memority

DECENTRALIZED CLOUD STORAGE
OF VALUABLE DATA ON BLOCKCHAIN

CONTENT

1. ABSTRACT

Memority is a blockchain-based platform for encrypted decentralized cloud storage of valuable data. Memority's mission is to create a self-sufficient ecosystem that includes many applications to meet the needs of businesses, government organizations and individuals in the ultra-secure storage of all kinds of valuable data.

The platform includes a collection of independent repositories from around the world, which are based on computers of users who have provided a part of the memory of their hard drives for file storage. To ensure a high degree of data security, 10 copies are created for each of the stored files, integrity and authenticity of which are constantly monitored. If the number of file copies is insufficient or the copies have been forged, new copies of the original file are automatically created for new hosters. The processes for verifying availability, authenticity and recovery of files are independent from the file owner and will work autonomously as long as the files storage in the system is paid for.

Data security is ensured by encrypting the file when it is loaded into the system with a private key, which is stored only by the data owner. Access to the content of the data is possible only with the help of this private key.

Unique hash identifiers of data are stored in a blockchain database, so it is impossible to delete files, to forge them, or to forge information about storing files.

All above mentioned allows unprecedented files protection from deletion and forgery.

The motivation mechanism for hosters (people who provide a physical memory of electronic devices for data storage) is aimed at connecting as many ordinary computer users as possible with the system to maximize the number of independent repositories.

Such a system will function with user data protection even if there are no more developers of platform-based applications, developers of the platform itself, or up to 90% of hosters are lost at the same time. Full self-sufficiency, the built-in self-cleaning mechanism and the decentralized nature of the functioning allow the system to exist and work for many years without outside management.

The work of Memority is based on its own MMR tokens, the transaction history of which is also recorded in blockchain.

The payment functionality is provided by the system of smart contracts, which pro-

ABSTRACT

tects interests of all system participants and constantly cleans the platform from unnecessary files.

The data owner can provide space on his device, thereby gaining the ability to store his data free of charge. This possibility is directed, among other things, to expanding the network of hosters, by including ordinary users in the system of computers.

Memority API allows third-party developers to create desktop and online applications for decentralized encrypted storage of various types of data without a lengthy investigation into the technical details of blockchain technology. Developers are rewarded with 5% of payments for all stored files uploaded through their applications.

The creation of new applications will trigger the popularization of Memority, and an even greater influx of hosters and users, which will positively affect the work of the platform.

Miners receive MMR tokens reward for ensuring the system is operational. Between all the miners who participate in the creation of the block, 5% of the payment for all files, entries of which are contained in the block, is distributed.

The platform uses Proof of Authority, so the computing power is irrelevant to the process of blocks creation and will not increase with time. This is substituted with miner's authority that they prove by having a large stake in the system. Therefore, a limited number of tokens is issued, and mining commissions will be charged when paying for file storage.

Token investments and the token cost are protected from inflation. This is achieved by limiting the number of tokens and rewarding all participants in the system. In its turn, this will popularize the project and increase invectores' profits in the long term perspective.
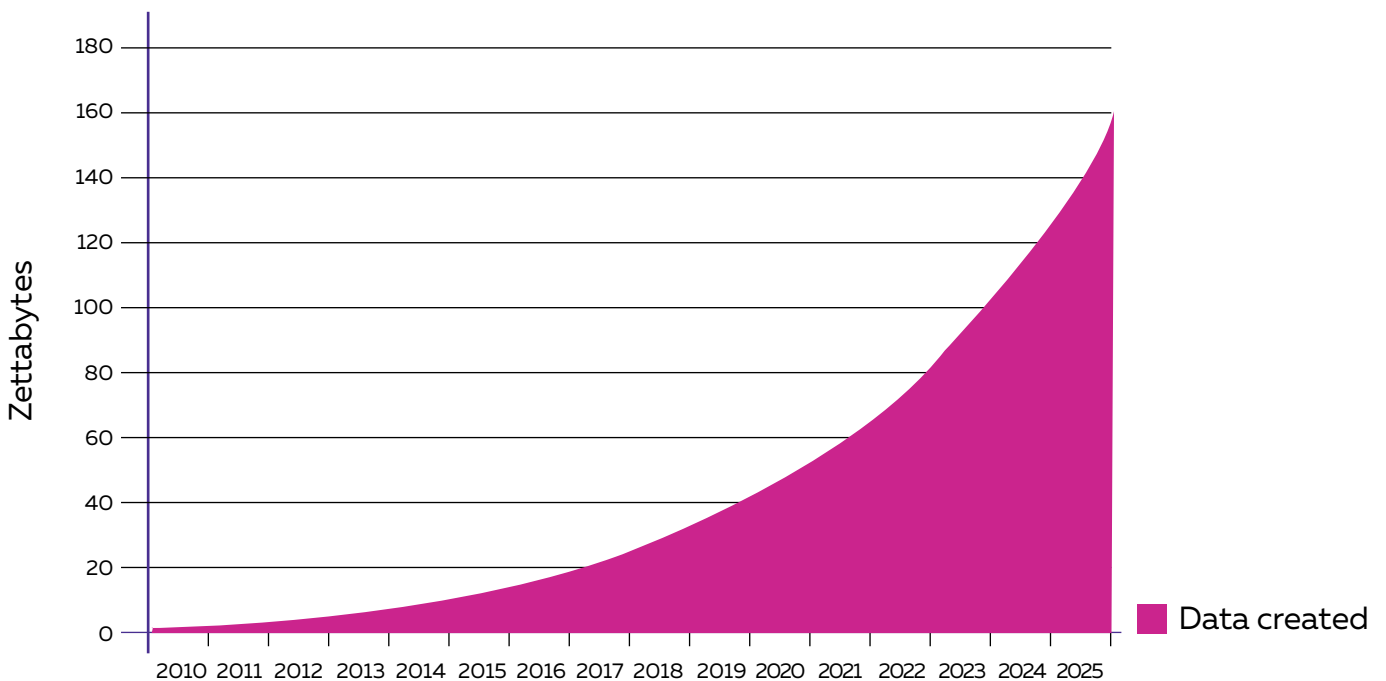
2. BACKGROUND

2. 1. THE REASON FOR CREATING MEMORITY

At the moment, the problem of reliable and convenient way of data storage is very relevant in the world. Besides application in the financial field, blockchain-based encrypted decentralized information storage technology can be used for long-term storage of secure data, with protection from modification, deletion or unpermitted viewing.

First of all, we should assess the state of the data storage market. It exponentially grows (Figure 1) therefore it is very promising both for the growth of existing products, and for the emergence of new ones.

