FairCoin V2 white paper

DRAFT

Document version 1.0
Thomas König, May 2015
tom@fair-coin.org

FairCoin is the monetary base system for **FairCoop** The Earth Cooperative for a Fair Economy (see https://fair.coop). In FairCoop we develop tools and transfer knowledge that enable everybody to participate in a fair global economy. The existing version of the FairCoin wallet relies on mining and minting technology to secure the block chain. The problem 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 FairCoin2 (in short **FC2**) we can create block chain-based software that is **fair**, **secure** and **power-saving**. It is based on **cooperation** and not on competition.

It is built on the code-base of a recent version of the Bitcoin core client. This enables us to benefit from the latest developments made by the dedicated Bitcoin developers. Also the comprehensive infrastructure that already exists around Bitcoin can be adopted for FairCoin with minimal effort.

This document describes the design concepts we have implemented in FairCoin2. Some knowledge about how Bitcoin works is required to fully understand the contents of this document. The first paragraphs provide a rather high-level view of the FC2 concept and the further you read the more technical and detailed it becomes.

1 Overview

In contrast to other cryptocurrencies FC2 does not implement any mining or minting (aka. staking) 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. To run a CVN one needs to complete a certification procedure which is called **node certification procedure** (in short **NCP**) 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 definition of the NCP is out of the scope of this document and will be defined in a separate document. In the long run the NCP should be powered by a reputation system.

There is no reward for block creation (no coinbase/stake transaction). Therefore the money supply does not change over time and is fixed at the time we migrate to FC2. Nevertheless, the transaction fees go to the respective block creators to compensate their efforts for running a CVN.

Certain chain parameters, e.g. the transaction fee will be dynamically adjustable (without the need of releasing a new wallet version) by democratic community consensus. The FairCoin team needs the approval (digital signatures) of a high percentage of all the active CVN.

2 Block generation

Block generation takes place in a collaborative way. All CVN work together to bundle pending transactions into transaction blocks. These blocks can only be created by CVN every 3 minutes. Which CVN will generate the next block is determined by its **time-weight**. The time-weight describes how much time has passed since a CVN created its last block. If for example CVN **A** created a block 50 blocks ago and CVN **B** created it 55 blocks ago CVN **B** will be chosen to create the next block in the network. There can always only be exactly **one** CVN with the highest time-weight. If a **new** CVN joins the network for the first time it will be elected to create the next block. Between two blocks only one new CVN can join in.

Block generation is performed in 3 phases. New transactions are accepted during all these phases.

2.1 Transaction accumulation phase

In this phase all nodes relay transactions they receive from other nodes to any node they are currently connected to. This phase lasts at least 170 sec. If there are no pending transactions in the network it takes as long as the next transaction hits the network. In other words, this phase only ends when there is at least 1 pending transaction in the network.

2.2 Time-weight announcement phase

In this phase each CVN determines its **own** time-weight based on the local block chain information and announces it to all other connected nodes. Announcement messages are relayed by all nodes just like transactions. The higher the nodes time-weight the sooner the announce message is sent to the network according to the following simple formula:

$$delay = 10 - \left(\frac{10 * otw}{tn}\right)$$

Where:

delay is the *time* in seconds *to wait* before a CVN sends its own time-weight
otw is the CVN calculated *own time-weight*
tn is the *total number* of active nodes
10 is the constant of ten seconds, which is the duration of this phase

This will greatly reduce the amount of announcement packets sent over the network because if a CVN receives and correctly validates a time-weight announcement message from an other node with a higher time-weight it will not send its weight to the network.

Every CVN verifies that each time-weight announcement it receive is correct using the local block chain data (bogus announcements are discarded and a DoS ban score of 50 is proposed).

Time-weight announcements are used to determine the node with the highest time weight that is **currently connected** to the network.

This phase starts 10 sec. before the actual block target time.

2.3 Block creator election phase

This phase starts right after the Time-weight announcement phase. Every CVN determines the CVN with the greatest time-weight according to the announcements it received. It then signs and sends their candidate vote message to the network, which is relayed by every node just like transactions.

This phase has no defined length. It stops once the elected CVN has received enough vote messages for its own id from over 90% of all active nodes. This is the point in time when the collaboratively-elected CVN finally **creates the next block** in the chain containing all pending transactions from the so called “rawmempool”. Also parts of the signed vote messages are incorporated into the block to prove that optimally 100% but at least 90% of all active connected nodes agreed on the elected CVN.

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 each 3 minutes (180 sec.). Transactions are confirmed after they have been added to a block. If there are no pending transactions **no further blocks are created**, which will not happen anymore after FairCoin has been widely adopted.

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 full fill these rules.

1. The system must be connected to the Internet all the time (24/7) and the TCP port 46392 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, preferably pool.ntp.org to ensure that the system time is always correct
3. The entity must have an account at the FairCoop web site
4. The wallet software must be configured with certification data issued by FairCoop

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

4 Node certification

But why would we need certification at all? A decent certification procedure ensures that a high percentage of all CVNs are **honest** creator nodes. At the moment the author sees no easy way of ensuring that each node has only **one** identity without a well established reputation system. If every node was a creator node a skilled attacker could modify the client software in such a way to create thousands of different identities and could then perform numerous different attacks against the network.

5 Transaction fees

The transaction fees go to the node which created the block. Transaction fees exist to avoid block chain spam and give block creators a small reward for taking the effort to leave their node running and pass through the certification procedure. Fees should be dynamically adjustable to satisfy any change in the value of FairCoin.