ForCash Cryptocurrency

Whitepaper v 1.1

update 2019-02-17

2019-01-01

Content

Abstract

Cryptocurrency ForCash is built on a fully decentralized peer-to-peer network. It is a pre-mined cryptocurrency in a fixed number of 1 billion coins, so it is a deflationary one. Like other cryptocurrencies, it is based on its own and publicly available blockchain. ForCash uses the Proof of Stake consensus.

1 Blockchain

Blockchain is a special kind of distributed decentralized database so-called accounting book. It keeps an ever-expanding number of records that are protected against unauthorized interference both from the outside and from peer-to-peer nodes themselves. The ForCash Blockchain encrypts and keep transactions made by users. In combination with cryptography it makes possible to ensure the atomicity of operations and to prevent unauthorized transactions.

Blockchain implementation consists of two types of records: transactions and blocks.

Transactions represent data embedded in the blockchain by users, blocks are records to confirm when and how a particular transaction was added to the blockchain. Transactions are created by users who use the system as an accounting book. Blocks, on the other hand, are created by miners who use software to create blocks.

Transactions created by users are transmitted from node to node, depending on who has the connection with whom. A valid transaction is a transaction that has the correct electronic signature of the user. It spends a disposal from an existing wallet to which the user demonstrates true ownership, and at the same time fulfills several other conditions, such as the appropriate fee for the miners.

Main advantages of ForCash blockchain are:

- Ability of a large number of nodes to reach a consensus on the current blockchain status.
- The ability of any node to decide with an acceptable degree of certainty that the transaction entered into a blockchain belongs to block or not. After a certain period of time decides with a reasonable degree of certainty whether the transaction is valid and integrable into the blockchain permanently and whether there has been a collision between two transactions. This is important to solve the double-spending problem.
- A sufficient quantity of measures that prevents attackers from editing or transcribing of transactions.
- An automatic form of conflict solution that ensures that invalid transactions (such as trying to spend the balance more than once) never become part of a confirmed blockchain.

The first block of ForCash blockchain „Genesis block“ was generated on the 1st of January, 2019.

2 Decentralization and nodes

Any device in the ForCash Network running ForCash software can send transactions or blocks to the network and is a regular node. Each node in the ForCash network has the ability to process and transmit transactions and block information.

Thus, no central element is needed to run the ForCash cryptocurrency, the peer-to-peer network ensures full decentralization of ForCash. With the peer-to-peer network, the ForCash infrastructure is robust and will exist as long as there is at least one node connected to the network.

Each node in the ForCash decentralized network contains a complete or partial copy of the blockchain. This solves the problem of a centralized database that other technologies use, such as banking or PayPal. While a standard accounting book only passively records money transfers, bank checks, or payment orders that exist independently of this book, in the case of ForCash tokens / currency coins and blockchain are firmly linked. Blockchain can be considered as the only place where ForCash tokens / coins exist.

Transactions in the form of "payer X sends Y currency coins to Z recipients "are widened across the network using software operations and asymmetric cryptography. Any network node is able to verify this transaction in a valid block, add a copy of into accounting book and forward these increments to other nodes.

Blocks are authenticated as they are received from other nodes. In cases where block validation fails, nodes may be temporarily blocked to prevent invalid block distribution. Each node contains a built-in defense against DDOS (Distributed Denial of Services) that limits the maximum number of requests distributed from one node.

3 Proof of Stake (PoS)

Proof of stake (PoS) is a proof of ownership of the share of the ForCash tokens.

It is a type of algorithm that aims to achieve a distributed consensus in a blockchain network. Unlike Proof of Work (PoW) cryptocurrencies, where the algorithm rewards participants who solve complicated cryptographic puzzles to verify transactions and create new blocks (i.e. mining). In PoS based cryptocurrencies the creator of the next block is chosen randomly. The probability of choosing depends on its amount of tokens (stake). This is not the percentage representation of the computing power, but the percentage representation of the amount of "Stake" coins - the effective balance of coins in the account.

Effective balance is the sum of FCH tokens / coins that have equal or over 1 440 confirmations.

Sufficient decentralization of payment confirmators (miners) is ensured by the fair distribution of coins among users, ensuring that no user owns more than 51% of the coins (Stake) – analogically to 51% PoW computing power.

