



Futuro€coin

Peer to peer electronic cash system
for instant transactions

Executive summary

In order to keep up with the economic growth, we developed an extraordinary idea of "FuturoCoin". The market demands faster and more reliable coins which can be used in all market transactions and are time sensitive and more secure. Since FuturoCoin aims to remove the current barriers in the adoption of cryptocurrencies, it will open new doors in the economy making this a perfectly timed coin and technology for the market. We developed a user-friendly and secure digital currency to create a world which is faster and smarter and uses cryptography to secure the transactions and does not need any institution to settle transactions and is borderless.

We have used Dash as a codebase for FuturoCoin. Dash is a cryptocurrency which aims to become an on-chain scalable currency and is the first currency with decentralized and autonomous system.

FuturoCoin's exceptional idea for the impending future of cryptocurrency is to combine proven solutions with innovative technology. We are proud to be in this sector where we can shape the world

by making it smarter and safer. FuturoCoin has a clear vision of the future plans and will emphasize on building a strong team with your support to create an easier and better organized world .

"The power of the crowd"

In the era of despotism, people were not happy because of their king's dominating and selfish attitude. However, in that scenario at least they had control over their finances and lives. So, people replaced dictatorship with democracy to have power to choose governing authority with mandate to control their lives. Therefore, governments across the world can manage finances of their citizens responsibly. Nowadays, people are not happy even with the government, because it is corrupted and taking the shape of dictatorship again. So, people have decided to take direct control over their finances and operational activities by using of blockchain and its currency.

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 to confirm all pending transactions 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 at least 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 for an hour which translates into more or less six confirmations.

Today, e-commerce undoubtedly cannot wait for such a long time while delivering the goods. FuturoCoin was created to resolve this problem and it guarantees instant transactions with the constant fees at the competitive level.



Mission

At FuturoCoin our aim is to make digital cash easy and accessible to all users around the world. Everyone should have the right to use the full potential of the blockchain, store and it's value. Join our payment network and get access to fast and cheap transactions in everyday payments.

Vision

Our vision is to make a change in the fundamental structure of the global economy and banking systems by transacting, investing and spending FuturoCoins in the same way as any traditional currency but way faster, transparent and secure.



Background and introduction

Before we introduce FuturoCoin, we need to focus on cryptocurrency and how FuturoCoin fits with all its features.

“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 is how Satoshi Nakamoto described cryptocurrency in his first article titled Whitepaper of a cryptocurrency named Bitcoin. It sums up the features and the basic principle of a cryptocurrency. In 1995, Tim May published his manifesto to the Cypherpunks group and calling them to invent a decentralized digital currency. Some of the most prominent people who responded were Nick Szabo, Hal Finney, Adam Back, Tim May himself and a few more. They

started some projects like Hashash, Bmoney, and BitGold but with no remarkable 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. SHA-256 was used as a cryptographic hash function, as its proof-of-work scheme. On January 3, 2009, the revolution began with the mining of first Bitcoin block or the genesis block. Bitcoin source was published so that it could maintain transparency. This move changed the cultural and technological paradigm and ultimately modified the way people transfer currencies. After that many other blockchain projects came into existence. Currently, blockchain is not only used to transfer currencies but it also helps to resolve many real-time problems.

In order to be called a public cryptocurrency, a specific currency has to meet the following

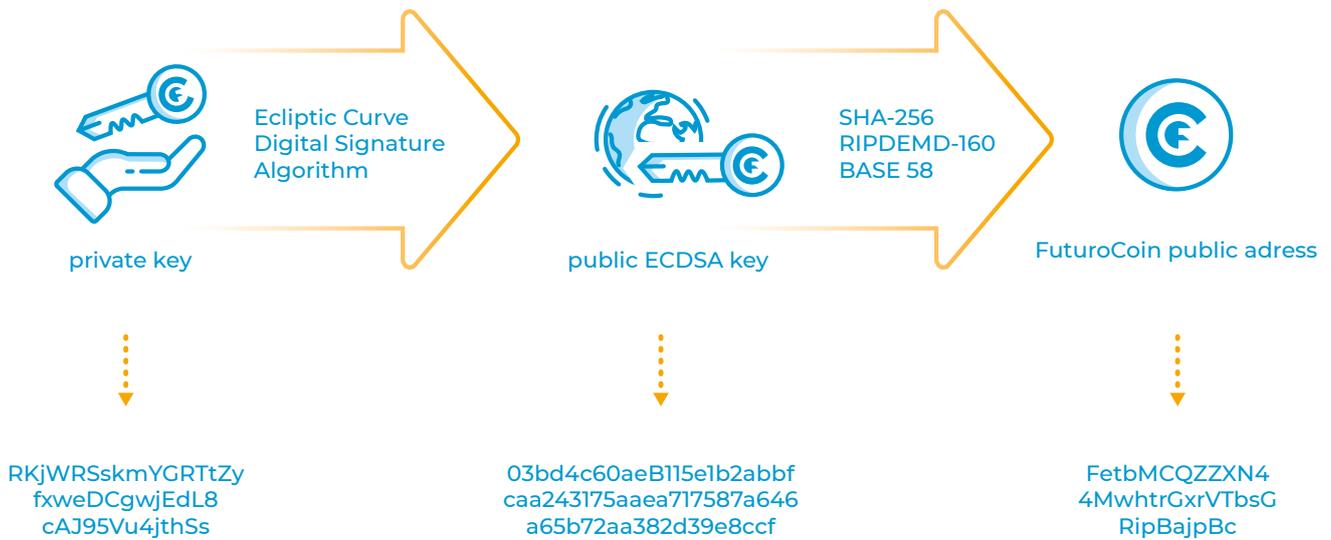
- its source code must be published and publicly available
- the ledger containing historical transactions must be unalterable
- it is decentralized
- cryptography should be used for security purpose
- it is digital
- no authority should be given the power to interrupt the process
- no institution settles its transactions
- no one has control over issuing its electronic tokens
- transactions have no borders
- everyone should be able to access it

