Censo: Building a Unique Protocol to Solve Seed Phrase Security for Good

OUR MISSION & VISION

In the volatile world of cryptocurrency, a persistent and costly issue has plagued investors and enthusiasts alike: seed phrase mismanagement, leading to over $200 billion in losses. This staggering figure highlights a critical vulnerability in the digital asset ecosystem, where traditional methods of seed phrase storage, such as pen-and-paper or digital password managers, have fallen short in providing the necessary security.

Censo was born out of necessity. We've witnessed firsthand the devastating impact of seed phrase mismanagement on individuals and the broader crypto community. Our mission is to empower users to ensure their digital assets are secure, yet easily accessible to them and them alone.

Censo is a potentially groundbreaking seed phrase management protocol leveraging zero-knowledge authentication and strong encryption to address this pervasive problem. With its innovative approach, Censo aims to revolutionize the way users secure their crypto assets, promising an end to the era of significant losses due to seed phrase mismanagement.

OUR PRINCIPLES

Censo provides users for the first time ever the ability to store, manage, and access their seed phrases without anxiety, knowing that they'll never lose access to their crypto. To achieve these goals, Censo has been designed in compliance with the following guiding principles:

Robust security

Seed phrases are users' most precious digital records. Censo is designed so that no matter how large the value of those records, Censo's security exceeds the standards required to protect them and keep them safe.

Total privacy

Users never need, nor can, identify themselves with Personally Identifiable Information or by any other means that link back to their real-world identities to use Censo. Users do not need to rely upon Censo protecting their information; they are guaranteed that Censo has never collected any of their information to start, making it impossible to be compromised.

Complete control

No one other than the user managing their seed phrase can ever be able to access or read any part of that seed phrase whatsoever. Users have complete control and sole access to their seed phrases.

Censorship resistance
Users are guaranteed that they can access their seed phrases at any time without the permission, assistance, or operation of Censo, or for that matter, any other 3rd-party. Users cannot be subject to forfeiture risk owing to sovereign or corporate encroachment.

Loss tolerant
Users must be protected against a permanent loss of both their authentication credentials and/or encrypted shares of their seed phrases, and they must have the ability to restore either in those loss circumstances. This data persistence and redundancy is best enforced with on-chain mechanisms.

Decentralization
Users must not be dependent upon centralized entities for the integrity, security, and access to their data. The Censo Protocol enables decentralized and secure data storage, policy management, authentication enforcement, and communication; completely free from the interference of centralized 3rd-parties.

Open-Source & accessible to all
Users must be provided with choices and an environment that fosters healthy competition amongst providers and developers working on solutions. Censo Labs has produced mobile apps that are built to interact with the Censo Chain, but this ultimately should just be one choice of many for consumers. The Censo Chain is open-source and permissionless, and Censo Labs will work to provide SDKs and tooling to foster a strong developer community.

Acceptance of human nature
Virtually all of us are not good at things like remembering passwords or securely storing physical items for retrieval at a later date. We cannot be relied upon for extraordinary feats of memory, nor to ensure that our computers or mobile phones will not be lost or damaged in the future. Censo recognizes all these things and is designed to conform to human nature, rather than hoping that human beings will change and conform themselves to something unnatural.

THE CENSO APP CHAIN: A VISION OF DECENTRALIZATION

Purpose-Built Blockchain
The Censo App Chain, designed from the ground up, will provide decentralized storage of seed phrases, security policy management, and enforcement of strong authentication, ensuring that users have perpetual and secure access to their digital assets.

Governance via Smart Contracts
The governance of key operations and policies within the Censo ecosystem will be vested in smart contracts. These autonomous and immutable protocols enforce transparency and facilitate a trustless environment within the Censo ecosystem.

Chain Functions:

Data Storage

Decentralized storage and guaranteed censorship-resistant persistence of seed phrase owners' crypted data, including both seed phrases and security policy configurations.

