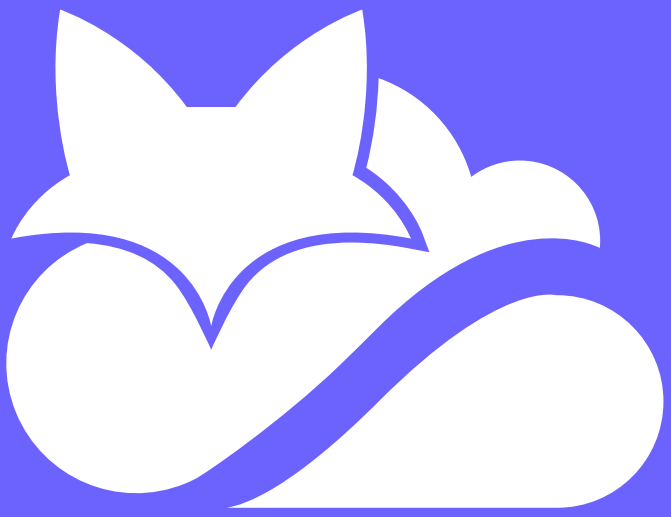
smartfox.com



SmartFox

Whitepaper

Contents

Introduction

Not only the Internet has made global information and data exchange possible, but also put file synchronization and storage in the spotlight.

A typical user has at least a few devices connected to the Internet and utilizes the most convenient one. Therefore, providing the ability to quickly access the updated data from any device is of an utmost importance.

Shared access services grow in popularity, as they allow many people to work on the same data at one time. Shared access is provided by the majority of traditional centralized cloud data storage and file synchronization systems, but all they have security and availability issues.

A centralized system is not able to ensure the appropriate level of security, reliability, and the possibility of a continuous operation. On the other hand, all of these criteria could be met by well-thought and structured decentralized blockchain-based data cloud storage granting confidentiality, decentralization, security, and other components necessary for an uninterrupted and safe operation.

1. Vulnerabilities in Modern Centralized Cloud Data Storage

In recent years, cloud services have become widespread due to the flexibility and availability of computing resources.

Centralized cloud data storage is an online storage that saves data on remote servers accessed through the Internet. A typical model of centralized cloud data storage includes:

- a cloud user who has his files stored in the cloud storage;
- cloud storage with significant storage space and computing resources, managed by a service provider that charges some fee.

Although cloud technologies do have some advantages, such as self-service on demand, and flexible monthly payments that depend on the amount of storage space, the central aspect of these technologies – centralized transferring and storage of files – is unacceptable for users willing to get the maximum possible safety and security.

Despite the fact that cloud infrastructures are much more powerful and reliable compared to computing devices, they still face a wide range of internal and external threats to the integrity of data.

There are several potential problems with centralized data could storage.

1.1 Access Control

Access control is authentication and authorization. Typically, cloud service providers use weak authentication mechanisms (for example, only login and password) and authorization control, which is not secure enough.

1.2 Data Protection Level

A user entrusting data to a third-party should be reasonably worried about the next questions:

- How is the data protected?
- Is it encrypted? If yes, by what algorithm?
- To what extent the encryption algorithm is safe?

Not all encryption algorithms provide sufficient informational security. A common encryption for centralized could storage is a symmetric one, which uses one key for encryption and decryption. This type has the highest encryption speed for large amounts of data, but its security level varies depending on the key length and management. The longer the key, the higher the level of security, which may seem good at first glance, but an increase in the length of the key also increases the computing intensity, which can ultimately go beyond the capabilities of computer processors.

The other issue is using the same encryption key for all users by the provider.

1.3 Data Integrity

Encryption is reliable enough to ensure confidentiality, but data integrity also requires the message authentication code – a special set of characters added to the message. When choosing cloud storage, you need to make sure that the provider uses this method of protection against falsification of transferred information.

Another important aspect is checking the already uploaded data for integrity. To verify the data, the provider needs to download it from the cloud storage, then check, and then re-upload it to the cloud storage. This is accompanied by certain expenses undesirable for users interested in checking data integrity directly on the cloud storage. And it becomes even more complex due to the fact that the testing must be conducted without knowing the entire data set.

1.4 Data Availability

There are two main threats to data availability:

1. Network-based attacks – DoS (Denial of Service) and DDoS (Distributed Denial of Service).
2. Availability of the cloud service provider itself. Big failures have already happened in the past, and since then no cloud storage improved enough to guarantee 100% availability.

A centralized model of cloud storage is unsafe in terms of privacy, data integrity and availability. It has vulnerabilities that can be solved with the help of blockchain technologies.

2. Why Blockchain?

A decentralized blockchain-based data cloud storage model is obviously the best solution to the problems of confidentiality, accessibility, and integrity.

Being a distributed network of personal computers, it is trustless and has no central point of failure.

