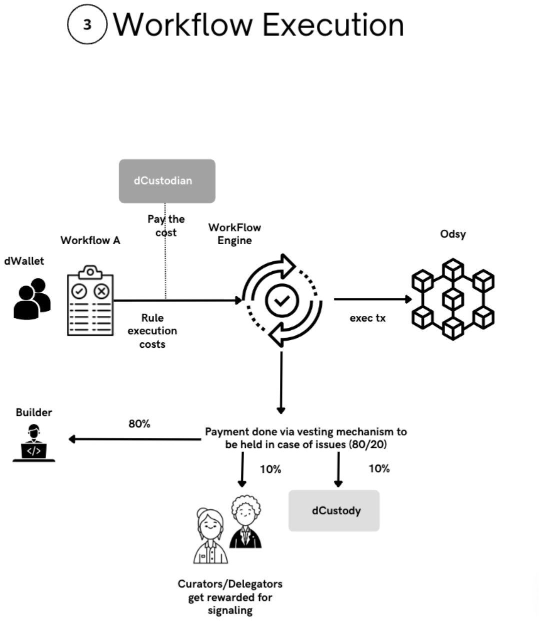
The initial set of workflow templates is likely to be co-developed with the founding team and based on the first identified and most relevant use cases.

Incorporating various economic agents operating at the protocol layer, the architecture of the dCustody protocol has been carefully designed. Governance actors are instrumental in ensuring the protocol's integrity and consistency by fostering consensus among all agents. Upon completion, the dCustody protocol aims to offer a secure and seamless infrastructure for digital asset custody, where each participant contributes to its overarching success.

Protocol Workflow Flywheel description:




2 Workflow Acceptance
Workflow A
Builder
Once approved by dCustodian
WorkFlow Engine
dCustodian
dWallets
80%
Payment done via vesting mechanism to be held in case of issues (80/20)
10%
10%
dCustody



2.1.1 Protocol Economic Agents

The dCustody Protocol encapsulates a distributed network of four primary economic entities, all functioning in harmony to establish a decentralized mechanism for digital asset custody. The primary objective of the protocol is to optimize the distribution of value (a harmonious and efficient mode of value creation) towards high-utility groups, as opposed to focusing on the value exchange between individual participants. Each participant contributes distinctive capabilities to a modular system, which is reminiscent of Lego blocks (workflows), where individual workflows are sets of features or rights encapsulated within smart contracts, developed and integrated by developers into the system, and leveraged by the dCustodians.

1. Builders: The initial economic actors are the Builders, who are the innovators, adaptors, and verifiers holding end-to-end responsibilities for workflow formulation and upkeep. Their profit margins are linked to the usage frequency of the workflows they establish. This role necessitates an advanced level of technical expertise.

2. Curators: The Curators function as auditors for the workflows, tasked with signaling either endorsements or denouncements. Their responsibilities demand a moderate level of technical proficiency.

3. Delegators: The Delegators help secure the protocol by engaging in signaling activities. This role requires a basic level of technical understanding.

4. Users: The final set of actors are the Users, primarily comprising dCustodian organizations that employ various workflow sets to deliver a range of services to their end-users.

In this manner, the dCustody Protocol effectively blends technical acumen and economic incentives across different roles, thus illustrating a decentralized, community-driven approach to the digital asset custody, underpinned by robust governance mechanisms

3 Governance Model

dCustody integrates diverse contributions from a wide range of participants to enable its effective operation and continuous evolution. To ensure the protocol's integrity and reliability, dCustody employs its own token within a staking and slashing framework. Participants stake a predetermined quantity of the protocol token as collateral for engagement. Violations of protocol rules lead to the instigation of a slashing process, whereby offenders forfeit their staked collateral.

Governance within dCustody is enacted via a vote escrow model, implemented by token holders or their appointed delegates. This model facilitates a democratic environment, enabling token holders to shape the protocol's future trajectory and development. The decision-making consortium, composed of token holders and their delegates, assesses and determines key aspects of the protocol. These aspects encompass proposal amendments concerning the dCustody Software Development Kit (SDK) and smart contracts, workflows for token slashing, and the strategic deployment of token holdings and treasury funds.

dCustody uses a decentralized governance model to adhere to the principles of transparency and community involvement. This model is predicated on a token-based voting system, wherein the protocol's token is utilized to cast votes on significant protocol decisions. Token holders can submit proposals, which are then subjected to community-wide voting. To amplify network effects and streamline the voting process, token holders can delegate their voting power to other community members.

Moreover, the dCustody token extends its utility beyond staking and governance. It also serves as the 'gas' for transactions, reminiscent of a concept prevalent in many blockchain platforms. Each operation within the protocol incurs a specific gas cost, commensurate with the computational resources demanded by the operation. The computation cost of each workflow is based on the most efficient path, ensuring optimal use of resources. Users compensate for these resources by paying gas fees using dCustody tokens.

The voting process takes place on-chain, assuring transparency and the immutability of decisions. dCustody incorporates a quadratic voting mechanism to safeguard the integrity of the voting process. This mechanism augments the influence of smaller token holders, engendering a fair and inclusive governance process. It incentivizes participation from smaller token holders, developing a more decentralized network and strengthening the network effect.

In summation, dCustody is a decentralized protocol that capitalizes on a community-centric ethos, transparency, and robust governance. Its token has several roles, including staking, governance, and transactional utility, thereby engaging and securing stakeholders within the protocol while also optimizing computational efficiency.

4 Conclusion

This paper investigates the inherent risks of centralized digital asset custody within decentralized systems, such as significant loss of assets and the contradiction with the principles of decentralization. It presents decentralized custody as a superior alternative, highlighting the innovations of dCustody, which offer advanced user control and security. dCustody is introduced as a groundbreaking protocol built on a community-driven workflow engine mechanism, complete with a Software Development Kit (SDK) for ease of adoption. With its economic model revolving around a Workflow Marketplace and governance actors ensuring integrity, dCustody is positioned as a key solution that aligns with the fundamentals of decentralized systems, poised to significantly transform the digital asset custody landscape.

References

[1] Cheyenne Ligon, Coindesk.com, Celsius Bankruptcy Filings Hint Retail Customers Will Bear Brunt of Its Failure. July 18, 2022.

[2] Cbsnews.com, Crypto lender BlockFi declares bankruptcy as FTX contagion spreads. November 29, 2022.

[3] Kyle Barr, Yahoo.com, FTX Confirms $9 Billion in Customer Funds Vanished. March 23, 2023.

[4] Allon Sinai, Calcalistech.com, Loss of $75 million in Ether highlights infancy of crypto infrastructure. June 24, 2021.

[5] Will McCurdy, Decrypt.co, Genesis Owes Gemini Earn Users $900M: Report. Dec 3, 2022

[6] Andreessen Horowitz, https://api.a16zcrypto.com/wp-content/uploads/2023/04/State-of-Crypto.pdf. Page 44.

[7] Gnosis Safe https://twitter.com/safe/status/1661004085376733185. May 23, 2023