Odsy Litepaper

August 2022 - version 1.0

Omer Sadika	omer@odsy.xyz
David Lachmish	david@odsy.xyz
Sean Lee	sean@odsy.xyz
Yehonatan Cohen Scaly	yehonatan@odsy.xyz

Contents

Abstract 3

The Missing Piece of Crypto 4

Access today 5

- Centralized Access Control 5
- Decentralized Access Control 5

Introducing dWallets 6

Odsy: A Security-First Network 8

Odsy Network Architecture 10

- Odsy Network Uses t-out-of-n MPC with TEEs as an Extra Layer of Security 12
- What Makes an MPC Implementation Truly Decentralized and Secure? 16
- Access Control of Odsy Network Itself 17
- Odsy Wallet Contracts SDK 19
- Odsy SDK 20

dWallet Use Cases 21

- Digital Asset Custody 21
  - How custody works today 21
  - Better Custody using dWallets 22
- Multi-Chain Decentralized Organizations 23
  - How DAOs Work Today 23
  - Better DAOs Using dWallets 23
- Granular Access Sharing, Delegation and Control 24
- Custody-as-a-Service 27
- Interoperable Infrastructure and DeFi 27
- dWallet Marketplace 28
- Gaming 29

The ODSY Token 30

- Tokenomics 30
- Token Genesis Supply and Distribution 31
- Crypto - A 10 Year Odyssey 32
- The Nostos Model 33

Conclusion 35

Abstract

During the past years in the crypto space, there has been heavy investment in solving major problems such as network security, speed and scale, with one big problem at the core infrastructure level that hasn't been addressed yet: trustless access control.
Today, when it comes to access control, crypto users are forced to choose between the default poor decentralized access control in blockchains and robust, flexible access control that is centralized. No decentralized solution allows the owner of a wallet the flexibility of stateful and programmable access control.

We propose the concept of a *dWallet*, a new blockchain primitive, as an evolution of today's poor decentralized access control. A dWallet allows generating digital signatures corresponding to a public key, just like regular private keys in traditional wallets. However, unlike the default blockchains' access control, a dWallet adds a fully decentralized layer of a dynamic and stateful access control that currently exists only in centralized solutions. Another major advantage is that a dWallet also allows for a transfer of wallet ownership, which was impossible to date.

While dWallets can live only on a purposefully-built dedicated blockchain, their signing mechanism is blockchain-agnostic by nature, so users can use a single dWallet to sign transactions for any other blockchain. This is due to the fact that most blockchains share the same authentication method (largely ECDSA, EdDSA), and all operate by validating the digital signature of a transaction against the public key that corresponds to the account's address.

The Odsy Network (pronounced Odyssey: **od**-uh-see) is a security-first dedicated blockchain where dWallets are the key utility. In Odsy Network, a dWallet is a native entity that lives indefinitely on the blockchain and is bound to a *wallet contract* – a smart contract that manages access to the dWallet. The Odsy Network was not built to be a generic layer-1 blockchain, although it fulfills all the requirements of one.

This brings, for the very first time, trustless yet robust access control to any blockchain account - as the accounts that are controlled by an Odsy dWallet have deterministic and predictable behavior determined by the wallet contract.

With the dWallet functionality as the building block of protocols and solutions in the Odsy ecosystem, the Odsy Network will become the main access control layer for all of Web3, and serve as an infrastructure to bring trustless access control to any network.

The Missing Piece of Crypto

Over the last decade crypto has focused on implementing existing concepts in a decentralized way. In the process of building these decentralized blockchains, protocols and technologies, the access to them was treated as a given.

As crypto gained adoption and became fragmented with new protocols, assets and chains, the access to crypto moved from being completely decentralized - holding the private key directly - to being very centralized with the popularization of solutions (e.g. custodians, exchanges etc.) that hold the assets or keys for the users. As a result, it is hard to say that crypto today is truly decentralized.

From the standpoint of the user, the inelasticity of decentralized access in crypto forces them to access blockchains and protocols using centralized solutions. Managing access to decentralized solutions in a centralized way - undermines the decentralized nature of those solutions - missing the whole point of being decentralized in the first place.

Perhaps most importantly, relying on centralized access for decentralized solutions hinders the solving of real world problems and use cases, and inhibits the maturity of the space.

In order to provide users with the level of access control they are accustomed to in the non-crypto financial world, centralized and semi-centralized crypto access solutions (key and asset management) remove, reduce and dilute the functionality and utility of crypto technology.

As we are nearing a point where the major problems in crypto (e.g. scale, speed, standards, use cases etc.) have proposed solutions with many projects actively working on them, we must shift our focus to the missing piece of crypto - access and security - so crypto can be mature enough to solve our real world problems.

The past decade was dedicated to conceiving and implementing the possibilities of what we can achieve with crypto - we believe the next decade has to be dedicated to connecting all that we've achieved in crypto to the real world, without giving up or compromising decentralization.

Access Control today

Centralized Access Control

The real-world applicability and utility of crypto, much like many other technologies, relies on robust and flexible access control. As crypto gained adoption, centralized solutions that hold the keys and assets on behalf of crypto users and offer simple and powerful access control - e.g. crypto exchanges, custody providers, custodial wallets etc. - filled the void created by poor decentralized access control.

The advantages of decentralization over centralization as we know them - e.g. trustlessness, security, transparency, democratization etc. - are valid and apply in the same way to decentralized over centralized access control.

The fact that centralized solutions have been widely adopted in crypto despite not possessing those advantages, speaks volumes of the value that robust and flexible access control holds for crypto users.

Decentralized Access Control

Today, decentralized access control to blockchains' accounts is poor and limited, because a crypto user can either keep 100% of the access themselves by holding a private key personally or irrevocably give away 100% of the access to someone else by sharing their private key. Anything else requires either using centralized solutions or trying to address the same use cases by moving from user-owned accounts to smart contracts.

That means decentralized access control today is binary. We call that [private key and signing mechanism] a *static decentralized wallet*. Today, static decentralized wallets can not be used as a building block when building a fully decentralized solution.

Introducing dWallets

We propose a concept that solves access in a decentralized way - the *dynamic decentralized wallet* or simply *dWallet* - a new blockchain primitive.

A dWallet is a signing mechanism paired to a public key and constrained by dynamic access control, that operates within a decentralized state machine (e.g. blockchain).

The requirements for constituting a dWallet are:

- **Strong Decentralization**

  The dWallet creation, signing and access control mechanisms, as well as the decentralized state machine they operate in, must all exhibit strong decentralization. A permissioned network or one with a small number of nodes does not suffice.

- **Genericity**

  the signing mechanism must generate a digital signature for any valid message, independent of its destination or purpose. For example, a dWallet that supports the ECDSA signing algorithm can be used to sign transactions of any blockchain that uses ECDSA for authentication.

- **Trustlessness**

  The dWallet must deterministically adhere to the access control mechanism.

- **Dynamicity**

  The access control mechanism must be Turing-complete and dynamic.

- **Transferability**

  The owner of a dWallet must be able to completely transfer ownership of a dWallet to a new owner, with previous ownership being revoked.

dWallets may also keep record of approved transactions on other blockchains and keep track of assets on other blockchains / protocols, but that is not a requirement.

Important clarification

Multisig is a name given to tailor-made mechanisms that require multiple signatures in order to perform a specific action, unlike dWallets that create a standard single signature based on programmable logic. Multisig may be confused as fulfilling the requirements and/or providing the same value as a dWallet. That is not true for the following reasons:

- **Multi-chain**

  Multisig are ad-hoc unique solutions, designed to “patch” a specific access problem. That means that every blockchain, and sometimes even specific protocols, require a purposefully-built multisig solution. With dWallets - the logic written applies to every blockchain and protocol in the same way - same code base, same language, same framework etc.

