BANK
of memories

ECOSYSTEM

Mobile app

A mobile application features a secure local terminal for accessing infrastructure, and a centralized element responsible for coordinating decentralized service nodes.

Scaling occurs due to the exchange of information between mobile terminals and a centralized server, and then, all information is stored in decentralized nodes. These are configurable servers along with system servers. Custom servers are the servers that ensure the expansion of services for their storage, transaction processing, and security infrastructure.

We've taken Stellar as the basis for the architectural solution of the Global Bank of Memories (GBM) blockchain, which has brought a number of important advantages to the GBM blockchain.

- Transaction speed less than 10 seconds
- Large community
- Multi-signature, which is a scheme for the implementation of a digital signature, involving the participation of various parties in the transaction. All parties provide their keys to confirm the validity and sign the transaction to complete it.
- Grouping/atomicity thanks to this function, a transaction can include several operations at once. Atomicity ensures that if a group of operations is submitted to be included in the network, but one operation is rejected, then all transactions of the group will be rejected.
- Sequence in the GBM network, the concept of a sequence is represented as a sequence number. Using the sequence number can ensure that certain transactions will not enter the network, if alternative transactions have been previously submitted for consideration.
- Time frames are the frames within which a transaction is considered valid. Thanks to this feature, GBM can operate at specific time intervals.

All this formed the basis of the following functions:

- a digital will
- messages to the future
- a family tree.

GBM intro

Notary system

It performs the function of authorizing access; the blockchain implements a mechanism for confirming access and connections between participants of this system. When users establish a connection with each other, for instance, a family tree (a kinship), this connection is maintained on the blockchain, and it determines the ability of participants to interact at a more trusting level. Accordingly, access keys can be distributed among the participants through the blockchain.

Initially, upon registration in the system, a unique wallet, and an account corresponding to this wallet, is generated for each user with internal methods of blockchain, such as storing data in the blockchain accounts. A user works inside the system. In addition to the payment function, he/she can count on the wallet to store all the necessary information about the connections built by a user, and these connections are anonymous to other members. This is achieved by storing the connections in a blockchain address format. When a digital asset transfer request is made, a data transfer transaction check is performed.

In addition to the decentralized digital asset transfer system, it also performs the role of an arbiter in the pre-established functions of accessing data in the blockchain, being available for control only by the user and no one else.

Access to the account is provided only to the user; this data is not stored on the server. Responsibility for the loss of this data rests with the user. In this case, the service uses a convenient and safe tool to save data on external media. In case of data loss, the user will use his/her own family connections to recover the data chain. Family connections will come to the rescue as a support project helps to restore the memory.

The procedure for restoring access to this data is to perform. To do this, the user must confirm his/her connections through the system for accessing service records in the system inside the application. After these confirmations, the number of confirmations depends on the settings of the digital will system, on the level of settings, but the main idea is to restore connections with relatives through external systems of connections, and to confirm one's role in the family tree or the tree of connections. After that, the user will receive a new temporary password that he/she can use when entering the external shim of the account and set his/her permanent password.

After that, an IPFS file system is used, i.e. a decentralized distributed Internet file system that provides a web interface to files, which can be stored on any node. An ability to securely store this data on nodes that do not require identification. The data is encrypted, access to them is provided

with anonymous keys, giving an additional opportunity to scale the service with the help of external users called keeper.

Bank of Memories security is built on 2 principles

The first principle is to provide users with maximum control over their keys and data, when resource access keys are stored on mobile devices, and not on the server, so that they do not depend on the security of the server and on other participants.

The second principle is to ensure the exchange of data between participants over encrypted channels. For these purposes, tools such as asymmetric encryption and block encryption are used. All loaded keys and files are created on user devices.

Accordingly, access and management of private keys is carried out directly on the mobile device, and the server does not have access to this data. The asymmetric public element is used to encrypt the data to a recipient during the exchange of data between participants. With this scheme, the server also does not have access to the transmitted data.

As for the centralized element of the service, it includes the coordination of requests between the participants, and in this case, the service functions as a switch and acts as a tunnel between the participants who transfer messages to each other. In this case, the server does not have access to the transmitted content of this data. The data is encrypted with a key accessible only by the recipient.

The operability of the service does not affect access to this data, and in case of emergency access to the service, or problems associated with service interruption, or related to restricting access to the service, for example, caused in some countries, they are bypassed by direct access to distributed nodes that are controlled by the keeper.

Keeper act as active backup. Keeper act as a CDMA network for distributed access to the content. The payment keeper receive is completely fair and corresponds to the function they perform. Along with the keeper, the company also keeps copies of the data on decentralized servers, so as not to depend on the keeper, though this data is not centralized as the service itself, which is available on the domain WEB 3.0.

Using AR and storing data in a distributed file storage system The application also allows accessing the memorial data saved as a certain tag about some object. The data is stored on a distributed file system; the image is the key to the data, and such an image may or may not contain a QR-code.

Requirement for monuments and places of QR-code non-use.

This data is accessed through augmented reality tools. With the help of these tools, the user can access and interact with information, and learn about any information. All data is stored on IPFS, and this is a point of scaling and security.

The main zest is a combination of technologies to solve each task, in combining the implementation of a common idea, each task is solved with its own tool; this approach is practiced for systems such as Unix – when one tool performs one task, but does it well, respectively, the combination of these tools for solving a common idea gives an opportunity for participants to communicate securely to save and transfer the data to the future, as a key function of this service, which is implemented in this way.

The key feature that required the development of rather non-trivial algorithms is a work with non-existing users, ensuring the security of data transmitted between them. Since the users of the Bank of Memories system can be in several different life states. Alive. Just born and those who left this world. Accordingly, taking into account these conditions, it is necessary to transfer data, to ensure security between accounts, and the most important thing is to ensure the authenticity of requests. We must be sure that a recipient is the right person. An example of transferring inheritance (information as capital) to unborn children, grandchildren, great-grandchildren or children, who do not have an account – it is necessary to ensure the transfer of wills and data archives to them.

These are the tasks that required the implementation of atypical approaches for web development, uncharacteristic for current data storage systems available on the market. This is a key feature. Such functions are in demand, and such tasks exist. But there are not so many tools that provide convenient solutions, and there are probably no tools that provide a comprehensive solution. It is partly know-how. It is an ideological and technological innovation.