GENESIS BLOCK

Individual solutions development for secure communication based on blockchain technology



Genesis Block Protected Products for Businesses

The best, modern information security solution for Finance industry, Information security, state institutions, governments, research and science, healthcare, legal and security organizations.

1

The world's first corporate communications tool that uses blockchain to provide a unique level of security and privacy in corporate networks. It is based on the technology of the Decentralized Public Key Infrastructure (DPKI) and uses its capabilities to authenticate users and encrypt transmitted data.

2

It's a further development of GenesisMessenger - public communication solution based on a decentralized network and the CSMP secure data exchange protocol.

3

Provides a unique level of data protection and privacy for companies and organizations for which the security of business data is of paramount importance. Using a decentralized infrastructure, it is also an ideal choice for creating a reliable data exchange system within an enterprise.

Problems

Security flaws of traditional solutions

Although there are a number of enterprise-level communication tools on the market, they are all subject to major security flaws, such as:





Outdated Cryptographic Models

Most of the tools use the old key exchange algorithm Diffie-Hellman RSA and legacy ciphers like AES256 This creates weak protection and vulnerability from man-in-the-middle attacks.



Local data is stored in an unencrypted format

In most cases, in traditional solutions, data is stored locally in an unencrypted, open format. This creates a threat of data leakage in case of hacking, loss or theft of physical devices.



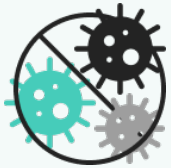
Public keys are managed by a trusted Centralized Certificate Authority (PKI)

Centralized Public Key Distribution Services (CA) serve as a single authentication (confirmation) of the identity of the encryption key center (PKI), which creates the likelihood of a serious threat of intentional key manipulation or as a result of hacker attacks.



Sole administration and access control

In many cases, this means that the administrator has access to confidential data or can easily get this access. This is a big problem for large geographically distributed organizations, which makes it almost impossible to securely exchange data between remote enterprise objects.

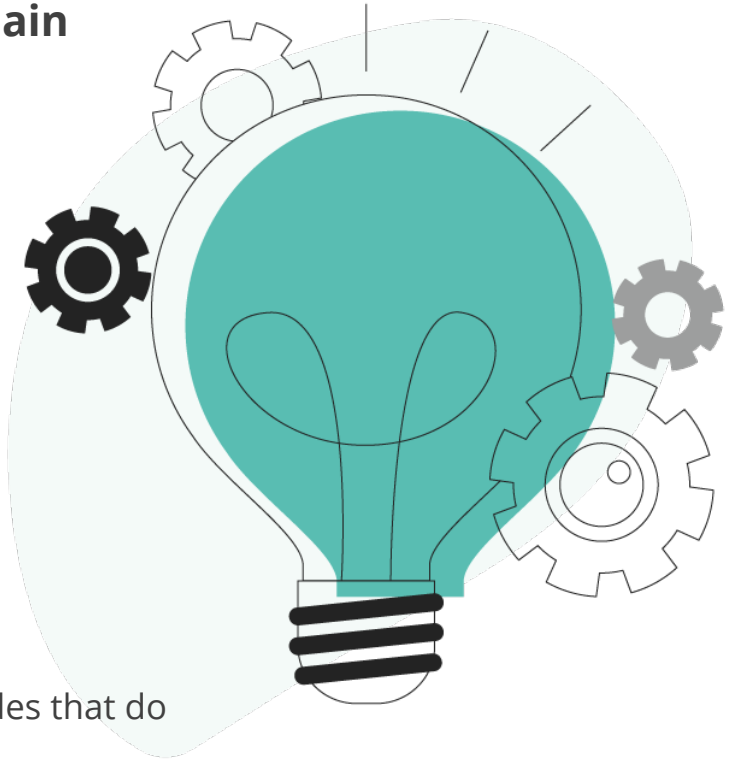


BYOD (Bring your Device) Policy Threats

In recent years, many employees of the company have appreciated the many benefits of implementing the BYOD policy. However, in addition to the benefits, the associated security and privacy threats are the main BYOD risks for data leakage, infection with malicious and fraudulent viruses.

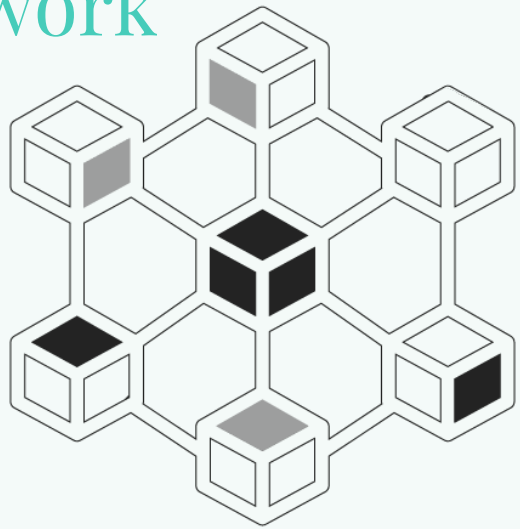
Solution

Decentralized infrastructure based on the Blockchain



To solve the above problems, the Genesis Block solution implements a completely different approach to security in its DNA. The cryptographic model is based on an asymmetric encryption algorithm with decentralized storage and automated exchange of public keys. The private keys associated with their account are stored on the user's local devices, and the management and distribution of public keys is carried out through the DPKI Blockchain (Decentralized Public Key Distribution Center). This allows you to ensure the confidentiality and security of data on a new level, since the storage and management of encryption keys is carried out by consensus of independent nodes that do not require to trust each other.