It's time to discuss how FuturoCoin fits the features of cryptocurrency.

The quote from „Crypto Anarchist Manifesto” should be known, then.

“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.”



Analysis of the competition

Features	Bitcoin	Dash	FuturoCoin
Network Layer	<i>Bitcoin works based on the principle of one-tier network where there is only one layer of nodes.</i>	<i>Dash works based on the principle of two-tier network where the second layer of node is a master node.</i>	<i>FuturoCoin also works based on the principle of two-tier network in which master node acts as the second layer of node. It will be more efficient than other two coins.</i>
Rate of Transaction Verification	<i>Bitcoin takes around 10 minutes to verify the transaction.</i>	<i>Since it uses two-tier network it takes a few seconds to verify the transaction.</i>	<i>FuturoCoin hardly takes a few seconds (and sometimes even less than a second) to verify the transaction and is much faster than compared to Dash and Bitcoin.</i>
Mining	<i>Bitcoin requires a lot of resources for the mining process.</i>	<i>Dash mining is extremely difficult and complex because it requires solving a lot of complicated math problems.</i>	<i>FuturoCoin mining procedure is same as mining of Dash.</i>
Transaction Fees	<i>The transaction fees are quite high in Bitcoin.</i>	<i>Dash tries to minimize the transaction cost.</i>	<i>In FuturoCoin, the transaction fee is fixed and negligible when compared to other two coins.</i>

Current market issues

Here are some problems of a traditional centralized banking system and its fiat currencies:



Government intervention - Banks have a disturbing amount of command over personal data and fiat currencies which ultimately troubles people.



Centralized banking - When a bank confiscates a personal account for any reason, specific processes and procedures takes a lot of time.



Under-resourced economy - The inefficient and the ineffective distribution of resources between people and economy



Financial exclusion - According to a report published in 2018, there are more than 2 billion people of the adults in the world who are either not accessing any traditional banking system facilities or are able to access only some of them.



Unsatisfactory systems and unfair practices - The current banking systems are not created to support local or global micro-economy, nor do they encourage financial inclusion



Restricted number of clients - The number of clients is limited by country and system barriers.



Speed of transaction - It takes several days and depends on the bank-to-bank relations.



Scalability - It is expensive and slow.



Transfer values - The transfer values are limited and restricted by law and certain procedures.



International transfers - are restricted, slow and expensive.

FuturoCoin: a valuable alternative to all market problems

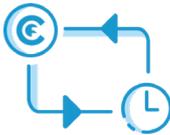
FuturoCoin is a solution to all of the above problems. FuturoCoin will make the digital cash easy and accessible to all users in a much faster and safer way where no authority will be given

to a single hand. It will promote digitalization and decentralization where privacy will be respected and everyone will be able to freely access its network.

Here are some solutions provided by FuturoCoin



Fraud-proof: When FuturoCoin is created, all confirmed transactions will be stored in a public ledger. Identifications of coin owners will be encrypted to secure the legitimacy of record keeping. Because the FuturoCoin is a cryptocurrency, it is decentralized, which means you will own it. Neither government nor bank has any control over it.



Instant settlement: FuturoCoin will be easy to use, so it will become high in demand. A smart device and internet connection is all you need for instant payments and money transfers.



Accessible: There are more than two billion people who have access to the Internet but don't have the rights to use traditional exchange systems. These individuals will be able to use FuturoCoin without any restrictions.



Identity theft: Blockchain technology used by FuturoCoin ensures secure digital transactions through encryption and "smart contracts" that make the entity virtually unhackable and void of fraud.



