AMALGAMA SECURITY

CWD GLOBAL AUDIT

AMALGAMA SECURITY

The technical audit was held by Almalgama Security in the period from the 10th of December, 2021 till the 3rd of February, 2022.

The purpose of this audit is to comprehensively evaluate the operation of the blockchain and confirm the compliance of the platform parameters with the declared characteristics.

Tasks:
Conduct code testing for functionality and absence of vulnerabilities;
Determine network bandwidth;
Check the decentralization of the platform;
Analyze the blockchain for security;
Investigate the correctness of smart contracts;
Evaluate the functionality of the web application on the cwd.global website;
Describe the discovered vulnerabilities;
Provide recommendations for fixing problems found.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

BLOCKCHAIN

The CWD blockchain is based entirely on the codebase of the Graphene blockchain (better known as Bitshares).
The main blockchain code has remained practically unchanged, there are additions from the CWD team.
There are 118299 addresses and 148 assets in the network.
This suggests that the network is quite active.
A block is produced every 5 seconds and there are an average of 1-2 transactions per block.

\BLOCKCHAIN

CONSENSUS ALGORITHM

Delegated Proof of Stake (DPoS))

NETWORK BANDWIDTH

Testnet testing on VPS showed performance up to 30.00 TPS.
At the same time, the indicators declared by Bitshares are 100.00 TPS.

NETWORK FUNCTIONING

To keep the network running, the blockchain must be collected and validated by at least 70% of the Validators.
If the block is confirmed by more than 70% of Validators, then it cannot be canceled.

At the moment, the unconfirmed block reversal depth is 10,000.
In the event that more than 10,000 unconfirmed blocks accumulate in the blockchain, this may mean that most of the Validators are not functioning and manual validation of the network is necessary, and block generation will stop.
The minimum recommended number of nodes is 11.
There are currently 48 nodes in the network.

GENERATION OF BLOCKS

Blocks are generated by nodes defined as active Validators (Witnesses).
Each block creator is a Validator.
Block generation time - 5 seconds.
Within this time interval, the Validator participates in tracking and validating transactions and creating a block with unpublished transactions.

The validator cannot generate multiple blocks in a row, so at the end of each Round, the consensus algorithm sorts the block creators. Round - the process of creating a block by each Validator from the Validator's set.
The set of Validators includes the Validators elected by the owners of the coin.

VALIDATORS (WITNESSES)

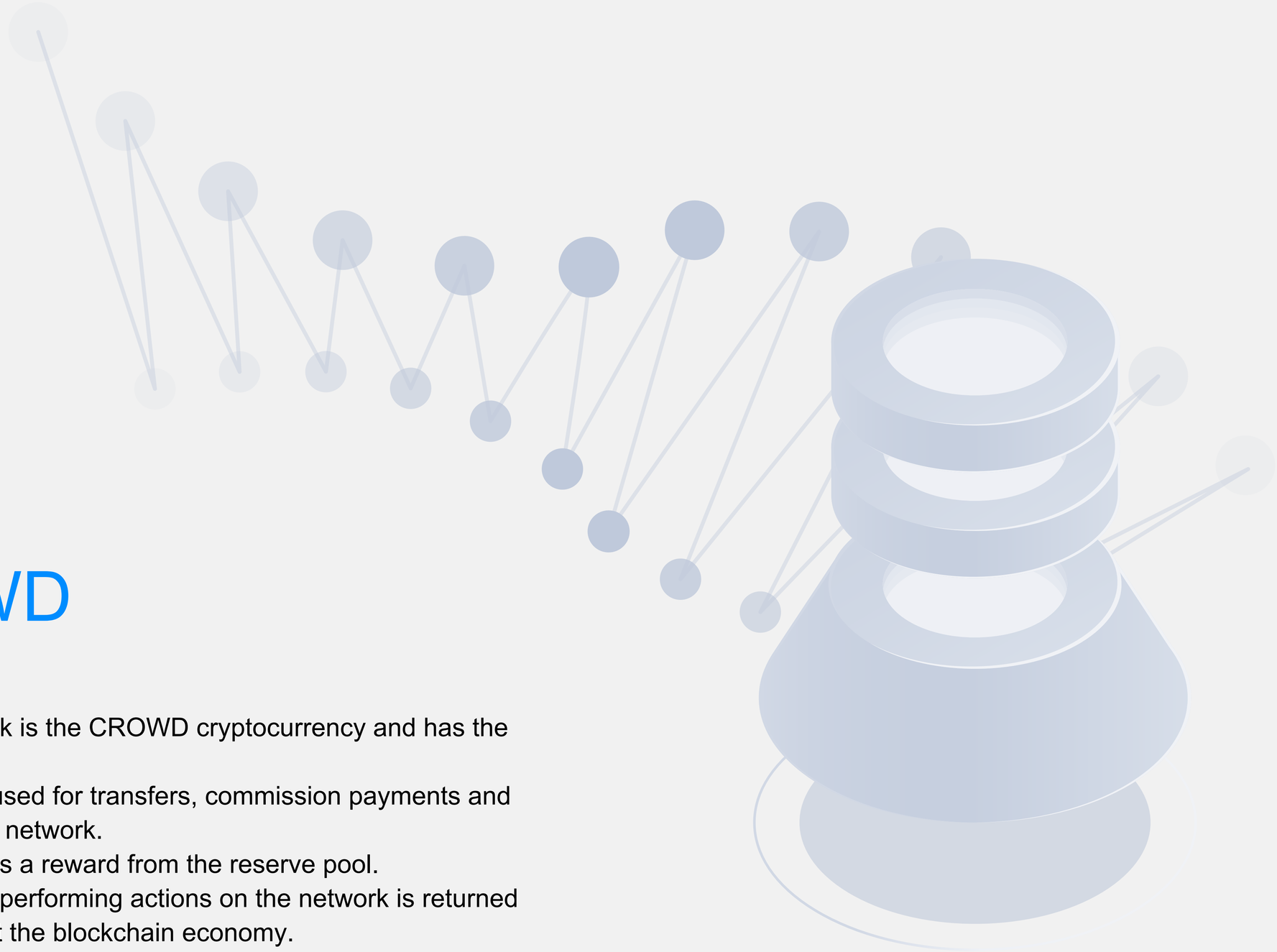
Any member of the network can run the software to claim the role of the Validator.
In order to become an active Validator, you need to reach a threshold number of votes of coin holders.
Only in this case the node will be able to sign the blocks accepted by the network.

