UWIM - YELLOWPAPER

UWIM - Network distributed cryptographic platform for easy creation, utilization and accounting of decentralized applications (smart contracts).
We put the idea of a perfect centralization and decentralization balance of data and system functions as the core of our technolog. The system development, addition and updating take place through the company, and the validation, control, decision-making (consent or disagreement) with the updates is decentralized and is determined only by the platform participants.
The architecture of the UWIM platform was designed taking into account a large number of custom tokens with smart contracts. UWIM is based on its own blockchain technology, an independent software product that is not a fork of Bitcoin.

Decentralized part

The reliability and transparency of the platform is achieved by blockchain technology (distributed data registry) with its own Proof Of Stake consensus modified version (decision-making model between participants).
All data is distributed between servers (The nodes source code is in the public access with a free license). Any network participant can deploy one of the nodes types (a full node - with the entire network operations history, with the ability to validate blocks and with all the JSON-RPC API functionality, a light node - with the JSON-RPC API functionality). A full node can become a validator when requirements are fulfilled and participate in the main consensus.
The network can include an unlimited number of tokens, smart contracts and participants (addresses) and can be controlled by the participants.
Own node builds were created for further optimization and development of the platform.

Technological features

Data storage and encryption
To optimize the volume and fast access to the necessary data, leveldb with an open license is used (Technology for storing large amounts of non-relational data of the key> value format).
Access to the data of network participants can be granted using hierarchically generated BIP39 keys.
In the bech32 format, addresses for each participant are divided into three types: main address (uw prefix), smart contract address (sc prefix), node address (nd prefix).
Then the participants exchange data by sending messages to the node and sign the messages with their secret key. The data undergoes primary validation on the node that received the message, then the data is sent to all validators, combined into blocks and sent to consensus. Hashing is implemented using sha256 encoding.
We have created several levels of data validation in the core of the node for complete errors verification and elimination from the moment they arrive at the node until the moment of consensus.

Consensus

The modified version of the ProofOfStake consensus includes making decisions depending on the number of coins on the validator nd address (or nd + sc, depending on the presence of a smart contract for delegation), and on the total number of validators. Each node constantly accepts transactions from network participants. The data goes to the initial pool for processing eliminating data overflow and consensus delay. Then the node validates the transaction based on its own blockchain and makes a decision: to approve or immediately reject the transaction. The accepted transactions are immediately sent to other network validators, which are automatically loaded from the main or other nodes.
Nodes that have received the status of a validator take part in the consensus when accepting data: validators become a proposer in a predetermined order (proposer is a validator that offers data for consideration). If the block is accepted, the proposer receives a reward. Reward data has its own type of transaction. The proposer adds a reward transaction when a block is sent to consensus, it is validated along with the rest.

Each consensus round has the following order:

1) Proposer creates a block based on its own pool of incoming transactions (own and others), signs and sends it to other validators. Other validators save it to their temporary memory after receiving the block. If the proposer has not submitted a block, the system collectively assigns him penalties. Proposer also adds a transaction to the block with its own reward for creating the correct block (All reward transactions come from the Genesis address if funds are available on it).

2) Validators analyze blocks based on their data and respond to other validators about acceptance or rejection.

3) Each validator evaluates the answers of the others according to two criteria (The total number of validators balances who voted FOR must be at least 66% and the number of validators who voted FOR must be at least 50% of their total number). If both requirements are met, each validator sends a block for writing and execution of all transactions.

4) Each validator analyzes metrics, clears temporary memory and prepares for a new round.

Contracts

The system may contain smart contracts that have their own logic and RAM in addition to normal addresses. Both the logic and memory of contracts are also used in a decentralized manner (stored in an specific state on all nodes).
Smart contracts are divided into main groups: Contracts to support system development and user contracts.

Contracts can be added exclusively through the centralized node (More details in the "Centralized part" section). The contract can accept a transaction and then perform a number of calculations and multiple transactions based on its own logic. Each contract is

represented by a separate application on the nodes. All the results of the contracts operations are sent to consensus for confirmation by other participants after execution to exclude modification of the code or memory data.

There is a main token in the system and many participant tokens (alts) can be created. The token is a smart contract and has an owner (address). The holder can use the smart contract balance but cannot change the contract terms directly in the blockchain. Additionally, in some cases, the holder may refuse smart contract ownership. In that case, their signature will not be accepted by validators when processing transactions.

