FuturoCoin

A Peer-to-Peer Electronic Cash System for Instant Transactions

v1.0
31.01.2018

Abstract:

Bitcoin and other cryptocurrencies use a distributed network and database system called the blockchain to acquire consensus across all system participants. This approach requires time needed to confirm all pending transactions in the queue to protect against double spend attack. A double spend is the situation where an attacker tries to send a transaction to a merchant and at the same time sends the other one with the same coins to himself.

Confirmation time varies across hundreds of cryptocurrencies in existence. In Bitcoin it takes 10 minutes on average, but the number of confirmations needed depends on merchant security. It is assumed that to be fully certain one needs to wait up to 6 confirmations which takes an hour.

Today's world of e-commerce undoubtedly can not wait for such a long time with delivering the goods. **FuturoCoin** is created for resolving this problem and guarantees **instant** transactions with the **constant** fees at the competing level.

Contents

1 Introduction

What is cryptocurrency and what is FuturoCoin?

How does FuturoCoin work under the hood?

- Asymmetric cryptography
- Transaction
- Mining process

2 Dash as a codebase for FuturoCoin

Two-Tier Network

Instant payments

Low and constant transaction fees

Governance model

Advanced Security

3 FuturoCoin approach

Instant transactions

Total coin emission

Emission rate

Block reward allocation

PrivateSend functionality

Flat fee for all kinds of transactions

Big and growing community of supporters

Introduction

What is cryptocurrency and what is FuturoCoin?

When introducing **FuturoCoin** we need to understand better what cryptocurrency is and how FuturoCoin meets all the criteria required.

“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.” This sentence starts the Whitepaper of the first cryptocurrency - Bitcoin - written by Satoshi Nakamoto. It summarizes the main principle on which all cryptocurrencies are built. In 1995, Tim May posted the call to the Cypherpunks group to create a decentralised electronic currency. Among other members who answered the call was Nick Szabo, Tim May, Hal Finney, Adam Back and a few others. They started some projects like Hashash, Bmoney, BitGold but didn’t gain much success. In 2007, right in the middle of the economic crisis, Satoshi Nakamoto appeared out of thin air and introduced the blockchain idea which connected all previous concepts in a brilliant way. It uses SHA-256, a cryptographic hash function, as its proof-of-work scheme. The revolution started on January 3, 2009 when a first Bitcoin block, so called genesis block, was mined. As all cryptocurrencies must be fully transparent to be trustful, Bitcoin source was published. This step initiated a shift in technological and cultural paradigm, which changed the way people transfer value, and hundreds other blockchain projects entered the stage. Every blockchain project is based on the immutable ledger of historical events - transactions which are interconnected. Today we have a plenty of blockchain projects which are focused not only on transferring of value, but rather on resolving many business cases in a decentralised way.

To sum up, every public cryptocurrency to be called by such name must meet the following conditions:

a) its source code must be published and publicly available
b) the ledger which contains historical transaction must be immutable
c) is digital
d) is decentralised

e) uses cryptography to secure the transactions, to control the creation of new tokens and to verify the transfer of assets
f) there is no authority which can stop it or interfere in any way
g) there is no institution which settles the transactions
h) no one has control over issuing its electronic tokens
i) is borderless
j) every human on earth can freely connect to its network, take part in transaction verification, sustain the network with the incentive to generate new coins and use them to transact with others participants.

In the next paragraphs we will see how **FuturoCoin** implements all these points.

Let's finish this section with Crypto Anarchist Manifesto quotation: *"Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions"*

How does FuturoCoin work under the hood?

Asymmetric cryptography

Up to 1976, if two parties wanted to communicate in an encrypted manner, they needed to exchange a key, which was used to encrypt and decrypt a message. The only way was to meet face-to-face or use a trusted courier to deliver a cryptographic key.

