vendible

vendible

Privacy-preserving identity network

Litepaper V1.0 / August 2022

This paper was issued by Vendible BVI Inc, a non-US entity formed for the purpose of issuing the VEND token

vendible

01

overview

vendible

Overview

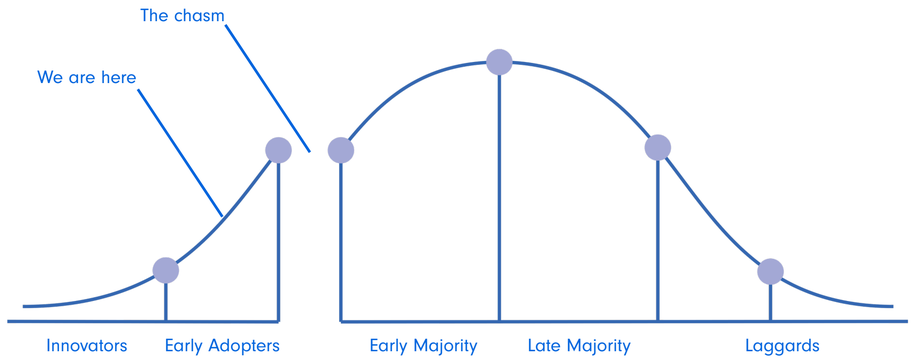
Bitcoin started the blockchain revolution as a method to securely transmit transactions across the internet between people who did not know or trust one another.

The fundamental technology behind Bitcoin, blockchain, has been so successful that between 200 and 300 million people and 12,000 businesses have interacted with the technology.

While impressive, this only represents 4% of the world's population. Like many new technologies, there is a chasm blocking mainstream adoption.

While decentralized finance and improved business processes can fundamentally change our way of life, open blockchain networks, by design, have several limitations which will keep the vast majority of people and businesses from participating without the aid of custodians or permissioned blockchain networks.

Since 2017, Vendible has researched the measures required to bridge the adoption chasm. Our solution for open networks will help realize the early innovator's dreams of a decentralized and user-owned internet.



Originally constructed for a closed permissioned system in 2018, Vendible received a grant from the Algorand Foundation in 2021 to translate our system to open networks. Our services can extend from Algorand to all open networks.

vendible

02

approach

vendible

Identity

Nothing is more fundamental to our interactions with others than our identity. Who we are matters. While a trustless, pseudonymous network is attractive to a small minority, it is human nature to want to know with whom one is dealing.

Vendible uses identity to construct a trust layer over open, trustless systems. In our model, each participant is unique. There is only ever one account for each of our members. Even if you do not know who you are transacting with, in Vendible, you have the assurance that they are accountable and that you are not transacting with bots or someone hiding behind many pseudonymous accounts.

Decentralized identifiers, or DIDs, manage the Vendible network. We work with identity validators using biometrics and documents to validate our members and ensure uniqueness. Vendible never sees or stores member data. The validator returns the verified member's data to the client, where end-to-end encryption stores this essential information in our decentralized data layer. A DID document with claims to the data is registered on-chain. No one can view this encrypted data except for you. This main account becomes your anchor point in web3.

Vendible allows you to manage all of your data and who is allowed to view or access this information. Our DIDs give you ownership of not only your assets but also your data. We believe to be genuinely web3, this is crucial.

vendible

Privacy

Having an anchor point for identity is only as valuable as its application. Given the nature of open blockchain networks, outside parties can quickly identify others without proper controls.

It is a common misconception that blockchains are anonymous. They are pseudonymous. Any time you disclose your public address to a counterparty that can identify you, the state and activity of your assets from origin to present and beyond are now fully available to them. No payment system can reach widespread adoption with this limitation.

This feature is not an issue solely for individuals. The majority of Fortune 500 companies are exploring blockchain solutions. However, these companies will only build on private, permissioned networks as they cannot risk exposing data to their trade partners.

Vendible has solved this issue on open networks with the concept of associated accounts. We use zero-knowledge circuits and advanced cryptography to generate specific addresses on-chain for asset and data transactions. These addresses link to the main DID identity account without exposing those connections to outside parties. From this foundation, we create unique addresses for each instance or trade partner.

Examples include connections between a friend, web2 social media application, or dApp. Transactions move between associated accounts in a privacy-preserving manner to mask the origination. Members have the option to share data.

vendible

Data

With our central DID anchor point, privacy-preserving associated accounts that link counterparties, and our decentralized data layer, Vendible can provide data ownership to individuals in the spirit of web3.