Figure 1. **The annual size of the global datasphere**
Source: https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-Data-Age2025-March-2017.pdf

BACKGROUND.
THE REASON FOR CREATING MEMORITY

The greatest burden falls on the corporate sector. Our platform allows to distribute this load over a wide network of private computers, providing both data confidentiality and flexible, convenient access to the files. The effectiveness and versatility of the Memority platform is ensured by the Law of Metcalf, according to which the network utility is proportional to the square of the number of the network users. Since the number of hosters in our network has a huge growth potential, as well as the number of users (background for this is indicated below), consequently the efficiency of the system has a tendency to grow.

Below, in Table 1, a visual analysis of the Memority functionality is presented, explaining the main components of the system, and the advantages that the data owner gets when using the platform. Memority is compared both with the most popular centralized data storages and with competitive blockchain-based projects.

Table 1. **Explanation of the Memority platform functionality**

Required Characteristic	What will happen if the storage system does not have this characteristic	Memority's solution
Decentralization of storage facilities	If you use centralized servers, which serve as a basis for traditional cloud storages, then your files and files of other users are stored in one specific place, which increases the probability of their loss, deletion, modification or viewing by third parties. Dropbox, Amazon S3, Google Drive – storages are centralized. FortKnoxter - all connections are established through the FortKnoxter server.	The storage system is a collection of independent repositories from around the world, including not only specialized hosting providers, but also computers of ordinary users.

THE REASON FOR CREATING MEMORITY

Creation of multiple file copies	Storing only one copy of the file increases the risk to lose the stored data .	The system stores several data copies (10 by default) on unrelated storages.
	A decentralized storage system consisting of potentially unreliable hosters computers has a high risk of data loss or deletion if the file is stored in a single copy.	
	Dropbox, Google Drive - do not create file copies. Amazon S3 - can create file copies, but does not guarantee this.	
A large number of independent hosters in the network	A small number of active hosters enhances the level of centralization. This increases the risk of access to copies by third parties and reduces the security level of storage.	The mechanism of hosters motivation is aimed at connecting as many computers as possible to maximize the number of independent repositories.
	Dropbox, Amazon S3, Google Drive - have only a few independent storage units. If problems occur on any of them, files or access to them disappears for a lot (sometimes most) of users. FortKnoxter - it is possible to store a limited amount of data for free. Not attractive for hosters. Sia - usually only about 900-950 online hosts, it is not enough for the stable operation of a huge system. Filecoin - does not offer a clear reward program for hosters. No product available.	

BACKGROUND.
THE REASON FOR CREATING MEMORITY

Decentralized monitoring and recovery of the required number of file copies	The lack of recovery function for stored file copies may result in data loss after the shutdown of computers on which the data was stored: less and less copies will remain until the file becomes unavailable. Dropbox, Amazon S3, Google Drive – all processes are centralized. FortKnoxter – checks and restores files only from the file owner's computer. Storj, Sia – check and restore files only from the file owner's computer. Filecoin – checks files only from the file owner's computer. They do not report the recovery system, if they have any.	Memority continuously checks and restores multiple copies of each file using a decentralized monitoring system to provide reliable protection from data loss.
Protecting storages from cluttering with unnecessary data	The system may be a subject to attack with purpose of overloading storage facilities with unnecessary data. Even without a purposeful attack, over time, storage facilities can be cluttered with unnecessary data and the entire system will become unusable. For decentralized systems there will be very few users who want to provide their computer as a storage for free, so there will be a small number of active storages in the system. Dropbox, Google drive – allows storing files for free. After a long period of time this will result in a large amount of unnecessary data and cluttering of a storage. FortKnoxter – all users get space for free storage. Host computers will be quickly cluttered with freely stored information.	Memority continuously checks and restores multiple copies of each file using a decentralized monitoring system to provide reliable protection from data loss.

BACKGROUND.
THE REASON FOR CREATING MEMORITY

Use of crypto-currency as a means of payment for storage	The use of traditional electronic money as means of payment is a dependence on a centralized financial system, the legal and technical features of which may change over time. This creates additional risks for data storage. Dropbox, Amazon S3, Google Drive – there is no cryptocurrency payment methods.	The mechanism of Memority operation is based on payments for storage with its own cryptocurrency tokens MMR, the transaction history of which is kept by the participants of the blockchain system. The functioning of tokens system occurs independently of any centralized financial systems.
The interface for creating applications by third-party developers	Without the ability to create third-party applications for storing specific types of information, the product becomes another app for storing files and gradually loses popularity with the emergence of similar individual highly specialized applications. The lack of new developments and the creation of more sophisticated applications cools interest in the app, the number of those who want to entrust their data falls, as well as the number of hosters, which endangers the safety of already stored data. Dropbox, Google Drive FortKnoxter, Sia, Storj, Filecoin – there is no interface for creating applications by third-party developers.	Memority's mission is to create a self-sufficient ecosystem that includes many applications to meet the needs of business, government organizations and individuals in the ultra-secure storage of all kinds of valuable data. The Memority API allows third-party developers to create desktop and online applications for decentralized encrypted storage of various types of data without a lengthy investigation into the technical details of the blockchain technology. The creation of new products based on the platform is aimed at popularizing Memority, attracting even more users and hosters and expanding the platform community.

BACKGROUND.
THE REASON FOR CREATING MEMORITY

Financial motivation of third-party application developers	Without the motivation of developers, the number of new applications decreases, interest in the platform diminishes, and the risks for stored data get higher. Developers do not receive additional resources to promote their own applications. Dropbox, Amazon S3, Google Drive, FortKnoxter, Sia, Storj, Filecoin - the financial motivation of third-party developers of platform-based applications is not provided.	Developers of all applications receive rewards for storing each byte of data uploaded through their application. This will create a lively competitive environment for creating popular applications and provide developers with additional tools to promote their own products and, as a result, to further popularize the platform.
Encryption of data with a private key, which is stored only by the user	Without encryption of files with a private key, which is stored only by the data owner, a technical opportunity to access the data exists for third parties. Dropbox, Amazon S3, Google Drive - private key encryption is not provided. FortKnoxter - the key is passed through the FortKnoxter server. Sia - hosters even have the ability to view the data before storing it. So there is no protection.	When you are uploading files to the repository, they are encrypted with a private key, which is stored only by the user. Access to the data is possible only with this private key as well..
Free data storage	The lack of free storage reduces the popularity of the product and encourages data owners to use less secure services. Amazon S3 - you can store data only for a fee.	Users can store their own data free of charge in exchange for storing the data of other system members on their computers. This possibility is directed, among other things, at expanding the network of hosters by including ordinary users into the network.

