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 1.2 (July 2018)

Abstract. FairCoin facilitates a next generation approach for creating blocks in a blockchain. Blocks are created in cooperation, by so called "cooperatively 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 admins in accordance with a consensus based assembly decision. The FairCoop community has built several tools and a market to foster a fair global economy with FairCoin.

1 Introduction

FairCoin 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, we created an asset to transfer value. Thirdly, FairCoin is a tool for the FairCoop[1] community 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 1, 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 advantage the rich and thus can not be considered as fair.
Therefore, the whole blockchain was refurbished for version 2 to make it a fair, secure, resources-saving and decentralized block chain-based asset. It is based on cooperation

[1] https://fair.coop

between nodes and not on competition, which provides a much better efficiency. FairCoin v2 is a fork of the Bitcoin Core version 0.12[2] with heavy modifications.

2 Economic Aspects

Whilst FIAT money supply is controlled and flooded by central banks[3] and is being created out of thin air by banks when providing credit[4], and whilst most cryptocurrencies' number of coin grow with mining rewards, FairCoin does not create any new coins[[5]. CVN's do 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, cooperatives and regional initiatives. Through the FairCoin block chain - 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 of the FairCoop community, FairCoin users find an environment of synergies at multiple levels, which will allow them to advance their goals more rapidly. The FairCoop Circular Economy Group facilitates the use of P2P technologies[6], which will facilitate 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. Hence, we see the FairCoin blockchain also as a generic tool for managing the common good.

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[7] by one of the CVN's. A CVN is a standard FairCoin core client, verified in the network by FairCoop. Every node is unique.

---

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

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

[4] 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 have from savings, see e.g. https://www.youtube.com/watch?v=SA9UkHhFU6g

[5] The circulating supply has been frozen at 53.193.831 FairCoins when migrating from FairCoin 1 to FaoirCoin 2.

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

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

3.1 CVN Requirements

For the FairCoin main blockchain the operation of CVNs is 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 the FairCoop community. Tasks like supporting a local node or contributing to a technical, management or communication issue is being reported by the candidate in a FairCoop assembly and needs to be confirmed by at least two active members of the community. This is to ensure an alignment with cooperative values and hacker ethics. The open FairCoop chat assembly[8] then accepts the application by consensus. Furthermore, a CVN operator has to fulfil technical requirements[9]:

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[10] to synchronise its system time to.
3. The CVN and routers must be available 24/7 and ideally backed up with a UPS[11]
4. Monitor the CVN availability[[12]

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[13]. The device is able to create EC-Schnorr4.2 partial signatures. It is based on the Teensy3.2 USB development board[14] 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.

4 The Proof-of-Cooperation Mechanism

Proof-of-Cooperation (PoC) is a consensus algorithm developed by Thomas König[15]. Every node must obey the same set of rules to maintain the networks integrity and

[8] Since 2016 scheduled every 3rd Thursday of the month at 7 p.m. CET on Telegram and mirrored to https://fairchat.net/channel/faircoop-assemblies . Any frequency or date change would be agreed in the assembly and announced on various channels.

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

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

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

[12] After one year of operations of the FairCoin PoC blockchain we can see that an 98% average uptime among 19 CVNs is absolutely sufficient to keep the network running smooth. Source of data: https://chain.fair.to/cvnstats

[13] FAircoin SIgnature TOken

[14] https://www.pjrc.com/teensy/

[15] Dornbirn, Austria in 2017

security. All connected clients have the same data available to verify the state of the network. The FairCoin blockchain requires a limited number[16] 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 the FairCoop general assembly collaboratively, whereas chain admins execute decisions. Candidates for operators of CVN need to apply and go through a peer process, however their real identities is 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 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!

[16] Maximum allowed CVNs: 100, mid term target is 30-50, active operating CVNs see https://chain.fair.to/activecvns

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 (see below) 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 The FairCoin Blockchain

The PoC mechanism is being used with the FairCoin blockchain, which is mainly used for storing and transferring assets. 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. Chain administrators may co-sign new instruction data to fine-tune blockchain parameters[17]. These administrators execute what is being decided in the FairCoop 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[18]. This number is dynamic and stored in the block chain and can be changed, as decided in the assembly.

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 FairCoin block:

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

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

[18] 5 out of 8 chain admins have to co-sign within a block period (currently 180 seconds

5.2 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 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.

5.3 Parameters of Blockchain

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. 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 one year of smooth operations[19], the PoC blockchain mechanism has proven to work in managing funds and for day-to-day transactions. Based on requirements of the FairCoop community additional features will be implemented in the near future or are already available as prototypes on the FairCoin testnet[20].

6.1 Application areas

FairCoin is the monetary base system for *FairCoop* - The Earth Cooperative for a Fair Economy. FairCoop is a community to transfer knowledge and develop tools that enable everybody to participate in a fair global economy. FairCoin plays a central role within the FairCoop ecosystem with online markets and point of exchanges and sales in more than 50 local nodes worldwide[21].

[19] All balances from the PoW/PoS FairCoin 1 to the new PoC FairCoin 2 blockchain have been transferred on 18th of July 2017.
[20] Any FairCoin node can be configured to work on the FairCoin testnet blockchain.
[21] as of July 2018, 55 local nodes are listed on https://map.fairplayground.info/map-localnodes/

6.2 Micro payments

The high efficiency of the FairCoin network, trusted node relations, low energy cost 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.

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

6.4 Restraining Volatility

FairCoin is not made for speculators, but for participants on markets to trade real goods and services. An official exchange value is being set in public assemblies[22]. To escape pump and dump games, the FairCoin community is usually rejecting listings on big exchanges, such as Bittrex [23]. Fiat money from FairCoin sales is being used to stabilise the value by buying FairCoins from people outside the FairCoop ecosystem. Various concepts for stabilizing the FairCoin currency are being discussed[24].

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

[22] https://fair-coin.org/en/create-value
[23] https://fair-coin.org/en/bittrex-delisting
[24] Stability discussion in chat https://fairchat.net/channel/faircoin-economy-strategies?msg=uXs3eDYu9kbP89NGv and pad https://board.net/p/r.1823fb01c762e7d402ae580993375548 as of July 2018

7.3 Changelog

This white paper version 1.2 is based on 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.