Each associated account has an accompanying DID document, which governs the private links to the main DID and any attributed encrypted data.

Connected members can choose to share specific information without exposing the rest of their controlled data. Sharing data can be as simple as viewing the name of a contact, a message between friends, or a client contract.

This control structure allows Vendible to offer developers methods to board users by querying DIDs using zero-knowledge proofs to ensure compliance while preserving the user's privacy. If a developer wants to ensure that a social media dApp does not have bots, simple on-chain checks can prevent Sybil attacks.

Developers can perform authorization checks based on geography, age, and other metrics to ensure compliance without needing to view the actual data. They can also create new data attributes that users can opt into and attribute to their DIDs. All data is then encrypted, stored in decentralized storage, and controlled by the user. If the user no longer wishes to access an application, the application and developer no longer have access to that data.

vendible

Security

For widespread adoption of blockchain technology, individuals and businesses need to feel secure. Security comes in many forms and depends upon the participant. A network must account for all of its members.

While exciting and full of possibilities, decentralized finance is highly volatile and risky. Only those willing to overcome the technical burdens and understand the potential rewards are eager to take those risks. Before engaging, most will need some assurances.

Vendible couples identity to assets. This core component allows developers options to program BSA, travel rule, and central banking practices at the transactional level. Our credit ledger system merged with our associated accounts is the perfect balance of privacy and compliance.

What sets our system apart from current web2 financial solutions and emerging permissioned blockchains is the removal of centralized controls as we remain on the open network so that transparency and fairness are maintained. Most importantly, ownership of assets and data is always in the user's hands.

Our network ensures privacy as long as a member is not a bad actor. Members can lose that privilege if they abuse the system or another member. Working with our validators, we can extend KYC and ongoing AML services as required to wallet providers and applications in web2 and web3.

vendible

03

focus

vendible

wallet

The Vendible wallet was released to alpha testing in January 2021 and closed beta in April 2021. Besides our first product release, the wallet provides the first example of a direct link between identity and assets.

Our early testing and discovery focused on user experience. To generate our main DID account, an individual must first undergo a verification process. We understand this is not intuitive and may turn some people away from using the product. To ensure success, we needed to explain several vital points in the process correctly.

First, identity verification is necessary to produce the primary decentralized identifier, ensuring our network's uniqueness. Without this initial check, most of our services would not be possible.

Second, Vendible does not have access to any data or assets as part of this account creation process, nor do we desire to manage member assets. We operate on a sovereign model and do not believe that key custody or control over member assets is necessary for the proper operation of the network. Our validators and other participants on the network must make the same pledge to uphold member sovereignty.

Developers can embed our wallet infrastructure in their applications to manage user accounts with hierarchy controls while maintaining web3 principles.

vendible

Trustible

The fear of losing private keys is one of the main barriers to widespread adoption. Potentially 20% of all Bitcoin has been irrevocably lost as there is no tolerance for mistakes with self-sovereignty.

Trustible is a sovereign private key recovery service for all blockchain networks. In harmony with the Vendible sovereign model, no central party or service sees, stores, or holds a member's private keys. This service provides members security and peace of mind without needing custodians.

Trustible can accept private keys from the leading blockchain networks. We create a new associated account on Algorand, run our zero-knowledge proof and encryption setup, and store the results in our decentralized data layer with a new DID. The DID contains the encryption information necessary to recover a lost key.

All keys are recoverable through the main DID private key. If the main DID private key is lost, the member can return to the identity verification module. Biometric scans confirm a cyphertext for the member for the member's device. The device searches the DIDs for a match and then asks a series of questions previously answered and known only by the member. This process is the standard for most members to confirm the account and regain access to their private keys across all blockchain networks.

Costs for Trustible will be low to ensure as many people can take advantage as possible. Additional insurance offerings will be available through our partners.

vendible

Connectible

Vendible is working with the Algorand Foundation to produce an open-source middleware solution for identity on the Algorand network. Sharing goals, architecture, and codebase directly with the research team, Vendible will release Connectible.

Connectible is a general framework for sovereign identity with access points for validators, verifiers, producers, and consumers. This suite of developer tools scales from dApps to corporations to provide the flexibility of tailored solutions with identity at the core.

Connectible will regularly publish documentation on best practices in identity management and cutting-edge research as we look toward the future.