- **Turing Complete**

  A dWallet enables, in a straightforward way, to write Turing complete logic that is generic to any type of blockchain, from simple protocols to very complex ones.

- **Signature**

  Unlike multisig solutions, dWallets create one signature that is identical to the signature created when using traditional wallets with a private key. That enables use cases (e.g. identity) that require a signature to be generated that way.

Odsy: A Security-First Network

We truly believe the concept of dWallets has the potential to introduce a new standard to Web3 in a similar vein to how smart contracts have become a fundamental building block. However, we also know that its success is dependent on flawless execution: for a dWallet to be trustless, it must adhere to its defining characteristics.

As more dWallets are used to manage accounts of traditional blockchains, the financial incentive to attack the network and compromise the dWallet signing mechanism would become higher (total value of assets managed by dWallets on all blockchains). This means that attackers can have access to virtually unrestricted resources in order to perform the attack (both financially, and technologically).

For this reason, security is the number one priority for the design and implementation of the Odsy Network.

Our team includes both offensive and defensive cyber-security and cryptography researchers from the top establishments in the world, gathered for the sole purpose of creating a dWallet implementation as close to unbreakable as possible. During the purpose of designing the network, we are constantly evaluating the unique attack landscape and are making sure every detail in our design and implementation is consistent with our threat management plan.

A comprehensive and detailed threat analysis and management will be included in the whitepaper. In this litepaper, we will highlight the security requirements that the dWallet implementation must adhere to:

Non-weakening

Using a dWallet should never weaken security, only strengthen it; the owner of a dWallet must be at least as secure as if they had held the private key in self-custody. That is, the blockchain cannot sign a transaction unless a sufficiently-privileged user of the respective dWallet has signed that transaction as well.

Revocability

Following a transfer of ownership, the previous owners of a dWallet cannot use it to sign transactions.

Availability

A dWallet should be available at all times, and never censor valid signing requests.

Soundness

the logic that governs the various operations a user or owner can do with a dWallet (signing, change of wallet contract, transfer of ownership) must be precisely determined by the wallet contract it is bound to. Operations that are determined as invalid by the wallet contract's logic must never be executed, and all valid operations must be allowed.

Odsy.
The future is
Secure.

Odsy Network Architecture

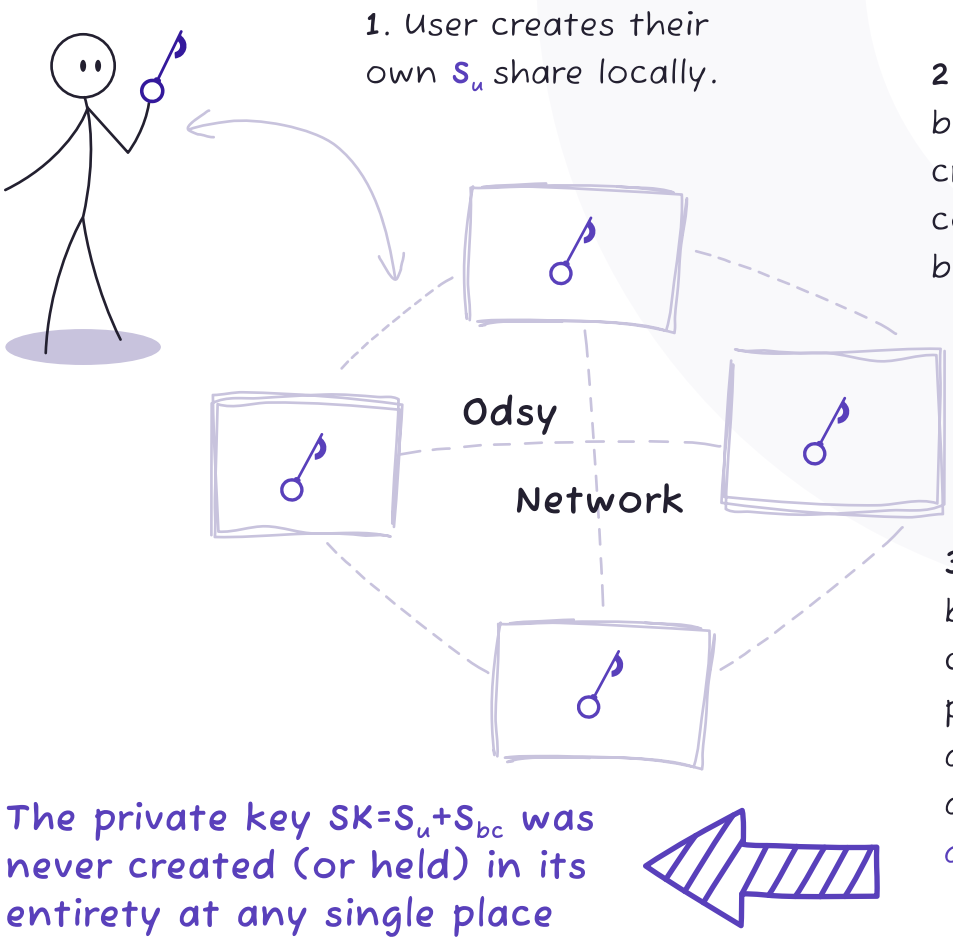
We designed the Odsy Network so that owners and users of a dWallet interact with the blockchain to sign transactions. Neither the user nor the blockchain may sign without the other's consent to sign that particular message.

This is possible through a cryptographic protocol called Multi-Party Computation (MPC). MPC allows multiple parties to perform a computation and learn its result without any party learning the other parties' secret inputs or anything about the computation itself.

More specifically, we are using Threshold Signature Schemes (TSS). In this type of MPC, the computation done by the parties yields a distributed key with which they can jointly sign messages.

