The Proof-of-Cooperation Blockchain FairCoin

Thomas König, Enric Duran, Niklas Fessler, Roland Alton
tom@fair-coin.org, enric@fair-coin.org, niklas.fessler@gmial.com, roland@alton.at

White paper version 1.3 (February 2022)

Abstract. FairCoin is a mature blockchain project with a focus on ecology and sustainability. Blocks are created in cooperation, by so called "co-operatively validated nodes" (CVNs). The proof-of-cooperation (PoC) power consumption is negligible compared to mining and minting found in other blockchain mechanisms. To avoid spam in the blockchain and cover operation expenses, the creator of a block earns a very low transaction fee. Operational parameters such as the fee can be adjusted dynamically by chain servants in accordance with a consensus based assembly decision. Several communities have built tools and established markets to foster a fair global economy with FairCoin.

1 Introduction

FairCoin[1] has several faces. First of all, FairCoin is an implementation of an innovative and ecological blockchain mechanism based on the proof-of-cooperation algorithm. Secondly, by using FairCoin in various projects and markets, assets can be stored and be transferred. Thirdly, FairCoin is a tool for several communities to support a cooperative economy around the globe. In this paper, we will be focusing on the first aspect and will be explaining the technology and the governance model. FairCoin v1, which was used from 2014 until mid 2017 relied on mining and minting to secure the blockchain. Both mechanisms are widely used, but consume a lot of energy and mechanisms such as proof-of-stake advantage the rich and thus can not be considered as fair.

The underlying blockchain mechanism was refurbished for version 2 to make it a fair,

[1] https://faircoin.world

secure, resources-saving and decentralized block chain-based asset. It is based on cooperation between nodes and not on competition, which provides a much better efficiency. FairCoin v1 has been transferred on July 18th 2017 to FairCoin v2, which is a fork of the Bitcoin Core version 0.12[2] with heavy modifications. The blockchain status has been analysed[3] at the FairCoin wintercamp in January 2022 and can be considered in a healthy and secure state.

2 Economic Aspects

Whilst FIAT money supply is controlled and flooded by central banks[4] and is being created out of thin air by banks when providing credit[5], and whilst most cryptocurrencies' number of coin grow with mining rewards, FairCoin does not create any new coins[[6]. CVN's do not need to create new coins in order to provide security to transactions. In the early days one fifth of the FairCoins have been frozen in funds to be used for social and ecological inovations: the Global South Fund, Commons Fund, Technological Infrastructure Fund and Refugees Fund. As of 2022, the governance of those funds shall be transferred from the non-formal FairCoop community to a formal organisation.

By fixing the supply, FairCoin becomes stronger at the level of store of value for the solidarity economy, cooperatives and regional initiatives. Through the FairCoin blockchain - besides being a currency in itself - FairCoin will be a perfectly adapted platform to be used also by social currencies worldwide with no obligation to abandon their own principles.

With support several communities, FairCoin users find an environment of synergies at multiple levels, which allows them to advance their goals more rapidly. The FairCoin Circular Economy Group facilitates the use of P2P technologies[7], which facilitates its daily use and its interoperability with other currencies and payment systems. This in turn, may 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. The FairCoin blockchain is also considered as a generic tool for managing common good assets.

FairCoins have been heavily used in 2017 and 2018 by the former FairCoop community in countries like Spain, Italy or Greece. Whilst FairCoin was de-listing from some crypto exchanges over the past years, the FairCoin wintercamp in 2022 is aiming again at to

[2] https://bitcoin.org/en/bitcoin-core

[3] Blocks, payloads and CVN statistics can be observed at block explorers such as https://chain.fair.to/

[4] https://policyexchange.org.uk/an-overdue-political-debate-monetary-policy-and-the-role-of-central-banks/

[5] This is a controversial issue, as banks say they have the debt in their books. Fact is, that they can issue much more credit then they manage from savings, see e.g. https://www.youtube.com/watch?v=SA9UkHhFU6g

[6] The circulating supply has been frozen at 53.193.831 FairCoins when migrating from FairCoin v1 to FairCoin v2.

[7] https://p2pfoundation.net/infrastructure/our-guiding-principles

get FairCoin listed on more exchanges[8].

3 Node Network

The blockchain network consists of full nodes and cooperatively validated nodes (CVN). All nodes secure the network by validating all the transactions in the network and put them into a transaction block chain. Blocks are created in a round-robin manner every three minutes[9] by one of the CVN's. A CVN is a standard FairCoin core client, equipped with a hardware dongle (FASITO) and enabled as a CVN in a chain servant session. Every node is unique.

