https://github.com/staroy/gyro
staroy@pm.me

Gyro blockchain.

Based on the consensus algorithm "Proof of Gyro". Instead of spending energy to achieve consensus is used frozen forever coins, which in the form of newly generated, return and pay network support. The blockchain is initialized based on the file configurations, which allows to implement different strategies of token or coins. Primary initialization with the lack of further emissions, or on the contrary, smooth emission. Freeze large paws for sustainability and mutual confidence of partners. Based on the transaction pool implemented SMS subsystem - short text messages, they are used to multisign addresses. All these operations occur based on the Cryptonote protocol, that is opaque for a third-party observer. But available to observe the "view" owner of the keys. Added subsystem of P2P interaction at the local network level, based on framework zyre. On an orchestra can be created, with encryption of services groups. The interface is implemented by wallet, and in the zyre-lua control utility, allowing to run management scenarios, analysis and interaction. The zyre-lua also added the implementation of the HTTP server and websocket.

Proof of Gyro.

New blocks generate so-called "spinners". To become a spinner need freeze some coins (spinner_lock <address> <amount>). Each the formed block spin spin associated with the address based on the price additional energy — SPINNER_ENERGY_COST_MULTIPLIER, taking into account resistance rotation — SPINNER_DAMPING_RATIO_DIVIDER.

$$dE = SPINNER\_ENERGY\_COST\_MULTIPLIER \times amount$$

$$spin_N = \sqrt{2 \times (E + dE - damp^{dT}) \Big/ SPINNER\_MOMENT\_OF\_INERTIA}$$

где:

$$damp^{dT} = spin_{prev}^2 \times dT \Big/ SPINNER\_DAMPING\_RATIO\_DIVIDER$$

The interval when the formation of the next block is available for spinner, the formation of the next block is calculated from the accumulated back, the more spin, the less the interval, respectively, more often blocks:

$$interval_{next} = medium\_spin \times approximately\_count \times DURATION\_TARGET \Big/ spin_N$$

After some time (SPINNER_SPIN_BLOCK_WINDOW blocks) interval starts increase, then locked coins need to add (spinner_lock <address> <amount> <prev_lock_txid>).

When freezing coins, a unique 256-dimensional vector is created. And with each new not only the cumulative spin GYRO is summed by the unit, but also its vector value. The weight Alternative and base branches of the blockchain defined as the ratio of the sum of the vectors modules (GYRO) to the module of the sum of the vectors:

$$P_N = \sum |V_{256}| \Big/ \left|\sum V_{256}\right|$$

From the properties of vector algebra - the numerator is always greater than the denominator, and the more participants in the branch of the blockchain, the smaller the denominator, and the weight is respectively more. Vector generated randomly as "Publicly Verifiable Random Beacon" (PVRB), based on

created subsequent SPINNER_PVRB_BLOCK_WINDOW blocks, that is, to determine in advance Its value, Spinner has no opportunity. Creation of multiple addresses with small amounts will exclude honest spinners that will take ignored transactions, and after SPINNER_SPIN_BLOCK_WINDOW blocks, you will need to update all fictitious transactions. Freezing, otherwise the coins will be simply lost.

In developing.

Contracts based on the built-in JIT interpreter LLVM / CLANG (C ++). In contracts will be p2p zyre interface is available with which you can organize the interaction of blockchas directly from contracts.