Distributed Cloud Storage Powered by Solana Blockchain Network

Build on Solana (SOL) Blockchain Network as an open source initiative.

Table of Contents

Disclaimer 3

2. Market Opportunity 4

3. Problems of Centralized Cloud Storage 6

3.1 Data Privacy
3.2 Cyber Attacks
3.3 Data Manipulation
3.4 Remote Work Force

4. What is Decentralized Cloud Storage 8

5. Stasis Storage 9

5.1 Core Focus of Stasis Storage Platform
5.2 Stasis for Node Operators
5.3 Stasis for Customers
5.4 Stasis Guarantees
5.5 Our Support Channels

7. Stasis Features 12

6.1 Security
6.2 Reliability
6.3 Robust
6.4 Cost Effective
6.5 Storage Nodes
6.6 Redundancy Risk & Solutions
6.7 Metadata
6.8 Encryption
6.9 Audits and Reputation
6.10 Data Repair: File Redundancy

7. Stasis Ecosystem 17

7.1 User
7.2 Node
7.3 Satellite
7.4 Environmental Impact

8. Stasis Token 18

8.1 Allocations
8.2 Tokenomics

9. Staking 19

10. Roadmap 20

11. References 21

1. Disclaimer

The purpose of this document is to present information about Stasis Protocol.

The information set forth above may not be exhaustive and does not imply any elements of a contractual relationship. Its sole purpose is to provide relevant and reasonable information on whether to undertake a thorough analysis of the company with the intent of acquiring tokens.

Whilst every effort is made to ensure that statements of fact made in this document are accurate, all estimates, projections, forecasts, prospects, expressions of opinion, and other subjective judgments contained in this paper are based on assumptions considered to be reasonable as of the date of the document and must not be construed as a representation that the matters referred to therein will occur. Any plans, projections, or forecasts mentioned in this paper may not be achieved due to multiple risk factors. No information in this Whitepaper should be considered to be business, legal, financial, or tax advice. You should consult your own legal, financial, tax, or other professional advisers regarding the Stasis tokens and their respective businesses and operations.

This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction. No person is bound to enter into any contract or make a binding legal commitment.

No regulatory authority has examined or approved any of the information set out in this Whitepaper. No such action has been or will be taken under the laws, regulatory requirements, or rules of any jurisdiction. The publication, distribution, or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements, or rules have been complied with.

This whitepaper is subject to change as coin progression and development advances. Changes will be reflected in future updated/revised whitepaper versions.

2. Market Opportunity

In today's fast-paced and information-driven business landscape, data is not just a resource; it has become the core fuel powering innovation, decision-making, and growth across industries.

Companies are becoming increasingly aware that the more insights

decision-makers have about their employees' needs, shifts in the competitive landscape, and the evolving demands of customers, the better they can plan for future expansion. This growing reliance on data to inform strategy and drive competitive advantage has led to a rapid and continuous expansion of cloud storage solutions.

Cloud storage enables organizations to handle massive volumes of data efficiently, providing flexibility, security, and scalability that traditional on-premise storage solutions often cannot match.

The global cloud storage market is on track for significant growth, with projections showing that it will increase from USD 89.9 billion in 2024 to a staggering USD 265.3 billion by 2030. This represents a robust Compound Annual Growth Rate (CAGR) of 19.4%. Several factors contribute to this remarkable expansion. Chief among them is the increasing need for businesses to scale their operations and adapt quickly to changing demands without the burden of expanding physical data infrastructure. Additionally, cloud storage offers significant cost advantages, allowing organizations to reduce their capital expenditures on hardware while benefiting from pay-as-you-go models for data storage.

This flexibility is especially critical as enterprises face an unprecedented rise in the volume of data generated from various sources, such as digital transactions, IoT devices, and customer interactions. Remote workforces, which surged in number following the global pandemic, continue to expand, further fueling the need for seamless, ubiquitous access to data and files from anywhere in the world. Cloud storage's ability to offer low Total Cost of Ownership (TCO) while maintaining operational efficiency makes it an increasingly attractive option for enterprises of all sizes. In 2024, the solutions segment remains a key player in the market, accounting for the largest market share.