3.1 CVN Requirements

For the FairCoin main blockchain the operation of CVNs is fully decentralized. CVN operators are only known by their nicknames in chat groups. Candidates for running a CVN need to follow a combined p2p-consenus certification procedure. First of all, the candidate has to prove active involvement in one of the communities that is using FairCoin. Tasks like supporting a local node or contributing to a technical, management or communication issue is being reported by the candidate in an assembly and needs to be confirmed by at least two active members of the community. This is to ensure an alignment with cooperative and ecological values and a basic understanding of the technology. For 2022 it is proposed that two fixed dates per year will be set for accepting new CVN candidates. Furthermore, any CVN operator has to fulfil technical requirements[10]:

1. The system must be connected to the internet and the TCP port 40404 must be reachable by all remote nodes from the internet at any time.
2. The system must use a public NTP server[11] to synchronise its system time to.
3. The CVN and routers must be available 24/7 and ideally backed up with a UPS[12]
4. Monitor the CVN availability[[13] . Main downtime reasons are operating system update issues. In case of lack of interest of a CVN hoster, the CVN may be offboarded by chain servants after a cooling off period.

[8] FairCoin will be made available at the crypto exchange tulipex.io mid 2022

[9] The 180 seconds block time is an adjustable parameter.

[10] For a detailed requirements list see https://github.com/faircoin/faircoin/blob/master/doc/CVN-operators-guide.md

[11] e.g. pool.ntp.org

[12] Uninterruptable Power Supply, recommended for areas with unreliable electricity supply

[13] After more than four year of operations of the FairCoin v2 PoC blockchain we can see that even with some downtime of some of the 20 CVNs is absolutely sufficient to keep the network running smooth. Source of data: https://chain.fair.to/cvnstats

3.2 FASITO Hardware Device

To achieve maximum security for the FairCoin network the private key of a CVN, that is required to create and sign blocks, is generated in a hardware device which we call FASITO[14]. The device is able to create EC-Schnorr4.2 partial signatures. It is based on the Teensy3.2 USB development board[15] which features a 32 bit ARM processor and memory protection. It is secured by a six numbers pin code. After three invalid tries the card is locked and must be returned to the FairCoin development team to unlock. It can be unlocked only by an owner of one of three administration keys. To reduce the risk that a CVN operator is being threatened to change the PIN by some offending party, a FASITO must not be deployed by the CVN operator him/herself, but by another CVN hoster or chain servant. As an additional measure to secure the network, we start in 2022 to distribute each of the FASITO chain administration keys among them.

4 The Proof-of-Cooperation Mechanism

Proof-of-Cooperation (PoC) is a consensus algorithm developed by Thomas König[16]. Every node must obey the same set of rules to maintain the networks integrity and security. All connected clients have the same data available to verify the state of the network. The FairCoin blockchain requires a limited number[17] of called cooperatively validated nodes collaborating with each other to create new blocks in a secure network. To assure the integrity of the CVNs, they are authorized by a social p2p-consensus mechanism. All CVNs of FairCoin are authorized by a general assembly collaboratively, whereas chain servants execute decisions. Candidates for operators of CVN need to apply and go through a peer process, however their real identities are not known. The private key is stored on a small device, called FASITO3.2. Its important, that the private key is non-retrievable. This ensures the integrity and confidentiality of the exchanged information. Dynamic blockchain values are stored in each block.

4.1 Creating and Proofing Blocks

Every CVN takes part in an iterative 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 when we've just received a new block from some other CVN.

1. 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

[14] FAircoin SIgnature TOken
[15] https://www.pjrc.com/teensy/
[16] Dornbirn, Austria in 2017
[17] Maximum allowed CVNs: 100, mid term target is 30-50, active operating CVNs see https://chain.fair.to/activecvns

of that node in the last couple of blocks. If the node was active, then this CVN will be chosen as the next block creator.

2. 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 with the EC-Schnorr algorithm for best efficiency:
   - 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 block
3. We send our signature out to the network, so everybody knows our opinion about how the chain should continue.
4. 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 passed. In the meantime we are busy collecting all the signatures of the other CVNs.
5. OK, block spacing time is over, so we check again which CVN should proceed. And it happens to be our turn, great!
6. 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 17 and we received 18 - so one of the CVNs just came back online, awesome! We have more than enough.
7. 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.
8. 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.

Although this iteration looks like a simple round-robin-system, we are facing some complexity when handling exceptional cases. E.g. a CVN could go offline at any time, or a split-brain situation could occur in the network.

4.2 Efficient EC-Schnorr Signing of Blocks

The security of this algorithm is based on the intractability of certain discrete logarithm problems. The private key is generated on the FASITO hardware device and is non-retrievable. This is mostly for two reasons:

- Prevent accidentally or maliciously starting more than one CVN with the same credentials which would interfere with the network.
- Prevent key cancellation attacks.

The EC-Schnorr multi-signature system is processed in 3 phases:

1. All CVNs use a random nonce pair, exchange the public part to every other CVN, and keep the private part secret on the FASITO.
2. All CVNs combine the public nonce of all other CVNs and create their partial signature for the current chain tip.
3. The agreed block creator combines all partial signatures into one and puts it into the block.

4.2.1 1st Phase: The nonce exchange

Because this multi-step signature system is rather complex and has to happen in the time between the creation of two blocks, and also requires CVNs to send numerous messages back and forth, they pre-compute a number of nonce pairs into a nonce pool and share that with all other CVNs. This approach decouples the first phase from a time-sensitive process and thus makes our PoC mechanism more robust. Every nonce pool is associated with a chain tip and one nonce is used up per block height. If the pool is empty a new one is created and sent. This is done right after a new tip has been received.