4 Tokens

There is a total of 1 billion FCH tokens that are divisible into 8 decimal places. All tokens were released when the Genesis block was created (the first block in the FCH blockchain). This first block left the Genesis account with a negative balance of FCH 1 billion. The existence of anti-token on the Genesis account has several features:

- Genesis account can not issue any transactions because it has a negative balance and can not pay transaction fees. For this reason the publicly available security phrases of the Genesis account for anyone interested is:
  „house kept large puff cell weapon brave problem leaf torment enough art“.
- All Tokens sent to the Genesis account are effectively destroyed because they would decrease the negative balance of this account.

The choice of word "token" is based on the understanding of current cryptocurrencies, which do not focus only on the original payment system, but try to be a basic protocol with a wider use potential. The same principle is pursued by the ForCash, which besides the payment system, offers a number of other uses of its blockchain technology.

5 Blocks

As in other cryptocurrencies, the accounting book of all ForCash transactions is created and maintained as a mutually linked blocks, known as blockchain. This accounting book provides a permanent record of all the transactions that have taken place and also determines the order in which the transactions took place. A blockchain copy is maintained on each ForCash node. FCH accounts can participate in mining if they are "unlocked" (the user delivers the FCH software to the private key of their account). Such an account is then able to generate blocks if there is at least one incoming transaction to that account, with at least 1 440 block confirmations. Any account that meets these criteria is referred as an active account.

In ForCash can each block contain up to 255 transactions. It is a 192-byte header containing identifying parameters. Each transaction in a block is represented by maximum 176 Bytes and the total block size can be up to 45 KB. The new blocks are generated by miners approximately every 60-80 seconds. The ForCash peer-to-peer network is thus able to verify up to 367 200 transactions a day (1 block / minute = 1440 blocks).

Each block include following parameters:

- Version, height (sequence), identification
- Time stamp in seconds from creation of the Genesis block
- ID of creating account including its public key
- ID and hash of previous block
- Number of transactions in block
- Total FCH amount represented as a sum of transaction amounts and fees in block
- All transactions and their parameters in the block including their ID
- Payload and hash of data input
- Signature of the block
- Base target value and cumulative difficulty

5.1 New block creation process

In order to derive which account will be allowed to generate a new block and which block will be considered as authoritative in the case of conflicts, three key parameters are used: Base Target value, Target value, and Cumulative difficulty.

a) Base target value
All active FCH accounts "compete" to try to generate a hash value that is lower than the Base Target value to create the block. This Base target value varies from a block to a block and derives from the Base Target value of the previous block multiplied by the time period in seconds that was required to create this block.

b) Target value
Each FCH account counts its own Target Value that is based on its current effective balance. This value is calculated as:

$$T = T_b * S * B_e,$$

where:

T is new Target value

T_b is Base target value

S is time in seconds since last generated block

B_e is Effective account balance

This formula shows that the Target value increases with every second that has passed from the timestamp of the previously generated block. The Base target value and time are the same for all accounts that compete for block extraction. The only different parameter for competing accounts is the Effective account balance.

c) Cumulative difficulty
Cumulative difficulty is derived from Base target value:

$$D_{cb} = D_{pb} + (2^{64} / T_b),$$

where:

D_cb is the difficulty of the current block

D_pb is the difficulty of the previous block

T_b is Base target value (of current block)

ForCash provides efficient mining without the need to build computing power and any user who has a non-zero effective balance can participate.

The miners are trying to create a block that confirms and integrates valid transactions into a blockchain. Miners are motivated to forge with reward - transaction fees, which are paid to any miners who correctly validate the transaction.

The peer-to-peer network user who generates the block will be rewarded for all transactions confirmed by this block. FCH blockchain technology allows you to place a transaction into a blockchain with a minimum charge of 0.01 FCH. One block can confirm up to 255 transactions, maximum reward for miners is = 255 * 0.01 = 2.25 FCHs, which are automatically credited to the mining account within the blockchain.

The effective account balance indicates the probability that the user will create the block in competition against all the effective balances that are part of the mining process.

5.2 Mining algorithm - forging

Each block in the blockchain has the "signature of the previous block" parameter. To participate in the mining process an active account is required to sign the signature of the previous block using cryptographic methods by using its public key. This creates 64 Bytes signature, which is then hashed with SHA256 function. The first 8 Bytes of the resulting hash is converted to a number labeled as an account hit value. The hit value is compared to the current Target value. If the calculated hit value is lower than the Target value, another block can be generated.