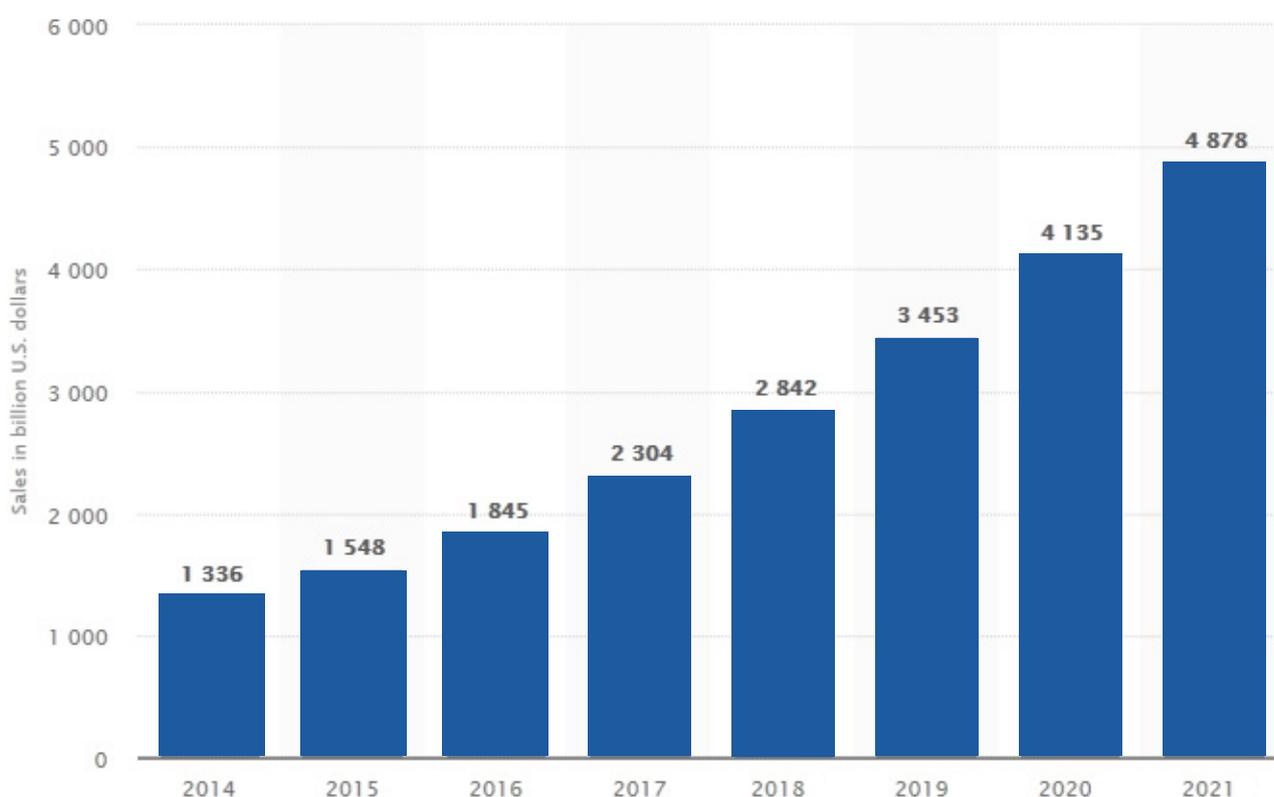
You are the owner: When using FuturoCoin, your privacy is safe and you don't need to rely on any third party.

Market analysis

According to the chief executive of a top digital currency exchange, the entire cryptocurrency market will reach up to \$ 1 trillion this year. There are more than 250 exchanges and around 4500 cryptocurrencies available on

the market. Whereas world is moving towards e-commerce and its growth is commendable.

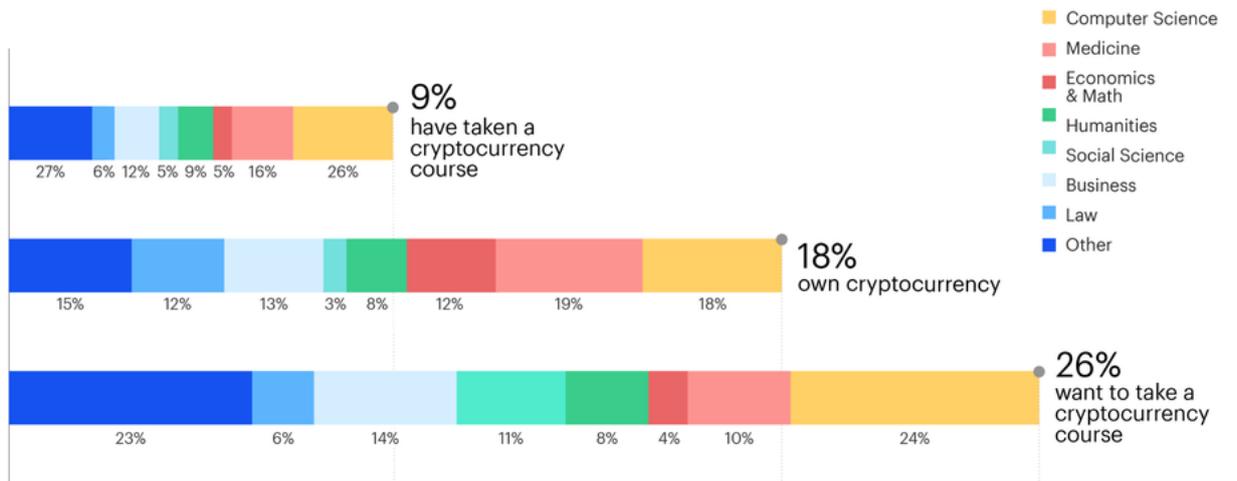
In 2017, retail e-commerce sales worldwide amounted to 2.3 trillion US dollars and e-retail revenues are projected to grow to 4.88 trillion US dollars in 2021.¹