A blockchain is a distributed database in which you can write down any data or transactions. It stores the information of the entire network, which in turn creates a decentralized, distributed, and independent from any single point space. Every network user supports its functioning, so it is very difficult for one person to hack or completely destroy it.

Another advantage is that transactions carried out in a blockchain cannot be changed or faked. A cryptocurrency-based blockchain allows creating a decentralized Internet while providing freedom and security. It ensures:

Decentralization and required redundancy

Centralized file storage provides data backup by distributing files to regional data centers, which are quite attractive to attack. Decentralized file storage distributes pieces of data among all network users, thereby eliminating a single point of failure.

Absolute confidentiality

No third-party controls users' data of or can access it. Each node stores some encrypted pieces of user's data, while the user is the only one manager of his key.

Low storage cost

Decentralized cloud storage is much cheaper than any centralized one.

3. SmartFox: Taking Decentralized Cloud Storage to the Next Level

SmartFox is a pioneer in the world of blockchain-based decentralized cloud data storage solutions.

It provides reliable storage of text information, media files, and even websites, as well as rewards users in exchange for sharing their disk space!

The main advantage of using Smartfox is that it's trustless, which means data is stored without relying on a third party. Decentralization perfectly solves the problem of easily identifiable central points of attack of traditional cloud storage.

SmartFox provides:

Confidentiality

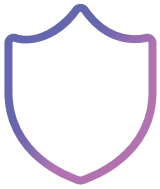
The storage is absolutely private and confidential. All data is encrypted, and no one except for the user who uploads information and has a special cryptographic key can get access to it.

Fast upload of files to the cloud storage

Due to its decentralized nature, the upload speed to SmartFox is limited only by the max. speed on the user's end, which means the user can quickly upload confidential data to the cloud storage if necessary.

Profit for sharing free disk space

The use of SmartFox is not just safe, reliable and convenient, but also economically justified: every GB of your free disk space brings you good profits with absolutely zero risks!



High security and reliability

Since all information is shared among the SmartFox network, there is no single data storage device by accessing which an attacker could restore the whole text or file. With SmartFox, data theft or fraud is technically impossible. Moreover, the failure of one or several nodes does not affect the availability of information and operation of the decentralized cloud storage.

Censorship-resistant

Traffic is distributed over a number of channels, which makes tracing and blocking almost impossible. SmartFox provides the ability to store files of any content, including files that would be blocked by authorities if they were in free public access on a centralized resource.

4. SmartFox Development Stages

Stage One

The development of the masternode network up to 1000 mastenodes, which are a solid basis for the future development of SmartFox. The rapid development of the masternode network is ensured by the high profitability at the initial stage and aggressive promotion in social media, including bounty campaigns.

Stage Two

1000 masternodes provide sufficient redundancy necessary for the network stable operation. In other words, renters are insured against unreliable disk space providers. Stage II goes along with the release of the beta version of wallets with an inbuilt sharing (renting) option, which in fact allows all FOX holders use the cloud data storage technologies. At the same time, masternode owners receive some privileges and bonuses.

Stage Three

Steady development and expansion of the SmartFox platform functionality, including the ability to store media files and use the decentralized cloud hosting for websites with own DNS.

5. Data Security

Based on the analysis of the existing technical solutions in decentralized cloud data storage, the operations necessary to ensure the desired level of data security on the SmartFox decentralized cloud data storage were established:

File encryption

After the file is encrypted, its hash is its unique identifier and the method of detecting any unauthorized access. Any iteration with a file changes its hash, so it's possible to check the file without accessing it directly.

Sharding

Encrypted files are divided into parts (shards), or several files are combined to create one shard.

Distribution of files

X copies of each file are randomly distributed over the network. X is a dynamically calculated number of file copies. Depending on the number of copies, additional copies (shards) can be sent to support the required redundancy level if necessary.

Sharding is the most reliable mechanism to grant data confidentiality, integrity, and availability. The data is encrypted on the client's side before sharding starts. No one but the user controls his private key and access to data. The client can also confirm the authenticity and integrity of the file using its hash. The hash along with the location of X copies of a file is written to the file system immediately after the file is uploaded to the network.

As the number of shards increases, it becomes more difficult to find any given set of parts of files without knowing their location. The data security is proportional to the square of the network size. Copies of shards ensure data availability, which is proportional to the number of nodes in the SmartFox network.

6. Data Sharing

Smartfox allows not only safely storing data but also conveniently working with it.

File encryption

Any SmartFox user will be able to share this or that information with colleagues or relatives so that the group would be able to change documents collectively the same way that Google Drive and similar services work.

SmarftFox Sharing works as follows:

The data that the user wants to share with a group is encrypted with a separate random key, which in turn is encrypted with the keys of all the group members and then placed in the blockchain. This allows any user to access the data by decrypting the public key with his private key.

At the same time, every data change leaves a trace: any file or document changed retains its entire history – from the beginning to the latest version.

SmarftFox Data Sharing provides increased security when dealing with corporate and secret documentation and is more reliable than the widely available centralized options.

