FuturoCoin

Peer to peer electronic cash system

for instant transactions

Executive summary

To keep up with economic growth, we developed an extraordinary idea of "FuturoCoin." The market demands faster and more reliable coins that 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 have developed a user-friendly and secure digital currency to create a world that is faster and smarter. Our digital currency uses cryptography to secure the transactions. It does not need any institution to settle transactions and is borderless. We have used some economic and technical ideas from existing cryptocurrencies and introduced our new concepts to become an on-chain scalable currency with a 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 clear 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 dominance and selfish attitude. However, in that scenario, at least they had control over their finances and lives. People replaced dictatorship with democracy to have the power to choose governing authority with a mandate to control their lives. Therefore, governments across the world can manage the finances of their citizens responsibly. Nowadays, people are not happy even with the government. They are corrupt, and they are taking the shape of dictatorship. So, people have decided to take direct control over their finances and operational activities by using 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 a double-spend attack. A double spend is a 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 entirely sure, 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, guaranteeing instant transactions with fixed fees at a competitive level.

Mission

At FuturoCoin, we aim 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.”

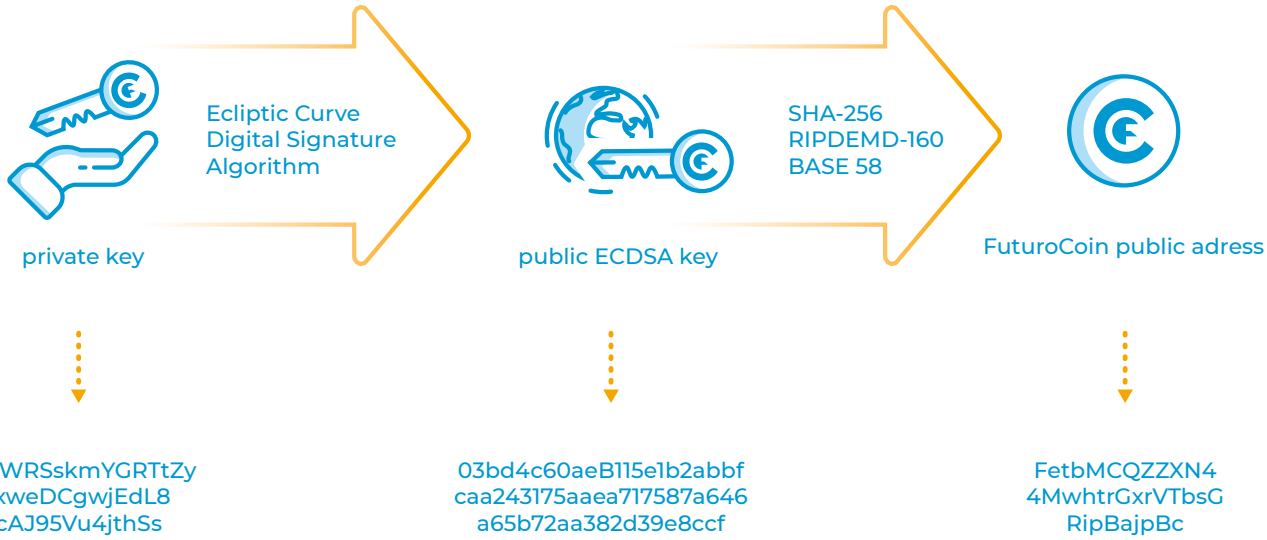
This is how Satoshi Nakamoto described cryptocurrency in his first article titled Whitepaper of a cryptocurrency named Bitcoin. It sums up the features and the basic principle of a cryptocurrency. In 1995, Tim May published his manifesto to the Cypherpunks group, calling them to invent a decentralized 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 brilliantly connected all previous concepts. 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 the 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 coins, but it also helps to resolve many real-time problems.

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. This quote from the „Crypto Anarchist Manifesto” should be known:

“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	*Bitcoin takes around 10 minutes to verify the transaction.*	*Bitcoin works based on the principle of one-tier network where there is only one layer of nodes.*	*FuturoCoin operates on the two-tier network. The masternode acts as the second layer of the node. It will be more efficient than the other two coins.*
Rate of Transaction Verification	*Bitcoin takes around 10 minutes to verify the transaction.*	*Since it uses a two-tier network, it takes a few seconds to verify the transaction.*	*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.*
Mining	*Bitcoin requires a lot of resources for the mining process.*	*Dash mining is extremely difficult and complex because it requires solving a lot of complicated math problems.*	*FuturoCoin's mining procedure is the same as the mining process of Dash.*
Transaction Fees	*The transaction fees are quite high in Bitcoin.*	*Dash tries to minimize transaction costs.*	*FuturoCoin's transaction fee is fixed and negligible when compared to the other two coins.*

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 take a lot of time.