The cloud storage market continues to offer significant opportunities. While the solutions segment is expected to maintain its lead, the services segment is projected to grow faster between 2024 and 2030. As businesses shift from hardware-based storage, they are adopting cloud environments for 24/7 data access, enhancing agility and operational efficiency. Cloud storage meets enterprise demands for cost-effective data management and security. The rising need for data backup and disaster recovery solutions also fuels growth, as organizations become more vigilant about protecting data from cyberattacks and disasters.

At the same time, growing concerns around data privacy, highlighted by controversies like WhatsApp's data misuse, are driving demand for decentralized services. These platforms, built on blockchain and similar technologies, give users control over their personal information, offering cloud-like accessibility and scalability while preventing monopolization of data by any single entity. As data security concerns rise, decentralized, privacy-focused platforms are poised to influence the future of cloud storage.

This shift aligns with broader trends toward transparency and control. As more decentralized players enter the market, offering solutions where user data remains private, cloud storage will see further innovation. Companies that blend the scalability of traditional cloud services with decentralized privacy solutions are positioned to lead the next phase of market growth.

The convergence of scalability, cost-efficiency, privacy, and data security will continue driving investment in cloud storage technologies through 2030, making it a highly competitive sector.

(**Source:** www.researchandmarkets.com)

3. Problems of Centralized Cloud Storage

Global Cloud storage is currently serviced by companies like Dropbox, Apple, and Google have revolutionized company operations thanks to their cloud storage service. Not only has third-party cloud storage met the ever-increasing demand for more storage, but they have managed to save businesses thousands of dollars in IT investments. Unfortunately, despite their obvious utilities, they do suffer from a lot of issues.

3.1 Data Privacy

By agreeing to use monopolistic cloud computing, we are forced to provide complete control of our proprietary data to third-party cloud storage service providers, It's like the company hands over their data to a third-party for storing services. Since the data is outside the company's control, the data privacy settings are beyond their control as well. All cloud storage companies have builtin data sniffing clauses in their privacy settings.

3.2 Cyber Attacks

Since all the data is stored inside a third-party, centralized server, they are susceptible to hackings. Over the years there has been a significant rise in cyber attacks, These can be simple hacks to more sophisticated attacks like ransomware. This not just some random assumption, third-party servers have been repeatedly hacked to obtain sensitive and private information. There have been multiple counts of data hacks on personal data, including social security and driver license numbers.

3.3 Data Manipulation

Facebook's Cambridge Analytica debacle is the best example of a third-party mismanaging their client's data. Cambridge Analytica was able to get their hands on the personal data of a staggering 87 million Facebook users, of which 70.6 million were from the United States. In another infamous case, media analytics company "Deep Roots Analytics," used the Amazon cloud server to store information about as much as 61% of the US population without password protection for almost two weeks. This information included names, email and home addresses, telephone numbers, voter ID, etc.

3.4 Remote Work Force

Pandemic made staggering changes to lives of employees/business Many companies have now encouraged employees to work from home, This has significant security risks. Employers might lose or misuse access to enterprise networks and critical data from home, which could compromise the client's privacy. Also, if a data breach does occur, then it is quite difficult to track down all the employee devices and discover the point of failure.

3.5 Insider Threats

Another major concern with centralized cloud storage systems is the risk posed by insider threats. Employees or contractors with access to sensitive data can misuse it for personal gain or malicious purposes. There have been numerous cases where insiders have leaked confidential information, leading to significant financial and reputational damage. For instance, in 2020, a former employee of a major tech company was convicted of stealing confidential data and attempting to sell it to competitors. Insider threats are particularly challenging to detect and prevent, as the malicious actors already have legitimate access to critical systems and data. This makes monitoring and safeguarding against these threats a top priority for enterprises using centralized cloud services.