BACKGROUND.
THE REASON FOR CREATING MEMORITY

Complete anonymity	Personal data about the owner of files in the system creates additional risks for data security and for data owner. Dropbox, Amazon S3, Google Drive - try to identify users as well as possible.	Data storage in the system is completely anonymous and requires only the private key from the data owner.
File storing and recovery systems are completely independent from the file owner	If checking of files availability and authenticity is conducted from the file owner's device, a risk of data loss occurs in case of device malfunction. This mechanics significantly increases the risk of data loss due to the fact that the owner of the file is the center of its storage. Dropbox, Google Drive - file recovery is not provided. Amazon S3 - can restore files independently from their owner, but does not guarantee this. FortKnoxter, Sia, Storj, Filecoin - check and restore copies only from the owner's computer.	The processes for verifying the availability, authenticity and recovery of the file are completely independent from file owners. The data owner just uploads a file and, provided that he has the required number of MMR tokens on the account, enjoys the safe storage on the platform.
Complete independence from centralized systems	Dependence from centralized systems at any stage puts potential risk on each stored file: third parties can gain control over such systems or damage their work and this will endanger the operation of the entire storage. Dropbox, Amazon S3, Google Drive storages are centralized. FortKnoxter - all operations go through the FortKnoxter server. Sia, Storj, Filecoin - Scan and restore depend on the file owner's computer.	Data storage, processes of file copies checking and re-covering, encryption and verification of data authenticity are completely decentralized, there is no dependence on any centralized systems. Memority is completely self-sufficient and independent even from its own creators.

BACKGROUND.
THE REASON FOR CREATING MEMORITY

Storage of hash codes for each file in the block-chain-based database for data authentication	Without storing hash codes (unique file identifiers) in the blockchain-based database, the data can be forged. Dropbox, Amazon S3, Google Drive - do not use blockchain. FortKnoxter, Sia, Storj, Filecoin - do not write original file hash codes into block-chain.	Unique data hash identifiers are stored in blockchain database, the system regularly checks forgery and restores the required number of copies of the original data if the files have been forged.

Existing projects for blockchain-based data storage are, in fact, not self-sufficient systems. This is due to the fact that some projects do not implement self-cleaning mechanisms from unnecessary data, and they do not guarantee storing the required number of copies of this data, that would be independent from the centralized system or the data owner.

Often, these products are highly specialized applications with partial centralization created for certain types of data (user files, user identification data, legal information, etc.). In addition, the mechanics of these applications is not always focused on the additional motivation of hosters, users, miners, third-party developers and investors.

As a result, such products do not get wide popularity, despite the availability of many potential features of blockchain technology for safe data storage.

Below is a comparison of the Memority platform with competing offers.

BACKGROUND.
THE REASON FOR CREATING MEMORITY

Table 2. **Competitive analysis of the functionality of storage platforms.**

Feature	Dropbox	Amazon S3	Google drive	FortKnoxter	Storj	Sia.tech	Filecoin	Memority
Storage decentralization	–	–	–	–	+	+	+	+
Creation of several file copies in independent storages	–	+	–	+	+	+	+	+
High payments to hosters for providing space for users' files storage	–	–	–	–	+	–	–	+
Decentralized process of file copies checking and restoration	–	–	–	–	–	–	–	+
Storage protection from cluttering with useless data	–	+	–	–	+	+	+	+
Anonymous cryptocurrency as means for storage payment	–	–	–	+	+	+	+	+
Interface for third-party app developers	–	+	–	–	–	–	–	+
Material rewards for third-party app developers	–	–	–	–	–	–	–	+
Data encryption with a private key that only data owner has	–	–	–	–	+	–	+	+
Free data storage availability	+	–	+	+	+	+	+	+
Complete anonymity	–	–	–	+	+	+	+	+
Storage safety and files restoration independent from file owners	–	+	–	–	–	–	–	+
Complete independence from centralized systems	–	–	–	–	–	–	–	+
Files' hash-codes storage in blockchain for data authenticity verification	–	–	–	–	–	–	–	+

From the table above it is obvious that general advantages of the listed features belong to Memority. Advantages of other systems can not compensate their weak points, and long-term, decentralized, anonymous, reliable data storage with encryption can be provided only by Memority.

2. 2. WHAT IS MEMORITY?

Memority is a blockchain-based platform for encrypted decentralized cloud storage of valuable data. The system automatically keeps 10 file copies on independent storages all over the world at all times. Files are encrypted with a private key obtained only by their owner while account is created. Nobody can see the data without first decrypting it with this key.

The advantages of Memority system in comparison with other solutions are shown in Table 1.

Each participant of the system receives certain opportunities:

1. Data owner - can store data in an encrypted form in a decentralized and completely secure manner, paying for the storage with MMR tokens. Also, he can provide his disk space for data of other users, becoming a hoster, and receive tokens to pay for the stored data.

2. Hoster - can receive MMR tokens for providing their disk space to users of the Memority

MMR tokens are necessary for the functioning of the entire ecosystem. Tokens can be obtained for:

1. providing space for data (hosting files of other participants);

2. becoming an investor in the ICO process and exchanging purchased tokens to MMR (paragraph 5.1);

3. becoming a miner;

4. developing applications for Memority platform.

platform to store their data.

   3. Third-party developers - will be able to implement their ideas and create their own applications, using the infrastructure of Memority, and receiving MMR tokens for this.

   4. Miner - receives rewards in the form of MMR tokens for supporting the working capacity of blockchain executing their authority (only 10,000 or more token owners can become miners).

3. INTRODUCTION TO PRODUCT

3. 1. SYSTEM OPERATION MECHANICS

Hosters provide a part of their computers' memory to host files of other users using Memority application.

The data owner uses Memority app to upload data to the system. He can download his files at any time using the same app. Those can be confidential documents, lists, files with personal information, etc. Due to the use of blockchain technology for storing unique file identifiers (hash codes), the downloaded data can not be forged or modified.

Data security is ensured by encrypting the file when it is loaded into the system with a private 128-bit key, which is stored only by the data owner. Access to the content of the data is possible only with the help of this private key and a password.

The data itself is not stored in blockchain to avoid overloading the system, only hash codes are stored there. Deletion protection is ensured by the permanent storage of several data copies in several independent storages.

Applications that are created by third-party developers use all the functionality of the Memority platform to build services that can offer special conditions for handling data, additional add-ons for working with files online or for corporate use.