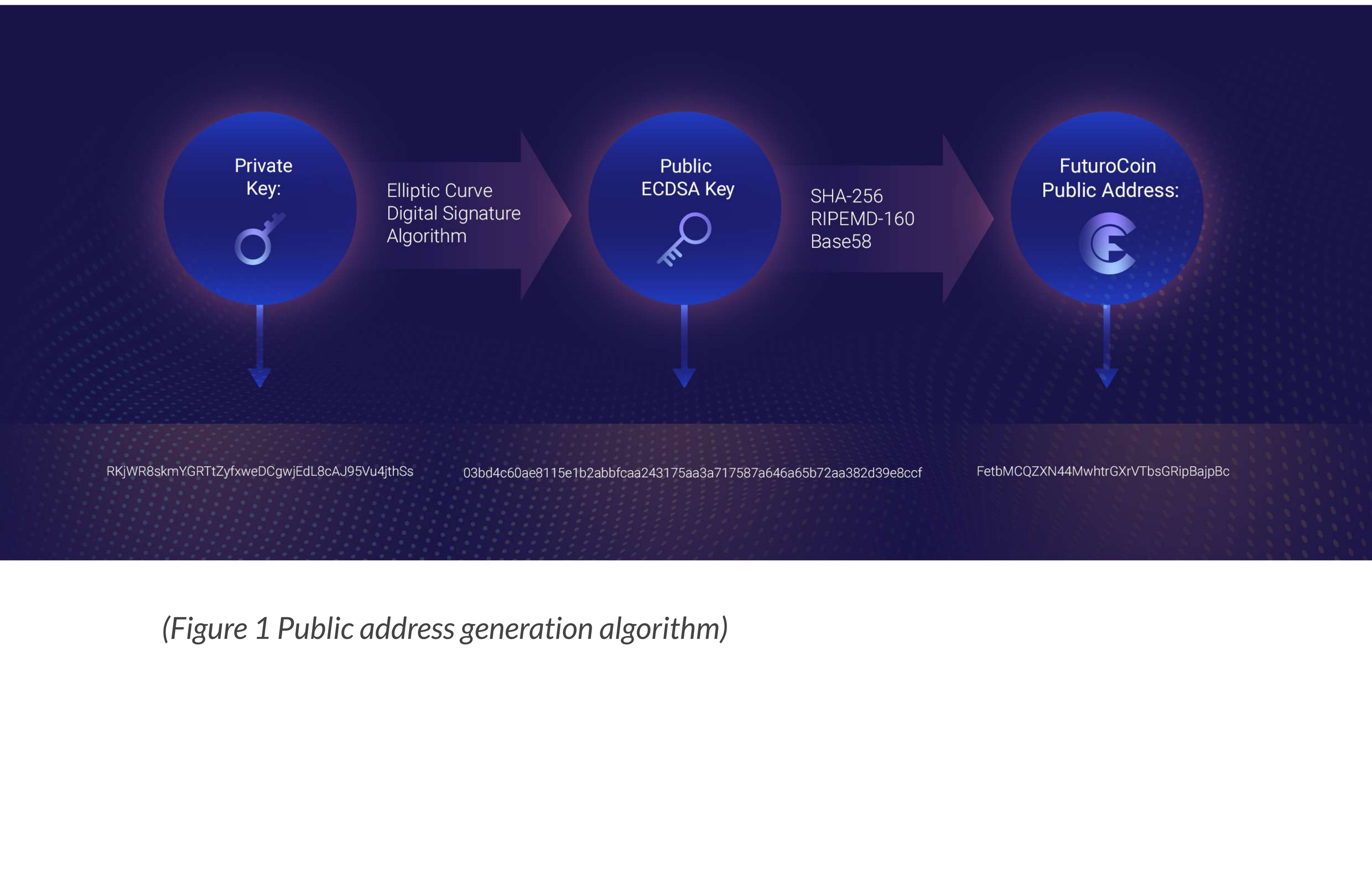
In 1976, Whitfield Diffie and Martin Hellman published the document describing the algorithm where no secret key is exchanged and the message can still be properly encrypted and decrypted or signed. This approach is called asymmetric (public key) cryptography.

FuturoCoin like Bitcoin and other cryptocurrencies uses this technique to sign the transactions.