Our Mission at Stasis:

To develop the world's most secure, reliable and decentralized cloud storage services. At Stasis, we are committed to creating a platform where data security and privacy are paramount. By leveraging decentralized technology, we ensure that no single entity has control over your data, eliminating the risks associated with centralized storage. Our goal is to provide a storage solution that not only offers flexibility and scalability but also guarantees robust protection against cyberattacks, data breaches, and unauthorized access. With Stasis, users can confidently store and access their information, knowing their privacy is safeguarded at every level.

4. What is Decentralized Cloud Storage

Decentralized cloud storage offers a democratized solution for storing data by distributing it across multiple storage providers. This innovative service is powered by hundreds of individuals and enterprises who lease out their unused cloud space. Unlike centralized cloud systems, decentralized storage has no single operator or entity responsible for running the service or managing interruptions, ensuring that control is shared across the network.

One of the primary motivations for preferring decentralization is to break the monopolistic hold a few large corporations currently have over the cloud computing market. These corporations not only manage a significant portion of internet traffic but also raise security concerns around privacy and the protection of personal data.

Decentralized storage seeks to reduce infrastructure costs for maintenance, utilities, and bandwidth while offering enhanced security and greater control over data.

Our research reveals that there are vast underutilized resources at the network's edge, particularly among smaller operators. These operators possess a large amount of unused or underused resources that could be effectively utilized to create a more affordable and geographically diverse cloud storage solution. For instance, some operators might have access to lower-cost electricity compared to traditional data centers, while others might benefit from cheaper cooling solutions. While these smaller environments may not have the capacity to run a full-scale data center individually, when combined, they can power much larger decentralized cloud computing operations.

This model leverages these distributed resources, offering a scalable, secure, and cost-effective alternative to traditional cloud storage systems. By decentralizing cloud storage, the market becomes more inclusive, with opportunities for smaller operators to participate and thrive while providing end-users with greater privacy, security, and cost savings.

5. Stasis Storage

Stasis is dedicated to becoming a robust decentralized cloud storage platform. Our solution merges the convenience and user-friendliness of enterprise-grade storage services, such as Google Drive, with the reliability and transparency of open-source technology. We aim to challenge the current monopolization of the cloud service provider market by offering a decentralized alternative. Stasis enables users to rent storage space from individual or storage node operators, instead of relying on centralized providers. This decentralized approach not only diversifies the market but also empowers individuals and smaller operators to participate in the growing cloud storage ecosystem.

5.1 Core Focus of the Stasis Storage Platform

Expanding the network by recruiting and supporting storage node operators who contribute to the decentralized system. Generating demand for cloud storage from a growing base of paying users looking for more secure, cost-effective alternatives to traditional providers.

5.2 Stasis for Node Operators

Stasis offers an additional revenue stream for small businesses or Network Attached Storage (NAS) operators, particularly those who may have enough resources to operate several hard drives but lack the capacity to run large data centers. By aggregating these small operators, Stasis creates a powerful network that offers faster, cheaper, and more geographically distributed cloud storage solutions. This model allows operators with surplus electricity and hardware to contribute to the platform, creating a mutually beneficial ecosystem where smaller players can compete alongside larger providers.

5.3 Stasis for Customers

Stasis ensures that customers' data is securely encrypted, fragmented, and distributed across multiple hosting nodes worldwide. By using a decentralized blockchain network, Stasis creates a democratic marketplace for data hosting, where users maintain complete control over their information. There are no centralized intermediaries to interfere with data access, granting users full authority to manage and secure their data. This model provides not only greater privacy and security but also the freedom to decide who has access to specific data sets, makingStasis a powerful alternative to traditional cloud services.