And the storage algorithm uses its own private blockchain network based on Ethereum. Memority uses much less computing resources to maintain performance than Ethereum. This prevents computing power and time costs from becoming main resources of mining. We use smart PoA contracts technology (for more details on this technology see paragraph 3.2). This approach has made it possible to significantly relieve the blockchain system and to minimize the cost of all transactions.

The decentralized mechanics of work also offers an opportunity that centralized storage systems do not have. Regardless of what happens to the company or individual hosters, the data will be stored in the system. Theoretically, files can be stored for hundreds of years. Compared to other services (especially centralized ones), our product provides much greater reliability.

INTRODUCTION TO PRODUCT.
SYSTEM OPERATION MECHANICS

When the file is uploaded by the data owner, the following occurs:

1.The desired number of hosters is selected from the prioritized list of potential hosters. Priority is given to hosters who store their own files in the system, have a better Internet bandwidth, allocate more space for storing user files, have better uptime history, etc.

2. File copies are sent to the selected hosters.

3. The files upload date, time and the hosters addresses (where the file copies are stored) are written into the user's smart contract to regularly check the data authenticity in repositories.

4. At the same time, copies of the first file monitoring system are created (their number corresponds to the number of file copies). The first monitoring system is an automatic process for authenticating stored data, controlling the availability and recovery of the required number of file copies.

To ensure reliable operation, the system constantly checks the presence of all file copies, the availability of hosters on the network, the download date, size and hash codes of files. Information about the files is stored in blockchain database, so it can not be faked.

During the check, a unique hash code is extracted from the random part of each file, which is compared between all the hosts. If one of the hosters has a hash code different from the others, the file is considered to be modified or deleted, so the hoster is excluded from this file network with a downgrade, and a new copy of the file is created at the next random hoster's storage.

If the number of file copies is insufficient or the copies have been forged, new copies of the original file are automatically created for new hosters.

INTRODUCTION TO PRODUCT.
SYSTEM OPERATION MECHANICS

5. Copies of the second file monitoring system are created (their number corresponds to the number of file copies). The second monitoring system is an automatic process for checking the availability and restoring the correct number of copies of the first file monitoring system.

6. Six times a day (at random time during 4-hour intervals), the first monitoring system checks the availability and authenticity of all file copies and restores missing copies on the devices of new hosters.

If the hoster is not online, he does not receive fee for the previous 4 hours of storage. If the hoster is not online during 6 consecutive checks (he is offline for 24 hours), he is excluded from the list of hosters for this file and his rating is reduced. A new file copy is created for a new random hoster.

At the hoster's initiative, MMR tokens are credited to the hoster as well as to the app developer (through which the data owner uses Memority services) and the miners from the amount that was reserved from MMR wallets of file owners. A hoster can request the first payment just 4 hours after the first file was downloaded. Each next payment can be requested only after 24 hours or more.

Funds for data storage are charged from the account of file owner for each next period of storage (a week by default). Also, there is an opportunity to make a one-time deposit for an unlimited period of time and to launch the Memority app only if you need to download files. The amount of payments can be determined by the formula from paragraph 3.3.

If the file owner does not have enough money to pay for the next week of file storage, he will receive 3 reminders by email: 7 days, 3 days and 1 day before the end of the paid period. If the data owner does not replenish his account, files smaller than 25 MB will be sent to him by e-mail (in encrypted form) and deleted from the system. Files larger than 25 MB will be irretrievably deleted. The mechanism of self-cleaning from unpaid files will help to avoid cluttering the system and will contribute to its long-term work

INTRODUCTION TO PRODUCT.
SYSTEM OPERATION MECHANICS

Hosters receive 90% of the user's payment for data storing for the period during which they stored files. You can get acquainted with the mechanism of this calculations in paragraph 3.3 "Token rewards for data storage".

5% of the user's payment for file storage is distributed between miners MMR wallets, to ensure system's reliability and security.

INTRODUCTION TO PRODUCT.
SYSTEM OPERATION MECHANICS

Downloading user-owned files is available in the "Files" section of the application.

You can get acquainted with the mechanics of data storage on the diagram below:

Figure 2. **Schematic presentation of Memority storage system**
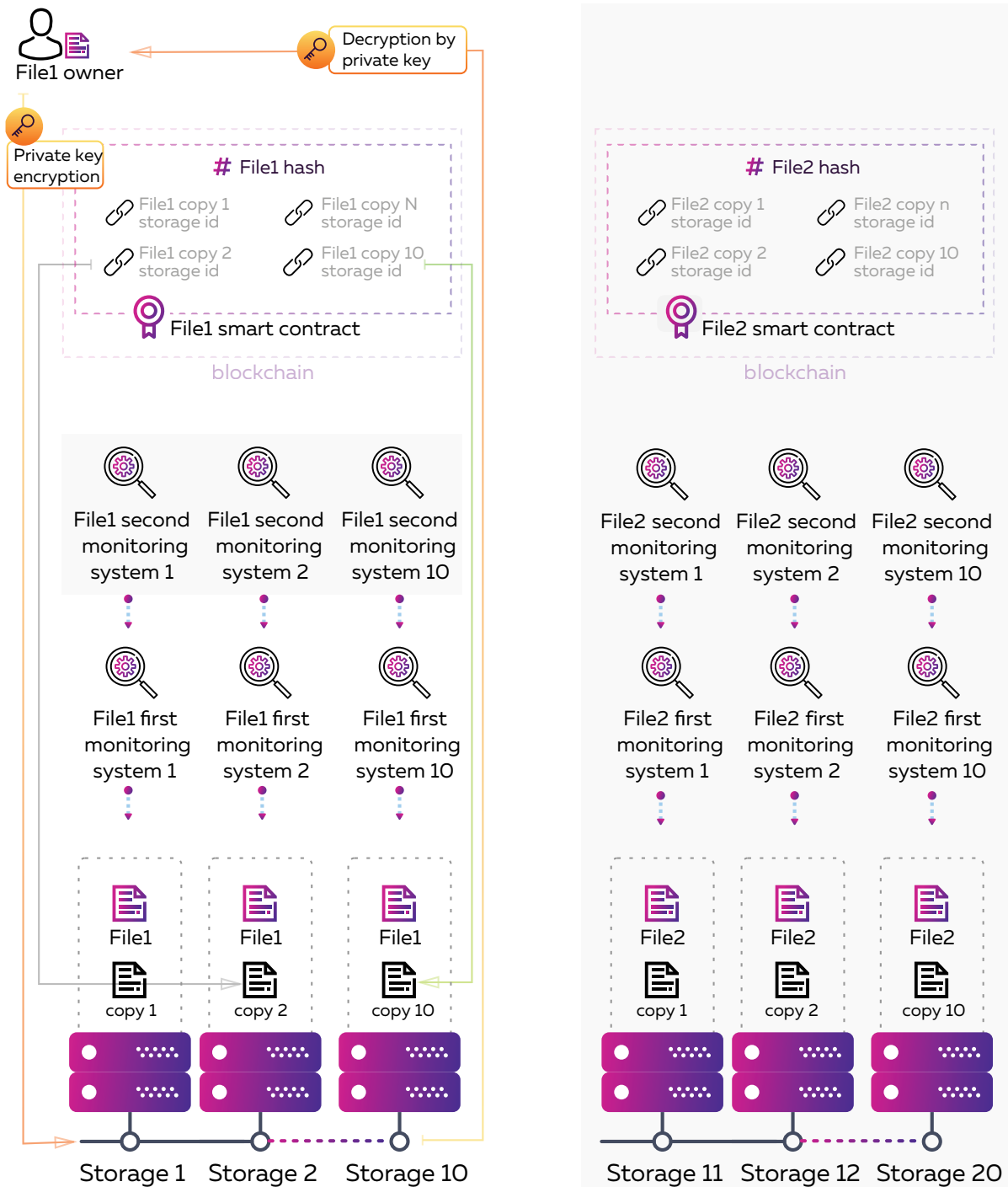
3. 2. ROLES OF PARTICIPANTS

