FairCoin V2 white paper

DRAFT

June, 2016 by Thomas König and Enric Duran
tom@fair-coin.org, enric@fair-coin.org

Document version 1.1
Code development: https://github.com/FairCoinTeam/faircoin2

FairCoin is the monetary base system for FairCoop - The Earth Cooperative for a Fair Economy (see https://fair.coop). At FairCoop we develop tools and transfer knowledge that enable everybody to participate in a fair global economy. FairCoin plays a central role within the FairCoop ecosystem and is constantly being developed to further our values. Version 1 of the FairCoin wallet software which was used from 2014 until 2016 relied on mining and minting technology to secure the block chain. Our objection is that neither mining nor minting can truly be considered fair, because both confer an advantage on the already rich. Therefore we decided to create a new version of FairCoin which corrects these issues.

With FairCoin version 2 we create block chain-based software that is fair, secure, resources-saving and decentralised. It is based on **cooperation** and not on competition, which creates better efficiency.

The code-base of the Bitcoin core client in version 0.12 served as the starting point. This enables us to benefit from the latest developments made by the dedicated Bitcoin developers. Furthermore, the comprehensive infrastructure that already exists around Bitcoin can be adopted for FairCoin with minimal effort.

1 Overview

- When we refer to FairCoin in this document we refer to version 2 if not otherwise stated -

In contrast to other cryptocurrencies FairCoin does not implement any mining or minting functionality, which are both competitive systems. Block generation is instead performed by so-called **certified validation nodes** (in short CVN). These nodes **cooperate** to secure the network. Therefore we call this system **proof-of-cooperation** (PoC).

To run a CVN one needs to complete a certification procedure which is called a node certification procedure that is operated by FairCoop (https://fair.coop/node-certification-procedure/). The requirements to operate such a node are described in chapter 3.1. Please note that the definition of the certification procedure is not covered here but in a separate document.

There is no reward for block creation. Therefore, the money supply is not changed by creating blocks.

The mandatory transaction fees go to the respective block creators to compensate their efforts for running a CVN.

CVNs can be added or removed from the network dynamically. This way if a misbehaving CVN is identified it can quickly be removed, and new supporters can easily be added. CVN information is stored in the block chain. More information about how information can be stored in the FairCoin block chain can be found in chapter 5.

Certain chain parameters, e.g. the time between blocks, the amount of the transaction fee, etc. are dynamically adjustable without the need of releasing a new wallet version. These dynamic chain parameters are stored in the block chain. The FairCoin block chain administrators take on the task of managing these parameters, in accordance with decisions from the FairCoop assembly.

Information about the FairCoin block chain administrators are also stored in the block chain.

2 Proof-of-cooperation (PoC)

2.1 What is PoC

PoC is a consensus algorithm which is required in the P2P network of a crypto currency. Every node in such a network must obey the same set of rules to maintain the networks integrity. All connected clients have the same data available to verify the state of the network.

In the case of FairCoin a limited number of trusted nodes (CVNs) collaborate to create the FairCoin block chain. They do this by completing the following tasks:

1. By examining the past blocks they determine what CVN should create the next block and publish their conclusion on the network.
2. They verify the validity and integrity of the last block, its transactions and if it was indeed the respective CVNs turn. The resulting information from point 1. and 2. are digitally signed

and sent to all other nodes.

3. These signatures are collected by the CVN that creates the next block. They are the actual consensus proof and thus the proof of cooperation of all the CVNs. This bundle of signatures is stored in the block chain together with the new block, which is only valid if it contains enough signatures according to the algorithm.
4. When the new block is completely built it is singed by the creating CVN and sent to the network.

2.2 How does it work

As mentioned above every CVN takes part in this ongoing consensus process by signing pieces of data to confirm its approval. Let's put ourselves into the shoes of a CVN and accompany it for 2 blocks. We start at the moment where we've just received a new block from some other CVN.

1. We verify the overall block validity and integrity and its transactions and other payloads.
2. If everything is fine we start searching backwards through the chain to find out which CVN has created its last block the furthest in the past. Once we've identified that node, we check if it was recently actively collaborating in the network by trying to find the signatures of that node in the last couple of blocks. If the node was active, then it will be chosen as the next block creator.
3. Now that we know who should create the next block we have everything together to start collaborating. We do this by signing a specific piece of information which contains the following:
   - the hash of the last block that we checked to approve that we agree on that parent block
   - the ID of the CVN who should create the next block
   - and finally our own CVN ID to confirm that we signed the information
4. We send our signature out to the network, so everybody knows our opinion about how the chain should continue.
5. Well, good job so far. Let's check now if it is already time to create the next block. For this purpose we look up the current block spacing in the dynamic chain parameters data. We see, it's 3 minutes. So we have to wait until this time has past. In the meantime we are busy collecting all the signatures of the other CVNs.
6. OK, block spacing time is over, so we check again which CVN should proceed. And it happens to be our turn, great!
7. But before we go on we need to check if we have at least 50% of the number of signatures of the last block. Suppose the last block had 27 and we received 28 - so some CVN just came back online, awesome! We have more than enough.

