KELVPN

# LIGHT PAPER

MOTIVATION

ADVANTAGES

ARCHITECTURE

NETWORK

NODES

SUBCHAINS

SERVICES

# DECENTRALIZED VPN ON BLOCKCHAIN

## BUILT ON THE ORIGINAL CELLFRAME SDK FRAMEWORK

Ordinary decentralized VPN networks are divided into two categories: free and paid.

Free ones have the low motivation of service providers and high influx of freeloaders. This leads to a low level of quality of service, or it starts to be provided by secret services, which overrides its security.

Paid networks require the purchase of tokens, are more complicated to use, and, as usual, have slow operations of buying the service and finding a connection.
We decided to make a paid network, but without its typical disadvantages.

# OUR ADVANTAGES

Quantum-resistant cryptographic algorithms allow to add new algorithms on the fly or even use multiple algorithms simultaneously.

Thin VPN without a wallet, allowing to keep traffic anonymous and at the same time to authorize and pay for services in the usual user way (card).

An easy-to-use node allows a person without much technical knowledge to easily deploy VPN service on the simplest and weakest hardware and get income from providing the service to others.

A system of checks and orders makes it possible to regulate prices for services by market mechanisms. As well as seamlessly provide services to users, excluding long waiting times for service payment, especially in the periods of service prolongation. This system also gives many servers on the list, reduces the risk of service overload, and reduces the delay in the system.

The ability to run own VPN brand, using the network's resources, and not worrying about the need to keep a staff of system administrators to maintain the servers, reducing its functions to marketing, accepting payments, and buying tokens.

Our developer-friendly CellFrame SDK lets make your own private blockchain solution based on our technology with minimal effort.

Open API for plugins, including Python plugins, for  easier than the  extension of node capabilities.

An open API for services that allows creating your own services sold via the blockchain. All you need to do is run a service, and the issues of accepting payments, their verification, and interaction with the client are already implemented.

Fast and well-optimized code in low-level C with optimizing assembler inserts makes it possible to run the software on absolutely any platform with minimal costs. It also maximizes energy savings, conserves the battery of mobile devices, and contributes to environmental protection in the case of large servers.

The Python version of the SDK enables application programmers to create simple and elegant solutions on our platform while maintaining high-performance C code that takes care of all the basic functionality, leaving Python to do only what the programmer wants to do.

Sharding and P2P inter-shard communication and the internal architecture of the node allow infinite scaling of the system.

# ARCHITECTURE

The KelVPN network consists of two chains, zerochain and plasma, combined into the KelVPN network. The same node can handle many networks at once, both public and private.

Also, special service and informational subchains within each network can be connected, which are optional to distribute. For example, a subchain for informing about malicious actions of network participants, a subchain for registering orders to exchange tokens, a private encrypted subchain distributed by a limited number of nodes for payment, and so on.

# NETWORK

Nodes connect to each other directly, establishing 1-3 or more links, trying to choose the closest, constantly measuring the quality of communication with each other and the signal delay. The connection is made by a proprietary DAP protocol, including key exchange, encrypted Request-Response requests, and encrypted streaming protocol, multiplexing many different streams in one network connection - blockchain exchange, VPN, nodlists, and so on

# ROLES OF NODES

Nodes themselves have different roles: root, archive, master nodes, full nodes, light nodes. Sometimes service nodes (which provide service, for example, VPN) are distinguished separately, but it is only a name - a service node may have a formal role. Similarly, there is a concept of seed nodes, which may have different formal roles. A new network client connects to a seed node to download general lists of nodes and other information.

# DESCRIPTION OF THE SUBCHAINS

## ZEROCHAIN

Zerochain is formed on so-called root nodes. Within a testnet, they are also the seed nodes. The zerochain has a linear structure without branches or shards.
It declares tokens, specifying maximum emission, restrictions on token transactions and other data, declaration of changes of these restrictions, and the emission of funds to specific wallets. In addition, it also declares shards important for the entire network certificates and possibly other data in the future.
Transactions and other data in the zerochain are not available.

## PLASMA

A classic Directed Acyclic Graph, divided into shards and maintained by master nodes via the Proof-Of-Stake consensus. It stores transactions, certificates, and private user data.

# SERVICES

A service whose type is described for the whole network and can be provided by any node at will. The service cost is published through warrants, which contain addresses, transactions, characteristics of the service, the address of the node providing it, and other data, if necessary.
The service itself is provided through a system of checks and conditional transactions.

## CHECK

The check is issued by the node that provides the service. The check contains a description of the service, its cost, and, optionally, some other additional data. The check is signed by the consumer and the seller and then used in conditional transactions.

# CONDITIONAL TRANSACTIONS

They can be both inbound and outbound. An inbound conditional transaction differs from a regular transaction only in that it contains a check.
An outgoing conditional transaction does not have a specific recipient address, only a description of the service for which the transaction is supposed to be paid for and the key fingerprint that signs the check (required for a walletless or thin VPN client). It can also be used as an input for multiple incoming conditional transactions, allowing you to immediately allocate a certain amount to multiple services and slowly spend it without waiting for the transaction every time you need to extend service or switch to another merchant.

# PLANS FOR DEVELOPMENT

Anonymous transactions and built-in anonymous transaction mixer.

Services for token exchange, data storage, source code storage, software releases, and many others.

Integration of the CellFrame Dashboard super-application with network services, as well as with plug-ins and widgets.

I2P-like multihop routing for multiple embedded connections.

Hardware VPN clients.

Additional tools to complicate traffic detection with AI powered DPI.

Chats and video calls, both public free and corporate paid.

Browser plugins for using the decentralized certificate storage and VPN services.