Currently, the world is looking for a solution which combines cryptocurrency and e-commerce market. According to a survey by Coinbase, cryptocurrency will hit the mainstream as a way of paying for services and goods within the next decade as many of those students surveyed by Coinbase will become part of the working world.

¹<https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>

U.S. student experience with cryptocurrency



Source: Survey by Coinbase, conducted by Qriously of 675 U.S. students ages 16 and older



This is the right time for FuturoCoin to expand in the market where people are eager to use cryptocurrency and adopt a digital banking system. Nowadays, the market needs a cryptocurrency coin which is fast, secure and easily accessible, so it can fill the gap between traditional fiat and advanced crypto.

Product description

FuturoCoin is a cryptocurrency which mainly aims at quick transactions to protect against double spend attack and to minimize the transaction fees, so everyone can easily access it.

Cryptocurrencies like Dash, FuturoCoin and Bitcoin use asymmetric cryptography to sign the transactions. Dash, for example, uses x-11 algorithm consisting of 11 different hashes for hashing blocks. This was invented to keep the network more decentralized.

FuturoCoin source code is sub-derived from Dash due to the number of benefits it provides.

- Two-tier network - FuturoCoin works based on the principle of two-tier network where master nodes behave as a second layer of nodes.
- Instant payments - Master nodes are responsible for the correct execution of instant payments. Instant payment allows for improvement of the speed of the transaction process.
- Low and constant transaction fees - We have introduced the flat rate for all transactions so that every person can easily access them.
- The fee does not depend on the amount of coins being sent.
- Governance model - In FuturoCoin, the block reward is divided equally.
- Advanced securities - FuturoCoin securities system is inspired by Dash, so it prevents from all the latest known attacks.

The above features of FuturoCoin shows that it is entirely decentralized, relying on a ledger of transactions distributed across a worldwide network of computers and is based on a technology called blockchain.

How does FuturoCoin work under the hood?

Asymmetric cryptography

Till 1976, if two parties wanted to convey a message in an encrypted manner, they were required to exchange a key, which was used to encrypt and decrypt a message. There was only one way to do that, namely meet face-to-face or use a trusted courier to deliver a cryptographic key.

In 1976, Whitfield Diffie and Martin Hellman issued a document providing description of the algorithm where no secret key is exchanged and the message can still be properly encrypted and decrypted or signed. This technique is called asymmetric (public key) cryptography. Cryptocurrencies like FuturoCoin and Bitcoin use this technique to sign the transactions. Here are some important details about asymmetric cryptography used in FuturoCoin (and other cryptocurrencies):