By default, the number of Validators is 11, their number should always be odd.
The set of Validators is chosen by the holders of the coin.
The set of Validators are those Validators that received the most votes for the cycle.

VALIDATORS (WITNESSES)

The default cycle time is 10 minutes, however, this time can be changed by voting.
At the beginning of each cycle, the votes are counted and a set of Validators is determined until the next vote.
The more coins a network member has, the greater the weight of his vote, that is, the stake.
The number of Validators depends on the number of coins delegated to all Validators of the network.
When voting for Validators, users also vote for the number of active Validators, but this value cannot be less than 11.

N.B.
The current composition of the Validators contains init nodes, which may be the nodes of the project creators.
This can break decentralization if the number of init nodes is greater than the number of user nodes.



ASSET CWD

The main asset of the network is the CROWD cryptocurrency and has the ticker CWD.
The CWD cryptocurrency is used for transfers, commission payments and distribution of rewards on the network.
Each active Validator receives a reward from the reserve pool.
The commission charged for performing actions on the network is returned to the reserve pool to support the blockchain economy.

TRANSACTION VALIDATION PROCEDURE

Confirmation of transactions and blocks is made by Validators.

The user submits a transaction containing the following information:

- Commission
- Sender's address, recipient's address
- Assets
- Transfer amount
- Additional information

Validation steps:

- Transaction receipt, confirmation and transmission to peers;
- Formation of a block, confirmation of a transaction in a mempool, removal of a transaction from a mempool, creation of a block;
- Passing the block generation time, adding a transaction from the mempool to a new block and transfer the block to peers.

\BLOCKCHAIN\TRANSACTION VALIDATION PROCEDURE

The transaction can be proposed by the user and after receiving the required number of valid signatures, it will be confirmed.
This procedure allows you to send a transaction immediately to the network, without the need to collect the required number of signatures before sending.

Such transactions may have a time limit
and in the absence of a threshold number of signatures, will be cancelled.
In addition, until the required number of signatures is reached, any signature may be removed.