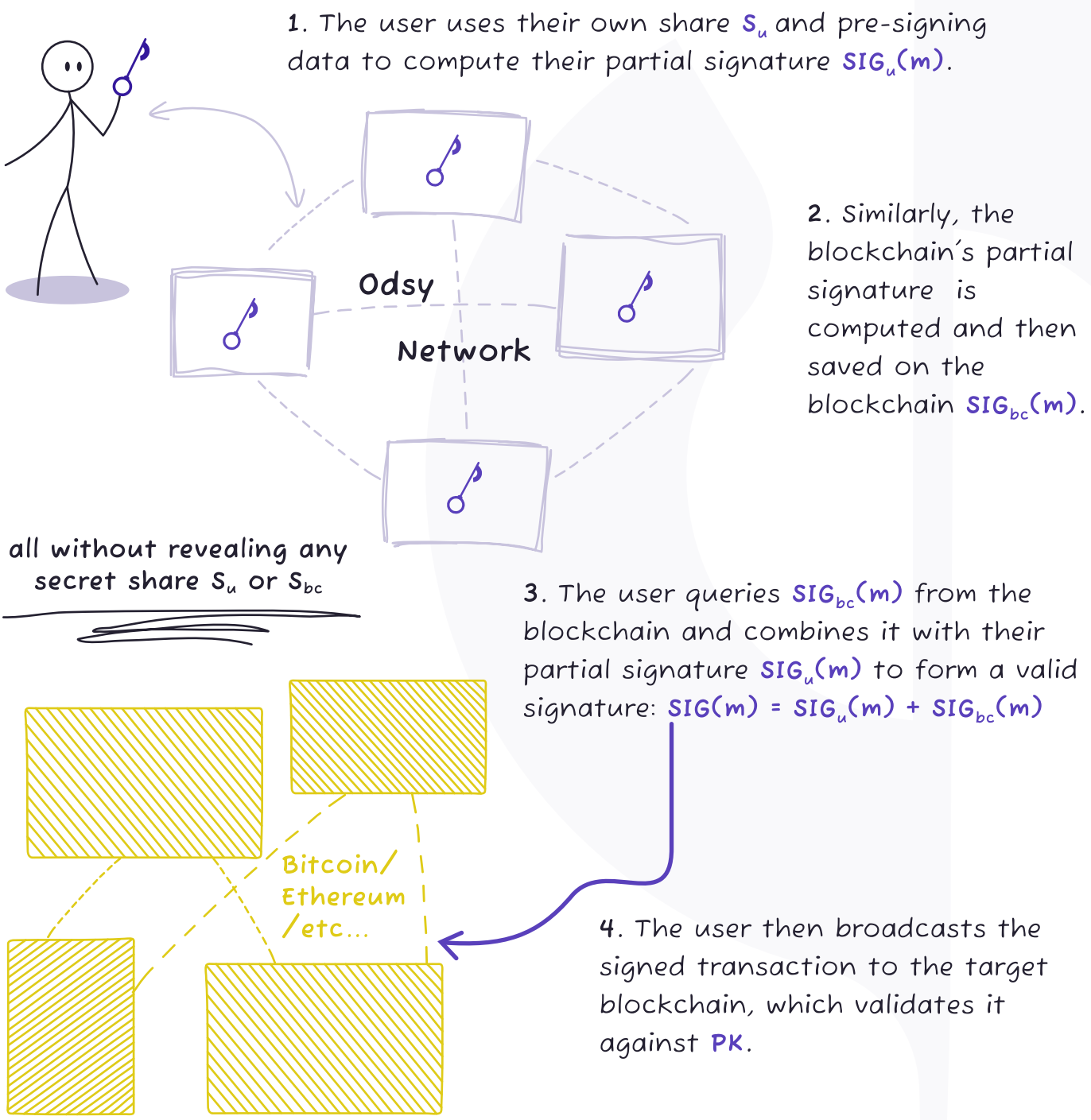
In a *t-out-of-n* setting of TSS we have a total number of n parties and threshold t such that any subgroup of t parties or more will be sufficient to sign together. The process looks as follows; when a user wishes to create a new dWallet, it engages in a process called *Distributed Key Generation (DKG)* with the blockchain:

New dWallet Creation via Distributed Key Generation



Following a DKG, the distributed private key of the new dWallet can be used to sign messages in the following way:

Signing using dWallets



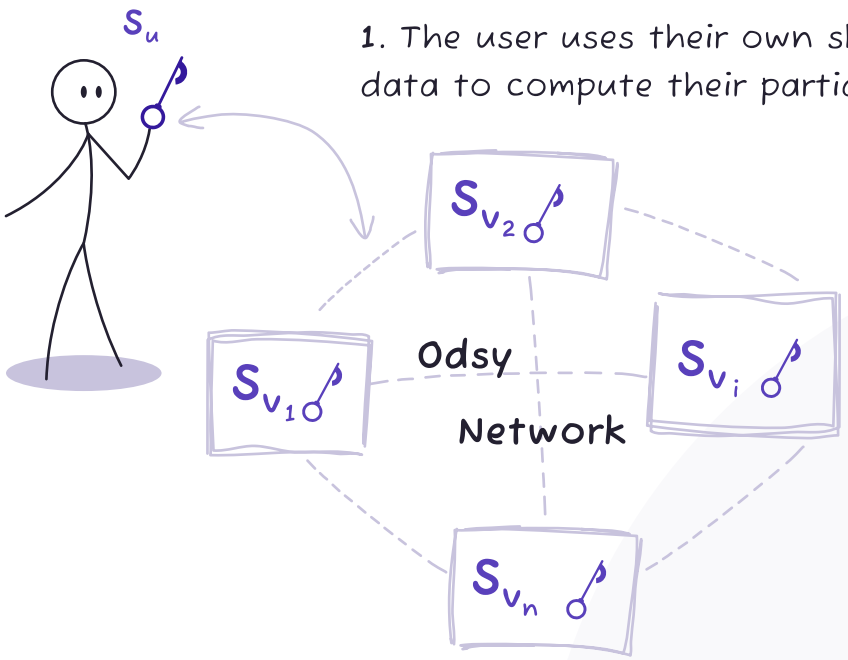
Odsy Network Uses *t-out-of-n* MPC with TEEs as an Extra Layer of Security

At first sight, it might be tempting to think a simple 2-out-of-2 scheme can be used for this purpose, with one secret share saved by the owner of the dWallet and another saved on the blockchain. However, because blockchains are public, one cannot keep secrets on the blockchain and it would essentially be equivalent to the owner holding the key in its entirety by themselves, which defeats the purpose.

Because of this, our approach is to utilize TSS in a fully decentralized manner by not only splitting the secret between the user and the blockchain, but also splitting the blockchain's secret between validators so the validators shares are never revealed publicly on the blockchain.

This way, in order for a message to be signed by a dWallet, the cooperation of both the owner/user of the dWallet and a certain threshold t out of the n validators is required.

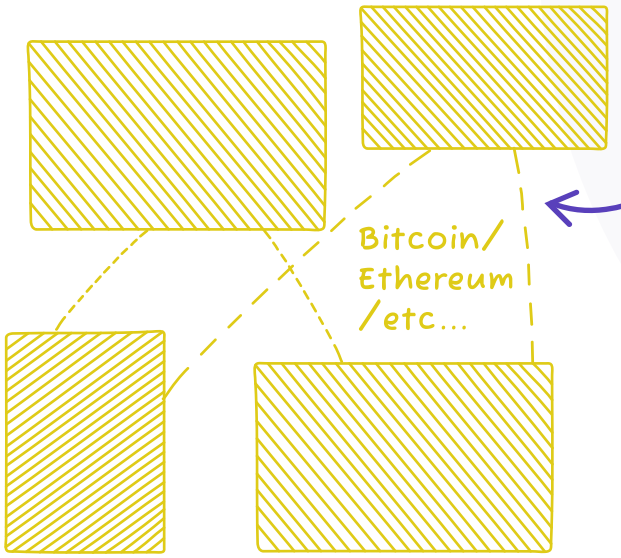
Signing with a t-out-of-n MPC dWallet implementation



1. The user uses their own share S_u and pre-signing data to compute their partial signature $SIG_u(m)$.

2. Every validator uses their unique share S_{v_i} and pre-signing data to compute their partial signature $SIG_{v_i}(m)$ and broadcast it to the other validators.

3. The validators' partial signatures are combined to form the blockchain's partial signature $SIG_{bc}(m) = SIG_{v_i}(m) + ... + SIG_{v_n}(m)$ which is then saved on the blockchain.



4. The user queries $SIG_{bc}(m)$ from the blockchain and combines it with their partial signature $SIG_u(m)$ to form a valid signature $SIG(m) = SIG_u(m) + SIG_{bc}(m)$.

5. The user then broadcasts the signed transaction to the target blockchain, which validates it against PK.

all without revealing any secret share S_u or S_{vi}

The above sketch described an *mpc-only* design for a network of dWallets. This design is cryptographically secure and indeed may offer a secure implementation of dWallets by itself.