7. SmartFox Specifications: Ensuring Redundancy through Optimal Distribution of Rewards

TITLE SmartFox

TICKER FOX

TYPE PoS

ALGORITHM X11

BLOCK TIME 40 sec

COLLATERAL 1000

TOTAL SUPPLY 22,600,000

MASTERNODE BLOCK REWARD 80%

STAKING BLOCK REWARD 20%

TRANSACTION CONFIRMATIONS 6

PREMINE 226,000 (1%)

STAKE MIN AGE 60 min

P2P PORT 40428

RPC PORT 40424

Based on the fact that the availability of data in a decentralized peer-to-peer environment is proportional to the number of nodes, ensuring the maximum rate of increase in the number of masternodes is one of the main goals to achieve at the initial stage (Stage I).

REWARD DISTRIBUTION

Blocks	Block Reward	MN	Stakers	Number of MN*	ROI
2-17280	1	0,8	0,2	10	6307
17281-30240	2	1,6	0,4	50	2523
30241-38880	4	3,2	0,8	100	2523
38881-47520	6	4,8	1,2	150	2523
47521-56160	8	6,4	1,6	200	2523
56161-108000	10	8	2	250	2523
108001-118800	9	7,2	1,8	300	1892
118801-129600	8	6,4	1,6	350	1442
129601-140400	7	5,6	1,4	400	1104
140401-151200	6	4,8	1,2	450	841
151201>	5	4	1	500	631

** the number is conditional*

Maintaining redundancy ensures fault tolerance of the system. For reliable storage of information, it is necessary to have several backup copies of each shard. This guarantees the safety of information even if one or a few disk space providers leave the network, lose data or somehow violate the storing conditions.

Sharding occurs according to the following algorithm:

An encrypted file A is divided into B parts, which in turn create C fragments that are distributed to nodes. Accordingly, the A file can be restored from C encrypted fragments. Due to the ability to determine the level of tolerance to the loss of a certain number of shards, redundancy significantly reduces the likelihood of losing access to the file.

1000 masternodes will be sufficient to achieve the level of redundancy required to protect users against data loss by dividing files into more parts.

8. Staking & Masternodes

Owning a masternode grants not only a part of the block reward but also by 10% more profits from providing free disk space, which is a bonus in exchange for the contribution to the development of SmartFox.

Masternode owners will also get:

1. A privilege to provide the maximum allowable amount of free disk space*
2. Timeless access to all the functionality that will ever appear on the SmartFox cloud storage.

However, running a masternode is not a prerequisite for using SmartFox advantages. The ability to store information on SmartFox will be available to all users having at least 1 FOX coin in their wallets. 1 FOX coin will give the opportunity to share 1 MB of free disk space. The more coins you have, the more you can earn on renting your free disk space.

Proof-of-Stake is an excellent way to access the SmartFox storage at no cost. With staking, the chance of getting the block reward increases with an increase in the number of coins staked. At the same time, even a 1-coin wallet can mint coins if lucky enough.

**The maximum allowable amount of free disk space that the SmartFox wallet owner can share – whether he runs masternodes or stake coins – is 100 GB. This amount is sufficient for high profitability and ensures fault tolerance and decentralization.*

9. The Interaction between Storage Providers and Renters

In a decentralized SmartFox network, the interaction takes place between a storage provider that shares his free disk space and a storage renter that borrows this place for storing files.

The interaction happens via the UI that will be available in the 2.0 wallet. In the 2.0 wallet:

1. Storage providers will be able to regulate the amount of free disk space and the price for 1MB, which will allow them to remain competitive and receive the desired profit.
2. Storage renters will get a wide range of options and the ability to rent the disk space at the lowest price.

10. FOX Existence Justification and Purposes

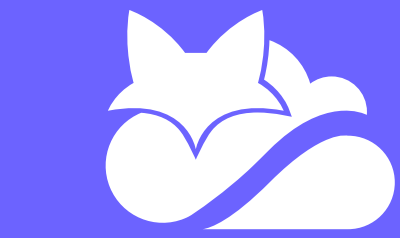
File storage is impossible in a blockchain, as otherwise it would reach an enormous size and could be processed by very powerful computers only.

The well-known blockchain bloat problem is that with the increase in the number of transactions, the number of records also increases, and it becomes very difficult to continue adding new records.

This problem can be solved by storing only a small amount of information about the storage transaction – metadata that contains the hash of the file and the location of the backup file copies.

The concept of SmartFox implies the existence of FOX coins and a blockchain for storage of the metadata of about 1KB in weight that includes the hash of the file and the location of X copies of shards. According to this, storing 100 million files would enlarge the blockchain to 100 GB.

SmartFox is a reliable, safe and effective trustless way of storing information that allows users to interact with each other on mutually beneficial conditions. It's an open-sourced project that seeks to show that cloud storage can be more decentralized, safer, and efficient.



SmartFox