Louis d'or

crypto_zoidberg, doe1138

1 Ce qui est Louis d'or?

Louis d'or is the first CryptoNote-based Proof-of-Stake cryptocurrency. We implemented a hybrid protocol, combining Proof-of-Stake (PoS) with traditional Proof-of-Work (PoW), and doubled the security.

Every new block can be PoS or PoW, they count nearly equally. Total branch "value" is higher if blocks of two types intercharge rather than appear consecutively. As a result, it is almost infeasible for an attacker who has even gained a large potion of PoS or PoW powers to perform a double-spend or 51% attack.

Specifications

- *Codebase:* **CryptoNote**
- *Consensus protocol:* **Hybrid** (Proof-of-Work + Proof-of-Stake)
- *Privacy:* **Untraceability** (Ring Signatures + One-time addresses)
- *Proof-of-work:* **CryptoNight Lite** (ASIC-resistant + faster than CN)
- *Proof-of-Stake annual dividends:* **3–5%**
- *Transaction confirmation time:* **2 minutes** (block interval)
- *Blockchain pruning:* **up to 80%** (BBR prunable signatures)

2 Proof-of-stake protocol

Proof-of-Stake is a distributed consensus mechanism similar to Proof-of-Work in the the following sense: every second you have a small chance to "win" (create a new block). In PoW approach your chances are proportinal to your CPU powers, and in PoS they are proportional to the amount of coins you own. Therefore the network is protected while 50% of coins are distributed among the honest active participants.

The main goal while implementing any PoS scheme is to prevent user from manipulating his chances of winning (i.e. from increasing his expectation value with constant resourses). We adopted the Peercoin/Novacoin/Blackcoin approach with *kernel* hashing to CryptoNote technology. The kernel is an output-specific structure and includes:

1. Current **timestamp**. It should be same as in the new block.

2. **Key Image**, which corresponds to the output key. Literally, key image is 32 random-looking bytes derived from the key, and it is hard to find the key given the image.

3. **StakeModifier**. Another 32 pseudorandom bytes which in turn are derived from the last blocks (so it is hard to predict StakeModifier in a few blocks ahead)

You "win", if $Hash(kernel) < CoinAmount \cdot PosTarget$, where $CoinAmount$ is amount of coins for the particular output, and $PosTarget$ is an adaptive parameter (to keep the block creation rate constant).

User iterates timestamp (within allowed boundaries) for his every unspent output and check the equation. If "won", he spends this particular output **anonymously** with ring signature. Note, that with CryptoNote signature he must also provide the key image (which is used in kernel), and it does not compromise amonymity. He signs both the transaction and the block header.

Reasoning

Here we will discuss some of design decisions we made.

- **Kernel structure** Peercoin kernel includes direct references to the "winning" output (i.e. "Offset of previous transaction inside the block"). We could not use it, because the main benefit from ring signatures (untraceability of the output) would be lost. We replace all these data with CryptoNote *key image* which in fact is like a hash of output's private key. So it contains 32 bytes of *pseudorandom unpredictable data*, corresponding to the "winning" output (in comparison with Peercoin's 16 bytes of data which can be manipulated).

- **StakeModifier** The purpose of StakeModifier is to make kernel unpredictible (thus protect it from machinations). We recalculate StakeModifier on each PoW block, which goes right after a PoS block. Its value is a hash of 720 past blocks' IDs. PoW block IDs are unpredictible, but PoS IDs can be manipulated (by adding/changing a transaction and changing the merkle root). That's why the last 6 PoS blocks' ID are omitted.

- **Age of coins** Louis d'or does not count the age of coins, as opposed to Peercoin/Novacoin, and the chances of winning are proportional only to the amount. The first reason is to make the process of PoS mining more egalitarian, as well as PoW. Users are free to spend/transfer their money and do not obliged to wait months to slightly increase their chances to win. The second reason is security consideration. In order to protect the network we want more "honest" coins to participate in PoS mining. Eliminating the age of coins we increase the "honest hashrate", allowing even recently spent coin to produce a block. And last reason is privacy. For CryptoNote ring signature you need to mix you output among the other outputs with the same characteristics: amount, age etc. If we had restricted the age, we would have also bound your privacy.

3 Other features

Untraceability

All CryptoNote-based coins use ring signatures instead of usual signatures. Ring signature allows you to hide your key (and therefore, your indentity) in the transaction among the other spenders. Thus one can only trace your transaction to a set of possible senders, not to your key. You can choose this set *ad arbitrium*: include any number of any users' keys.

Proof-of-work

CryptoNight Lite is a light version of CryptoNote default PoW function. Here is the list of changes:

1. The size of scratchpad is lowered from 2 MB to 1 MB
2. The number of main loop iterations is lowered from 1 million to 500k

The main benefit is a performance, while we still hold the memory-bound property and preserve the ASIC-resistance (the memory bound ratio is constant).

Fee policy

50% of fees "return to the pot". It means that miner gets only the half of all transactions fees in his block. The rest will be substracted from the amount of already generated coins. This is intended, like in Peercoin, "to offset inflation by deflating the money supply and serves to self-regulate transaction volume, and stop network spam". But unlike Peercoin we don't destroy 100% of fees to keep the miners motivation for including new transactions.

Block score

In order to encourage both PoS and PoW miners and protect from an attack of a powerful miner/pool (with only one type of power: PoS or PoW) we introduced a penalty for several blocks of one type in a row.

This rule only affects the local policy of a peer when blockchain fork occurs. He decides to switch if cumulative score of one branch is larger than another one, as usual. But every block's score is reduced if it was preceded by a block of the same type. For example, a second PoW block in a row will be penaltised by 10%, the third — by $10\% \cdot 10\%$ and so on. On the contrary, a chain like "PoS - PoW - PoS - PoW ..." will get the full score.

4 Authors

- **crypto_zoidberg** `https://bitcointalk.org/index.php?action=profile;u=170073`
- **doe1138** `https://bitcointalk.org/index.php?action=profile;u=401227`