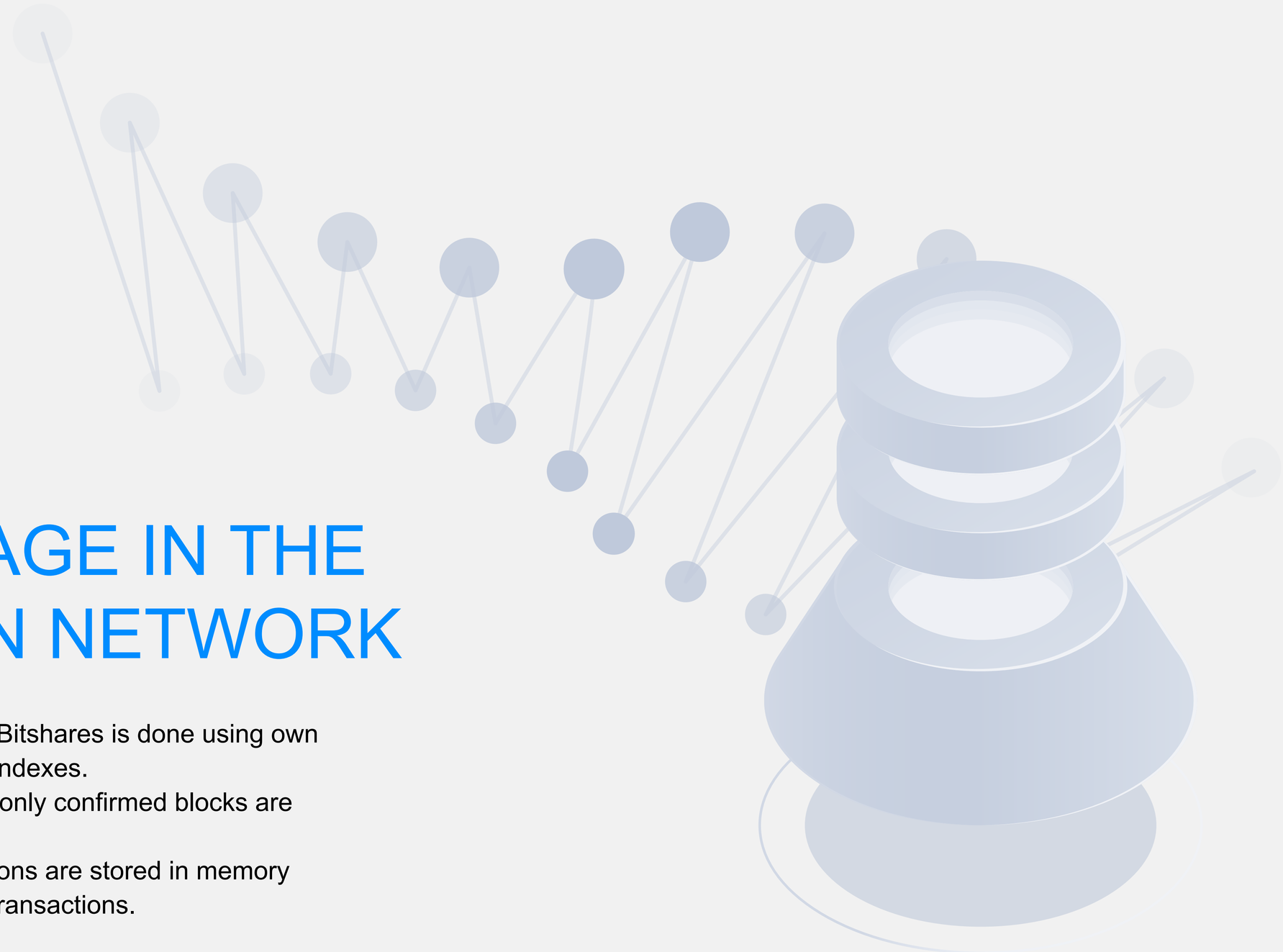
A transaction is considered confirmed if the majority of Validators (50% + 1) have joined the block in question.

In addition, a Validator can propose a fork of a particular transaction and all subsequent Validators will choose which chain to follow by signing their preferred variant..

REACHING A CONSENSUS

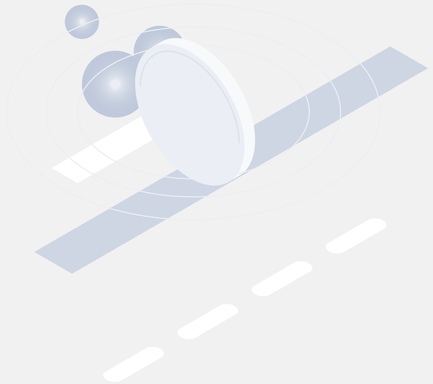
Consensus is reached when more than half of the active Validators (50%+1) have confirmed the block.

Network synchronization occurs through consensus.
Each node validates transactions and blocks independently of the others.
To generate a block, the Validator (Witness) must be synchronized with the peer.



DATA STORAGE IN THE BLOCKCHAIN NETWORK

Data storage in the basic version of Bitshares is done using own development based on boost:multi_indexes.
To track the state of the blockchain, only confirmed blocks are written to the database.
All accounts, balances and transactions are stored in memory and used to evaluate the validity of transactions.



THE BLOCKCHAIN NETWORK SECURITY

Maintaining the operation of the blockchain is possible with a single node.
However, this may affect the speed of block generation.
Deviation from the five-second block generation is not recommended due to the possibility of network delays, block replication, double spending transactions.

Protection against DDOS attacks is carried out using Fault Tolerance technology.