Main facts about asymmetric cryptography used in FuturoCoin (and other cryptocurrencies)

- every public key is derived from its corresponding private key
- FuturoCoins are assigned to a public key
- The owner of FuturoCoins assigned to a public key is the person who controls the corresponding private key
- to make a transaction the owner of FuturoCoins needs to use his/her private key to authenticate the ownership of FuturoCoins assigned to a corresponding public key
- no one should grant on the private key he/she controls to anybody. This means losing the control to his/her FuturoCoins
- private key is a random 32 bytes number

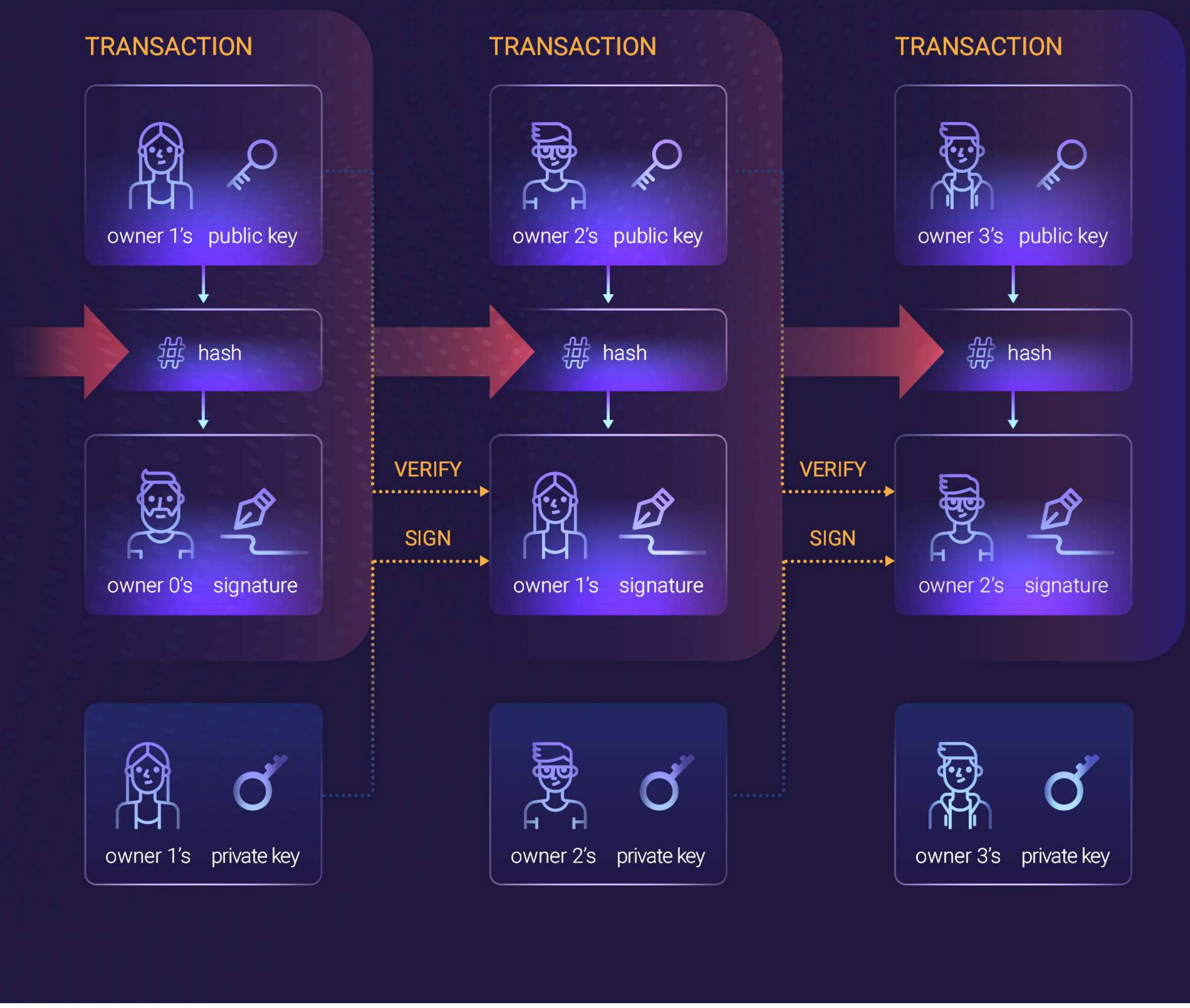
The simplified process of public key creation in FuturoCoin network is described in the schema below.