As stated in the formula for the Target value, Target value increases with each passing second. Despite a small number of active network accounts, a new block is finally generated by one of the accounts, as the target value grows to a large number. As a result it is possible to estimate the time needed to confirm a new block by any account, by comparing the hit values of the account with the Target value.

The last point is very important because each node can get the Effective balance of any active account. It is possible to pass all active accounts and calculate the Hit value of all such accounts. This means that it is possible to predict (with acceptable precision) which account gets the right as the next one in the order to confirm (mine) the block.

When the active account gets the right to confirm the block, it collects up to 255 available unverified transactions and creates this new block with all the appropriate parameters. The new block is then sent to all nodes in the network as a blockchain candidate. The payload, creator of the block and all signatures in each block can be verified by all the receiving nodes in the network.

In a situation when multiple blocks are generated the nodes select the block with the highest Cumulative difficulty as the authoritative block. Because data is shared between nodes, forks (unauthorized blockchain fragments) are recognized and removed (based on the Cumulative difficulty of each fork).

6 Transactions

Transactions are the only way by which FCH accounts can change their balance and status. The record of each transaction is permanently stored in the network after the transaction has been integrated into the block.

6.1 Fees

Transaction fees are the primary mechanism by which miners are encouraged to generate new blocks and to redistribute tokens into the network. Each transaction requires a marginal fee of 0.01 FCH. Fees are also form of defense to limit the intent to flood the network. Such an attack is not worth it because of its financial difficulty, which is simply quantifiable (number of transactions * fee). When a mining account creates a block, all of the transaction fees included in this block are credited as a reward for this account. In situations where the number of unconfirmed transactions exceeds a number that can be placed into a block, miners will select transactions with the highest fees. This suggests that transaction processing may favor transactions with a charge (fee) that is higher than the defined minimum.

6.2 Transaction Confirmation

All FCH transactions are considered unconfirmed until they are included in a valid block. Created blocks are distributed to the network by a node (and an associated account) that created them. The transaction that is part of the new block is deemed to be accepted and confirmed by a one confirmation. Once the following blocks are put into an existing blockchain each subsequent block adds another one confirmation to the transaction. If the transaction is not inserted into a block before its deadline, the transaction expires and is removed from the list of unconfirmed transactions.

6.3 Transaction Deadline

Each transaction contains a deadline parameter determined as the number of minutes since the transaction is distributed to the peer-to-peer network. The default value of the deadline is set to 1 440 minutes (24 hours). A transaction that is distributed into a network, but is not included in a block is marked as an unconfirmed transaction. The transaction may remain unconfirmed when the transaction data are damaged or all of the generated blocks have been filled with transactions that offer higher transaction fees.

6.4 Transactions

Categorization of transactions into types allows modular development of FCH without creating dependencies on other functions. This modular architecture thus supports the expansion of new functionality by implementing new types of transactions. The FCH protocol supports the following types of transactions, where each type determines the required and optional parameters of the transaction, as well as the method of its processing.

a) Standard payment
The basic feature is the ability to forward (pay with) tokens from one account to another. This is the most common type of FCH transaction and provides basic payment functionality.

b) Pseudonym, URI, variable
A pseudonymous system allows you to permanently assign any text string to a specified FCH account. FCH technology formalized the storage of these strings using JSON notation. As a result the pseudonym may be a user-friendly account naming (substitute of Reed-Solomon format), a uniform resource identifier (URI) or a fixed-value variable. The ability of a FCH blockchain to store any URIs allows you to create any number of decentralized services that are based on short and persistent strings. As an example we may use a Domain Name System (DNS).

c) Messaging
In the FCH blockchain messages up to 1,000 Bytes can be stored. Messages can be optionally encrypted using the AES algorithm. At the basic level, messages can be used for communication between users to form a decentralized chat system. However, the messages allow for an advanced application - they can store structured data such as JSON objects that can be used to trigger additional services that are built on ForCash technology (Smart Contracts).

d) Balance leasing
This type of transaction allows you to lease to another account the effective balance (mining power) used for mining. Tokens transferred by this transaction do not allow the tenants to dispose with the amount in any way. Using a leased effective balance allows the owner to temporarily reduce the effective balance and raise it to the payee's account.
Balance Leasing is introduced for safety reasons, so users with high balance do not need to indicate their security phrase (private key) during mining. It will be provided only by a tenant who may have much lower balance in his account. The lessor thus reduces the risk of possible loss.
The leased balance does not affect the lessor's account in any way, except for the opportunity to mine (forge). The effective balance can be leased to a minimum of 1,440 blocks and a maximum of 32,767 blocks. After a defined number of blocks has passed the leased effective balance is automatically credited back to the lessor's account.