To accept the fork, the confirmation of the majority of Validators (50% + 1) is required.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

GOVERNANCE, RISK AND CONTROL

MANAGEMENT AND CONTROL OF THE BLOCKCHAIN NETWORK

Network regulation is ensured by the work of active Validators.

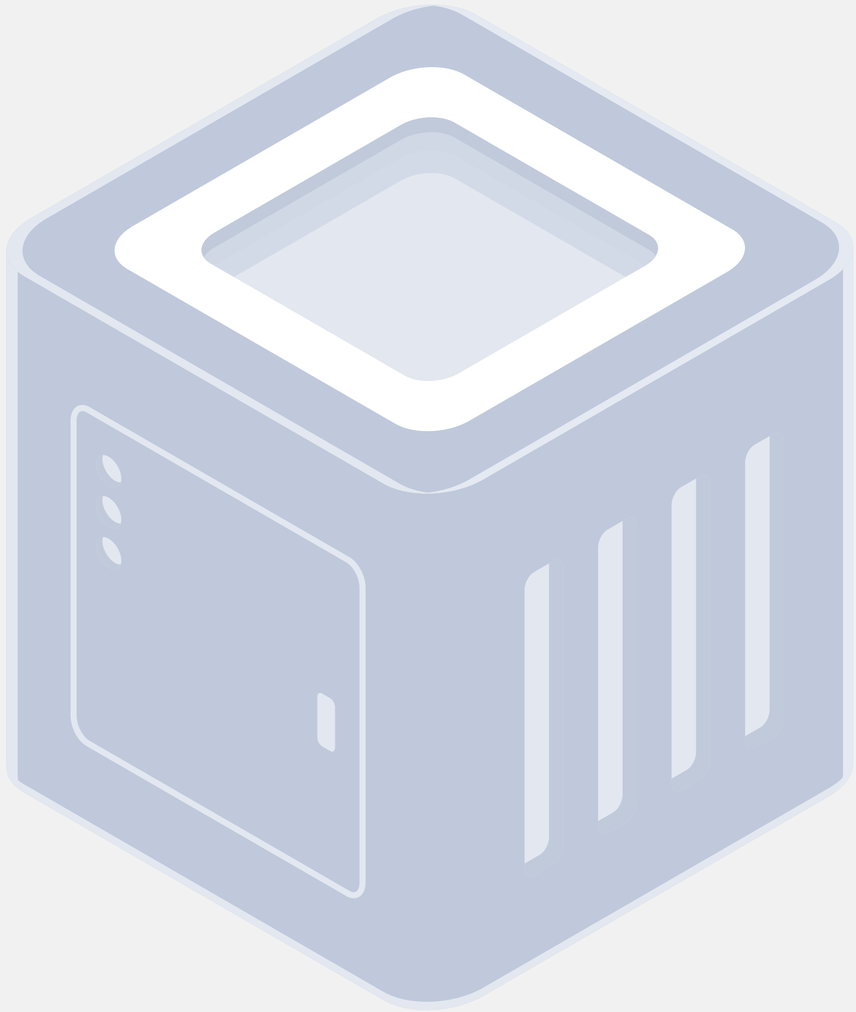
Nodes need to be kept in sync to ensure consensus is reached and there are no forks.

Blockchain parameters can be changed by voting.

Innovations are automatically read by Validators from the block chains, which allows the network to be dynamic without changing the current code of the Validators themselves.

To support the idea of decentralization, the functionality of the network is divided between roles:

- Developers implement the code;
- Validators confirm transactions and blocks, thereby leveling risks and regulating the operation of the network;
- Blockchain parameters are adopted by voting of the Committee.



VOTING

The network management and control process is dynamic and is carried out through voting.

The weight of a vote depends on the amount of CWD on the balance.

Coin owners can vote for any number of Validators, and the stake is not shared between them. Thus, if a user with a balance of 1000 CWD votes for 11 Validators, each of them will receive 1000 votes.

If more than one Validator votes after that, they will also receive 1000 votes.

When voting, user coins are not blocked, and when the balance changes, the number of votes is automatically recalculated, in accordance with the balance of the wallet.

The voting of the Committee is carried out in a similar way.

THE ROLE OF THE CONSENSUS MECHANISM IN NETWORK GOVERNANCE

Consensus is reached during the work of the Validators.
Any user can claim to be a Validator by running the required software, however, in order to become an active Validator, a threshold number of votes must be reached.

Coin holders vote for one or another Validator, thereby entrusting him with network management, including confirmation of transactions and blocks.

To a lesser extent, this applies to Committee voting, as they set the parameters of the blockchain.

If the Validator produces blocks in several forks, then its work will be rejected. This solution avoids the problems that are common with many other PoS consensus implementations.