(Figure 1 Public address generation algorithm)

Transaction

Cryptocurrency is an electronic token which can not be copied nor double spent. It is defined as a chain of digital signatures. If an owner transfers the coin, he digitally signs a hash of the previous transaction and the public key of the receiver and adds it to the transaction message. The receiver verifies the signature to validate the chain of ownership. Satoshi described it in the following schema:



(Figure 2 Transaction chain)

This process is not time/power consuming and makes a receiver assured that the sender is the true owner of coins and can make the transactions. But the problem of double spend is not resolved here. The owner can send the same coins twice or more times. In today's world this is resolved in a centralised manner where trusted parties (banks or other financial institutions) keep the accounting books and guarantee that the coin is not spent twice. There is only one way to confirm the absence of double spend: make all transactions in the whole system visible to everyone and make all system members agree on a single version of history of transactions. This historical ledger is named blockchain.

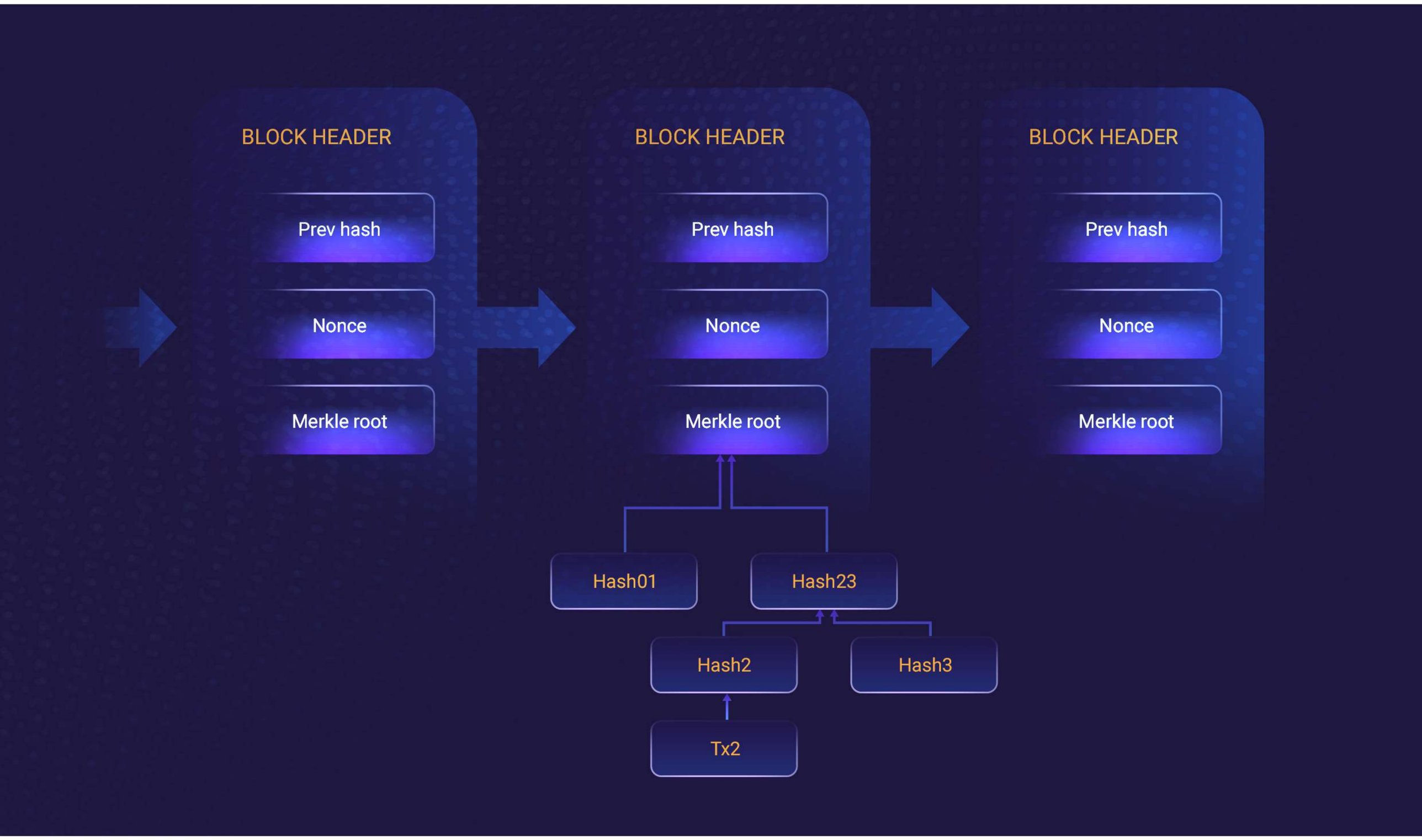
Mining process

FuturoCoin applied proof-of-work X11 algorithm, created by Evan Duffield, which uses multiple rounds of 11 different hashes (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo). It was invented to make ASICs much more difficult to create and to keep the network more decentralised in opposite to other more centralised cryptocurrencies.