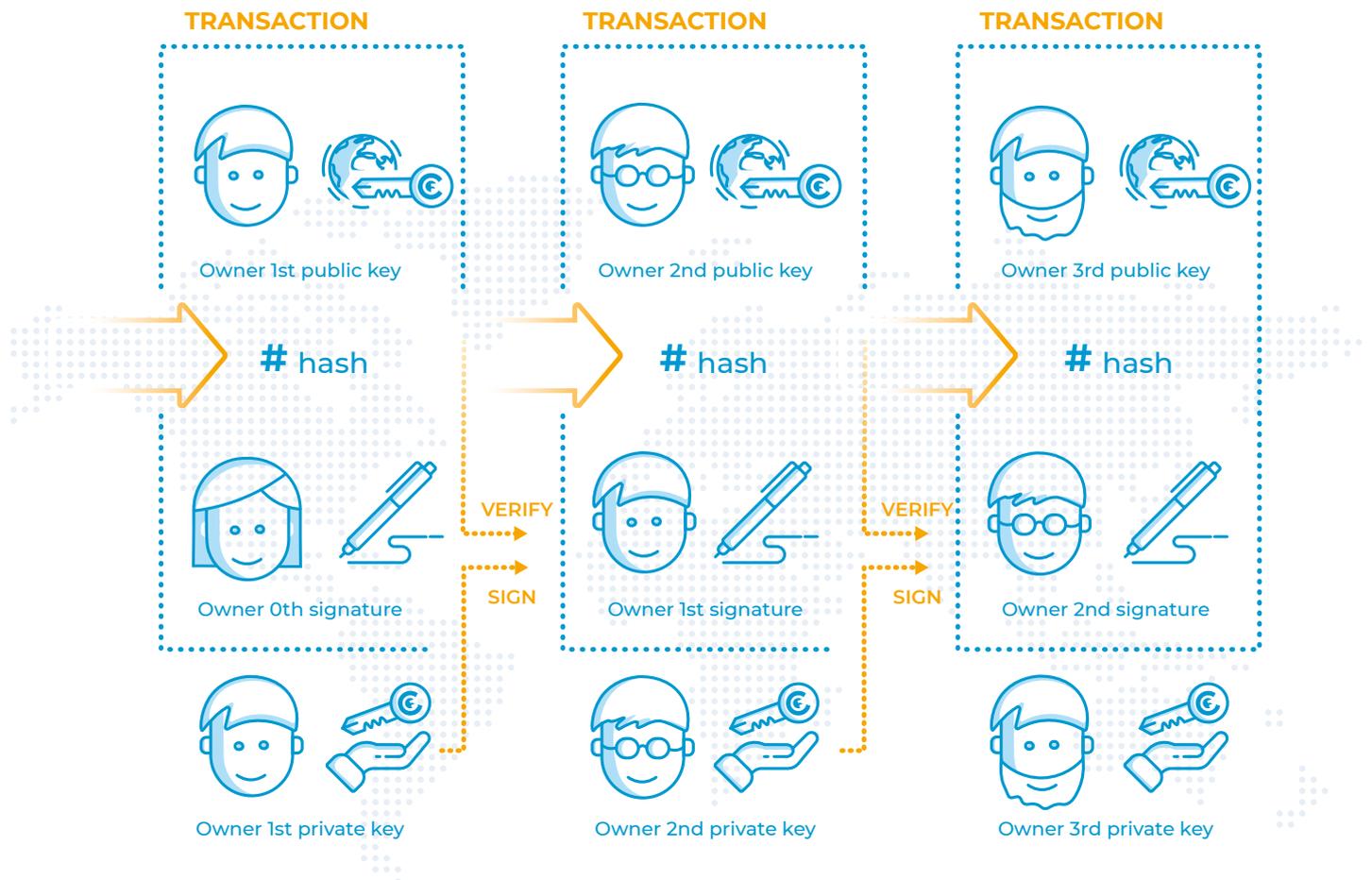
- Every public key originates from its corresponding private key
- A random 32-bytes number can be assigned as a private key
- FuturoCoins are allocated to a public key
- The holder of a public key is the person who controls the corresponding private key
- The owner of FuturoCoin needs to use their private key to verify the ownership of FuturoCoins assigned to a corresponding public key

No one apart from the owner should be allowed to control the private key. The simplified process of public key creation in FuturoCoin network is described in the scheme below.

Transaction

Cryptocurrency is a digital currency which cannot be copied nor double spent. It is defined as a chain of digital signatures. If there is a process of transferring a coin, the owner need to digitally sign a hash of the former transaction and the public key of the receiver and affix it to the transaction message. The signature is verified by the receiver to authenticate the chain of ownership. It was described by Santoshi in the following scheme:

This process is neither time nor power consuming and assures the receiver that the sender is the true possessor of coins and can perform transactions. But this process does not provide the solution for the double spend attack. The owner of the coin can send the same coins twice or more times. In the current scenario, this problem is resolved in a centralized manner where trusted parties (banks or other financial institutions) keep the accounting books and guarantee that the coin is not spent twice. Now the only way to confirm the absence of double spend is to make all transactions in the whole system visible to everyone and have all system users agree on a single version of a transaction history. This historical ledger is named blockchain.