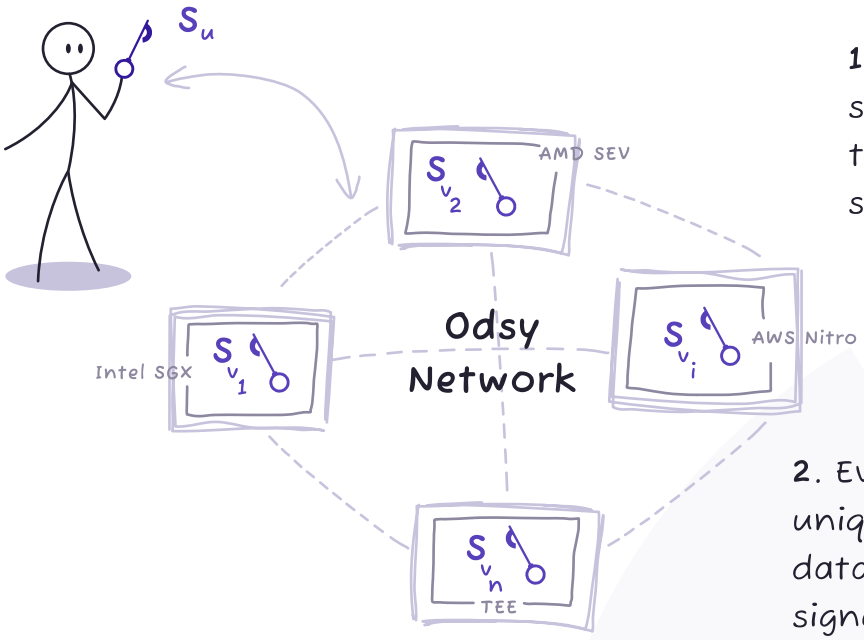
That being said, we chose to add another layer of security on top of MPC to make our network even more secure. We do that by storing the secret data of every validator on a Trusted Execution Environment (TEE) such as Intel SGX. This way, we have hardware security as an extra layer on top of the cryptographically secure MPC.

This yields an **ultra-secure system that is not reliant on any single point of failure:** compromising the network is not sufficient as the validators themselves cannot access their secret share because it is kept in the enclave, and breaking a single enclave doesn't suffice either as it only holds one secret share out of the required threshold t.

Additionally, we plan to support all of the different secure TEEs (Intel SGX, AMD SEV, AWS Nitro etc.) so that an attacker would need to have zero-day vulnerabilities to multiple different hardware implementations in order to break the system.

Odsy.
The future is trustless.

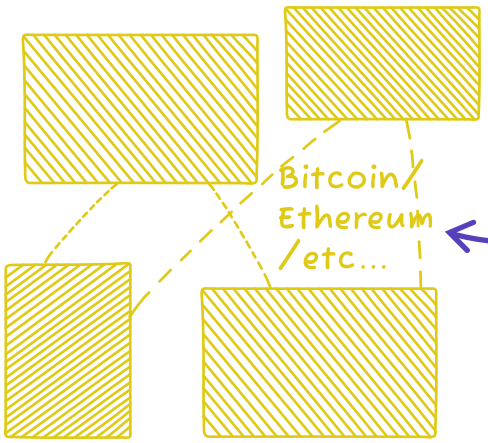
Signing with a t-out-of-n MPC in TEEs dWallet implementation



1. The user uses their own share S_u and pre-signing data to compute their partial signature $SIG_u(m)$.

2. Every validator uses their unique share S_{vi} and pre-signing data to compute their partial signature $SIG_{v_i}(m)$ and broadcast it to the other validators.

3. The validators' partial signatures are combined to form the blockchain's partial signature $SIG_{bc}(m) = SIG_{v_i}(m) + ... + SIG_{vn}(m)$ which is then saved on the blockchain.



4. The user queries $SIG_{bc}(m)$ from the blockchain and combines it with their partial signature $SIG_u(m)$ to form a valid signature $SIG(m) = SIG_u(m) + SIG_{bc}(m)$.

5. The user then broadcasts the signed transaction to the target blockchain, which validates it against PK.

all without revealing any secret share S_u or S_{vi}

The validators' shares $\{S_{vi}\}$ are privately kept inside different secure TEEs so no validator ever knows its share. The MPC code executed inside the TEE only returns partial signatures -- from which the private key cannot be reconstructed.

What Makes an MPC Implementation Truly Decentralized and Secure?

The choice of *t* and *n* is crucial to securely implement a decentralized network of dWallets using MPC. Firstly, in a truly permissionless network, the ratio between *t* and *n* must allow for redundancy – as the nodes holding the secret shares are not under the control of any centralized authority, and we cannot rely on their cooperation and availability.

Secondly, the larger number of parties *n* - the more decentralized and secure the network is.

Lastly, *t* and *n* should adjust dynamically in accordance with the changing network configuration which may include validators joining and leaving freely at any time. This is possible due to the concept of *key rotation* or *resharing*; when a validator leaves, the other validators can regenerate new shares, leading to that validator no longer being able to participate in signing (and the other validators can sign without that validator). Similarly, when a validator joins, the other validators can extend the sharing so that the joining validator will be able to participate in signing.

However, increasing the number of parties involved in an MPC computation, also increases the amount of communication between the parties and therefore the time required to complete the computation.

The balance between performance and security is a known battle. We are working with the world's best cryptographers in order to reach the perfect balance between the two, and our whitepaper will describe optimizations and modifications to the state-of-the-art MPC/TSS research (gg20, CMP) designed specifically for our purpose.

We believe this design of the Odsy Network is the most secure implementation of dWallets possible with today's cryptography. In parallel to building the first version of Odsy, with a plan to launch Odsy's testnet and mainnet in the near future - Our researchers, in cooperation with the world's best cryptographic research labs & universities, will engage in disruptive research to utilize under-researched-yet-promising cryptography with the aim of bringing them into practice, in order to offer a cryptologically unbreakable implementation of dWallets. This is our long term plan and a 5-year roadmap of our future research directions will be included in the whitepaper.

Access Control of Odsy Network Itself

Odsy Network is a network of dWallets, acting as the access control layer for the decentralized web. The natural question that comes to mind is how access control is managed for the Odsy Network itself.

The function of an account on other blockchains is fulfilled by a dWallet on the Odsy Network, with only dWallets being able to hold an ODSY token balance. The standard blockchain actions such as transfers, staking, voting etc. can also be done only through dWallets, in the exact same way that other blockchains are accessed using the Odsy Network. This means that access control starts with the Odsy Network, with user interactions that cascade into other networks, establishing dWallets as a single, multi-chain access point to all of Web3.

The remaining piece of the puzzle is how users authenticate when they perform actions with dWallets. The dWallet holds a list of users' public keys used by the wallet contract's logic, to verify authentication and authorization, and since there's always record on the blockchain, it serves as an audit log of the dWallet's access control.

A user that requests a dWallet to sign a transaction issues what we call a *Wrapped Transaction (wTx)* to the Odsy Network. We call it so because it wraps the transaction to be signed by the dWallet - which we call a *Wrappee transaction (weTx)*. The wTx also includes metadata (the wrapper) to identify which user signed the wTx and which dWallet they wish to sign the weTx with.

After the Odsy Networks authenticates the user against the wTx, and thus the weTx as well, the appropriate dWallet enforces the wallet contract logic to authorize the weTx for that user. After the weTx is authorized successfully, the weTx is partially signed by the validators of the network, which can be combined with the user's partial signature of the weTx to form the fully signed weTx – which is saved on the blockchain for the user to query and broadcast to the target blockchain.