The roles of the participants in the system are distributed as follows:

The owner of the file is a legal entity or an individual who wishes to save his data using the Memority storage.

The file storage algorithm for the data owner:

1. Data owner downloads the application.

2. The data owner uploads the file through the application.

3. The uploaded file is already encrypted with a private 128-bit key (which is stored only by the file owner). Together with the private key, a wallet for internal tokens of Memority platform (MMR) is automatically generated. The wallet is necessary for paying for data storage in the system and for receiving the storage compensations (for storing other users' files).

4. The data owner selects the number of file copies that will be stored in the system to prevent data loss (by default, 10).

If there are 10 file copies in the system, the probability of its preservation is on average 99.99999999996 %. The probability of access to each file at any time will be 99.998%. To ensure even higher security and access probabilities, the number of stored copies can be increased. To ensure data storage for several years or decades, the user only needs to upload his files to the system and have the necessary amount of tokens on his MMR wallet.

INTRODUCTION TO PRODUCT.
ROLES OF PARTICIPANTS

5. The amount of tokens needed to store the required amount of data for 2 weeks (the minimum period of data storage in the system) is reserved from the owner's MMR wallet. The amount is calculated by the formulas given in paragraph 3.3.

6. The data owner can also become a hoster to compensate the cost of storing his files.

Hoster is a legal entity or an individual who provides the memory of his computer for data storing of other users for a fee in MMR tokens. Hoster does not affect the work of the blockchain system and the process of file encryption.

Algorithm for becoming a hoster:

1. A user downloads the Memority application.

2. The user receives a private key and automatically generates a wallet for the internal tokens of Memority platform (MMR). The user will need the wallet to receive rewards for storing other users' files.

3. The user determines size of the disk space that he is ready to allocate on his computer to store data from other users of the platform. If the size of the allocated memory is greater than 0, then the system participant falls into the list of potential hosters. The size of the disk space can be changed in the application settings.

An owner of 10,000 or more tokens is a legal entity or an individual who has a sum of 10,000 MMR or more. If desired, he can become a miner. Mining provides additional income.

INTRODUCTION TO PRODUCT.
ROLES OF PARTICIPANTS

Miner is an owner of 10,000 or more tokens, who has applied for mining participation. Miners maintain the functionality of Memority blockchain system.

The registration procedure for the miner assumes the following procedure:

The platform uses Proof of Authority, so the computing power is irrelevant to the process of blocks creation and will not increase with time. This is substituted with miner's authority that they prove by having a large stake in the system. Therefore, a limited number of tokens is issued, and mining commissions will be charged when paying for file storage.

1. The holder of 10,000 or more tokens fills the form on our website, indicating his data.

2. After verification, the instruction is sent to him, following the actions of which he gets the status of the miner in the system.

3. Participation in the mining is automatic, with the PoA algorithm, without pressures on miners' systems.

3. 3. CHARGING TOKENS FOR DATA STORAGE

The mechanics of payment for data storing with MMR tokens is designed to protect the platform from an overload attack and is built in such a way that only the data necessary to users remains in the system: the platform has a self-cleaning mechanism to prevent cluttering and to keep working in the future. The mo-tivation of token owners, application develop-ers, hosters and miners is aimed at developing the platform and creating new applications.

Below is the formula by which the amount of payment for file storage that data owners provide is calculated.

DOP = STP / NTP * PSR * NB * NH

DOP – the amount of payment for the data owner in USD per hour of storage

STP – the starting price of the token in USD, the value does not change and is 0.1

NTP – market price of the token in USD at the time of calculation

PSR – the starting rate of payment for storage, the value does not change and is equal to 0.00000000000003 MMR for 1 byte of information stored for 1 hour

NB – the number of stored bytes of all file copies

NH – the number of full hours of storage of all file copies

INTRODUCTION TO PRODUCT.
CHARGING TOKENS FOR DATA STORAGE

Hosters (users who provide memory of their computers to store files of other users) receive MMR tokens for data storing. They can request earned tokens at any time not earlier than 4 hours after the start of file storage. Each time a hoster withdraws funds, a commission is paid to miners for writing the transaction into the blockchain. Payment commission is included in the cost of storing files for file owners, so the hoster does not pay it. The number of MMR tokens credited to the hosters is 90% of the storage fee and is calculated for each file according to the formula:

$$HR = STP / NTP * PSR * NB * NH$$

HR – the amount of hoster's reward

STP – starting price of the token in USD, the value does not change and is equal to 0.1

NTP is the average market price of the token, in USD at the time of calculation

PSR – the starting rate of payment for storage, the value does not change and is equal to 90% of the amount spent by the data owner for storing 1 byte of information in the system for 1 hour, namely 0.000000000000027 MMR.