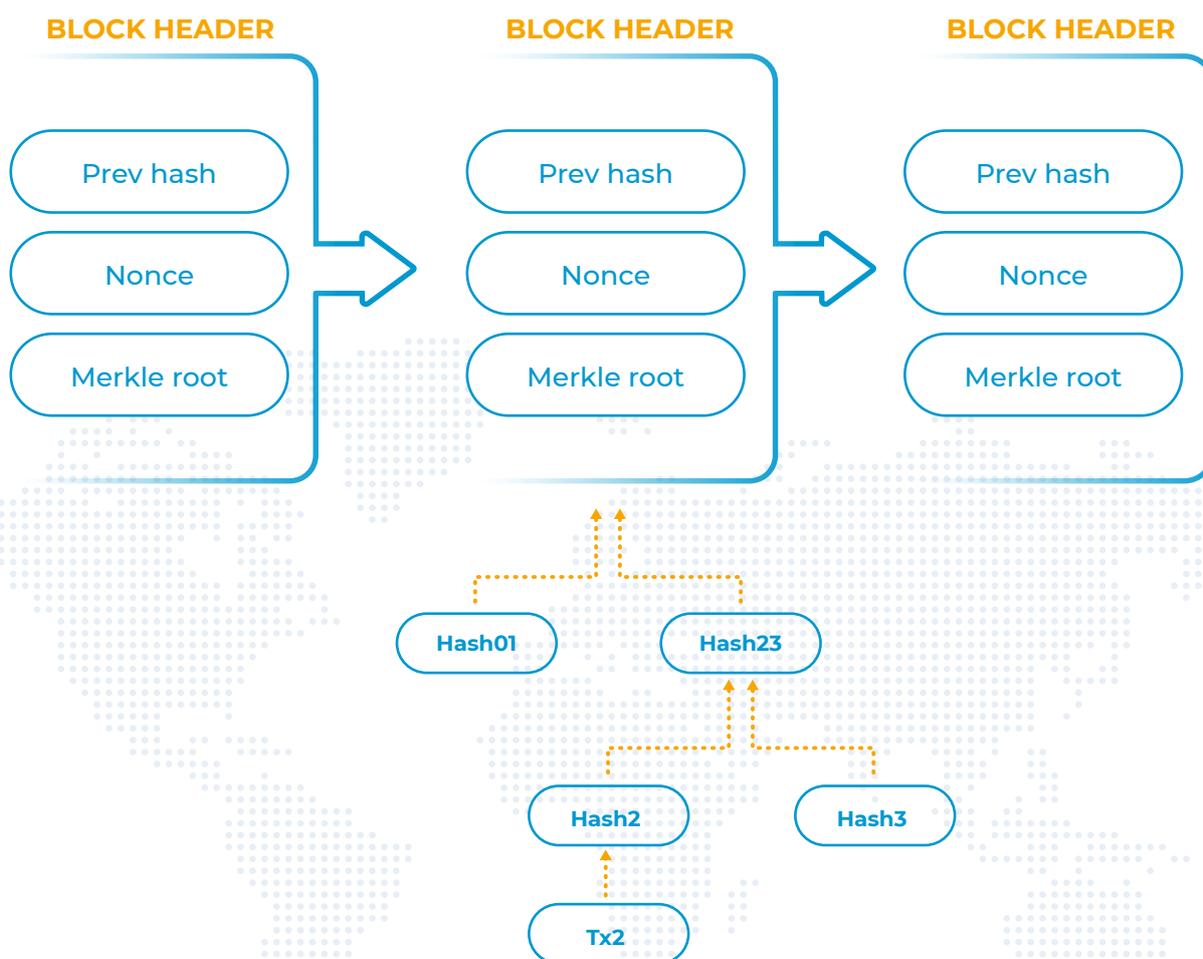
Mining is created in order to get rid of double spend attack and it's the process by which transactions are authenticated and affixed to the public ledger. The proof-of-work also gives the solution for establishment of the representation in majority of decision making. In FuturoCoin network every user has the power to run his node and maintain the network by providing hashing power to generate a new block of verified transactions.

Similar to other cryptocurrencies, all blocks to FuturoCoin are linked in a way that any change in the already existing block would require

recreation of all the blocks once this change is introduced from. A Merkle tree is constructed by all the transactions in a single block. It is done by joining each transaction ID with other transaction ID and hashing them together. Then, the results are hashed in pairs, up to the point where only one hash remains, the process is finished. This is called a Merkle root.

This decision was made due to the number of benefits provided by Dash cryptocurrency. Some of them are listed below and are incorporated in the FuturoCoin system.

The picture below shows the mining process with a merkle root.



