PriveSecure
PROTOCOL

WHITE PAPER

We are featured on

CoinMarketCap coinbase CoinGecko Forbes COINTELEGRAPH

TABLE OF CONTECT

ABSTRACT

The evolution of technology has come about with more threats to privacy and security. A new generation of technology is fueling rapid worldwide change. Throughout recent history, "waves" of technical progress, fueled by inventions ranging from steam power to electricity to the automobile, have fueled economic development and social revolution.

Given the global spread of the internet, the state of privacy in the twenty-first century is an international problem. When it comes to the impact of technology on privacy and security, several key themes emerge, including cybercrime (and crime-fighting), the application of old privacy laws to new technologies, and whether companies can share customer data without consent. However, different countries face different challenges.

With this cloud project, Privesecure will be able to address that data security concern through the use of encrypted text transfer. It will encrypt the data. It will exchange and store data using a SQL database due to its increased security.

For Cryptocurrency users, one of the most valuable assets they have is the burgeoning open-source community that enables this movement. Individuals throughout the world benefit from open-source software because it allows them to remain independent of governments and major businesses that are always attempting to follow, censor, and control them. Numerous of these initiatives are not for profit and are not supported by significant expenditures. Rather than that, they rely on an ever-growing network of individuals worldwide who volunteer their time and energy to help build them, frequently for free.

When safe collaboration is a critical component of your daily activities, you need security and compliance that you can trust. We deliver you the very best in security, privacy, and compliance with the Privesecure Cloud.

Privesecure will develop an open-source cloud storage platform aimed at providing data security solutions for cryptocurrency enthusiasts. At Privesecure, we use open source to innovate, and we release the open-source to share our innovations. We encourage you to browse through our projects to find work to use, share, and build on!

Privesecure, as an open-source storage platform, intends to disrupt the cloud storage industry by repurposing otherwise underutilized computer storage. We will examine the characteristics of the Privesecure platform and the company's efforts in the areas of security, compliance, privacy, and data processing in detail in this paper.

INTRODUCTION

Privesecure is a blockchain-based platform with database features (such as decentralization, immutability, and owner-controlled assets) (e.g., high transaction rate, low latency, indexing & querying of structured data)

Privesecure transforms cloud storage into a market for cryptocurrency users. The market is based on a blockchain that uses a native protocol token (also known as "Privesecure token") that allows users to earn by storing data for users, who pay with the Privesecure token to store or distribute data.

This creates a strong incentive for miners to accumulate as much storage space as possible and rent it to clients. This platform connects these accumulated resources into a self-healing storage network on which everyone can rely. The network achieves robustness by content replication and dispersal while also automatically identifying and fixing replica faults. Clients can configure replication parameters to safeguard against a variety of threat models. Additionally, the cloud storage platform ensures security, as content is encrypted end-to-end at the client, and storage providers are not provided with decryption keys.

Cloud storage, although being a huge strength for certain providers, is not without flaws. And in certain rare cases, this can result in major issues for its users. Privesecure is the ultra-secure cloud storage, sync, and sharing solution for organizations and individuals that want to store, sync, and share information with confidence.

The need to purchase, administer, and maintain in-house storage infrastructure is eliminated when data is stored on the cloud. Even while cloud storage security is often better than any on-premises protection, the absence of control over cloud-based data remains a major worry for enterprises.

Privesecure aspires to be an open-source cloud storage platform for cryptocurrency users. Privesecure strives to develop a strong security culture that allows cryptocurrency users to safely store and access data on the internet. Economic incentives embedded into the system will ensure that files are successfully and constantly stored and retrieved for the time selected by the user.

We will make its source code available to anyone who wishes to examine, copy, learn from, modify, or share it. Some individuals may be hesitant to migrate to the cloud owing to security concerns, but a reputable cloud service provider, such as Privesecure, will set your mind at ease by providing extremely secure cloud services.

At the core of Privesecure, the goal is to foster a robust security culture that enables everyone to securely store and access data on the internet and improve scalability while at the same time aiming to save money (reduce storage costs, reduce operation, and labour costs). We take security extremely seriously and will take extensive measures to protect the security of your files within the Privesecure platform on a user, application, data centre, and network level.

Data breaches, system vulnerabilities, inadequate identification, and credential and access management are just a few of the common security issues that cloud storage providers must deal with. Cloud computing security is critical for any user or corporation concerned about the safety of their data. As cloud computing becomes more generally accepted, it is important to maintain a robust cloud security posture to reap the benefits. Scalability, higher availability, and better DDoS protection are all advantages of cloud security.

The data security solutions and technology from Privesecure will meet the growing issues of safeguarding today's complex, distributed, hybrid, and/or multi-cloud computing environments. Understanding where data lives, keeping track of who has access to it, and limiting high-risk behaviours and possibly dangerous file moves are all examples of this. **Privesecure will prioritize the following features:**

Capabilities for advanced cybersecurity

Authentication systems and access control techniques that are secure.