Mining is invented to prevent double spend attack and it's the process by which transactions are verified and added to the public ledger. The proof-of-work also solves the problem of determining representation in majority decision making. In **FuturoCoin** network every user can run his own node and sustain the network by providing hashing power to generate a new block of verified transactions. It is incentivised by the fact that every mined block generates new **13.31811263** FuturoCoins and this amount is constant throughout all the time until last block will be mined. The calculation of this number will be described in coming *"FuturoCoin approach"* paragraph.

Like in other cryptocurrencies, all blocks in FuturoCoin are chained in a way that the change of an already existing block would require redoing all the blocks after it. All transactions in a single block construct merkle tree. It is done by pairing each txid (transaction ID) with other txid and hashing them together. In next steps the results are hashed in pairs. The whole process is finished when only one hash remains. It is called *merkle root*.

The mining process with merkle root is presented on the picture below:



(Figure 3 Mining and Merkle tree)

Dash as a codebase for FuturoCoin

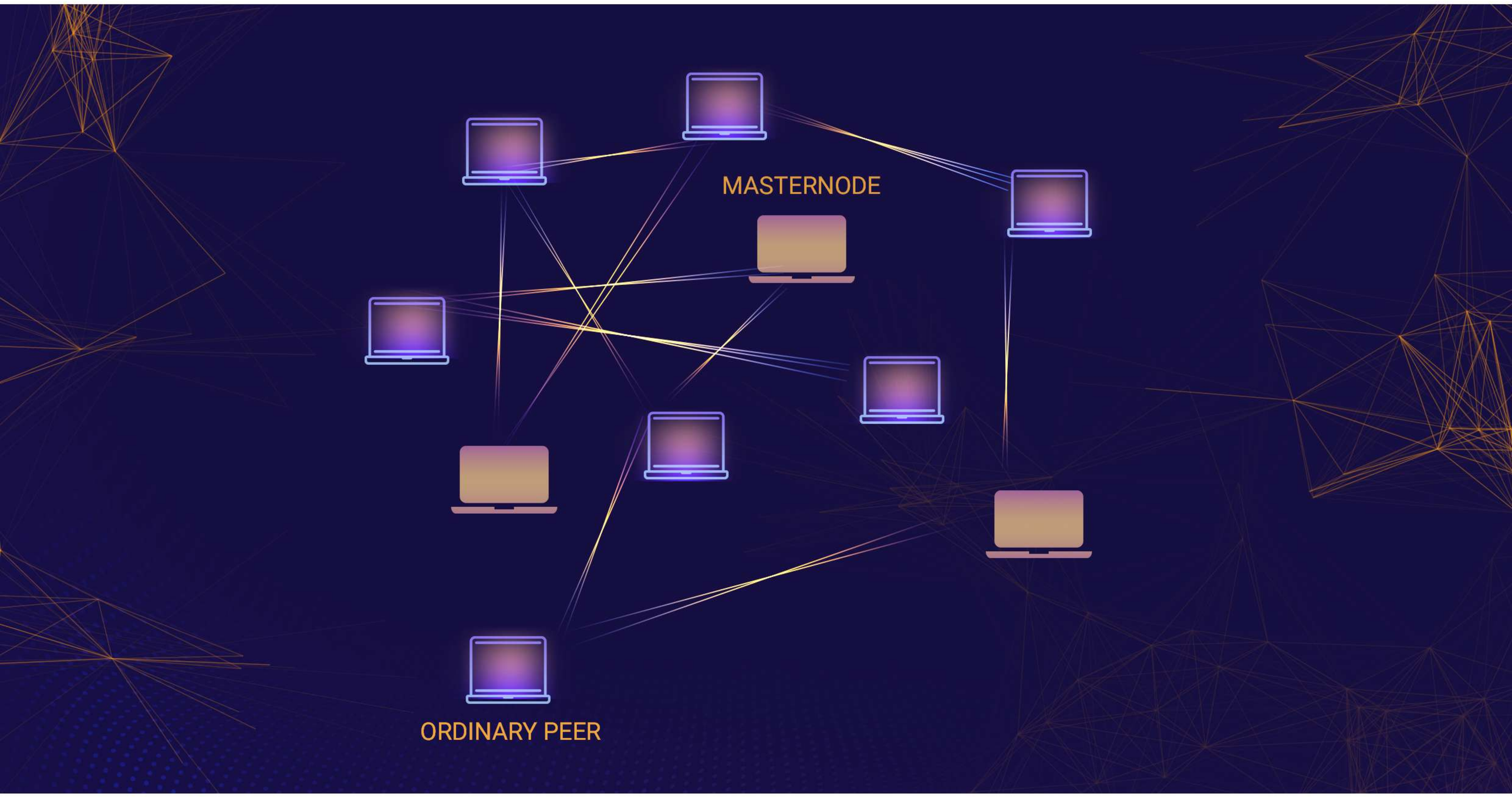
DASH is a cryptocurrency which was released in 2014. It is based on Bitcoin source code. Its aim is to become the most user-friendly and the most on-chain scalable currency. It is a rapidly growing community consisting of developers, marketers, merchants, traders and ordinary clients buying goods with DASH.