6.5 Transaction creating process

The creation and transaction processing is as follows:

1. The sender defines the transaction parameters. Selects the type of transaction to which specific parameters apply, but the following parameters must be met for all:
    - Sender´s private key
    - Transaction fee
    - Transaction deadline
    - Reference
      transaction (optional)

2. All specified parameters are verified. For example, a transaction fee may not be less than or equal to zero; the latest date for the transaction may not be less than one minute in the future according to the current time; if a referenced transaction is selected, the current transaction must not be processed before the referenced transaction.

3. If no error occurs, process continues as follows:
   a) The public key of the account is derived from the security phrase.
   b) Validation of additional account information (transaction-dependent):
      - Account balance may not be zero or less.
      - An unconfirmed balance may not be less than the sum of the transferred amount and the transfer fee

4. If the sender's account has a sufficient balance:
   a) A new transaction of the appropriate type will be created and all specified and completed parameters will be included. A unique transaction ID is created.
   b) The transaction is signed using the private key of the sender.
   c) Encrypted transaction data is embedded in a message containing instructions for processing a transaction in a peer-to-peer network.
   d) Transaction is distributed (broadcasted) to all nodes in the network.
   e) Delivery of the response with the result of the operation:
      - Transaction ID, if the creation and processing process has gone correctly
      - Error code and error message, if a parameter check has failed

7 Accounts

The native e-wallet serves as a client application that allows the user to access and work with their account, the so called ForCash address/account (FCH address). The FCH address can only be accessed on the basis of the correct input of security phrase.

The security phrase consists of 12 randomly selected English words. These words are selected from a 4,000 word database. There is 4 000 ^ 12 combinations, which is equivalent to about 142 bit password. The phrase can be selected manually when the check is made on at least 35 alphanumeric characters.

From the security phrase, a private key, a public key and also a FCH address are derived using the SHA256 hash function and the Curve25519 cryptographic function. This principle allows you to access a FCH address from any desktop wallet without having transfer a private key, a so-called brain wallet.

The FCH address is a unique 64-bit number. For user friendliness the FCH address is recoded to: FCH-XXXX-XXXX-XXXX-XXXXX (the prefix is always FCH) where Reed-Solomon error-correction codes are used to detect and correct errors in the FCH address.

Advantages of Reed-Solomon addresses:

- Probability of collision of randomly generated FCH addresses is 1: 1048576 (20-bit redundancy)
- Allows to correct up to 2 characters mismatch in the address
- Detects up to 4 characters mismatch in the address

The process of generating a FCH address from a security phrase:

1. The private key is derived from the security phrase using the SHA256 hash function.
2. From the private key, the public key of the account is derived using the Curve25519 cryptographic function.
3. The public key is hashed using the SHA256 function to derive the account ID.
4. The first 64 bits of an account ID represents the FCH address.
5. The resulting FCH address is created by encoding a 64-bit number using the Reed-Solomon error-correction code and the prefix "FCH-" is attached.

If a user access his/her account for the first time, this account is not currently protected by its public key. Once the user performs the first outgoing transaction from this account, its 256-bit public key derived from its security phrase is then stored in a blockchain and protects his/her account. The address space for public keys is 2 ^ 256. So it is larger than the address space for account numbers 2 ^ 64. There is no assignment of 1:1 security phrases and account numbers and there may be collisions.

However, collisions are detected and preceded by the following: Once a security phrase is accessed and the account has a 256-bit public key, no other public-private key pair can access this account.

7.1 Types of account balances

Each account has several types of balances, each type serving the specific purpose. Several of them are used to create and process transactions.

a) Effective balance
It is used as the basis for the forging (mining) of an account. It consists of all the tokens on your account for time period of 1,440 blocks or more. This balance may be leased to another mining account.

b) Guaranteed balance
It represents the sum of all the tokens on the account for time period more than 1,440 blocks. Unlike an effective balance, the guaranteed balance cannot be leased to another account.

c) Balance
It is the sum of all transactions that have at least 1 confirmation (1 block).

d) Forged balance
Displays the total amount in FCH that was received as a result of successful forging of new blocks.

e) Unconfirmed balance
It represents the balance that is calculated as the Balance (c) minus the sum of all transactions that have not been confirmed yet.

