White Paper

Apla Multi-Chain Platform (AMCP)

Apla Multi-Chain Platform is a two-level P2P network that deploys the original Apla distributed ledger technology. The network consists of a multiple number of privately-owned networks that implement the business cases of specific companies **(“Sidechains**”), and a common consortium network **(“Consortium Chain”)** that makes Sidechains immutable. The owners of Sidechains become the members of the Consortium Chain by default to maintain Consortium Chain nodes independent of each other.

With enough number of nodes (over 100), the reliability of the Consortium Chain (non-falsifiability and resistance to attacks) can be considered as being close to those of public blockchain networks. In ensuring data immutability, hashes of legally significant transactions, as well as texts of smart contracts processing these transactions, are stored in the Consortium Chain. This allows you to restore the business logic of transactions and confirm their validity in court even if the data of private sidechains has been lost.

Apla Multi-Chain Architecture

Sidechain owners enter into a service contract with Apla Luxembourg to deploy a Sidechain for them, install decentralized applications and connect to the Consortium Chain. A Sidechain consists of a random (more than three) number of nodes that support the performance of decentralized applications serving the needs of a specific business process. The Consortium Chain nodes are supported by all owners of Sidechains. The Consortium Chain contains only hashes of significant transactions in Sidechains, all versions of smart contracts, as well as identifiers (public keys) of all the nodes of all Sidechains.

Data Immutability

Transactions capturing the actions of users of Sidechain applications are stored in the servers of the relevant Sidechain owner. When developing applications, a list of legally significant transactions, whose hash is to be stored in the Consortium Chain is established by the Sidechain owner.

When a user sends such transactions to the Sidechain: (1) the transaction is signed with the user's private key, (2) the text, hash and description of the transaction is stored on the user's client device, (3) all the nodes of the Sidechain send the hash to the Consortium Chain, (4) when matching hashes are received from more than 2/3 of the Sidechain nodes, the Consortium Chain's special smart contract writes the hash to a special registry.

Since all legally significant smart contracts and changes to them are also stored in the Consortium Chain, all users are able to prove in court that the transaction was sent to the Sidechain, including the legal interpretation of this transaction on the network even if data has been completely lost in the Sidechain. The verification process is the following:

a. A user finds the file with information about the transaction, which he would like to control, on its computer.

b. The user goes to the particular website to check the presence of the transaction in the Consortium Chain.

c. The user copies the transaction hash and inserts it into the form on the website:

   i. The user receives an affirmative response if the transaction is recorded in the Consortium Chain, and

   ii. The user receives a denial response if the transaction is not recorded in the Consortium Chain.

d. To verify the accordance of the transaction contents and its hash, it is necessary to use the hashing function sha256(sha256(transaction)) for the contents of the transaction.

Data Backup in Sidechains

In order to prevent data loss in a Sidechain, the owner of the network can encrypt each next block with a public key and save it in several independent repositories. In this case, the corresponding private key can be kept by a notary or other legal representative. Such a data backup option many be needed to protect the rights of the Sidechain users, who, if necessary, can access the full data through a court.

Consensus

The Apla protocol uses the same logical consensus algorithm as in most blockchain networks (including Bitcoin and Ethereum) to maintain data integrity and protect against attacks, i.e., voting by chain length when random forks or forks specially created to disrupt the network emerge.

To ensure efficiency of this algorithm in public networks where neither the number nor the owners of full block-creating nodes are known, voting methods are traditionally used either with processor power (PoW) or with number of tokens (PoS). These methods of voting for a particular fork chain and the principles of selecting a block-generating node are not suitable for a network where there are no tokens, or where the number of validating nodes is always fixed or where all their owners are known.

In the Consortium Chain, node owners confirm their right to validate transactions and create blocks by entering into legal contracts with Apla Luxembourg to use the service – if they deliberately do not follow network protocols, they break contractual obligations and risk harming their own business and reputation. Consequently, the Consortium Chain implements a consensus algorithm for voting by chain length with a mechanism for determining the right of nodes to generate Proof-of-authority blocks. When using Proof-of-authority, it is implied that most Consortium Chain members comply with contractual obligations and vote with their authority to build a long chain in the event of a fork.