4.2.2 2nd Phase: The partial signature

By using the nonce pool, CVNs can create their partial signature right away after they have received a new block and don't have to wait for the public nonces to arrive. They first combine the public nonces of all other nodes for a given height and then use this sum of nonces and their private key to sign the following hash.
hash = H (hashPrevBlock || nNextCreator)

4.2.3 3rd Phase: Combining the signatures

The block creator validates and combines all the received partial signatures into one 64 byte EC-Schnorr signature which is verifiable against the signed hash and the sum of all public keys of the participating CVNs. This makes PoC validation very efficient because even if fifty CVNs co-signed the proof only one signature (64 bytes) needs to be stored and verified in the blockchain.

5 Data in the FairCoin Blockchain

The FairCoin blockchain is mainly used for storing and transferring assets. A few blocks hold adjustable parameters to keep the blockchain run smooth. They can be set in a chain servant session on demand.

5.1 Chain servants

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. To set parameters, chain servants have to meet in a chat channel and co-sign new instruction data to fine-tune blockchain parameters[18]. The node software reads those parameters and adapts its behaviour accordingly. The chain servants execute what is being decided in the assembly, where they are also appointed. For new instructions to be accepted by the network, these instructions must be signed by a defined minimum number of representatives[19]. This number is dynamic and stored as well in the blockchain and can be changed, as decided in the virtual assembly. The chain servants can neither stop the blockchain nor re-assign or add any coins. They are technical care-takers, just like a maintainer of an elevator checking screws and putting some oil to the door opening mechanism.

5.2 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 FairCoin block:

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

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 blockchain based on the FairCoin source code there is an option to increase the coin supply. Please note that this feature is not used in the main FairCoin blockchain. It is disabled at compile time by default. So the next paragraph applies

[18] For details see the chain servant's guide https://github.com/faircoin/faircoin/wiki/Chain-administrators-guide

[19] 5 out of 8 chain servants have to co-sign within a block period (currently 180 seconds

to forks of the FairCoin blockchain only (e.g. for research or development purposes): If it is decided to increase the coin supply all of the chain servants 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.

5.4 Parameters of Blockchain

To add or remove CVNs and chain servants or update the dynamic chain parameters at least the currently defined minimum number of chain servants have to sign the corresponding command which is then injected into the network via the wallets RPC interface. We would like to note, that those adjustments are not crucial for the PoC mechanism to continue, but it may run more sleek without the need to change the node software, especially if the number of transactions grows in future.

6 Conclusion

FairCoin is a socio-technical sculpture which has been implementing various innovations, both on social and technical levels. After more than four years of smooth operations[20], the PoC blockchain mechanism has proven to work in managing funds and for day-to-day transactions. Based on requirements of the various communities, additional features will be implemented or are already available as prototypes on the FairCoin testnet[21].

6.1 Micro payments

The high efficiency of the FairCoin network, trusted node relations, very low energy cost[22] and consequently low fees, nominates FairCoin as a candidate for micro payments. Usage scenarios are the gift economy, currency substitute in the global south or online remuneration systems.

6.2 Distributed sub chains and multi-currency

FairChains allows to create a token within the FairCoin main chain and runs alongside it. Smart contract rules expressed as OmniLayer functions provide a way to create chains with new properties. Such a sub-chain could 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 or a registry of commons goods. A smart contract could also define credit

[20] All balances from the PoW/PoS FairCoin v1 to the new PoC FairCoin v2 blockchain have been transferred on 18th of July 2017.

[21] Any FairCoin node can be configured to work on the FairCoin testnet blockchain.

[22] Most CVNs run on a RasperryPi consuming 8 Watts each, some on more powerful hardware consuming 30 Watts each. The total FairCoin blockchain network consumes only 200 Watts or 1,8 MWh per year. Solana requires 11 GWh per year and BitCoin 128 GWh per day.

relations among several partners or put options when exchanging virtual currencies to FIAT money.

7 Sources

7.1 Open Source Code

FairCoin node https://github.com/faircoin/faircoin.git
FairCoin wallets: http://download.faircoin.world/
FASITO https://github.com/faircoin/Fasito.git

7.2 Homepage

FairCoin homepage with comparisons and FAQs: https://fair-coin.org
FairCoin proof-of-cooperation mechanism https://github.com/faircoin/faircoin/blob/master/doc/on-proof-of-cooperation.md

7.3 Changelog

The white paper version 1.3 (February 2022) has integrated experiences made during more than four years of operations of the FairCoin blockchain, better explained the FASITO key management and the role of chain servants and reflected the usage by several communities. The white paper version 1.2 (July 2018) is based on the initial version 1.1 (June 2016) with an extended description of PoC and economic aspects, explaining Schnorr and chain admin roles, added more references, replaced logo, two additional authors.

7.4 License

This white paper is licensed under CC-by-sa[23] Thomas König, Enric Duran, Niklas Fessler, Roland Alton.

[23] https://creativecommons.org/licenses/by-sa/4.0/