5.4 Stasis Guarantees

5.1.1 Thoroughly Tested Platform for Quality Assurance
5.1.2 Dedicated support delivered directly by our engineers
5.1.3 Enterprise-grade SLA up to 24/7

5.5 Our Support Channels

5.1.4 Easy Documentation to help you migrate to Stasis
5.1.5 Access to expertise around scaling, security, and best practices
5.1.6 Access to optional workshops and training

By forming a contract, a storage provider agrees to store a client's data and to periodically submit proof of their continued storage until the contract expires. The host is compensated for every proof they submit and penalized for missing proof. Since these proofs are publicly verifiable network consensus can be used to automatically enforce storage contracts. Importantly, this means that clients do not need to personally verity storage proofs; they can simply upload their tile and let the network do the rest.

To avoid failures that can be caused due to storing data on a single

untrusted host, We would store data across multiple points that guarantees data redundantly across multiple hosts.

6. Stasis Features

Stasis stands out from the crowd of data storage technologies with these ten major key features:

1. Security
2. Reliability
3. Robust
4. Cost-Effective
5. Storage Nodes
6. Redundancy Risk & Solutions
7. Metadata
8. Encryption
9. Audits & Reputation
10. Data Repair: File Redundancy

6.1 Security

We are fully aware that security is the most important aspect that clients look for when they think of moving any data off-premise. Our system is designed to be the equivalent of spreading an encrypted droplet of water in the vast ocean. All data is encrypted client-side before reaching our system. Data is shredded and distributed across a large number of independently operated disk drives which are part of a much larger network of independently operated storage nodes. In a typical scenario (with a 20/40 Reed-Solomon setup), each file is distributed across 40 different disk drives in a global network of thousands of independently operated nodes.

6.2 Reliability

Data stored on a decentralized cloud is duplicated and deduplicated across multiple nodes in various geographical locations and networks, providing immunity against system-wide events. Storms, power outages, floods, earthquakes, operator error, design flaws, network overload, or attacks can compromise entire data centers. While the centralized providers may calculate and publish theoretically high availability numbers, these calculations depend on drive failures being uncorrelated.

6.3 Robust

Data stored across the Stasis network can provide superior read-intensive performance by deploying parallelism. The storage nodes are located close to “the edge,” reducing the latency experienced when recipients of data are physically far from the data center that houses the data. The particular erasure coding scheme that we use ensures that slow drives, slow networks, or networks and drives experiencing temporarily high load do not limit throughput. We can adjust the k/n ratio so that we dramatically improve download and streaming

speeds, without imposing the kinds of high costs associated with CDN networks.

6.4 Cost-Effective

Storage Node Operators on a Decentralized network are hosted by Individuals, Which reduces the investments significantly. In our experience, the vast majority of operators are using existing live equipment with significant spare capacity. There is no additional cost to a storage node operator in terms of capital or personnel. The operator does not have to make any investments to run storage drive at full capacity, Which helps him offer storage at comparatively cheaper rates than those put up by Public cloud storage operators who make large capital investments in building out a network of data centers and must incur significant costs for power, personnel, security, fire suppression, and so forth.
Even after providing a healthy margin to node operators, demand partners, and Satellite operators, we believe we should be able to provide profitable storage services at a fraction of the cost of equivalent centralized cloud storage providers.

6.5 Storage Nodes

Storage Node manages the supply side of the ecosystem. The primary function of the storage node is to store and return data. Aside from reliably storing data, nodes should provide network bandwidth and appropriate responsiveness. Storage nodes are selected to store data based on various criteria: ping time, latency, throughput, bandwidth caps, sufficient disk space, geographic location, uptime, history of responding accurately to audits, and so forth. In return for their service, nodes are paid.

6.6 Redundancy risk & Solutions

Since the Storage Nodes are operated by individual operators, there are higher chances of any storage node could go offline permanently, due to uncontrollable reasons. Our redundancy strategy must store data in a way that provides access to the data with high probability, even though any given number of individual nodes may be in an offline state. To achieve a specific level of durability (defined as the probability that data remains available in the face of failures), many products in this space use simple replication.
Unfortunately, this ties durability to the network expansion factor, which is the storage overhead for reliably storing data. This significantly increases the total cost relative to the stored data.