FuturoCoin source code is forked off from DASH sources. The choice was made due to arrays of benefits that come with DASH cryptocurrency. Some of them are listed below and are incorporated in FuturoCoin system.

Two-Tier Network

Unlike Bitcoin's single-tier network where all processes are performed by nodes, Dash is the first cryptocurrency to introduce masternodes as a second layer of nodes. These servers are responsible for maintaining several network services listed below, which are not available in other cryptocurrencies. The servers are always on and are connected to mining and all other relaying nodes. Masternodes **can not** participate in the mining process. It comes from the rules implemented in the code.

To be propagated around the network masternodes use a series of protocol extensions such as Masternode ping message and Masternode announce message.



(Figure 4 FuturoCoin network model)

Masternodes and ordinary peers are equal in their connection behaviour, forming a classical P2P network.

In the FuturoCoin ecosystem they are responsible for

- Instant Payments
- Governance
- Low and constant transaction fee.

Instant payments

Instant payment functionality is specific feature first introduced by DASH. This service allows almost instant transactions around the globe. Only masternodes are responsible for correct execution of this kind of payment. When it occurs, inputs to specific transaction are locked and verified by consensus of the masternode network. After a successful consensus of masternodes a message is broadcasted across the network after which all clients will respect lock of tokens. In this way double spending problem is solved without waiting for a confirmation time, which is needed in other cryptocurrencies such as Bitcoin.

Instant payments get rid of the issue related to waiting for confirmations when sending the transaction and merchants can deliver their goods right after the transaction occurs.

FuturoCoin introduces an additional feature where an instant transaction may contain more inputs and outputs in one transaction. This quantity is set to 10 for outputs (plus address change) and any number of inputs. Additionally, all transactions are instant. This feature requires additional level of security besides masternodes locking mechanism. Every input requires at least 6 confirmations (6 mined blocks) to become spendable.

An example of transaction:

1. Bob sends a transaction of 12 FuturoCoins for a software from merchant X using a “locked transaction” message.
2. The transaction is propagated throughout the network and reaches a set of elected authority nodes from the masternodes list.
3. The authority nodes form a consensus about the validation of the transaction and each sign “consensus transaction” message which is sent to the network.
4. When a node sees consensus messages, it considers the transaction confirmed.

In DASH masternodes receive an additional fee for processing instant transactions. In FuturoCoin no additional fee is required for this kind of operation as all transactions are instant.

Low and constant transaction fees

DASH brings a new solution to maintain transaction fees at the lowest point possible. With FuturoCoin we introduce the flat rate for all transactions. Fee model depends only on the number of inputs used in a transaction. In most cases this number is less than 10. In order to prevent flood attack, we need to introduce security measures. When the number of inputs exceeds 10, base fee is multiplied by 2 and so on. It can be presented by the formula:

*fee = max(base_fee, CEIL(n/10) * base_fee)*

where
fee: final transaction fee
base_fee: constant fee value
n: number of inputs

The fee is not dependent on the amount of coins being sent. Base fee can be changed by the spork functionality.