Wrapped Transaction (wTx)

dWallet Address
Gas Fee
Auto Info
.
.
.

Wrappee Transaction (weTx)

Transaction data
.
.
.
Partial signature - $SIG_u(weTx)$

Example - Signing Ethereum Tx with Odsy (wTx)

dWallet1a5H3.....
0.0032 ODSY
Odsy8af4.... / SIG(wTx)
.
.

Example - Ethereum weTx

From: 0x1a5H3...
To: 0xf16E9...
Value: 2 ETH
.
.
Partial signature $SIG_u(weTx)$

Odsy Wallet Contracts SDK

The Turing-complete dynamic access control mechanism of the dWallet encourages implementations to parse the binary data according to the target protocol specification and determine whether it is permitted based on the access control rules and the decentralized state of the dWallet.

We will standardize transaction parsing in an SDK designed for wallet contract developers. Using our SDK, a developer can easily parse a binary transaction of any other blockchain without needing to know anything about its implementation details.

In addition to parsing the transaction format of blockchains, we will also offer the ability to parse the inputs to smart contracts calls in accordance with the smart contract's ABI. This would allow a developer, for example, to determine that the transaction a user wishes to sign is an Ethereum smart contract call to Uniswap v2's swapExactTokensForTokens() function to swap 1 ETH for 1,000 USDC.

The developer can then determine whether the user who requested that sign request is allowed to sign this message. So, for example, if the user is a trader leveraging arbitrages for the dWallet owner's profit, this can be allowed. But if the user will later try to sign a message transferring the 1,000 USDC to their wallet, it will be denied as their address is not allowlisted in the policy (which only permits certain swaps on Uniswap specifically and nothing else).

In the beginning, the Odsy team will build out the support for key blockchains into the SDK. However, since we are open-sourced and decentralized, as our network grows in usage, the blockchain and dApps developers themselves will be incentivized to contribute code to our SDK that adds support to their projects. This will, in time, prove as one of the biggest advantages of decentralized custody: the rapid pace of development and support that only a truly decentralized project can enable.

Odsy SDK

The Odsy Network is a public infrastructure platform, so we do not plan to design user-facing applications. Instead, we will develop a software development kit (SDK) for developers to integrate Odsy Network functionality and protocols utilizing wallet contracts into their solutions.

The Odsy SDK will interact with the Odsy blockchain in a completely transparent manner.

We will export functions that offer new dWallet creation, policy update, signing, transfer of ownership and interacting with smart contracts - which the developers may utilize however they like, without needing to worry about issuing transactions to the blockchain and querying results.

Odsy.
The future is programmable.

dWallet Use Cases

dWallets open up a world of possibilities that will transform how digital assets are stored, used, accessed and connected to the real world.

Needless to say, the movement from the static, absolute and intimidating private key towards a dynamic, flexible and secure dWallet will lead to a larger adoption of digital assets across the board - individuals, businesses and institutions. That will in turn increase the market share for existing and new players in the space - from protocols and blockchains to exchanges and custody solutions.

Odsy will serve as an infrastructure for developers to build new and exciting implementations of dWallet use cases.

We believe that many potentially competing solutions and innovations will be built on Odsy. We plan to support as many as possible through the Odsy ecosystem programs and through Ulysses Digital*.

The following is by no means an exhaustive list, but rather a few examples of the many use cases made possible by dWallets. We believe that the introduction of dWallets by Odsy will lead to a paradigm shift, and that new and exciting use cases will be conceived at a rapid pace by the broader Odsy community and ecosystem.

*) The Odsy Ecosystem fund is managed by the Odsy Foundation, the community pool is managed by the Odsy community directly through the Odsy Network governance, and Ulysses Digital is the Odsy Network founders' investment vehicle.

1. Digital Asset Custody

How custody works today

Centralized custody providers are here to stay. Many users need a custodian they can trust that provides them with services and fulfills regulatory requirements. However, custody solutions today don't have a dWallet infrastructure they can use, so besides taking care of the ***operational custody*** - i.e. holding and managing keys, regulatory licensing, insurance, UI/UX, customer support, physical storage, etc. - they must also develop very complicated ***blockchain custody technology*** - i.e. connecting to different blockchains, signing transactions, integrating with 3rd party solutions, building out security etc.

This technical overhead makes integrating with the rapidly expanding number of protocols and assets an exercise in futility, and at the same time creates a high barrier to entry for new operators looking to serve customers in different markets.

dWallets decouple the operational custody from the blockchain custody technology, by serving as the decentralized, universal custody infrastructure. This allows custodians to focus their primary efforts on customer experience and regional specific regulatory requirements.

Better Custody using dWallets

With dWallets, the policies are managed and enforced by the dWallet, and users - whether individuals, businesses or institutions - have the freedom to easily choose to join, leave or transfer between different operational custody providers. From the standpoint of the user, this brings usability to possibilities unavailable today.

The user knows that regardless of the provider they chose, their private key MPC shares are stored in the Odsy network and managed by the same dWallet interface. This, for the first time, empowers the user to be able to migrate between MPC custody providers in a frictionless manner – all that's needed is a change of the dWallet's policy.

The lower barrier to entry will pave the way for many small, local or niche players to become digital asset custodians, increasing the adoption and usage of crypto. Furthermore, a strong universal standard for decentralized digital asset custody also leads to a higher standard of support, utility and security - allowing for outsiders to audit & contribute to a single code-base upon which the entire blockchain custody is built upon. This means for example that new blockchains and protocols can add support for custodians directly, instead of being added manually by each and every custodian separately, after a painfully long and expensive wait.

2. Multi-Chain Decentralized Organizations

How DAOs Work Today

DAOs and Guilds have gained popularity in areas such as investment and gaming because they offer ways to facilitate collaborative efforts on the blockchain. The potential and promise that lies in decentralized organizations spark the imagination, creating an image in one's mind of a decentralized world where companies, communities and even entire cities live and operate on the blockchain.

In reality however, decentralized organizations have been coming up short, and their actual use is very limited and specific.

The three main reasons decentralized organizations have not been living up to their full potential are all related to access:

- Decentralized organizations have a built-in restriction to sign transactions and hold assets solely on the specific blockchain they were formed on.
- Real-world organizations have important aspects that are not reflected in decentralized organizations today - team members with different privileges, agents, subsidiaries etc.
- Many operations can't happen on-chain in a decentralized and trustless way (e.g. payroll, daily operations, vendor payments etc.), but rather involve external mechanisms and require users to initiate and sign transactions.

Better DAOs Using dWallets

A decentralized organization formed on the Odsy Network controls a dWallet that can hold assets on any other blockchain, sign transactions on those blockchains and control other decentralized organizations on other blockchains.

Furthermore, the sophisticated decentralized access control capabilities of a dWallet allow for practically any operation to be executed in a trustless manner - with dynamic access control that limits each user to the exact type and volume of transactions they are authorized to sign on.

The transferability of a dWallet means that decentralized organizations can be bought, sold and transferred, either completely or partially, connecting them in yet another important way to the real world.

dWallets will dramatically change our perception of what can be possible to achieve with decentralized organizations. Real world applications and structures - from partnerships and businesses to communities and cities - will now have a viable decentralized and trustless alternative.

3. Granular Access Sharing, Delegation and Control

Access to a static decentralized wallet is absolute and irrevocable. A private key has full power to sign any transaction, and if a private key is shared, lost or stolen - access to the wallet can never be modified.