The high block processing speed (5 seconds) also solves the problem of creating and uploading to the network long chains of blocks that are not verified by other Validators, since all nodes track and confirm transactions and blocks and then add their signature.

LIABILITY AND SANCTIONS

In the event that the Validator fails to cope with the assigned tasks, for example, as a result of a hardware mismatch or network problems, then it will not receive enough votes during the voting.

Reputation and network rewards prevent possible problems with block generation. In the event of an attack on the network, the compromised node will be excluded from the network, and subsequent block producers will not be able to continue this block chain.

This is one of the advantages of DPoS consensus over PoW (Proof of Work), where only a hash is needed to control the network.

When errors occur in the code, the intervention of developers is required to debug the software.

To continue the block chain, one node with updated software is enough.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

NETWORK PERFORMANCE

\NETWORK PERFORMANCE

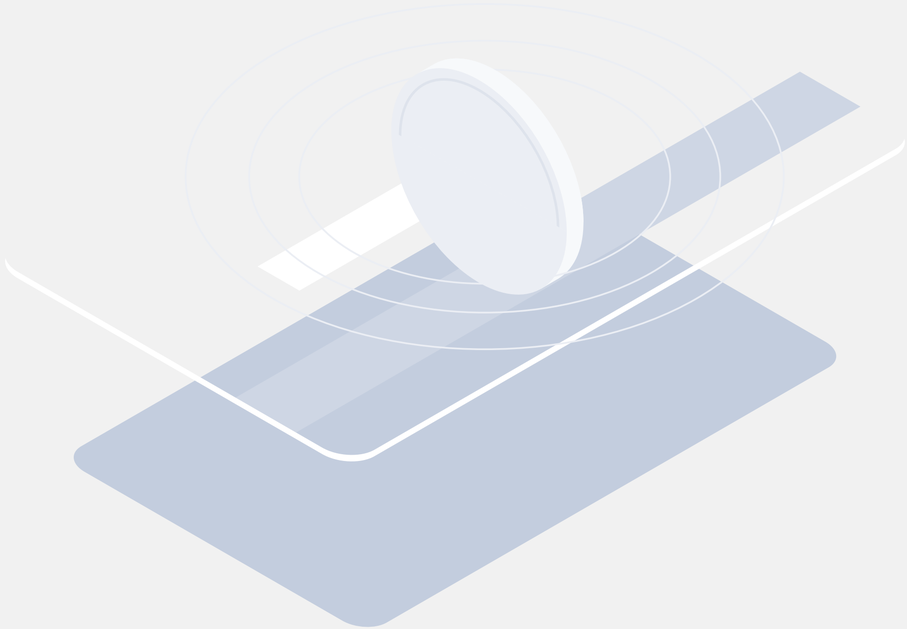
Tests on the main network have shown the ability to process over 30,000 transactions per second.

First of all, this is achieved through a high block generation speed - 5 seconds, which is one of the minimum time intervals, taking into account possible delays in the network. However, the block generation time can be changed during the voting of the Committee.

To assess the scalability and maximum network throughput parameters, it is necessary to focus on the indicators of the original BitShares and Steem blockchain, since CWD GLOBAL is an improved version of these blockchains, and not the original blockchain.

It is worth noting that high synchronization speed also affects scalability. Since the state of the blockchain is stored in memory in CWD GLOBAL, transaction verification is as fast as transaction signature verification, transaction evaluation, and balance updates.

Not all operations are signature verification, since objects in CWD GLOBAL are represented as an objectID, not a hash.
The ObjectID is associated with the key and is validated. At the same time, the objectID size is 48 bits, in contrast to 20 bytes in the Bitcoin network and 32 bytes in the Ethereum network, which significantly reduces the required computing resources.



Main tasks solved by CWD GLOBAL:

- Limiting database disk input and output by writing only new blocks to it;
- Storage of state objects in memory (name, key, balances <1 KB);
- Minimizing the hash operation, preference given to deterministic objects;
- Single threading (queue-based preprocessor);
- Validation is separated from blockchain state change;
- Preservation of the deterministic and explicit interpretation of the transaction (the final state is determined by the input data of the transaction);
- Separate permissions from the individual (hierarchical threshold with multi-signature).

AMALGAMA SECURITY

CWD GLOBAL AUDIT

SAFETY

\SAFETY

The consensus mechanism is the backbone of security.
The principles of its work are documented.

To maintain synchronization, the network uses the Network Time Protocol (NTP), as well as a single time interval for block generation (5 seconds).

To avoid compromised nodes, active Validators are chosen by coin holders.

It is assumed that the Validators act in the interests of the network, otherwise they will not get enough votes and will be excluded from the set of Validators.

\SAFETY

To eliminate the risk of double spending, all transactions and blocks are tracked and validated by active Validators.