Features that provide a high level of availability.

End-to-end data encryption.

Data is stored on servers that are spread across many locations.

Physical device and infrastructure security at the highest level.

Features for advanced cloud monitoring.

Privesecure will implement a technique known as Shared Security Responsibility. Privesecure depends on consumer collaboration in an ongoing effort to improve security.

BLOCKCHAIN

Data storage is a major issue with traditional blockchains. These issues necessitate the use of new third-party protocols on top of existing blockchains because on-chain storage fees are too high.

As a result, the content will always be subject to a fee on traditional blockchains.

The need for an open-source, low-cost, scalable data storage protocol grows as the demand for data storage grows exponentially.

For the first time, **Privesecure is a platform designed to provide scalable on-chain storage at a low cost.** A blockchain is a time-stamped collection of immutable data records administered by a group of computers rather than a single body. Using various cryptographic concepts, each block of data is secured and linked to the next, producing a chain. The blockchain network has no centralized authority. It's more like a democratized system with a shared and immutable ledger where everyone can see the information.

END-TO-END ENCRYPTION

Privesecure encrypts cloud data. A malevolent person or software will only discover jumbled data if they try to access a file. A decryption key is the sole means to decode encrypted data. Data at rest and in transit will be encrypted using Privesecure. Data in the cloud that isn't being used at the moment is protected by encryption at rest (AES 256-bit encryption is the most popular option). Data in transit (TLS/SSL 128-bit encryption) safeguards data while it travels between two cloud or network sites.

We strive to be an industry pioneer and the top provider of open-source cloud storage services. **Privesecure's key goals are information security, legal compliance, and data protection.** When developing Privesecure features, data security by design and default are critical concerns.

DATA RECOVERY

Data can be lost in a variety of ways in this world, including system failure or mechanical malfunction, hard drive failure, human mistake, virus infection, data theft, and accidentally overwritten or erased from a computer.

Not only is Privesecure resilient to storage, but it also sends encrypted data to safe offsite storage for redundant backup, thereby replicating the file in a new location to protect it from site-wide disasters. This off-site storage stores encrypted data but does not retain the encryption keys required to unlock it. Our additional layer of protection with immutable and isolated copies addresses today's developing threats and enables rapid recovery following a hack.

DATA GOVERNANCE

Data governance is currently plagued by a lack of cooperation and trust. In addition, there are no obvious incentives for participants to collaborate on governance topics. Privesecure's incentive-driven, easy-to-integrate platform aids in the resolution of these data governance challenges. Data governance topics, feedback, and economic incentives can be modelled as Privesecure assets in the approach. We can easily collaborate and define processes on top of data governance systems once we model them as a collection of **Privesecure assets, as the data is shared using a common substrate, and all participants can be incentivized to participate.**

OPEN SOURCE

The word "open source" refers to something that is modifiable and shareable by anybody due to its open design. The phrase developed in the domain of software development refers to a certain style of programming. However, the term "open source" now refers to a broader set of values—what we refer to as "the open-source approach." Open source projects, products, and initiatives uphold and promote the concepts of open exchange, collaborative involvement, rapid prototyping, transparency, meritocracy, and community-oriented development.

Privesecure’s open-source software will be available for free. Thousands of developers from around the world collaborate on Privesecure to create the most powerful, stable, and secure solution possible. Developers may investigate how the Privesecure code works and make modifications to dysfunctional or troublesome elements of the program to better suit their individual needs since Privesecure will be adaptable. Users may rely on Privesecure for long-term initiatives. **Privesecure encourages originality by allowing programmers to enhance software by modifying current code and even creating new ideas.** Privesecure includes a built-in community that updates and improves the source code on a regular basis.

PRIVESECURE ECOSYSTEM

Privesecure's mission is to provide cryptocurrency users with a long-term, robust, and ever-evolving open-source cloud storage infrastructure. The Privesecure ecosystem is made up of interconnected components that provide users with a complete experience. These are some of them:

User Control - You have complete control over your files.

By default, files uploaded to Privesecure are private. You may only share or make them public if you wish to share or make them public.

Granting Access: Share a collaboration folder with other Privesecure users - Any Privesecure user can share a folder with other Privesecure users.

Users can upload and download files, leave comments, and start discussions depending on the rights you provide them. At any moment, the folder owner can disable access to one or all of the users.

Distribute a public link: Link to the file download or embed the link directly in your website, blog, or another third-party program. Privesecure generates a unique **URL and ID from a randomly generated combination** of letters and numbers in both circumstances.

Construct a widget: Create a widget to share a file or folder on a public site. **After you've completed the form,** you'll receive HTML code that you may use to embed on any site you own. Your files will be shown in the widget, and visitors will be able to download them as needed.

Restrictions on access

Grant-specific rights: When sharing content, you may give different levels of access to different people. There are three levels: Preview only (only viewable on your web browser; downloading is not permitted), **Upload only, Download only, Full Access (which includes the right to delete files),** Upload and Download, or Download Only.