The platform divides tiles into multiple fragments and then encrypted using secure, high-performance encryption standard." before uploading, each targeted for distribution to hosts across the world. This distribution assures that no one host represents a single point of failure and reinforces overall network uptime and redundancy.

File segments are created using a technology called Reed-Solomon erasure coding, It empowersStasis to divide tiles in a redundant manner, where any 10 of 30 segments can fully recover a user's tiles. This means that it 20 out of 30 hosts go offline, a Stasis user is still able to download her tiles. Before leaving a renter's computer, each tile segment is encrypted. This ensures that hosts only store encrypted segments of user data.

6.7 Metadata

Once we split an object up with erasure codes and select storage nodes on which to store the new pieces, we now need to keep track of which storage nodes we selected. We allow users to choose storage based on geographic location, performance characteristics, available space, and other features. Additionally, to maintain Amazon S3 compatibility, the user must be able to choose an arbitrary key, often treated as a path, to identity this mapping of data pieces to the node. These features imply the necessity of a metadata storage system.

6.8 Encryption

The client generates a new secured Private key and uses it to encrypt the tile. This “tile key” is, in turn, encrypted by a master key that is only retrievable with the user’s password stored on the satellites, allowing the user to sign in and retrieve their keys from any device. “Regardless of the storage system, our design constraints require total security and privacy. All data or metadata will be encrypted. Data is encrypted before the data leaves the source computer. This means that an Amazon S3-compatible interface or appropriate similar client library should run 14ollocated on the same computer as the user’s application.”

6.9 Audits and Reputation

Incentivizing storage nodes to accurately store data is of paramount importance to the viability of this whole system. It is essential to be able to validate and verity that storage nodes are accurately storing what they have been asked to store

6.10 Data Repair: File Redundancy

Data loss is an ever-present risk in any distributed storage system. While there are many potential causes for tile loss, storage node churn (storage nodes joining and leaving the network) is the largest leading risk by a significant degree compared to other causes.

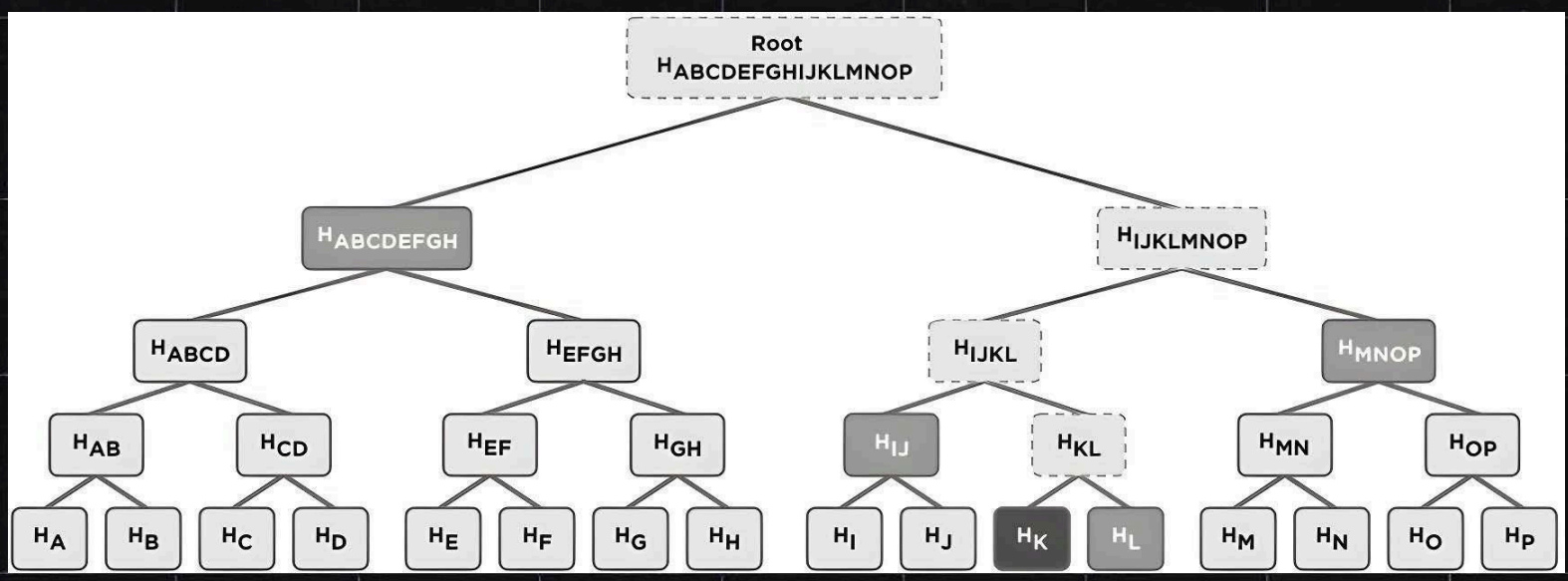
To ensure redundancy, The encrypted tile is split into N chunks and then processed into K additional redundancy shards through Reed Solomon error correcting codes. This procedure allows the retrieval of the payload even it individual cells go offline, as long as you can reach any set of N cells.
Parameters are dynamically chosen and optimized such that the probability of downtime is lower than 10”-6.