Two-tier network

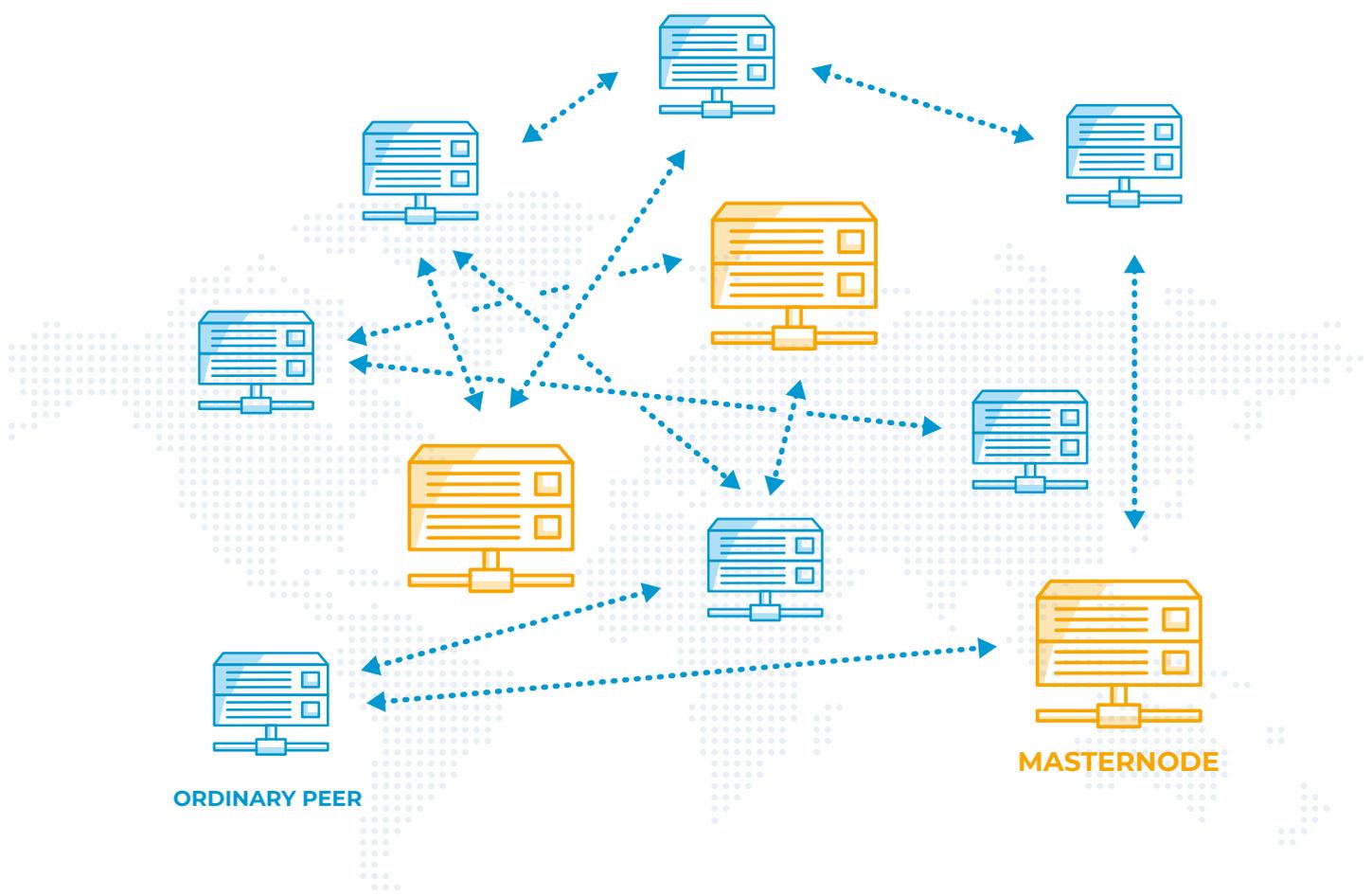
Bitcoin uses a single-tier network where all the process are executed through nodes while Dash, on the other hand utilizes a two-tier network where masternodes act as a second layer, which is responsible for maintaining numerous network services that are not there in the cryptocurrency. The servers are connected to mining and all other passing nodes, and are always on. Masternodes cannot be included in the mining process because of the rules enforced in the code.

Masternodes uses a series of protocol expansions such as Masternode ping message and Masternode announce message to be able to disperse around the network. Regular peers and masternodes are common in their con-

nection behaviour and form a classic P2P network. FuturoCoin ecosystems are responsible for fast transaction and management or administration with low and consistent transaction fees. In the future, we will describe this calculation.

Instant payments

Dash introduced the distinct feature of an instant payment. Thanks to this feature an instant transaction is possible around the world. This kind of payment is taken carried out only by masternodes. When it happens, inputs to particular transaction are locked and authenticated by agreement of the masternode network.



After a successful agreement of masternodes a message is transmitted over the network after which all clients will respect lock of tokens and this is how the problem of double spending is solved without having to wait for a confirmation time, which is required in other cryptocurrencies such as Bitcoin.

Instant payments provide the solution to the issue of a long wait for confirmation when sending the transaction. Merchants can deliver their goods right after the transaction occurs. FuturoCoin presents an additional feature where an instant transaction may include more inputs and outputs in one transaction. This quantity is set at up to ten for outputs (plus address change) and any number of inputs. Additionally, all transactions are instant. This special quality of FuturoCoin requires additional level of security, besides masternodes locking mechanism. Every input needs at least six confirmations (six mined blocks) to become usable.

An example of a transaction:

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

In Dash, masternodes accept an additional fee for processing instant transactions. In FuturoCoin no additional fee is needed for this kind of operation as all transactions are instant.

Low and constant transaction fees

Dash proposed a new solution to retain the transaction fees at the lowest point possible. With FuturoCoin we have introduced the flat rate for all transactions. Fee model depends completely on the number of inputs applied in a transaction. Most commonly this number is less than ten. For the purpose of preventing a flood attack, we need to introduce certain 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:

$$\text{fee} = \max(\text{base_fee}, \text{CEIL}(n/10) * \text{base_fee})$$

where fee: final transaction fee

base_fee: constant fee value

n: number of inputs

The fee depends on the amount of coins being sent. Base fee can be modified or altered by the spork functionality.

Governance model

Dash is the first ever decentralized digital currency with an autonomous system. It is influenced by Sybil proof decentralized and funding model. This system, known as Decentralized Governance by Blockchain (DGBB), is an approach of coming to a consensus on intended alterations to core functionality, and is used to fund development of Dash. 10% of each block reward is sent to the treasury. It is also used to hire employees, to 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 e-money from the treasury.