There is a commission with every transaction calculated in the main token, which depends on the current network load. It is possible to increase and decrease the commission to slow down and speed up transactions. The validator that offered the block with this transaction takes all commissions.

The exchange between tokens is implemented through a smart exchange contract: A " liquidity pool", which determines the exchange ratio, is created for each couple of the main and user tokens. In case of a custom token for another custom token exchange, two liquidity pools are applied (from each couple).

Each node has a gateway for sending and receiving data (API) in JSON-RPC format. Any network participant can connect their own IT solutions to the blockchain and link their own smart contract with their centralized product through the API depending on their needs.

The node implementation can use different programming languages and different operating systems.

Centralized part

The centralized part of the project is a convenient user interface for the UWIM blockchain utilization. The source code of the centralized part is the property of the company and is not distributed.

Users can get comprehensive information and use free products through the web service: Blockchain Explorer - allows you to view data and get statistics on all operations without launching a full-fledged node.

Web terminal with the personal key BIP39 access (already specified in the decentralized part).

Mobile terminal with the personal key BIP39 access (already specified in the decentralized part).

The user can store and use tokens presented in the blockchain by other participants in the personal account. The user can use a graphical interface to work with smart contracts presented in the blockchain and more:

Create standard templates for tokens and smart contracts.

Any network user can attach one of his own tokens to his address in his personal account. When a token is created, the label, issue (which cannot be changed in the future), the name and other data (which can be changed in the future through transactions) are determined. In addition, the user determines token type (personal - a token that is controlled only by the creator; team - a token for managing which requires the signatures of a certain number of participants; nft - a token with each unique instance that is managed by only one participant. Moreover, each token has an owner card and a token card where the data is updated through the owner's transactions (Details are described below in the section "Token Market"). Tokens are subdivided into standards depending on

the data in the cards. Various smart contracts can be added to the token depending on the standard. The created token / smart contract is uploaded to the general network and becomes decentralized and accessible to everyone after monitoring and safety systems approval. The user will be able to supplement it with new nodes in the process of development, but all the old parts become unchanged and directly dependent on the initial conditions.

Custom coins and smart contract creation and integration into the business

If a user (person or company) wants to implement non-standard solutions (token / smart contract / api / application), they can use the company services. This process starts with an application in his personal account and verification. An SDK will be developed for this situation and advanced solutions will be created on its basis.

The platform tools

Token platform

Each user token created in the blockchain has an owner card (or owners if the token type is team) and a token card. All data from this card is also subject to decentralization (each subsequent update is recorded and remains unchanged throughout its existence). The token can be attached to the identity of the holder through accreditation. A person or a company consistently goes through the stages of personal data confirmation (The amount and fidelity of data brings each specific token closer to full personalization). The user can also attach a specific product or resource to the token after the accreditation. The user can add their product roadmap, content, etc. Each passed stage makes the token more transparent, personalized and more attractive to other network members. All user tokens are divided into standards on the platform. Information about the standards is presented on the official website of the project.

Exchange for token dex-exchange

Users can exchange between different tokens in the blockchain through smart exchange contracts. The contract can be used through a personal account on the main project website, through any node (not necessarily a validator) and through a mobile application. The contract was based on the idea of liquidity pools: each pair of tokens always has a reserved volume of each token, an exchange operation can occur within this pool at any time, and the liquidity pool holders distribute the commission for the exchange among themselves (it can consist of an unlimited number of tokens). Token exchange can take place according to different algorithms depending on the token types created by the user. In addition, the token holders of certain standards can add additional smart contracts that complement the functionality on the exchange. For example, "Payable-token" can automatically distribute the main coin sent by the owner among all holders of the liquidity pool. The token holder can emit more to the address through Genesis sending an equivalent number (at the current exchange rate) of the main platform coin, etc.

Other instruments

In addition to the main instruments (token platform and exchange), the platform has a number of additional tools that will grow along with the platform such as
· "Mask Fund" - The UWIM team plans to nominate at least 10 famous personalities experts from all over the world who will evaluate the brightest initiatives of the platform participants. Any team can create a token, submit their project and fill in all the relevant details. Each project that has submitted an application will receive an assessment of independent experts. Based on the results of the assessment and experts voting, the project will be assigned a special status and the nominated person will receive a reward in the form of UWM (Basic Unit of the Platform).
· Support for personal tokens - A special smart contract to support new tokens on the platform. The contract distributes the main coin of the platform among the participants in the liquidity pool of the new personal token under certain conditions.
· Bounty company contract - A special smart contract for those who are actively promoting the platform.