However, in the real world, sharing access, revoking it, and managing different levels of permissions is fundamental both from a usability aspect and from a security aspect. Even when evaluating something as trivial as a note taking application, access control and sharing settings are amongst the most basic functionalities we have learned to expect - let alone when it comes to financial applications.

In order to solve this problem in crypto today, users must either trust a centralized custodian with their keys and/or assets, or trust a decentralized protocol with their assets - both options being extremely problematic, limiting usability and posing security risks.

A dWallet is by nature a trustless mechanism to share and control access to digital assets. Any type of condition - whether it's quorums, spending limits, allowlisted protocols etc. - can be used to control the shared access to a dWallet.

Consider the following few examples:

- **Delegated Asset Management**

  Taylor owns USDC tokens and would like to allow Jordan to carry out an investment strategy for her using DeFi. Today, Taylor's only option is to transfer the assets to Jordan, directly or through a smart contract that will allow Jordan to perform trades. With dWallets, Taylor is able to share access to her dWallet with Jordan.

Taylor configured Jordan's access so that she will only be able to perform actions on Uniswap with up to 1,000 USDC a month. The dWallet will block any attempt to transfer the assets outside of Uniswap, or invest more than 1,000 USDC a month. All the actions by Jordan are performed directly from Taylor's dWallet, and Taylor retains full control over Jordan's access, being able to edit or revoke it at any time.

- **Self Imposed Restrictions**

  Cameron holds a large amount of ETH in a cold wallet physically located in a safe deposit box in a bank. Cameron is also a big NFT enthusiast, and holds a hot MetaMask wallet they use to place bids on their favorite NFT artists' latest creations. Every few weeks Cameron goes to the bank to sign a transaction with their cold wallet topping up their hot wallet with funds.

  With a dWallet - Cameron can keep the secret for the main user controlling the privileges on the dWallet (owner) in the bank's safe, and share limited access with themself, a "hot" user with a weekly transactions limit of 30 ETH for example, that can only be spent on OpenSea or Rarible, with the "cold" secret now used solely for updating those permissions or for one-time large transactions.

  Reducing the interaction with the "cold" wallet increases both security and usability (no more weekly trips to the bank for Cameron!), and since both owner and user are of the same dWallet - everything Cameron now does is tied to the same address. This concept can of course be expanded to multiple users with different privileges that are kept in different environments based on their respective "heat", opening up a whole new spectrum of operational models.

- **Employee expense management**

  Drew manages a company with 800 employees located all over the world. Drew is a firm believer in delegating responsibilities and letting teams run their own budgets independently. Today, the way Drew can manage a distributed non-payroll expense system is through traditional solutions i.e. banks, credit cards and fintech.

  With dWallets, Drew will be able to create a unique user of the company's dWallet for each and every employee, with that user having the exact privileges that employee should have - what, where and how much they can spend. The company's dWallet can even have a cascading privilege management system, e.g. team leaders can create and manage users and privileges for their teams etc.

- **Household financial management**

  There are many banking and fintech solutions that allow households and families to manage their finances in a controlled way. Today, private keys don't allow that level of granular access control, but this is a necessity in order for crypto and digital assets to become widely accepted and used by the public.

  With dWallets households can be managed not just internally (household members' respective allowances) but also externally - providing spending authority for the landlord to collect rent, or for utility companies or for the local grocery store or anything else required to maintain the household.

- **Real World Financial Instruments**

  Real world financial instruments such as derivatives (e.g. option writing) or irrevocable proxies are implemented today in crypto using smart contracts. The main flaw in using smart contracts for those purposes, both from a usability and a security perspective, is that the user is forced to transfer the assets to the smart contract in order for the desired outcome to be enforced.

  With dWallets, these complex scenarios and instruments can be executed without transferring the asset anywhere. The assets stay in the dWallet, and authority to perform certain actions is granted to a user.
  As a side note - a dWallet might also be a powerful tool when planning certain real-world legal and/or tax structures, as it can be used to fulfill certain requirements of control / non-control - adding more real-world applications to crypto.

- **Identity**

  There are many identity protocols that utilize blockchain technology to provide trustless identification and authentication. The problem is that you must use your private key for web3 identity, putting your entire wallet ***including your identity*** at risk every time you sign-in or authenticate. With dWallets a dedicated *"view only"* user can be issued with no permissions but identifying as yourself, essentially proving you are the owner of a specific blockchain account, but with no risk of having your assets - and identity - compromised.

These examples are obviously not the only ways that controlled share access can be utilized, but demonstrate some of the fundamental issues today with access to crypto that can be solved with dWallets.

4. Custody-as-a-Service

Many centralized platforms such as exchanges, NFT marketplaces, funds etc. require a custody infrastructure to provide users with their services. Furthermore, existing players who want to add a crypto offering - e.g. banks, fintech apps, hedge funds etc. - require a crypto custody infrastructure as well.

Today, "custody as a service" solutions exist, however they are all centralized, usually provided through an API by an existing trusted custody service provider.

With dWallets, a new and decentralized model for custody-as-a-service is possible - a ***"Bring Your Own Wallet"*** model, where dWallets are used as the underlying custody infrastructure. Imagine a centralized exchange, where the order book is managed centrally, and dWallets are used as the universal and decentralized underlying infrastructure technology connecting them to the blockchain, or banks offering their customers a crypto account with specific predefined actions that are permitted by the local laws and regulations using a dWallet with access control.

This new model of "Bring Your Own Wallet" increases both the utility (supported blockchains and assets) and security (no more huge pools of money attracting attacks) of the projects utilizing it. Much like with Digital Asset Custody, it also reduces the barrier to entry for new and smaller participants and allows users to retain full control of their dWallet and simply and instantly join, leave and move between providers of similar services, or even join multiple providers with the same dWallet.

5. Interoperable Infrastructure and DeFi

One of the major problems with access in crypto today is interoperability between multiple chains and protocols. Today, in order to build interoperable DeFi projects such as DEXs, borrowing and lending, derivatives etc. or infrastructural projects like Layer-2s, wrapped assets, cross-chain communication etc. - developers are responsible for building everything from scratch.
The overhead in doing that is tremendous - setting up a bridge, building, running and managing the infrastructure, dealing with and managing security and being exposed to risks not directly related to the project's utility.

A dWallet, and its native interoperability, can be used as an infrastructure for any multi-chain DeFi or infrastructure project in a completely decentralized manner, removing all overhead and security operations on the developer side.

Each new implementation of interoperable infrastructure and DeFi projects with dWallets will involve a complete reimagining of the current state-of-the-art solutions. We believe that these solutions will be a big part of the Odsy ecosystem.

6. dWallet Marketplace

The transferability of dWallets enables users to treat the wallet itself as a tradeable asset, and creates a market pricing and liquidity where they didn't exist before.

The first most straightforward use for a dWallet marketplace would be transferring a multi-chain asset portfolio, with multiple assets, whether tokens or NFTs that live on different chains. The alternative would have been transferring assets one by one, which becomes increasingly expensive and time consuming as the wallet grows larger.

But a dWallet marketplace can also enable things that couldn't be done before. Certain assets today can't be transferred - whether those are vested tokens, bonded assets, veTokens or any other form of illiquid asset, there is currently no way for the market to properly price them, or for holders to liquidate them.

dWallets make that possible with the transfer of the entire wallet.

Pricing a dWallet also highlights the unique value that is held by the wallet itself. Each wallet's history holds not only historical or symbolic value*, but also real tangible value that should be priced efficiently by the market - e.g. rights for future fees, governance privileges, staked assets, potential airdrops eligibility, royalties from future sales of NFTs etc. Without dWallets, all of those can't be priced by the market and aren't liquid for owners.