Protect a link to a file or folder with a password: You can opt to **password-protect a public link** to a file or folder when you create it.

Set an expiration date for a file that will be **automatically removed and hence no longer available.**

Unshare a file — You can opt to unshare a file at any time, even if no expiration date has been selected. When a file is unshared, all **public links to it are deactivated**, and it is removed from any widgets.

User Privilege Management – Platform Security

Validated data access - Privesecure validates data access using proven **password and privilege mechanisms depending on a user's privileges.** Unauthorized access will result in failure.

With every request to the platform, Privesecure uses robust user authentication. In essence, any activity in Privesecure is only permitted once the system verifies that the user has the necessary permissions.

TOKEN ALLOCATION

The total supply of the **Privesecure Tokens** is 40M as it is distributed as follows:

Token Use	Token Use	Token Use
Team	6,000,000	15%
Team	6,000,000	15%
Team	6,000,000	15%
Team	6,000,000	15%
Team	6,000,000	15%
Team	6,000,000	15%
Team	6,000,000	15%

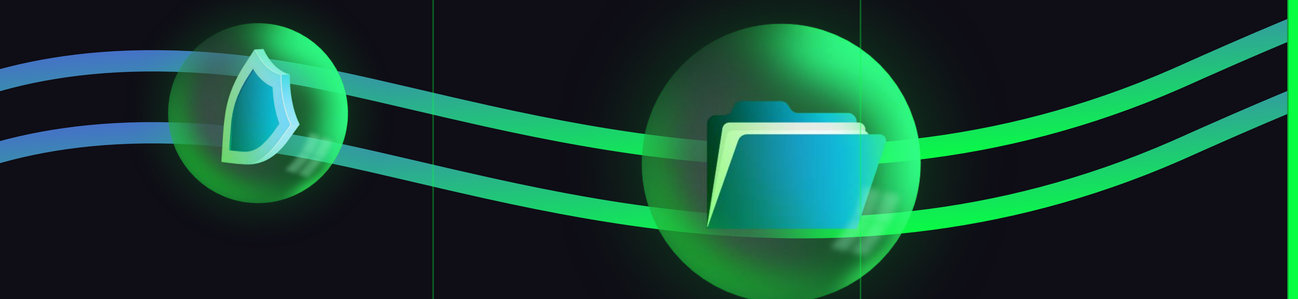
Use of Proceeds and Funds from Token Sales

Product Research and Development	45%
Sales &Marketing	20%
Operations	20%
Reserves& Liquidity	10%
Legal	5%

There will be at least a 2 month vesting period.

THE ROADMAP TO WIDESPREAD ADOPTION

This section outlines the main advances necessary to support Privesecure's widespread adoption.



ROADMAP

Stage 1: Creation of Website

The first stage will focus on designing and establishing the official website for Privesecure.

Stage III: Private Sale

At this point, only a small number of investors and other interested parties are allowed to participate in the initiative at this stage.

Stage V: Exchange Listing

The native tokens will be listed on major centralized and decentralized exchanges.

Stage 10: Launch of the Privesecure

Stage II: Whitepaper release.

Stage 3's major goal will be to release and publish project documentation. On this page, you'll find a complete breakdown of the project.

Stage IV: Public Sale

Access to the purchase of the Privesecure token.

Stage 9: Public Relations and Marketing

The procedure will be advertised extensively in order to promote awareness. We plan to use a range of marketing methods, including the help of renowned cryptocurrency influencers.

DISCLAIMER

Information in the White Paper is purely for the purpose of passing it forward to others. It should not be interpreted as an attempt to persuade anyone to invest in the company. All of Privesecure's future performance is not guaranteed by this Lite Paper and should not be interpreted as such. Privesecure makes every effort to ensure the accuracy and update of the content on its website. There are no guarantees or promises that the information provided by Privesecure will be accurate or complete.

Neither Privesecure nor any of its affiliates are liable for any direct or indirect damages resulting from access, use, or non-use of the information provided. Nothing in this lite paper or website should ever put Privesecure in the position of being held liable for any kind of loss, no matter how small.

REFERENCES

Greenemeier, L., 2022. International Report: What Impact Is Technology Having on Privacy around the World?. [online] Scientific American. Available at: <https://www.scientificamerican.com/article/international-report-technology/> [Accessed 13 April 2022].

Ibm.com. 2022. What is Data Security? Data Security Definition and Overview | IBM. [online] Available at: <https://www.ibm.com/topics/data-security> [Accessed 13 April 2022].

Opensource.com. 2022. What is open source?. [online] Available at: <https://opensource.com/resources/what-open-source> [Accessed 13 April 2022].

Synopsys.com. 2022. What Is Open Source Software and How Does It Work? | Synopsys. [online] Available at: <https://www.synopsys.com/glossary/what-is-open-source-software.html> [Accessed 13 April 2022].