A guarantee of security is the fact that only checked blocks are entered into the database, and all the rest are stored in memory to pass the check before writing.

Account security and, as a result, the safety of asset storage, is one of the key principles of CWD GLOBAL.

The technology of hierarchical threshold levels ensures the safe use of funds stored in the wallet.

\SAFETY

If an attacker gets hold of the private key, the funds stored in the account can be stolen.

To eliminate the possibility of transactions by an attacker, it is necessary to change the private keys associated with this account using the owner key (Owner key).

A node can download the entire chain from peers if its database is corrupted or a full sync is in progress.

It's better to run validation on an existing database, and then add delta blocks by validating those sent by peers.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

PRIVACY

\PRIVACY

The CWD GLOBAL platform uses the secp256k1 encryption model.

To ensure privacy between applications, OpenSSL for RPC and WebSockets is used when transferring data between the API server and the wallet.

At the same time, all operating nodes have access to all transactions. Only block producers can send them within a block.

\PRIVACY

When a transaction is made, all information such as commission, sender address, recipient address, asset, transfer amount, additional data becomes publicly available.

However, the field with additional data can be encrypted and readable only by the sender and recipient of the transaction.

However, the system requires authentication of messages sent between nodes. Validators place their public keys on the blockchain. The network uses this key to verify the Validator's signature.

The validator can update its signing key at any time, peers will see the update transaction and change the state of their chain to recognize the new signing key that is stored in memory.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

CRYPTOGRAPHY

\CRYPTOGRAPHY

The bulk of the code is built in C++ on top of Boost and FC (Larimer et al.).

The client wallet command line is a separate executable from the Validator blockchain executable.

The validator allows the client to expose an API endpoint over web sockets.

\CRYPTOGRAPHY

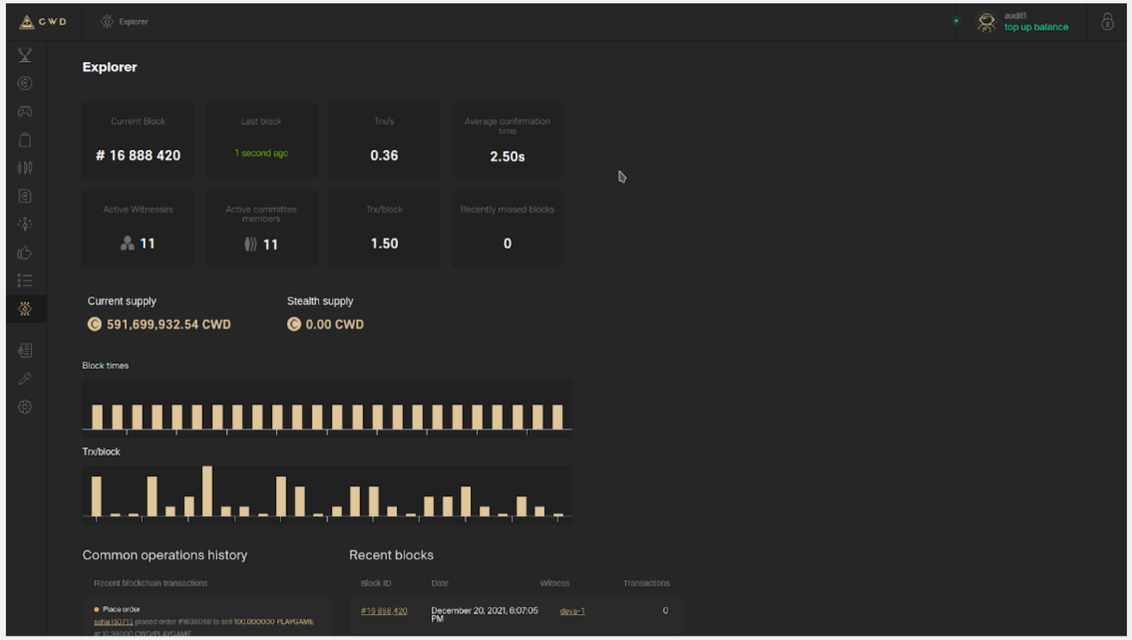
When creating an account, three pairs of keys are generated:

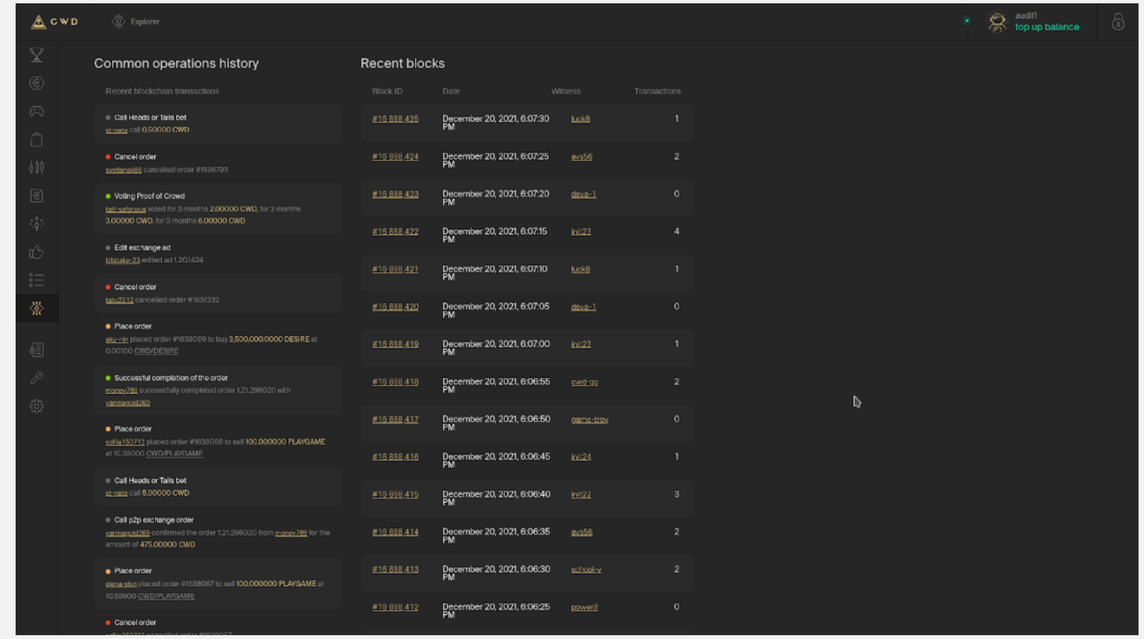
- Active key This key is used to sign transactions that do not change account settings.
- Owner key. This key is used to make changes to the account. In the event of an account being hacked, this key is required to change the keys associated with the account.
- Memo key. This key is used to encrypt additional information transmitted along with the transaction. When using encryption, this text will be readable only by the sender and recipient of the transaction.

\CRYPTOGRAPHY

The main way to manage funds is the official website https://cwd.global/

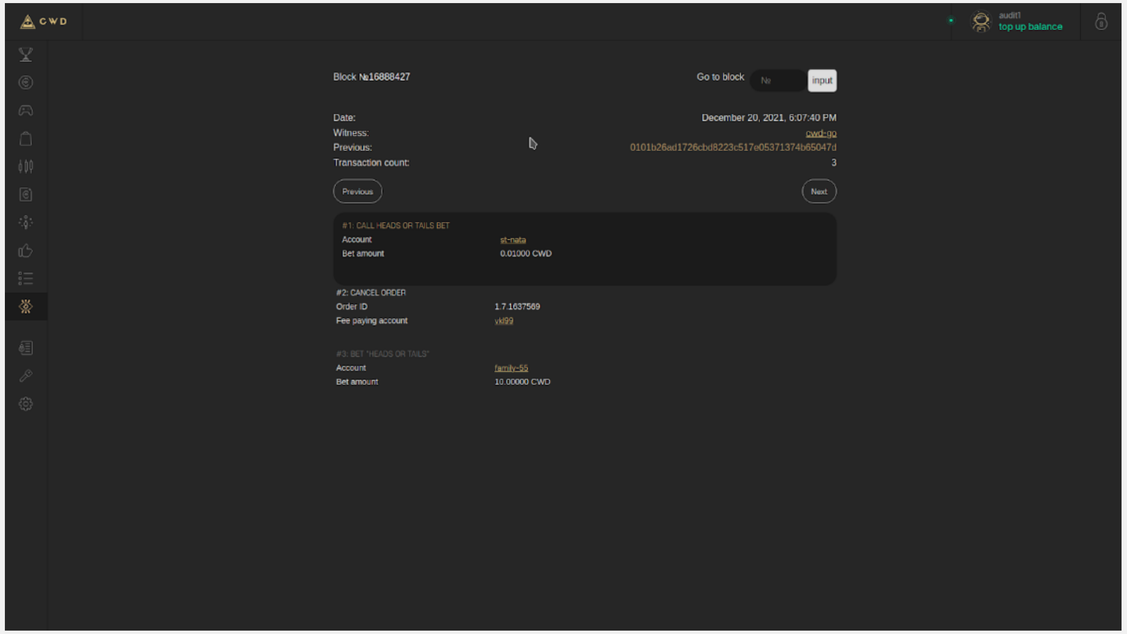
It is available as a Node.JS light client where the keys (generated from the secp256k1 model) are left in the browser and the chain state is obtained from a trusted API server running the Validator executable.