8 Security

The exchange of cryptographic keys is based on the Curve25519 algorithm, which generates a shared secret with fast, safe, and efficient Diffie-Hellman elliptic curves. The EC-KCDSA algorithm is used for electronic signature. Both algorithms were chosen for their speed, security, and key size of only 32 Bytes.

8.1 Encryption algorithm

a) Alice sends an encrypted message to Bob

1. Calculation of Shared Secret:

   a. shared_secret = Curve25519(Alice_private_key, Bob_public_key)

2. Calculation of N initialization vectors (seeds):

   b. seed_n = SHA256(seed_n-1), where seed_0 = SHA256(shared_secret)

3. Calculation of N keys:

   c. key_n = SHA256(Inv(seed_n)), where Inv(X) are inverted all bits X

4. Encryption of plaintext:

   d. ciphertext[n] = plaintext[n] XOR key_n

b) Bob decrypts the received message from Alice

1. Calculation of Shared Secret:

   e. shared_secret = Curve25519(Bob_private_key, Alice_public_key)

2. Calculation of N initialization vectors (seeds):

   f. seed_n = SHA256(seed_n-1), kde seed_0 = SHA256(shared_secret)

3. Calculation of N keys:

   g. key_n = SHA256(Inv(seed_n)), where Inv(X) are inverted all bits X

4. Decryption of ciphertext:

   h. plaintext[n] = ciphertext[n] XOR key_n

9 Native wallet

ForCash cryptocurrency wallet is a software implemented as both server and client. It is written in Java and its installers are currently available for Windows 32-bit, 64-bit, MacOS and Linux operating systems. Cryptocurrency wallet software is available for download at www.forcash.app.

After installation and subsequent startup, the server automatically connects to the peer-to-peer network. The communication between all wallets takes place at port 7884. The client part of the wallet communicates with the wallet server part on the 7886 port using the API interface and creates and processes requests for the server part.

API interface can be used by external applications without necessity to use the client part of the wallet.

When a wallet is attached to the peer-to-peer network, blockchain automatic synchronization will start (it will be downloaded during the first run). In the "blocks" section, you can browse through all blocks (and transactions they have confirmed).

10 Usability

Active widening of coin utility leads to growth of the value for all users.

The goal is to create a ForCash community through partnerships with merchants and partners. The benefit for traders is the speed and verification of transactions. Payment options are handled both via the mobile application and the QR code, which will further increase user friendliness and enhance the project. The transaction fee is set at 0.01 FCH, which will be reduced to a competitive level, depending on the growth rate to provide a minimum financial burden, but also to cover the cost of sustainability of the system.

11 Main features

- Blockchain core – NXT source code / fork (under MIT license)
- Proof of Stake (PoS)
- Block size: up to 255 transactions
- Block time 60-80 seconds
- Token name: ForCash (FCH)
- Supply: 1.000.000.000 FCH
- Minimum transaction fee: 0.01 FCH

References

Bernstein, Daniel J. "Curve25519: new Diffie-Hellman speed records." *International Workshop on Public Key Cryptography*. Springer, Berlin, Heidelberg, 2006.

Conley, John P. *Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings*. No. 17-00008. Vanderbilt University Department of Economics, 2017.

King, Sunny, and Scott Nadal. "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." *selfpublished paper, August* 19 (2012).

Learn Cryptography — 51% Attack. (n.d.). Retrieved July 06, 2014, from http://learncryptography.com/51-attack/
Liu, Debin, and L. Jean Camp. "Proof of Work can Work." WEIS. 2006.

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008): 28.

NXT Wiki: https://nxtwiki.org/wiki/

Pilkington, Marc. "Blockchain technology: principles and applications." papers.ssrn.com (2015).

Pump and Dump in Crypto: Cases, Measures, Warnings. Retrieved February 24, 2018, from https://cointelegraph.com/news/pump-and-dump-in-crypto-cases-measures-warnings

Qin, W., & Zhou, N. (2010, 12). New concurrent digital signature scheme based on the computational Diffie-Hellman problem. The Journal of China Universities of Posts and Telecommunications, 17(6), 89100. doi:10.1016/S1005-8885(09)60530-6

Swan, Melanie. *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.", 2015.

The Nxt community. „Nxt Whitepaper“ *self-published paper,* July 12, 2014

Whitepaper:Nxt: https://nxtwiki.org/wiki/Whitepaper:Nxt

Wicker, Stephen B., and Vijay K. Bhargava, eds. *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.