Policy Management

Trusted oracle for seed phrase owner and approver public keys and the source of truth for their security policy. Owners can update security policies stored on chain and are assured that they and only they have access their seed phrases because policies are on chain and supported by multisignature approvers.

Authentication Enforcement

The Censo Protocol supports strong authentication of users without the collection of PII or any information that can be tied back to a real-world identity. It is completely anonymous. The Chain works in tandem with the Censo Mobile Apps to enforce the integrity of this authentication.

Messaging & Communications

The Censo Chain supports and validates encrypted communications between different user types such as owners, approvers, and beneficiaries. It also importantly supports communications between owner/users and integration partners such as wallet providers, and these channels allow for the management and secure storage of seed phrases without the seed phrases ever having been exposed.

Payment

The Censo Token is used to pay for access, transaction, and storage on the Censo Chain.

Protocol Participants

Seed phrase owners

Seed phrase owners use a 3rd-party app such as the Censo Mobile App to interact with the Censo Chain to securely store, manage and access their seed phrases. Seed phrase owners pay usage fees (in the form of Censo tokens) to the protocol for these services.

Validators

Validators secure the Censo Chain through their participation in the consensus mechanism. They are compensated in the form of staking rewards for this provision of this security. The Censo Chain will likely use validators that are also providing security to the principal chain in the ecosystem in which Censo has built.

Censo Foundation

The Censo Foundation will be committed to continuing decentralization and evolution of the Censo Chain and Protocol, community building, and establishing deep and lasting relationships with protocols and service providers with which Censo Chain continues to integrate.

Censo Labs
Censo Labs is a for-profit, U.S. domiciled corporation. Censo is committed to improving and evolving the Censo Protocol, providing apps to end users so they can access the protocol, and providing developer tools so 3rd-parties can contribute more easily to the ecosystem. Censo Labs may charge users fees for some of its services and technologies.

Wallet providers, dApps, and other integrators
Using the SDK provided be Censo Labs or software of their own, wallet providers, dApp operators and others can provide their users with an improved experience that increases their security and allows them to manage their seed phrases without ever exposing them. The Censo Foundation will look to encourage these efforts and reward integrators that add value to the Censo ecosystem.

Developer community
The developer community is a critical element of a vibrant and robust ecosystem. Censo Labs and the Censo Foundation will work to build, support, and energize this community.

THE CENSO TOKEN AND ITS ECOSYSTEM
Token Utility

- Staking: The Censo token is pivotal for network participation, allowing users and node operators to stake tokens for network security and governance, with rewards proportionate to their contributions.
- Access and Transaction Fees: Within the platform, the Censo token is the currency for services that require gas, such as seed phrase access, authentication enforcement, and security policy management.
- Governance Participation: Token holders are entrusted with voting rights on crucial ecosystem decisions, including updates to protocols, feature enhancements, and governance policy shifts.

Incentive Mechanisms

- Validator Incentives: Validators engaged in securing the Censo App Chain receive token rewards, motivating them to maintain a resilient and secure network.
- User Engagement Rewards: Users can accrue tokens through engagement within the platform, including participation in app usage and vetting, referrals, and community-driven projects.
- Integrator Rewards: The Censo SDK allows wallet providers, dApp operators, and other developers to provide their users with a superior UX, while securing their seed phrases without ever exposing them. Integrators can accrue Censo tokens by engaging in these integrations and by referring their users to Censo.

Detailed Economic Model

- Strategic Token Supply Allocation: The distribution of the token supply is carefully calibrated among users, developers, validators, and the Censo treasury, harmonizing incentives across the ecosystem and fostering sustainable growth.
- Dynamic Incentive Structure: The Censo tokenomics model is crafted to support a dynamic ecosystem with incentives for validators, developers, and users. It

promotes network growth and user retention through a balanced reward system that recognizes and compensates value-adding activities.
- Sustainable Economic Model: The economic principles underpinning the Censo token supply and distribution are designed for sustainability. This includes mechanisms for token recycling, reward distribution, and a deflationary policy that aligns with long-term network health and value retention.