Governance model

DASH is the first cryptocurrency which is a decentralised autonomous organization. It is powered by Sybil proof decentralised and funding model. This treasury system, known as Decentralised Governance by Blockchain (DGBB) is a way of coming to a consensus on proposed changes to core functionality and is used to fund development of DASH. 10% of every block reward goes to the treasury. It is also used to hire other employees, fund conferences and everything what is related to marketing and integration with other systems like exchanges.

Each masternode operator receives one vote and when the project is presented they vote independently on how to spend the money from the treasury.

As we can see, masternodes provide vital functions, which are not available in other cryptocurrencies. In DASH the block reward is split between miners and masternodes. Each group earns 45% of block reward. 10% goes into the treasury system.

In FuturoCoin 50% of block reward goes to miners and 50% goes to masternodes. Masternodes are geographically dispersed and secured by specialized companies. Masternodes are owned by FutureNet company which is responsible for code development, organizing events, hiring employees, preparing and introducing marketing strategies and reward systems. FuturoCoin uses the same kinds of upgrade strategies that are available in DASH. Among them are Multi-Phased Forks (“sporks”) which are similar to global variables that can be changed by the team of developers. The example of such a variable is a transaction fee. It can be changed by the FutureNet developers and depends on many technical and economical parameters. The aim is to have the most competitive transaction fee on the cryptocurrency market. Masternodes can also force other nodes to upgrade its software.

Advanced Security

DASH introduces very sophisticated solutions to many kinds of attacks that occur in the cryptocurrency world and, specifically, in the DASH ecosystem. Among them you can find

- Finney attacks
- Sybil attacks
- Multiple consensus messages
- Transaction lock race attacks.

Their description is out of scope of this document. It’s worth mentioning that FuturoCoin, as a currency based on DASH, has all mitigations securing the network from these kinds of attacks.

FuturoCoin approach

In this paragraph, we will describe all the new features that come with FuturoCoin. Some of them were mentioned above, whilst some are new.

Instant transactions

FuturoCoin is the first cryptocurrency where all transactions are instant. Through this system the consensus is achieved by means of masternodes, which lock the inputs and validate transaction correctness.