As we can observe, masternodes grant some essential functions, which are not present in other cryptocurrencies. In Dash, the block reward is divided between miners and masternodes. Each group earns 45% of block reward. 10% goes into the treasury system.

In FuturoCoin, 50% of block reward is given to miners and 50% goes to masternodes. Masternodes are naturally distributed and secured by specialized companies. The creator of masternodes is FutureNet company (BCU Trading LLC) which is responsible for arranging events, developing code, hiring employees, developing and introducing marketing strategies and reward systems. FuturoCoin uses the similar kind of enhanced strategies that are available in Dash. Amongst them are Multi-Phased Forks (“sporks”) which are similar to global variables that can be altered by the developers team. The example of such variable is a transaction fee. It can be modified by the FutureNet developers and depends on many economical and technical parameters. The purpose is to have the most competitive transaction fee on the digital currency market. Masternodes also have the ability to force other nodes to upgrade its software.

Advanced security

Dash introduces refined solutions to numerous types of attacks that takes place in the cryptocurrency world and, particularly, in the Dash ecosystem. These include:

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

We will not focus on their description in this document. It is worth specifying that FuturoCoin, as a digital currency based on Dash, has all mitigations safeguarding the network from these kinds of attacks.

Instant transactions

FuturoCoin is digital currency that made all transactions instant. Through this system the consensus is achieved by means of masternodes, which lock the inputs and validate transaction correctness.

Big and growing community of supporters

FutureNet is a rapidly developing community with millions of associates. FuturoCoin enters the market with a considerable number of users. This feature makes FuturoCoin unique. Apart from the fact of having such a strong team, it is very important to emphasize the vision and the future plans for FuturoCoin. These features make FuturoCoin exceptional and increase its scope.

PrivateSend functionality

PrivateSend functionality is not available in FuturoCoin system due to law and regulations. Therefore, it has the same anonymity level as in Bitcoin-like currencies, which use pseudonymous anonymity level.

Economics

Total coin emission

There will be 100,000,000 FuturoCoins available. Taking into consideration the active progress of the company and the potential carried by over a 2.5 million community engaged in this project, the developers have made a decision to mine around 30 million FuturoCoins in the first block after the Genesis Block, which will then be used for advertising and other marketing purposes.

Our main aim is to bring FuturoCoin to the top of its category. This is the reason why it is considered important to support and reward active users.

It would be impossible to build a successful and sound brand without people involved. People using FuturoCoin will be the best illustration of this its success.

Emission rate

The time required to mine all the coins is fixed at ten years. Dark Gravity Wave algorithm is used in the case of difficulties retargeted. On an average, new blocks will be mined every minute.

If we consider all the remaining amount of co-

ins to be mined, which is 70,000,000 and the time parameters, then every block will be rewarded with 13.31811263 FuturoCoins.

The emission rate is constant - no halving reward blocks or any other events that could alter coins issuance. All blocks are mined by regular nodes only and not by masternodes.

Block reward allocation

In Dash, 45% goes to the miner, 45% goes to masternodes and 10% to the treasury, while in FuturoCoin every block reward is divided into a half:

- 50% goes to the winning miner,
- 50% goes to a masternode network. FuturoNet company takes care of the governance operations as described in a Governance model section.

Flat fee for all kind of transactions

Masternodes play numerous essential roles in the FuturoCoin ecosystem. One of them is to maintain transaction fee constant irrespective of the size in bytes or in value sent. The fee can be altered by spork functionality, which is the part of the governance model.

Team details



Stephan Morgenstern
FTO Creator



Roman Ziemian
FTO Creator

Stephan has over 25 years of experience as an entrepreneur and is also a leader of some of the popular MLM projects. He is a well-known face of net marketing. He is an owner of numerous companies located in Germany, Austria and other European countries. Stephan Morgenstern has applied all his cryptocurrency knowledge and experience to make this project successful.

Roman has a considerable amount of experience in management and communication which helped a lot in making this project so successful. He is also a well-experienced entrepreneur who looks at business from global perspective. He is an owner of many companies in Sweden, England, Brazil, Colombia, Austria and Cyprus and is also a manager of a business project in Ukraine. His hard work and strong vision have made him successful.

Conclusion

FuturoCoin's exceptional vision for the future of cryptocurrency is both revolutionary and achievable.

Cryptocoin will accredit each person and business within the microeconomy, through a decentralized and all-encompassing financial structure that we have created with passion.

The FuturoCoin has an amazing potential for development and growth that is possible thro-

ugh the FutureNet platform. The world is ready for a cryptocurrency like FuturoCoin, and now we need to ensure that the FuturoCoin is ready for the world.

With a big and growing community of supporters all we are confident about our vision and future plans for FuturoCoin, and believe it can and will play a crucial role in the world economy.



FuturoCoin

