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

Gyro blockchain.

Основан на алгоритме консенсуса «proof of gyro». Вместо траты энергии для достижения консенсуса используется замороженные навсегда монеты, которые в виде вновь сгенерированных, возвращаются и оплачивают поддержку сети. Блокчейн инициализируется на основе файла конфигурации, что позволяет реализвать разные стратегии токена или монеты. Начальную инициализацию с отсутствием дальнейшей эмиссии, или же наоборот плавную эмиссию. Заморозку крупных паёв для устойчивости и взаимного доверия партнёров. На основе пула транзакций реализована подсистема SMS — коротких текстовых сообщений, они же используются для мультиподписных адресов. Все эти операции происходят на основе протокола cryptonote, то есть непрозрачны для стороннего наблюдателя. Но доступны для наблюдения владельца «view» ключей. Добавлена подсистема p2p взаимодействия на уровне локальной сети, на основе framework zyre. На её основе может создаваться оркестр, с шифрованием групп сервисов. Интерфейс реализован в кошельке, и в управляющей утилите zyre-lua, позволяющей запускать сценарии управления, анализа и взаимодействия. В zyre-lua так же добавлена реализация http сервера и websocket.

Proof of Gyro.

Новые блоки генерируют так называемые «спиннеры». Чтобы стать спиннером, необходимо заморозить некоторое количество монет (spinner_lock <address> <amount>). Каждый сформированный блок раскручивает спин ассоциированный с адресом, исходя из цены дополнительной энергии — SPINNER_ENERGY_COST_MULTIPLIER, с учётом сопротивления вращению — SPINNER_DAMPING_RATIO_DIVIDER.

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

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

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

Интервал когда для спиннера доступно формирование следующего блока вычисляется исходя из накопленного спина, чем больше спин, тем меньше интервал, соответственно чаще генерация блоков:

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

Через некоторое время (SPINNER_SPIN_BLOCK_WINDOW блоков) интервал начинает увеличиваться, тогда залоченные монеты необходимо добавить (spinner_lock <address> <amount> <prev_lock_txid>).

При заморозке монет, создаётся так же уникальный 256-и мерный вектор. И с каждым новым блоком суммируется не только кумулятивный спин GYRO, но и его векторное значение. Вес альтернативной и основной веток блокчейна определяется как отношение суммы модулей векторов (GYRO) к модулю суммы векторов:

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

Из свойств векторной алгебры — числитель всегда больше знаменателя, а чем больше участников в ветке блокчейна, тем меньше знаменатель, а вес соответственно больше. Вектор генерируется случайным образом, как «Publicly Verifiable Random Beacon» (PVRB), на основе созданных последующих SPINNER_PVRB_BLOCK_WINDOW блоков, то есть определить заранее его значение, у спиннера нет возможности. Создание множества адресов с небольшими суммами не исключит честных спиннеров, которые будут забирать игнорируемые транзакции, а по прошествии SPINNER_SPIN_BLOCK_WINDOW блоков, потребуется обновлять все фиктивные транзакции заморозки, иначе монеты будут просто потеряны.

В разработке.

Контракты на основе встроенного JIT интерпретатора LLVM/Clang (C++). В контрактах будет доступен p2p zyre интерфейс, с помощью которого можно организовать взаимодействие блокчейнов напрямую из контрактов.