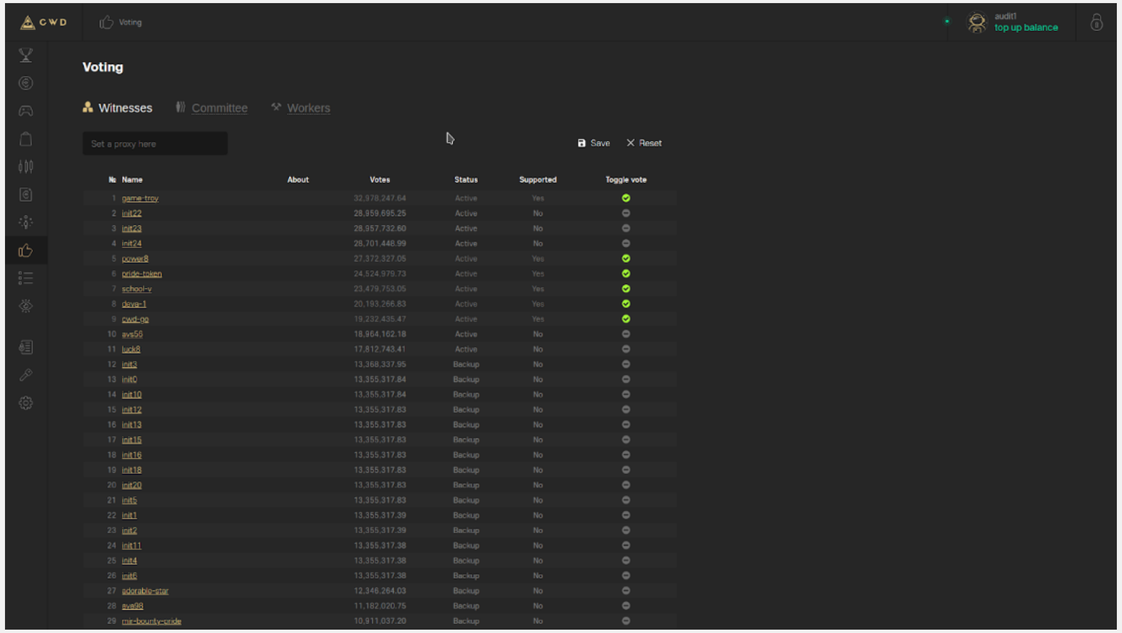




\CRYPTOGRAPHY

Blockchain parameters remain flexible. The fee, number of Validators, delegation time, delegation rewards, etc. are decided by the Committee, which is a separate group of elected coin holders. At the same time, they do not receive any remuneration, but they have the opportunity to change the global parameters of the blockchain by voting and apply them during the maintenance period.





AMALGAMA SECURITY

CWD GLOBAL AUDIT

TOKENIZATION

\TOKENIZATION

The underlying asset of the network is the CROWD (CWD) cryptocurrency. It is used for transfers, commission payments and distribution of rewards on the network.
The CWD asset is defined in the genesis block.

Other assets other than the base cryptocurrency may be represented by the Committee. The issuer can set the asset parameters at his own discretion: token ticker, description, number of tokens, number of decimal places, commission, etc.

All assets other than the base are managed by their issuers as part of the life cycle of the token.

The issuer has the ability to create black and white sheets, issue more tokens, cancel the token, etc.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

PROJECT IMPLEMENTATION

\PROJECT IMPLEMENTATION

The first block was generated on March 22, 2019, and at the time of writing this document (December 2021), the number of registered accounts exceeded 118,348.

On the CWD GLOBAL blockchain platform, you can use almost all the functionality of Bitshares, and besides it, about 50 new operations.

The timing of implementation depends on the goals set by the project.

The source code is open and free to use (MIT license).

Similar technical solutions have already been tested and applied on the basis of BitShares, Steem, and Graphene projects. To determine the economic justification for the implementation costs, it is necessary to focus on the above projects.

AMALGAMA SECURITY

CWD GLOBAL AUDIT

CONCLUSION

As a result of the audit and study of the functionality of the CWD GLOBAL platform, it can be concluded that this project uses blockchain technology.

The platform is decentralized and all management is in the hands of Validators.

The network is active and has regular users.

The exchange is also decentralized and has no controls.

Tokens issued on the platform are not always related to the founders of the project and can be created by any user.

AMALGAMA SECURITY

We are the developers union in the field of Blockchain technology, Big Data and AI.
We help our clients including private persons and businesses with an interest in development, art and digital collections. The company aim is to provide a robust development service and consulting in the field of Blockchain and digital arts.
We take on the full cycle of development an IT product: from building an integrated analytical model to implementing a growth strategy.

Contact us
security@amalgama.digital