Network Security

Using the Proof-of-authority virtually eliminates the possibility of spamming the Consortium Chain, since all network clients (sidechain nodes) who are authorized to send transactions are known. Besides, the Consortium Chain has a parameter that limits the number of transactions (per client) that can be included in one block.

If the number of the Consortium Chain members increases above a certain number (determined by the current network monitoring), the number of validating Consortium Chain nodes will be limited to a fixed value and an algorithm will be used to randomly select validators from the total number of full network nodes. This will maintain the performance of the Consortium Chain as the number of connected private networks (number of nodes) increases.

The number of transactions in one block is up to 1,000. This characteristic could be changed by voting of users with the role "ConsortiumChain. Member".

Anti-spam

Only the public keys of the Consortium Chain Members have the right to send transactions in the Consortium Chain.

The parameter "*max_tx_block_per_user"* regulates the number of transactions in the block from one key, the parameter could be changed by voting of users with the role "ConsortiumNetwork. Member." If the user exceeds the limit of transactions, these transactions would be banned without signing into the block. Therefore, each user has the equal throughput availability of the network.

Governance

The Apla protocol contains basic applications used to manage the rights of the network users by assigning roles and voting for a change of the network settings. When the Consortium Chain is launched, the right to vote to change network parameters, such as a list of validating nodes, number of transactions in a block, time between generation of a block, etc. is granted to the Consortium Chain members. This not only guarantees a decentralized management of the network, but also allows for flexible configuration of the network without hard forks (which are inevitable in such networks as Bitcoin and Ethereum).

In Sidechains, all rights to manage the list of nodes, users and roles, as well as access rights belong to their owners.

Contractual Framework

The contractual framework of the Apla Multi-Chain Platform is quite simple and straightforward. The Apla company is contracting with the owners of Sidechains and the latter once are entering into contractual relationships with the users of their networks.

The Apla company is in charge of setting up Sidechain nodes and rendering technical support to the users of Sidechains and Consortium Chain.

The owners of Sidechains define network parameters, business process logic, legal terms of use of their Sidechains, onboard the users and store the data sent to the network by the users. The owners of Sidechains pay service/license fees to the Apla company and can define their own pricing policy in relation to the users.

The Apla company and owners of Sidechains become members of the Consortium Chain by default. There is no payment for the use of the Consortium Chain by its users. The boarding process to the Consortium Chain is the following:

a. Apla Luxembourg enters into a service contract with the owner of the Sidechain and sets-up the Sidechain infrastructure.
b. Apla Luxembourg deploys the node for owner of the Sidechain in the Consortium Chain.
c. Apla Luxembourg verifies the accordance of the node to the resource requirements.
d. Apla adds the public keys of the Sidechain nodes to the Consortium Chain's registry of keys. It allows the Sidechain nodes to send transactions into the Consortium Chain.
e. The owner of the Sidechain generates the private and public keys in the software client and sends the public key via e-mail to Apla Luxembourg.
f. Apla Luxembourg adds the public key of a new user from the step "e" and assigns him the role "ConsortiumChain. Member."
g. The holder of the node from the step "b" sends a request to join the Consortium Chain.
h. The members with the role "ConsortiumChain. Member" vote for or against boarding the node.
i. If more than 50 % voted for, then the node joins the Consortium Chain network and becomes validating. Contrarily, the node does not have the right to generate new blocks, but at the same time, it can store the entire blockchain.

The users of Sidechains are responsible for the safe custody of their private keys. In case of loss of a private key, the access to the user’s account can be recovered by the user by generating another pair of keys linked to the account provided that they are validated by the Sidechain owner. The users participate in the corporate governance process and be able to trace hashes of their transactions in the Consortium Chain.

Advantages of Apla Consortium Chain

In principles, hashes of the transactions generated in the Sidechains can be sent to any public blockchain platform to ensure transparency and immutability. The use of the Apla Consortium Chain for the same purpose, however, has got the following advantages:

1. The simplicity of the Apla’s protocol architecture ensures less variation of nodes and increases the reliability of the system.

2. Potentially high throughput of the network due to proof-of-authority consensus algorithm involved.

3. All the activities concerning the network governance (users, roles, access etc.) occur in the blockchain, it protects the system from illegal amendments unnoticeably.

4. No one-person control.

5. Complete infrastructure for the development of applications including user interfaces, smart contracts, language recourses and other options.

6. True decentralization and immutability is achieved without using cryptocurrencies.