*) imagine you could buy the wallet address that made the first real-world crypto transaction buying two pizzas for 10,000 BTC

7. Gaming

Blockchain based gaming has enjoyed tremendous success and growth over the past few years, with multiple games and protocols on different chains. Whether it's play-to-earn games, or games that utilize NFTs as part of the reward and/or game mechanics - crypto gaming has amassed billions in value of gaming tokens and NFTs.

However, the world of crypto gaming today is fragmented, with games and gamers isolated from one another. Multiple protocols on different chains introduce complexity with no real interoperability, and the growing success of gaming only highlighted this problem.

Furthermore, gaming guilds today have very rudimentary tools to proactively manage their members, collective assets, and policies around privileges. These guilds have to either leverage completely centralized solutions to help with this challenge, or they have to build their own tools, which for the most part have basic functionality and security vulnerabilities.

When it comes to gaming - dWallets completely shift the paradigm. Right off the bat, dWallets are perfect for a cross-game wallet, holding multi-chain assets that may represent in-game rewards, avatars, artifacts, badges, etc. But that's only the tip of the iceberg.

Gaming protocols built on Odsy will be able to support multi-chain games, with actual cross-chain game functionality and assets could be minted across different chains by design.

For the players - a dWallet will let users share usage rights for any in-game artifact, letting other players use their corresponding NFTs temporarily or permanently, with different lending / hiring models built around those capabilities. Additionally, a dWallet marketplace (see above) will allow gamers to buy and sell entire "gaming users", including history, assets, avatars and achievements. As for gaming guilds or guild-centric platforms, they will now have a trustless infrastructure to help them manage their activity, members and assets directly.

Gaming and gamers by nature push towards a connected, flexible multi-chain reality, and dWallets are precisely the infrastructure that can make that happen.

The ODSY Token

Tokenomics

The ODSY token is the native token of the Odsy Network. The token serves as the medium of all transactional activities within the Odsy Network, and as all actions occur on-chain, the nature of the ODSY token is that it is a utility token. The utility of the ODSY token is threefold:

- **Fee Function**

  All actions on Odsy involve dWallets and incur fees paid with ODSY tokens. Those include the creation of dWallets, the signing of transactions, transfer of a dWallet, the creation or update of an access control scheme and deploying smart contracts.

  A percentage of all transaction fees paid by the users are allocated to the *Community Pool*. The pool is part of the Odsy ecosystem and the funds therein will be used to support the growth of the overall network. The pool is controlled by the holders of the ODSY token in a decentralized manner, whereby the members can create and vote on proposals related to the allocation of funds to various projects and initiatives.
  The Community Pool will be empty when the Odsy Network is launched and slowly fill up as fees are paid by Odsy users.

- **Validation Function**

  Token holders can stake/delegate ODSY tokens in order to participate in the consensus mechanism of the Odsy Network. In return for this validation function, token holders will be rewarded with gas fees and inflation. The requirements for becoming a validator on the Odsy Network will be defined before the testnet launch.

- **Governance Function**

  Token holders who have staked/ delegated their ODSY token (see above) will be able to participate in the governance of the Odsy Network.

Token Genesis Supply and Distribution

The genesis (initial) supply of ODSY tokens is 12,109,000 - the optimal number of “lines of code”. The Token Supply shall be distributed by the foundation as follows:

Insiders: 48%

- **Founders**: The founders will purchase **22%** of the Token Supply from the Foundation. 20% will be allocated to the founders according to the 10-year Nostos Model (see below), and 2% will go towards Ulysses Digital - an investment vehicle with the purpose of investing in the Odsy ecosystem.
- **Team: 5%** of the token supply is reserved for the research & development team. Each team member receiving tokens will be subject to a standard 1 year cliff / 4 year vesting schedule.
- **Investors: 21%** of the supply is reserved for individuals and venture capital partners. The investor token allocation will be subject by default to the standard 1 year cliff / 4 year lockup schedule, however all investors are welcome and encouraged to opt-in and adopt the 10-year Nostos Model as well.

Community: 52%

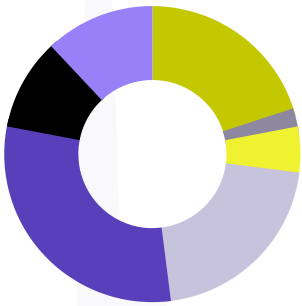
- **Foundation Treasury & Rewards: 30%** of the token supply will be retained in the Foundation treasury. That includes tokens that will be used for initial incentive rewards, future allocations for new ecosystem initiatives, potential future token sales, advisory services, payroll, day to day operation costs and contingency funds.
- **Ecosystem Fund: 12%** of the token supply will be used for ecosystem funding - including but not limited to - application grants, developer bounties, research partnerships and ecosystem support programs.
- **Public Sale: 10%** of the Token Supply is reserved for the public ODSY token sale to be facilitated by the Odsy Foundation for the community.

High Level

- Team
- Investors
- Foundation
- Community

Detailed

- Founders
- Ulysses Digital
- Team
- Investors
- Foundation
- Public Sale
- Ecosystem Fund



Crypto - A 10 Year Odyssey

We believe that token distribution, lockups and vesting schedules in crypto are broken as they exist today. Without standardized proper long term incentive structures, cases of abuse, opportunism and fraud are inevitable, making it hard for legitimate projects to build trust in the long term commitment of the team and founders.

When Odysseus set sail to return home after the Trojan War, he didn't know it would take him 10 years before he saw his wife Penelope and claimed his place as the rightful king of Ithaca. Luckily, we understand that building the future of crypto and digital assets by solving the problem of access will most likely take the better part of a decade.

We believe that a radical change is required as part of the maturity of the crypto space, especially considering the instant liquidity of tokens and the fact that crypto projects are long-lasting initiatives. Crypto projects should adopt longer lockup periods than traditional startups, not shorter ones.

The Nostos Model

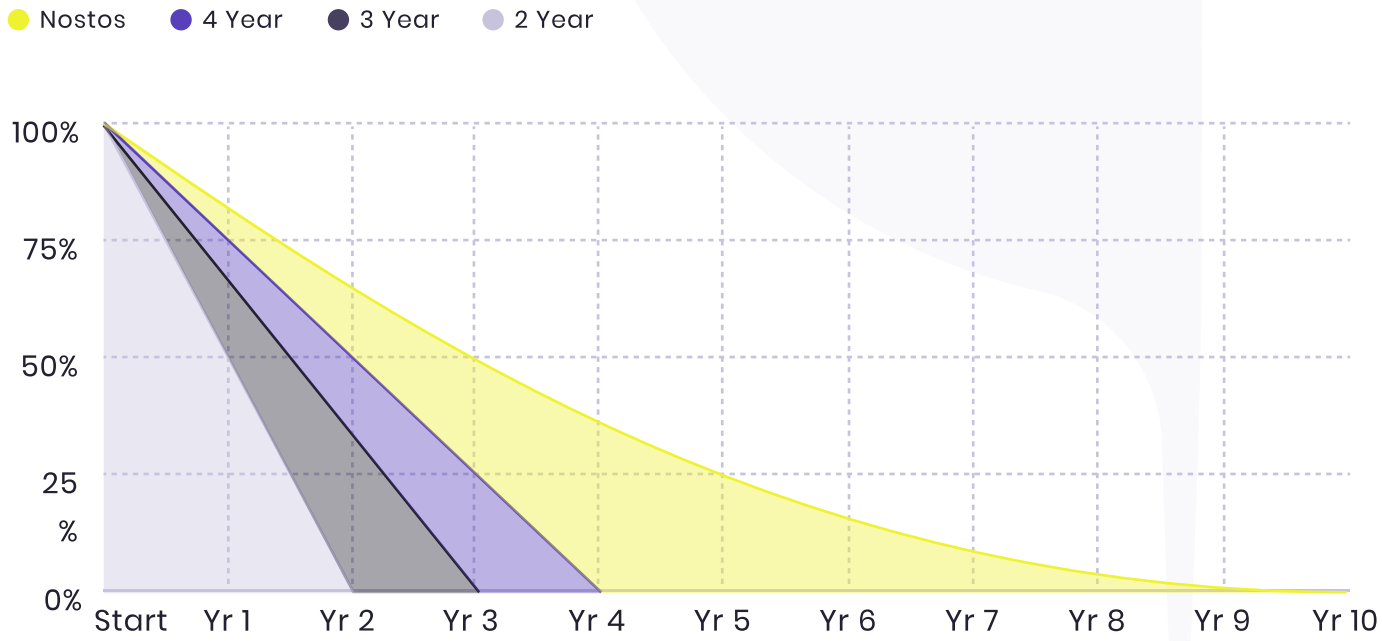
The Nostos theme of an epic hero's long journey back home, overcoming great challenges and obstacles to finally complete their quest, is the main theme of the Odyssey.