CRYPTOGRAPHIC FOUNDATIONS

At the core of Censo's security promise lies its robust cryptographic infrastructure, deployed in both its mobile applications (available on App Store and Google Play) as well as on the Censo Protocol Chain. A detailed discussion of Censo's present security design may be found here, https://assets.censo.co/media/docs/Censo_security-design.pdf. Immediately below are some highlights of Censo's implementation.

Keys & Encryption

Encryption

All cryptographic keys are generated on users' mobile devices, and all encryption and decryption operations are controlled by users and executed securely on their mobile devices. Industry-standard and long-proven asymmetric and symmetric encryption techniques are exclusively employed. Users always remain in sole control of any keys used for decryption.

Signed data in transit

All communication traffic between users and Censo or the Censo Chain, and users and each other is encrypted and signed, ensuring against man-in-the middle attacks or the possibility of being read while in transit.

Shamir secret sharing

Censo implements this robust cryptographic technique to split approval authorities required for users to access their seed phrases. This eliminates single points of failure and ensures that single points of compromise will not result in the leakage of seed phrase material.

Authentication & Privacy

Authentication resiliency

Censo relies upon multiple factors of authentication for users, and this enables resilience of authentication should a user lose access to one of their authentication factors.

Authentication accuracy

By utilizing 3D biometry with liveness check as one of several factors of authentication, users are authenticated with the highest degree of accuracy possible.

Authentication anonymity

When users authenticate to Censo or to the Censo Chain with Apple or Google, Censo collects a login ID (in the case of Apple, a Pairwise Pseudonymous Identifier, in the case of Google, an identifier unique to the user) or private key signature that is persistent and is not associated with any PII. Censo collects no PII whatsoever and all users remain

anonymous. Censo maintains only a SHA2 hashed version of user login IDs (in the case of an Apple or Google login) and has no other data such as PII to identify them. In addition, it is impossible for Censo to tie the 3D biometry data provided by users to any real-world credentials or identities.

Trust & Openness

Open-source code

All of the components of Censo that require trust are open-source and audited, including mobile apps and the Censo Chain. In addition, Censo mobile apps use attestation to ensure that only the signed Censo version of the app can access a user's data.

No trust in relay server

Censo acts as a relay server to allow communication between seed phrase owners and approvers and the Censo Chain, but no trust of the backend is required as all traffic is encrypted and signed, and out-of-band channels are used for important verification and establishment of trusted connections (typically via TOTP over phone call). The maximum damage an attacker could achieve on the backend would be a temporary denial of service.

In the future, users can choose to utilize their own relay servers should they desire.

Users' Trusted Approvers

Users may select those individuals whom they trust to assist them in the management of their seed phrases, rather than being compelled to use agents of Censo's choice.

Secure deletion

Users have complete control over all their data at every moment. This includes the right of deletion. Users may securely delete their data whenever they desire.

Collusion, Coercion & Censorship Resistance

Offline mode

Censo may be optionally operated in offline mode, without a connection to Censo, the Internet, or the Censo Chain. In offline mode it is impossible to censor user access to seed phrases, nor is it possible for a 3rd-party, such as a sovereign entity, to interfere with a user's actions.

Owner control

Seed phrases can only be accessed at the direction and control of the seed phrase owner. Even a theoretically plausible mathematical quorum of Shamir share holders cannot access a seed phrase without the owner's action and agreement.

Data persistence

Censo presently maintains fully encrypted versions of user seed phrases on its backend, an important function that will be assumed by the Censo Chain. Users may at any time delete the Censo app from their mobile devices, download it at a future date, and instantly reestablish a full connection and access. This ability to wipe the app from the phone may appeal to users crossing national borders or in other situations. As well, this data

persistence means that Censo is not hardware reliant, and users are resilient to the loss or replacement of any hardware device.