The first set of tools focuses on essential identity services and includes integrations for zero-knowledge proof authorization systems, anonymous or known KYC and AML monitoring, associated accounts, and DID provisioning.

A suite of smart contracts and node access opens the Vendible decentralized, encrypted data storage. The platform includes methods to create attributes, manage hierarchy and access, and monitor usage.

Finally, certified developers can leverage associated accounts and logic signatures to produce web2 experiences for web3 applications. These contracts and programmable transactions allow non-web3 natives to participate in DeFi in a sovereign manner without connecting wallets.

vendible

04

network

vendible

Unique

Vendible is a cooperative network built on privacy-preserving identity protocols. We are a people-first company and intend for our network to reflect our values. Every action we take is to ensure the safety, security, and sovereignty of those who put their faith in our technology in hopes of better outcomes for themselves and their loved ones.

We believe technology should serve the least of us, not the other way around. We desire to lift all who decide to participate and support Vendible and those around them. Our participation rewards directly reflect this desire.

In the Vendible network, each individual is unique and has an equal opportunity to participate in all our services regardless of background. We embrace a diversity of thought and experience. The more voices that help govern our network and take an active role in ensuring that our online experiences are outstanding, the better Vendible can serve the network.

We hope that, through our service, people and businesses will discover new ways to interact positively with one another and that this uplift will have impacts far beyond our balance sheets and accrued assets.

vendible

05

VEND

vendible

Purpose

As a cooperative network where every participant is unique, Vendible strives to help create environments where people and businesses can flourish. Vendible will issue VEND, a utility and governance token that helps secure the network and rewards beneficial action to accomplish this.

Each participant on the network must stake VEND in proportion to their involvement with the network. Auditors or Vendible can slash a participant's stake if they are a bad actor or abuse the system. Staking VEND happens during the creation and management of associated accounts.

Vendible believes it takes a tribe to compete successfully in today's world. Vendible issues VEND to members through various published activities to incentivize support. Members will manage a portion of these rewards as part of participation in governance, and, ideally, the members will take full ownership of these functions over time.

As a people-first company, employment with Vendible includes a profit-sharing program. We are extending the distribution of profits to those members who wish to participate in governance.

A treasury collects a percentage of all transactions. These pools are available to members to distribute as dividends, investments, or special projects.

There are no inflationary mechanisms connected to staking the VEND token. As VEND has a fixed supply, inflation through staking is not sustainable over time.

vendible

Utility

Every participant in the network must stake VEND as a cooperative action to ensure long-term stability for Vendible. There are multiple entry points for staking.

Members stake VEND in Trustible when securing new private keys. They can either participate when connecting their new associated account or allow another member to stake on their behalf.

Vendible stakes VEND for each new core associated account in the Vendible wallet. Members stake VEND in the wallet for additional accounts or to take a more active role in governance.

Certified developers stake VEND when creating associated accounts to manage users on their platform.

Data storage providers stake VEND for each associated account whose data store accesses their pledged availability.

Members who stake VEND can opt into governance. VEND governance includes oversight of the Vendible treasury and future accountability programs.

The treasury grows from the operation of the Vendible networks and products. Due to the flexible payment systems inside Vendible, the treasury comprises many digital assets, including BTC, ETH, ALGO, VEND, and more.

From the treasury, members have the freedom to make investments, issue dividends, and commission projects for the good of the network.

vendible

Distribution

Venidble will mint a fixed supply of 1,200,000,000 VEND at the token generation event (TGE). VEND will not burn, and there will be no additional mint after the TGE.

49% of VEND goes towards participation rewards. Rewards distribute as part of initiatives and contests announced by Vendible. Over time, Vendible will grant management of participation rewards to the members participating in governance.

24% of VEND goes to Vendible BVI Inc. This portion will go towards yearly employee incentives, partnerships, and forming or aligning with a governing body, the Foundation. The Foundation will audit Vendible, assist with regulatory matters, and guide the network towards decentralization.

12% of VEND has been committed through a private Reg S offering for our seed funding. Another 12% has been designated but not fully committed for our private funding round. Any portion of this allocation not fully committed before the TGE will return to Vendible.

3% of VEND is designated for advisory services to the company.

Vendible will administer no public sale of VEND. Decentralization of VEND will occur through participation, the natural distribution of VEND to associated accounts, and the exchange of VEND through DEXs and CEXs.

Early participation rewards have been assigned to those participating in the Vendible wallet beta program. There will be extensive rewards for the Trustible beta program as well.