NB – the number of stored bytes of all file copies

NH – the number of full hours of storage of all file copies

INTRODUCTION TO PRODUCT.
CHARGING TOKENS FOR DATA STORAGE

The developer of the application used for file uploading also receives a portion of the storage fee. It amounts to 5% of the storage fee and is calculated for each file by the formula:

DR = STP / NTP * DRR * NB * NH

DR is the amount of developer's reward

STP – starting price of the token in USD, the value does not change and is equal to 0.1

NTP – market price of the token in USD at the time of calculation

DRR – the developer's starting rate of reward, the value does not change and is equal to 5 % of the amount spent by the data owner for storing 1 byte of information in the system for 1 hour, namely 0.0000000000000015 MMR.

NB – the number of stored bytes of all file copies

NH – the number of full hours of storage of all file copies

INTRODUCTION TO PRODUCT.
CHARGING TOKENS FOR DATA STORAGE

If the holder of 10,000 or more tokens is also a miner, he is additionally rewarded with a portion of 5% of the fee for storing files, for which he participated in writing transactions in block-chain.

The number of tokens credited to a specific MMR wallet is calculated for each file that is stored on the Memority platform, using the formula:

All formulas take into account the further increase of MMR tokens cost and stipulate that for file owners the actual cost of storage does not grow.

MR = STP / NTP * HRR * NB * NH / ST

MR – the amount of miner's reward

STP – the starting token price in USD, the value does not change and is 0.1

NTP – market price of the token in USD at the time of calculation

HRR is the starting rate of payment for storage, the value does not change and is equal to 5% of the amount spent by the data owner for storing 1 byte of information in the system for 1 hour, namely 0.0000000000000015 MMR

NB – the number of stored bytes of all file copies

NH – the number of full hours of storage of all file copies

ST – the number of miners who participated in the creation of the block.

3. 4. PLATFORM SPECIFICATIONS

The Memority system operates on the basis of EVM (Ethereum Virtual Machine) using a new algorithm of PoA (proof of authority) consensus. This approach allowed us to multiply the network speed and reduce the computational cost of maintaining its performance. The choice of EVM is the result of the following factors:

1. a vast community of developers who are constantly developing this blockchain technology;

Memority works on the basis of branched nodes. The platform runs on its own blockchain based on Ethereum and uses its Proof of Authority technology. Due to the use of its own blockchain, Memority charges much lower fees for entering data into the blockchain while checking the files for availability and authenticity.

2. the possibility of using our own private blockchain network, which allows us to be independent from the market rate of Ethereum (which would significantly affect the cost of recording transactions in the blockchain system);

3. the availability of ready-made EVM tools for solving Memority tasks.

Encryption of files is provided by the algorithm: cryptography, Fernet (AES-128) - https://cryptography.io/en/latest/fernet/ and https://github.com/fernet/spec/blob/master/Spec.md

Keys generation is provided by a mechanism ecdsa.

The local database is built on the technology SQLite + sqlalchemy.

The graphical user interface (GUI) is built on the basis of PyQt5.

Interaction with Ethereum is conducted through web3.py.

Interaction between users is implemented via aiohttp.

4. USE CASES:
AN ECOSYSTEM OF DECENTRALIZED ENCRYPTED DATA STORAGE

Memority's mission is to create a self-sufficient ecosystem that includes many applications to meet the needs of businesses, government organizations and individuals in the ultra-secure storage of all kinds of valuable data.

Memority API allows third-party developers to create desktop and online applications for decentralized encrypted storage of various types of data without a lengthy investigation into the technical details of blockchain technology. Developers of such applications are awarded for storing each byte of data downloaded through their application.

The scope of applications is as wide as the number of types of valuable data that require safe long-term storage: confidential documents, digital evidence of authorship, user identification data, authorization data (logins and passwords), technical documentation, personal photos, videos, even Internet resources can use Memority for secure data storage .

The platform uses Proof of Authority, so the computing power is irrelevant to the process of blocks creation and will not increase with time. This is substituted with miner's authority that they prove by having a large stake in the system. Therefore, a limited number of tokens is issued, and mining fees will be charged when paying for file storage.
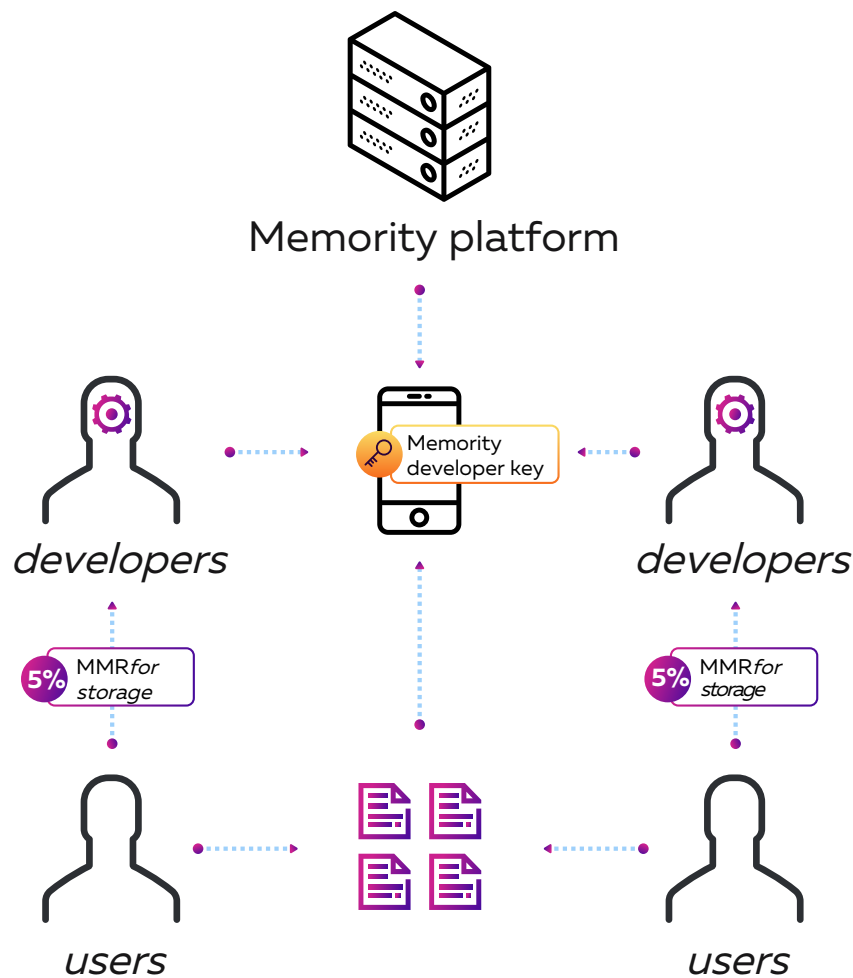
USE CASES: AN ECOSYSTEM OF DECENTRALIZED ENCRYPTED DATA STORAGE

The interface of individual applications can be focused on the convenience of entering and storing a particular type of data. An online or desktop application can directly upload files to the system or, for example, collect the results of a user–filled form in a separate file, encrypt it with a private user or company key, and send it to the Memority file system for storage.