Total coin emission

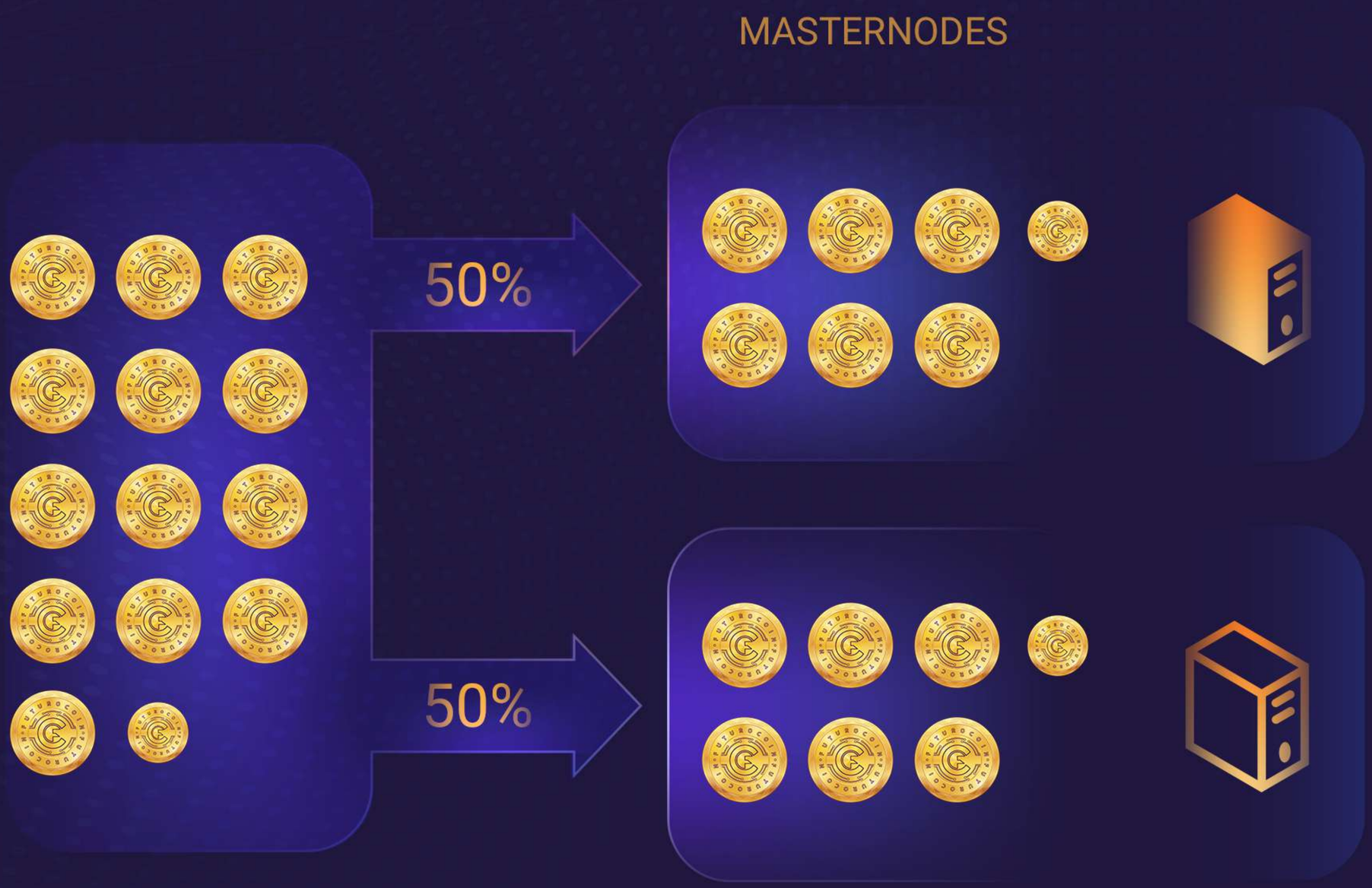
There will be 100.000.000 FuturoCoins in existence. Considering the dynamic development of the company and the potential carried by over a 2.5 million community engaged in this project, the developers decided to mine 30 million FuturoCoins in the first block after the Genesis Block, which then will be used for promotion and other marketing purposes. The main goal is to bring FuturoCoin to the top of its category, and that is why they have considered important to support and reward active users. It would be impossible to build a strong and successful brand without people involved. The wide space for everyone that has been created and the people who will use FuturoCoin will be the best showcase of this cryptocurrency.

Emission rate

The time needed to mine all the coins is set to 10 years. Difficulty retargets use Dark Gravity Wave algorithm. New blocks will be mined every minute on average. Considering all the remaining amount of coins to be mined, 70.000.000, and time parameters, every block will be rewarded by 13,31811263 FuturoCoins. The emission rate is constant - no halving reward blocks or any other events that could change coins issuance. All blocks are mined by ordinary nodes only, not by masternodes.

Block reward allocation

Otherwise than in DASH where 45% goes to miner, 45% goes to masternodes and 10% to the treasury, in FuturoCoin every block reward is divided into a half: 50% goes to winning miner, 50% goes to masternodes network. FutureNet company is responsible for governance operations as described in *Governance model*.



(Figure 5 Block reward program)

PrivateSend functionality

Due to law and regulations, PrivateSend functionality available in DASH was removed from FuturoCoin system. In result, everyone has the same anonymity level as in Bitcoin-like currencies, which use pseudonymous anonymity level.

Flat fee for all kinds of transactions

Masternodes play many vital roles in FuturoCoin ecosystem. One of them is to keep transaction fee constant no matter how big it is in bytes or in value sent. The fee can be changed by spork functionality which is the part of the governance model.

Big and growing community of supporters

FutureNet is a fast growing community with millions of members. FuturoCoin starts with a significant number of users. This is one of its unique features which other starting cryptocurrencies lack. Apart from the fact of having such a strong team, it is very important to emphasize the vision and the future plans that go along with FuturoCoin. The scope of the newly introduced features of this currency, compared to the wide spectrum of other cryptocurrencies, should play a crucial role in the world economy.