Using the Stasis blockchain, renters form file contracts with hosts. These contracts set pricing, uptime commitments, and other aspects of the relationship between the renters and the hosts. File contracts are a type of smart contract. They allow Stasis to create cryptographic service level agreements (SLAs) that are stored on the blockchain.

Since file contracts are automatically enforced by the network, We do not need intermediaries or trusted third parties. Both renters and hosts use Stasis, a unique cryptocurrency built on ERC-20 that powers Stasis Data Storage Marketplace. Renters use Stasis token to buy storage capacity from hosts, while hosts deposit Stasis token into tile contract as collateral.

Micropayments flow between renters and hosts using a technology called payment channels, which is similar to Bitcoin’s lightning Network. Payments between renters and hosts occur off-chain, greatly increasing network efficiency and scalability.

Since hosts pay collateral into every storage contract, they have a strong disincentive to go offline. Renters prepay for storage within tile contracts, setting aside a fixed amount of Stasis token to be spent on storing and transferring data. File contracts typically last 90 days. Stasis automatically renews contracts when they are within a certain window of expiring. It contracts are not renewed, Stasis returns any unused tokens to the renter at the end of the contract period.



7. Stasis Ecosystem

Stasis ecosystems incorporates the following components: The User, The Nodes, The Satellites.

7.1 User

The user access Stasis directly via your chosen device (computer or phone) to upload data on the Decentralized Storage System.

7.2 Nodes

Storage Nodes consist of individuals or companies which desire to lease out spare computing space on Stasis network to earn Stasistokens.

7.3 Satellites

A distributed, P2P network of nodes where data is stored. Satellite: Suite of machine learning algorithms that plans, optimize payload distribution on the star, while also taking care of security and metadata. It's also in charge of triggering the recovery procedure for tiles on the Nodes. These components interact to enable sate and private decentralized cloud storage inside a zero-knowledge architecture, ensuring that no one in the system, not even the satellites, can access the users data.

7.4 Environmental Impact

The internet infrastructure is responsible, as of today, for the enormous amount of energy demands worldwide. Data centers account for one-third of it, making "the Cloud", despite the ephemeral name, an ecological monster that consumes as much as the entire United Kingdom. Our architecture enables small, optimized single-board computers, to replace the storage requirement for users, which is 10 times smaller than data center racks. Moreover, it can leverage geographical proximity to avoid long data transfers, which, in certain cases, can be as consuming as storage itself.

8. Stasis Token

8.1 Allocations

Stasis's token allocation strategy is designed to foster a robust, sustainable and decentralized storage ecosystem. With a total supply of 100,000,000 $META tokens, our distribution model aims to balance network growth, user incentives and long-term development. This carefully crafted allocation ensures liquidity, rewards active participants, supports technological advancement and provides flexibility for future opportunities.