8. We create a new, fresh block containing all the pending transactions. The signatures we collected earlier that approve that we are the next in the line also go into the block. The more matching signatures we have the more likely our block will be accepted by the network. Usually we should get 100% of all the signatures but if there was a network outage we'd be missing some.
9. After the new block has passed all consensus checks we send it out to all other nodes. That's it! We helped to advance the FairCoin block chain.

3 Certified validation nodes (CVN)

The aim of the CVNs is to secure the network by validating all the transactions that had been sent to the network and put them into a transaction block chain. Blocks are created every 3 minutes (180 sec.). Transactions are confirmed after they have been added to a block.

A CVN is a standard FairCoin core client configured with additional information namely certification data issued by FairCoop which “upgrades” it to a CVN. Every node will be assigned a unique id.

3.1 Requirements for running a CVN:

Every entity running a CVN must agree upon the following technical requirements and must carry the responsibility to fulfil these rules.

1. The system must be connected to the Internet all the time (24/7) and the TCP port 40404 must be reachable by all remote nodes from the Internet.
2. The system must use a public NTP server to synchronize its system time to, e.g. pool.ntp.org to ensure that the system time is always correct.
3. The wallet software must be configured with certification data issued by FairCoop.
4. A smart card and an appropriate reader, which will be provided by the FairCoin development team.

Further requirements might be defined after public discussion. But this will be subject to the NCP document.

3.2 Smart card support

To achieve maximum security for the FairCoin network the private keys of the CVNs that are required to create and sign blocks are stored on smart cards. These keys are created directly on the card, cannot be retrieved and are also secured by a 6 number PIN. After 3 invalid tries the card is locked and must be returned to the FairCoin development team.

When an entity is approved to become a CVN it will receive a pre-configured card/reader set from the FairCoin development team.

4 Economic role of FairCoin

No more unfair money creation. FairCoin will not create new coins. Certified nodes will not need to create new coins in order to provide security to transactions. Instead, FairCoin will help to create the conditions for existing coins to be redistributed to amazing social projects worldwide, thanks to funds like Global South Fund, Commons Fund, Technological Infrastructure Fund and Refugees Fund.

By fixing the supply, FairCoin becomes stronger at the level of store of value for the solidarity economy and the cooperative initiatives.

Through the FairCoin block chain - besides being a currency in itself - FairCoin will be a perfectly adapted platform to be used by social currencies worldwide with no obligation to abandon their own principles.

On the contrary, they will find an environment of synergies at all levels, which will allow them to advance their goals more rapidly by making use of P2P technology, which will facilitate its daily use and its interoperability with other currencies and payment systems. This, in turn, will form a part of a growing plural ecosystem consisting of a number of currencies and cooperative initiatives, eventually becoming capable of challenging the incumbent system.

Therefore, the FairCoin block chain will be the closest thing to a block chain for the common good, and we can make it possible by working together.

5 Block chain management

To manage the block chain there are chain administrators who sign new instruction data for the block chain. These administrators act as spokesperson for the FairCoop assembly and are publicly appointed. For new instructions to be accepted by the network these instructions must be signed by a defined number of representatives. This number is dynamic and stored in the block chain and can be changed as decided in the assembly.

The spokespersons are obliged to perform just what the assembly decides. If a spokesperson does not collaborate as described he will be removed from the list of administrators and a substitute will be appointed by the FairCoop assembly. Note, that a **single** administrator has no special power. All he can do is to sign the decision made in the assembly or refuse to do so.

5.1 Payload

FairCoin blocks can hold different types of payload. They all serve a certain purpose. Most other crypto currencies only know one payload type: transactions.

The following types of payload can be integrated into a block.

- Transactions
- CVN information data
- Dynamic block chain parameters
- Block chain administrators
- Coin supply instruction data

5.2 Adding and removing CVNs

To add or remove CVNs and chain administrators or update the dynamic chain parameters at least the currently defined minimum number of chain administrators have to sign the corresponding command which is then injected into the network via the wallets RPC interface.

5.3 The coin supply

The coin supply is fixed and cannot be increased in FairCoin. But if FairCoin is forked to create a new coin based on the FairCoin source code there is a feature to increase the coin supply.

Please note that this feature **is not used in FairCoin**. It is disabled at compile time by default. So the next paragraph applies to **forks** of FairCoin only:

If it is decided to increase the coin supply **all** of the chain administrators have to sign the coin supply instruction data which is then injected into the network via the wallets RPC interface. This data instructs the CVN which creates the next block to include a second output in the coinbase transaction with the specified amount of coins to the defined address.

Coins can also be burned by creating an OP_RETURN transaction.

6 Outlook

So far we have implemented important innovations in FairCoin, but we won't stop here. We have analysed the requirements for a currency for a fair economy and have identified important features that will be implemented in the near future.

6.1 Micro payments

The high efficiency of the FairCoin network, trusted node relations, low energy cost and consequently low fees, will make FairCoin the best currency for micro payments which are very important for many needs like the gift economy and use in poor countries.

6.2 Distributed sub chains and multi-currency ecosystem

This proposed system enables everybody to create a separate chain that roots in the FairCoin main chain and runs alongside it. To drive a new Chain a selected number of CVNs can take part in any number of chains. A plug-in architecture provides a way to create chains with new properties. E.g. a chain can implement a local currency based on a local network of nodes of the same region or city, or a thematic currency based on the same principles.