The mechanism of the platform allows you to create and reliably protect the actual evidence that you are the author of a certain work of art, invention, technology or any other product, because you can not fake the upload date of files as they are stored in the blockchain database.

The entire mechanism of the system is shown clearly in Figure 3.

Figure 3. **Visual demonstration of self–sufficiency of the Memority system**

Memority platform

developers

Memority developer key

developers

5% MMR *for storage*

5% MMR *for storage*

users

users

USE CASES: AN ECOSYSTEM OF DECENTRALIZED ENCRYPTED DATA STORAGE

Below we give some examples of applications, the release of which is planned in the coming months based on Memority platform:

Memority is the main application for data storage in the system. The MMR-wallet is created at installation. Using the application, you can encrypt files, upload files into the storage and download them from it. At the moment a working alpha version is available.

file-chain.com is a file-sharing service for blockchain users with the ability to provide access for viewing and downloading files to anyone who wants to. Release date: IV quarter of 2018 - I quarter of 2019.

turtle.io - application for downloading and viewing data on patents and scientific inventions on the blockchain system with fixation of the download time (for confirmation of intellectual property rights). Release date: I quarter of 2019.

chain.gallery - an application for downloading and viewing works of art on the blockchain with fixation of the upload time (for copyright confirmation). Release date: IV quarter of 2018 - II quarter of 2019.

5. ICO (INITIAL COIN OFFERING)

Start date of public Pre-ICO: May 16, 2018

End date of the public Pre-ICO: May 30, 2018

ICO start date: May 31, 2018

ICO end date: October 1, 2018

Starting price of the EMT token: 0.1 USD

During Pre-ICO and ICO, you will only be able to buy the utility Ethereum-based Tokens EMT (Ethereum Memory Token). They do not assume any profits and exist only for the convenience of investors at the ICO.

At any time, through an application or site, they can be exchanged to internal MMR tokens at a rate of 1:1 without any commissions. There will be no return exchange. MMR tokens are used inside the platform for all operations and are necessary for the functioning of the ecosystem.

The strong point of the project is that we go to the ICO with a completely working alpha version of the product. It has the main part of the functionality (you can store your files, become a hoster, and the data is encrypted and automatically restored), but does not support the development of external applications, and many additional functions have not yet been tested or developed.

All EMTs that are exchanged to MMR will be automatically destroyed.

The current number of EMT tokens is 1,500,000,000. 57% of all tokens are available

ICO (INITIAL COIN OFFERING)

for purchase during Pre-ICO and ICO, namely 855,000,000 tokens. Unsold tokens will be destroyed.

Types of payment are accepted: Ethereum, VISA, MasterCard, Bitcoin, Bitcoin cash, Litecoin.

The current number of MMR tokens is 1,500,000,000. Their number will correspond to the amount of EMT at the end of the ICO, so the same number of MMRs as the unsold EMTs will be destroyed. We will not sell MMR tokens, they can only be exchanged for purchased EMT at a rate of 1: 1.

Depending on the date of investment, the program provides for a number of bonuses:

The Pre-ICO program allows the first investors to receive a reward of an additional 20% of the purchased EMT. This reward will be given only to those investors who purchase tokens from the pre-ICO dedicated pool: 60,000,000 MMR. All files, unsold during the Pre-ICO, will be added to the ICO reserve.

The ICO program also allows to receive MMR bonus tokens. Investors who purchase tokens from May 31 to June 30 will receive a 15% bonus, from July 1 to July 31 – a 10% bonus, and from August 1 to August 31 - a 5% bonus. No bonus are presupposed for purchases made after August 31.

Citizens of the United States, China (except Hong Kong, Macau and Taiwan), South Korea, Cuba, Iran, North Korea, Syria and the Crimean region are prohibited from participating in the ICO. To avoid the participation of citizens of these countries, users will be authenticated.

ICO (INITIAL COIN OFFERING)

All MMR tokens will be allocated as follows:

● In exchange for EMT tokens sold on an open presale is 4% of tokens (60,000,000 MMR)

● In exchange for EMT tokens sold during ICO – 53% of tokens (795,000,000 MMR)

● Remuneration to the team with a ban on sale during the year – 15% of tokens (225,000,000 MMR)

● Rewards to early investors with a ban on sale for 6 months – 15% of tokens (225,000,000 MMR)

● The reserve fund of tokens – 10% of tokens (150,000,000 MMR)

● Bounty campaign – 2% of tokens (30,000,000 MMR)

● Additional remuneration to early miners – 1% of tokens (15,000,000 MMR)

The campaign is considered successful after collection of 5,000,000 USD

ICO (INITIAL COIN OFFERING)

If the goal is not achieved, the funds will be returned to investors.

After the ICO completion, the collected funds will be used as follows:

1. If collected between 5,000,000 USD and 15,000,000 USD, the bulk of the budget will go to the development and improvement of the Memority platform (67%). We will also conduct a basic marketing campaign (16% of funds) to attract the audience to the product. The remaining funds will go to operational and administrative costs (7%), rewards to the team and advisors (5%) and legal costs (5%).

2. If collected between 15,000,001 USD and 40,000,000 USD, a large marketing campaign (55% of funds) will be conducted to provide a large number of platform users (both hosters and file owners), which in turn will lead to high demand for MMR tokens and, respectively, a significant increase in their value. 35% of funds will go to the development and improvement of the Memority platform, and the rest to administrative and operational costs (3%), legal costs (2%) and rewards to the team and advisers (5%).

3. If collected between 40,000,001 USD and 85,500,000 USD, the development and improvement of the platform will cost 15% of the budget, which means that the main forces and resources will be allocated for a large-scale marketing campaign (77%), which will provide a huge influx of users and application developers to the system. In this case, investors and miners will be able to get the most profit, as the system will perform many operations with MMR tokens, the share from which they will receive, as well as due to the rapid growth of the cost of the MMR token. 5% of the budget will be allocated for rewards to the team and advisers, 2% – for administrative and operational costs and 1% – for legal costs.

After the successful ICO conduct, new tokens will not be issued, and they will be available for purchase only from ICO-investors on exchanges.

6. INVESTING IN THE MMR TOKEN

6. 1. TOKEN HOLDERS POTEN-
TIAL REWARDS

Memority has a system of participants moti-
vation (regardless of their roles). Below we ex-
plain how exactly the system attracts users, in-
vestors, miners and hosters.