Blockchain Network



Key exchange via blockchain

Key exchange via blockchain

Secure Automated exchange "end-to-end encryption”

Secure Storage

Secure Storage

Smart administration

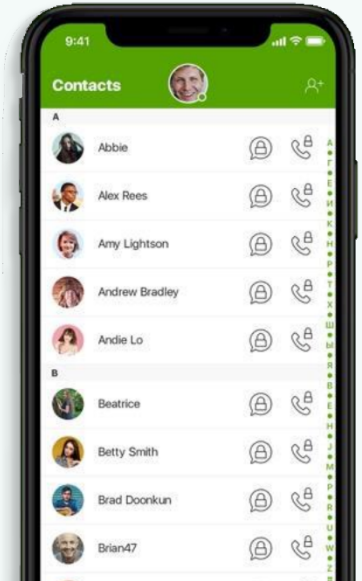
Despite the absence of a sole administrator, responsible persons may be given a certain level of control over the system and users. For example, you can register and delete accounts, set special access rules for them, etc., which allows you to build a multi-level administration model.
However, thanks to the consensus mechanism, the approach is decentralized and flexible, avoiding the concentration of risks in one hand.



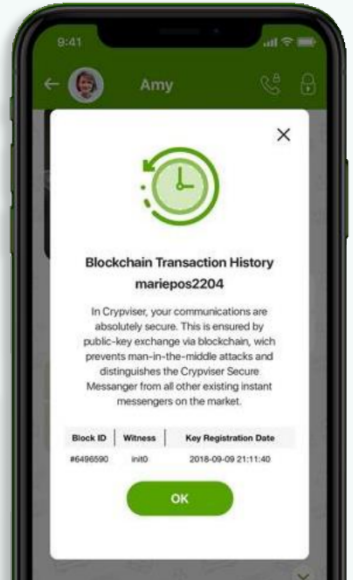
Advanced cryptography of the new generation

To ensure the maximum degree of security, the Cryptographer protocol implements the latest and modern cryptographic ciphers and algorithms, such as ECC Elliptic-Curve, Salsa20/20, SHA3-512 Hash.

A professional approach to all details, such as the use of external entropy sources to calculate encryption keys, resistance to post-quantum computing, provides the highest level of security during data storage and transmission. The supported algorithms and ciphers meet international standards and are approved for military and state use.









Features and Benefits


Instant messaging


File/Document sharing


Audio/ Video calls


Group conferences


Screen Sharing


Functions for confidential control


Destruction of data by timer


Hidden/Blocked Chats


Mobile (iOS and Android) and desktop versions


Decentralized access points


Unique level of data protection and security


True end-to-end encryption


Forward Secrecy algorithm support


Encrypted local storage


Dedicated Private Blockchain Network


Ideal for protecting data transfer between remote objects

Packages available for integration

	Blockchain Cloud	Private Network	Private Blockchain
Rebranding/Redesign	Yes	Yes	Yes
DPKI(blockchain hosting)	Decentralized Network (public Genesis Messenger blockchain)	Decentralized Network (public Genesis Messenger blockchain)	Private Blockchain
Transport Hosting	Cloud infrastructure	Dedicated infrastructure	Dedicated infrastructure
Number of licenses included	5 (annual)	15 (annual)	Unlimited quantity
Protection level	High	Highest	Ultimate
Pricing model	Deployment + User License	Deployment + User License	Deployment + Unlimited licenses

Expansion and integration opportunities

Genesis Messenger solutions are the best choice for secure corporate communications, but are not limited to built-in capabilities. The infrastructure of decentralized public keys (PKI) can be used to protect existing communication channels for the exchange and storage of information and data.
For example, integration with your corporate email system, collaboration tools or a file sharing platform will allow you to encrypt all types of data, ensure confidentiality and protect against internal and external unauthorized interference.

And also, Genesis Block company will be glad to offer our services for the development of new individual functions and the expansion/improvement of built-in capabilities to meet your requirements and business objectives.



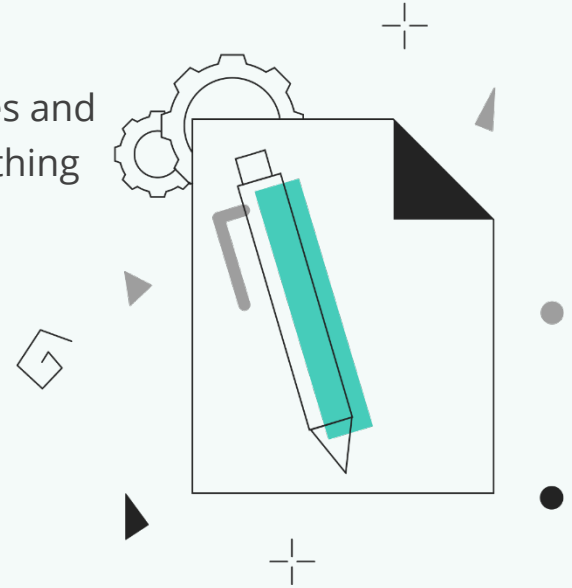
Information integrity chain control

Unique data integrity control algorithms
make it possible to eliminate the threat of intentional leakage by marking important documents/photos/videos with digital "watermarks" invisible to the eye containing data about the data transmission chain, such as user name, date/time of transmission, initial and last transmission source.
Digital markers can contain any necessary service information invisible to the eye, protected from fraud and allow you to track the chain of nodes in the event of a leak.



It's time to make the right decisions!

In the modern world, where huge information flows are transmitted and distributed between different business entities and business partners, confidentiality and data protection is something that cannot be underestimated!



Using the capabilities of modern technologies and a decentralized approach, Genesis Messenger solutions take you to a new level of security, providing advantages that have no equal and eliminating the slightest risks for your business.

Contact us now!

8 800 600 73 07

info@genesisblock.it

https://genesisblock.ru/p