We propose the ***Nostos Model*** of a 10-year linearly declining lockup for founders:

The Nostos Model					
Year	Released	Accumulated	Year	Released	Accumulated
1	19%	19%	6	9%	84%
2	17%	36%	7	7%	91%
3	15%	51%	8	5%	96%
4	13%	64%	9	3%	99%
5	11%	75%	10	1%	100%

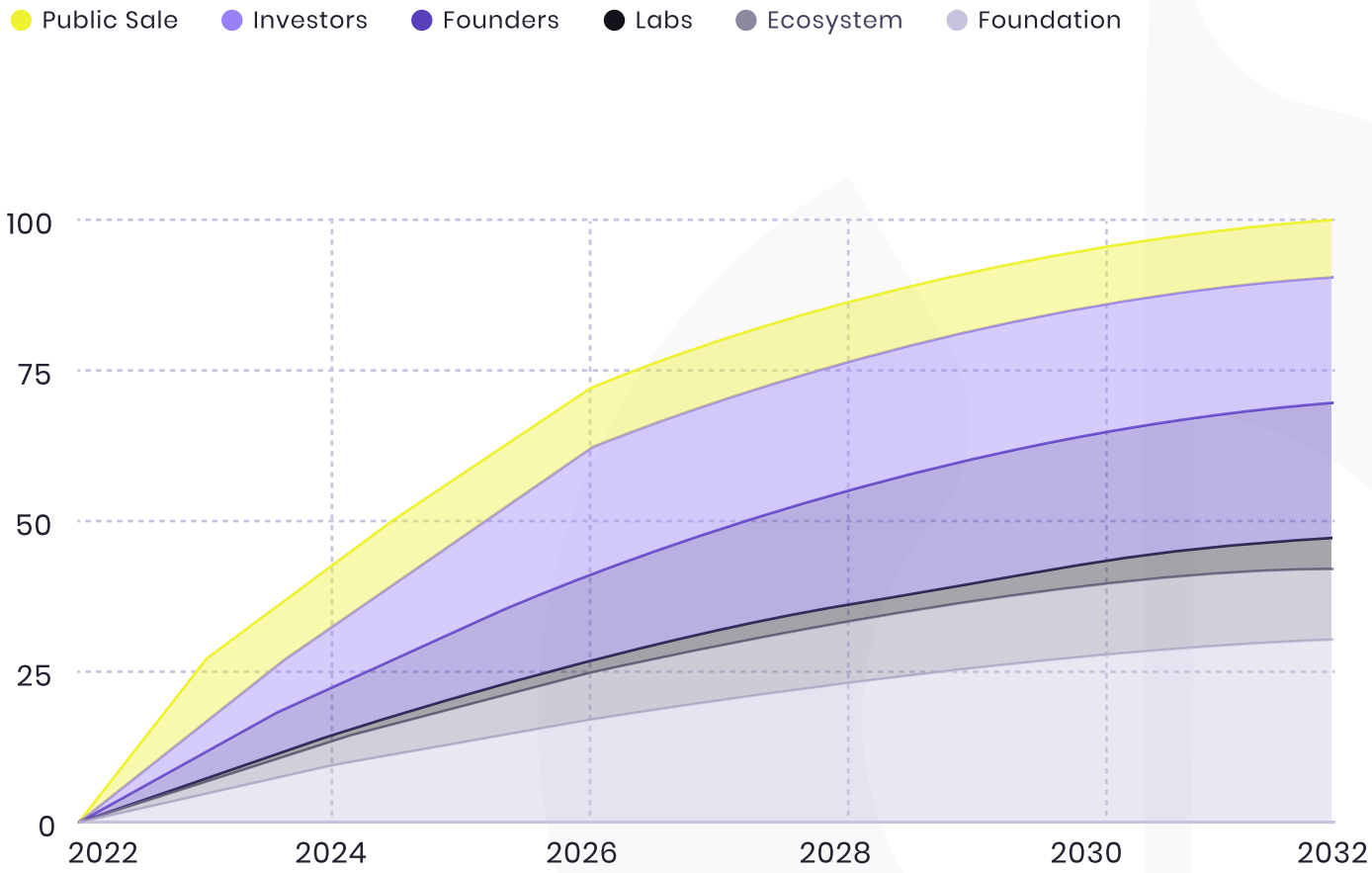
Our view is that the Nostos Model should be adopted by crypto projects as the new standard, replacing the 2-year, 3-year and 4-year models that are prevalent today:

Nostos model vs. Traditional models - % of tokens locked



The projection of the token release schedule on all categories also considers the 10 year mark as the long term goal to be aligned to:

ODSY Token. 10-year estimated release schedule



It's clear to us that for many investors, teams and contributors, the Nostos Model may be difficult to adopt for various reasons, and unlike founders it might be hard for them to commit for such a long term. That is why for others beside the founders a 4-year schedule is reasonable.

However, we strongly encourage investors, teams and contributors to show their support and commitment to projects' long-term vision by adopting the Nostos Model for themselves as well.

Conclusion

In this paper we propose the concept of dWallets and its first implementation - Odsy Network - a decentralized network of dWallets. We have not addressed all of the mechanics of how the Odsy Network will be implemented (e.g. consensus, incentives, stack etc.), and we intend to provide those details in our whitepaper.

While we have seen tremendous innovations with new protocols, assets and chains over the past few years, we are also seeing the access to crypto becoming increasingly centralized with solutions that hold the assets and keys for the users. We believe that in order for the industry to fulfill its promise and gain broader adoption for real-world use cases, access to digital assets must be extremely flexible, secure and most importantly - trustless.

This is why we are introducing the dWallet primitive, and implementing it as a core building block on the Odsy Network to serve as the universal layer of access control to decentralized networks - today and in the future.

We believe the concept of dWallets will shift the paradigm and shape crypto for years to come, much like the way smart contracts did when Ethereum introduced them as we know them today. We invite you to join our odyssey, to build out the future of access to crypto and be part of the ecosystem that will support the next decades of crypto development and growth.

August 2022 - version 1.0

hello@odsy.xyz