Timelock
Users may optionally employ a timelock that gates the speed at which a seed phrase can be accessed, after a valid approval of the access request. This timelock may be considered a useful security measure for some users.

Ease of Use
Simple operation
Users can activate in Censo and achieve their seed phrase security in a matter of minutes. While ease of use may not often be considered a security feature in common thought, it is a critical element of security – allowing users to secure their seed phrases easily and rapidly, and with comprehension, despite the sophistication of the underlying cryptography and operations.

CENSO'S MOBILE APPS
Censo's seed phrase management apps are available today and can be downloaded from the App Store or Google Play. Presently they are integrated with Censo's backend, which has been designed to be trustless, meaning that all communications and data the backend receives are signed and encrypted and cannot be corrupted.

Principal functions of the Censo Mobile Apps include:

- **Seed phrase input –** Users may securely input seed phrases by the following means:
    - Manual input through the keyboard
    - Pasting from the clipboard
    - Secure photograph that does not leave the app
    - Via Censo SDK from an integrated wallet or dApp
- **Seed phrase encryption –** Seed phrases are automatically encrypted without any actions taken by the user.
- **Adding and verifying approvers –** Users can add approvers to increase their security by distributing cryptographically provable approval rights required to access seed phrases.
- **Approval rights sharding –** Approval rights for access of seed phrases are sharded cryptographically by the app without any actions taken by the user once approvers are verified.
- **Seed phrase access –** Users may access their seed phrases at any time and in conformance with the security policies they have previously established.
- **Authentication recovery –** Users may recovery factors of authentication, such as biometry or login ID with the assistance of their approvers.
- **Beneficiary designation & legacy features –** Coming soon is the ability of a user to designate a beneficiary who can take control of the account in the event the user dies or is incapacitated, thus establishing a valuable legacy guarantee.

We encourage users to download the Censo App and see for yourself just how effortless and anxiety-free seed phrase management can be. It truly is a breakthrough in seed phrase security.

Although the Censo backend has been designed to be trustless and cannot corrupt or impersonate users, it nonetheless is centralized, and therefore Censo could theoretically quash users' transaction requests. It is this centralization of the backend that we intend on resolving with the migration to the Censo Chain over the coming months.

ROADMAP

Q4 – 2023

- Product conception & design
- Censo Security Design White Paper
- Beta release of Censo mobile Seed Phrase Manager
- Release of Developer SDK for Web, iOS & Android
- Completion of initial code audits

Q1 – 2024

- Production release utilizing Censo's trustless backend
- Reward points program release
- Wallet, dApp and developer integrations
- Censo Chain ecosystem selection

Q2 – 2024

- Censo Token Paper
- Migrate Censo backend to Testnet
- Testnet launch

Q3 – 2024

- Migrate Censo backend to Mainnet
- Censo Token launch
- Mainnet launch

LOOKING FORWARD: CENSO'S VISION FOR THE FUTURE

Censo's ultimate goal is to establish a new standard for cryptocurrency security, where seed phrase management is not only secure and private but also intuitive and user-friendly. The Censo App Chain and token represent the next steps in this vision, moving towards an ecosystem that is fully decentralized and governed by its users.

Censo stands at the threshold of a new era in digital asset security, ready to redefine what it means to manage seed phrases securely. With its advanced cryptographic infrastructure, user-centric design, and innovative tokenomics, Censo is building a platform that will serve as the gold standard for secure, decentralized, and user-empowered digital asset management for years to come. As we forge ahead, we welcome the global

cryptocurrency community to participate in this exciting and transformative journey with Censo.

As the blockchain space continues to grow and evolve, Censo remains committed to innovation and excellence in digital asset security. We invite the community to join us on this journey, contributing to an ecosystem that not only protects but also empowers its users.