Motivation of data owners

Data owners receive an absolutely secure and
decentralized repository. They can be sure that
no one else will have access to their files and
that they will not be lost anywhere during the
entire paid storage period.

Hosters Motivation

With the development of cloud technologies
and the spread of the high-speed Internet, us-
ers use less and less disk space on their PCs to
store their own data. Inclusion of this unused
disk space into the Memority storage will result
in rewards for its owners and will help expand
the platform.

Hosters will receive 90% of the funds spent
by data owners for their storage.

INVESTING IN THE MMR TOKEN.
TOKEN HOLDERS POTENTIAL REWARDS

Motivation for application developers

The platform allows third-party developers to create desktop and online applications for decentralized encrypted storage of various types of data without a lengthy investigation into the technical details of blockchain technology. Developers of such applications receive 5% of the total amount of MMR for each kilobyte of data uploaded and paid for through their application.

Motivation of miners

Miners receive an additional MMR tokens reward for ensuring the system is operational. Between all the miners who participate in the creation of the block, 5% of the payment for all files, entries of which are contained in the block, is distributed.

Thanks to the system of rewards for all participants, Memority will be a popular project in the long term perspective, which means that profits of investors can constantly increase.

6. 2. INVESTMENT PROTECTION

To attract attention and resources from investors, they can become miners and get rewarded with the share of tokens for storage of all information in the system. This allows us to create a mechanism of beneficial rewards.

Development of the system is also conditioned by the development of applications that use system resources. This will greatly aid the platform with attention from both developers and users. As a result we get a self-sufficient system.

The profitability of investments in MMR tokens can be provided by two main factors:

1. Miners get a constant share of tokens from all storage payments in the system.

2. The growth of token value, which is a result of interest in the product by users, developers and miners.

Token investments and the token cost are protected from inflation. This is achieved by limiting the number of tokens and rewarding all participants in the system. All participants have a direct incentive to store tokens and promote the platform.

6. 3. JUSTIFICATION OF SYSTEM POTENTIAL

Taking into account the interests of all users of the system, advantages in comparison with all competitive offers, flexible tools for creating your own applications and the ultra-reliable storage of data make it possible to consider Memority to become the best blockchain project in the market segment for decentralized data storage. The tables of the functionality rationale and comparison with competitors clearly demonstrate this.

And thanks to the well-developed motivational system of all platform participants, Memority becomes very promising and will be popular in the long term perspective.

6. 4. AN EXCLUSIVE OPPORTUNITY OF MINING FOR LARGE OWNERS OF TOKENS

Each owner of 10,000 or more tokens receives an exclusive opportunity for mining. Earlier we pointed out that the key elements of mining are not the time and computing power, but the "level of trust" to the miner. This level is determined by the mechanism of Proof of Authority.

Only a holder of 10,000 or more tokens can become a miner. The algorithm required to acquire this status is specified in paragraph 3.2.

The status of the miner allows you to get a portion of5% of the total number of tokens payed for data storage.

After the end of the ICO, first 15 million tokens will be distributed to the miners as a bonus for early mining. This bonus will be added on top of payment by data owners for storage. For example, in the case of the first miners, the data owner will pay for the storage of his files on the platform, of which 90% will go to hosters, 5% to application developers, 5% to the miners, and additional 5% from the dedicated Early mining pool to the miners as well. Thus, the first miners will receive 2 times higher payments.

Only a holder of 10,000 or more tokens can become a miner. The algorithm required to acquire this status is specified in paragraph 3.2.

The status of the miner allows you to get a portion of 0.5% of the total number of tokens payed for data storage.

INVESTING IN THE MMR TOKEN.
AN EXCLUSIVE OPPORTUNITY OF MINING FOR LARGE OWNERS OF TOKENS

The bonus reserve will be divided into 10 consecutive portions of 1.5 million tokens each as follows:

1.5 million tokens – to the first miners as additional 5% (rewards 2 times higher)

1.5 million tokens – early miners as additional 4.5% (1.9 times higher rewards)

1.5 million tokens – early miners as additional 4% (rewards 1.8 times higher)

1.5 million tokens – early miners as additional 3.5% (rewards 1.7 times higher)

1.5 million tokens – early miners as additional 3% (rewards 1.6 times higher)

1.5 million tokens – early miners as additional 2.5% (rewards 1.5 times higher)

1.5 million tokens – early miners as additional 2% (rewards 1.4 times higher)

1.5 million tokens – to early miners as additional 1.5% (rewards 1.3 times higher)

1.5 million tokens – early miners as additional 1% (rewards 1.2 times higher)

1.5 million tokens – early miners as additional 0.5% (rewards 1.1 times higher)

7. FINANCIAL PLAN

Our aim is to create a truly decentralized platform that will be operated and managed only by its users. Therefore we can not be a constant beneficial party, it would either create unnecessary centralization or even make us a distinct owner with administrating privileges.

During the early stages our company will earn 5% from all payments for data storage, as our apps will be first ones available to users. But as these 5% are credited to any developers whose apps are used for uploading files, with time most of these will be third-party developers, not us. And this is exactly how we want it to be, as this way our platform will be governed by its users and so truly decentralized.

Our team will also benefit from owning tokens, mining and being able to use our own platform.

8. MEMORITY CREATORS

The project is developed by a team from Estonia, Ukraine and the United Arab Emirates and consists of 15 people. Each of the participants has his own tasks and responsibilities, namely:

Ilya Ratovsky (CEO)

Stanislav Rubtsov (CTO)

Andrey Vityk (Blockchain Developer)

Alexander Petrenko (Python developer)

Vladimir Marchinsky (Head of Legal Department)

Vitaliy Miniyailo (Marketing manager)

Alexander Pivtorak (PR manager)

Dmitry Semiryazhko (Co-Founder and CIO at Pinxter Digital)

Oleg Reshtak (UX / UI Designer)

Alexandra Andryushina (Java Developer)

Alexander Kalmykov (QA Engineer)

Eugene Kharkkovenko (Objective C Developer)

Mikhail Dvornichenko (Business analyst)

Denis Saprykin (Financial Advisor)

Alexander Shulga (Business Development Advisor)

9. THE LEGAL BASIS OF THE SYSTEM OPERATION

The company involved in the development of the project is registered and regulated by the legislation of Estonia:

Registry code: 14453811

Name: Memority OÜ

Legal form: Private limited company

Address: Harju maakond, Tallinn, Kesklinna linnaosa,

Parda tn 4-411-1, 10151