Deployment Method:

Pump.fun

Description: The $Stasis token launch will take place on Pump.fun, ensuring a safe, open launch for all. It's crucial for maintaining a healthy trading ecosystem and supporting widespread adoption for Stasis

Node Operator Rewards:

Percentage: 30%

Description: Dedicated to incentivizing and rewarding node operators who provide storage and computational resources to the Stasis network. This fund is essential for maintaining a robust and decentralized infrastructure.

LVRG Farmer Rewards
Percentage: 15%

Description: Allocated to reward LVRG farmers who contribute to the network's stability and growth through various DeFi mechanisms within the Stasis ecosystem.

Partnership, Market Making, Listing:

Percentage: 5%

Description: This fund is strategically allocated for establishing key partnerships, supporting market-making activities, and securing listings on major exchanges to enhance $META's visibility and liquidity.

Technology Ops:

Percentage: 2.5%

Description: Focused on ongoing technological development, maintenance, and upgrades of the Stasis platform. This ensures the network remains at the cutting edge of decentralized storage technology.

Contingency:

Percentage: 2.5%

Description: Reserved for unforeseen circumstances or opportunities, providing flexibility to address challenges or capitalize on new developments in the rapidly evolving blockchain and storage landscape.

Our tokenomics reflects Stasis's commitment to creating a fair and efficient decentralized storage market. By allocating significant portions to liquidity and node operator rewards, we aim to build a strong foundation for widespread adoption and network resilience. Meanwhile, allocations for partnerships, technology operations and contingencies demonstrate our focus on sustainable growth and adaptability in the rapidly evolving blockchain landscape.

8.2 Tokenomics

On the Stasisstorage platform, the Stasis token would serve as a payment currency, the user hosting data would have to make payments in Stasis and the farmer hosting node would also receive payments in Stasis.

9. Staking

Stasis holders stake Stasis token to secure the Stasis network and in exchange earn rewards. Early adopters naturally gain higher rewards. Rewards comprise inflationary rewards and will include a share of the total network spend (Take Income) users pay.

Users can earn guaranteed returns of up to 11 % on staking. The staking system provides a prohibitive monetary disincentive for bad actors who consider participating in our network. To start with even we have decided to keep $500 as the minimum staking amount, but participation in Network governance is proportional to a provider's stake, taken as a fraction of the sum of all stakes.

Additionally, stake contribution is factored into a provider’s reputation score, which tenants may use as a deployment criterion.

10. Roadmap

Stage 1

Business Concept Development
Project Development Starts

Stage 2

Testnet Stasis Storage Launch
StasisLVRG Beta Launch
Testing Blockchain
StasisToken Launch
Exchange Listing
Marketing Campaign

Stage 3

Onboarding Testing Client Partnerships
Stasis Security Enhancements

Stage 4

Mainnet Stasis Storage Launch
Stasis LVRG V1 Launch
Client Onboarding
Pre-Mine Distribution
Bug Bounty Launch
Product Research & Development

Stage 5

Software 2.0 Upgrade (Storage & LVRG)
sDrive SAAS Development
Ecosystem Enhancement
Fiat Payment Integration
Multisig StasisNodes
Stasis Marketplace Expansion
Stasis Carbon Footprint
Stasis AI Bot trained on Stasis data
Expand Support to More Blockchains

11. References

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] R.C. Merkle, Protocols for public key cryptosystems, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[3] “Analysis of Centralized and Decentralized Cloud Architectures” by the School of Computing, University of South Alabama, 2016.

[4] Juan Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014.

[5] “Towards a Decentralized Cloud: Survey and Future Directions,” Computer Communications, Elsevier, Volume 162, pages 178-196, August 2020.

[6] Z. Wilcox-O'Hearn and B. Warner, "Tahoe-LAFS: A Cloud Storage System for Secure, Decentralized, Fault-tolerant File Storage," 2011.

[7] Swarm, "Swarm: Storage and Communication Infrastructure for a Self-Sovereign Digital Society," Ethereum Foundation, 2016.