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

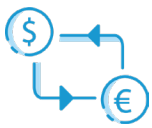
Financial exclusion - According to a report published in 2018, there are more than 2 billion people in the world who are either not accessing any traditional banking system facilities or are able to access only some of them.

Unsatisfactory systems and unfair practices - The current banking systems do not 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 laws and certain procedures.

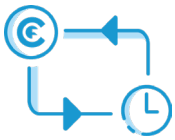
International transfers - are restricted, slow and expensive.

FuturoCoin: a valuable alternative to all market problems

FuturoCoin is a solution to all of the above issues. FuturoCoin makes the digital cash easy and accessible to all users in a much faster and safer way. No authority will be given to a single hand. It will promote digitalization and decentralization. Privacy will be respected, and everyone will be able to access the network freely.

Here are some solutions provided by FuturoCoin

Fraud-proof: All confirmed transactions are stored in a public ledger. Identification of coin owners is encrypted to secure the legitimacy of record keeping. FuturoCoin is decentralized, which means you own it. Neither government nor bank has any control over it.



Instant settlement: FuturoCoin is 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 lack the right to use traditional exchange systems. These individuals will be able to use FuturoCoin without any restrictions.

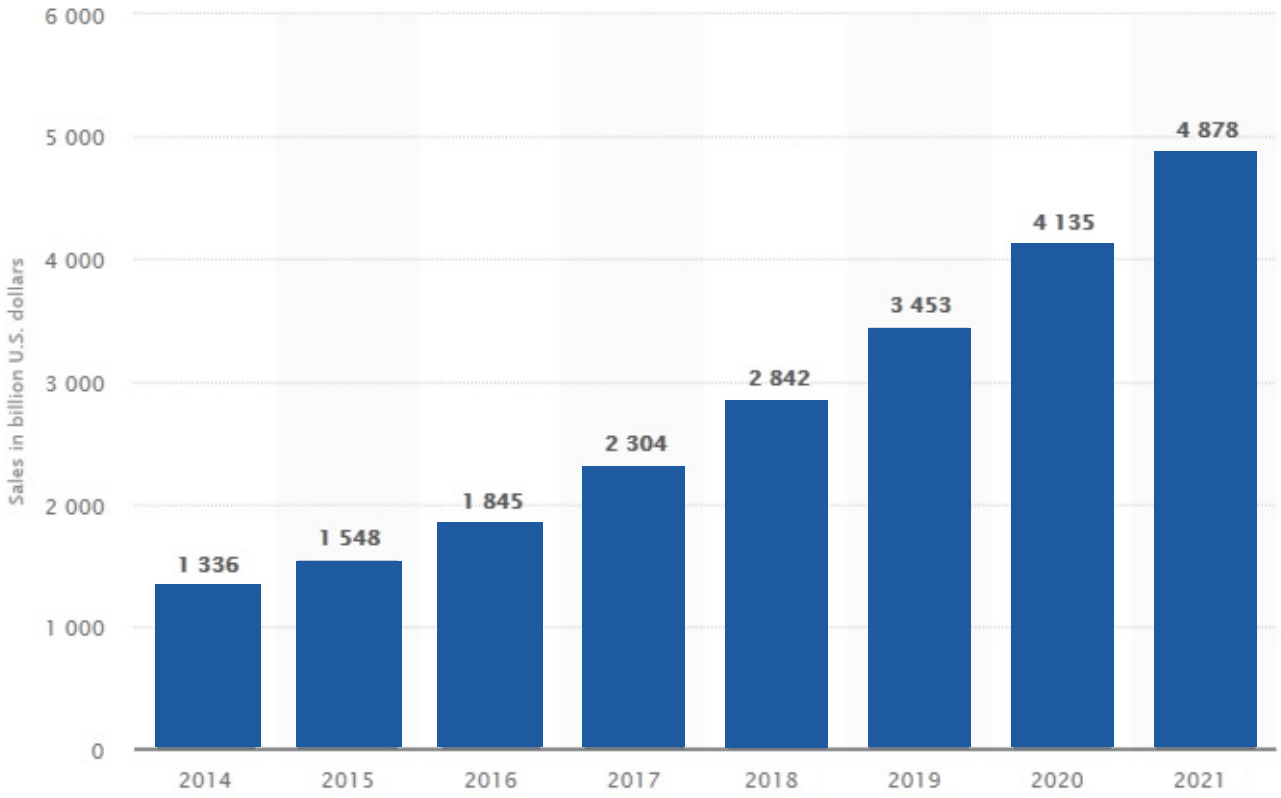
Identity theft: Blockchain technology used by FuturoCoin ensures secure digital transactions through encryption and „smart contracts" that make the entity virtually unhackable and void of fraud.

You are the owner: When using FuturoCoin, your privacy is safe without third parties.

Market analysis

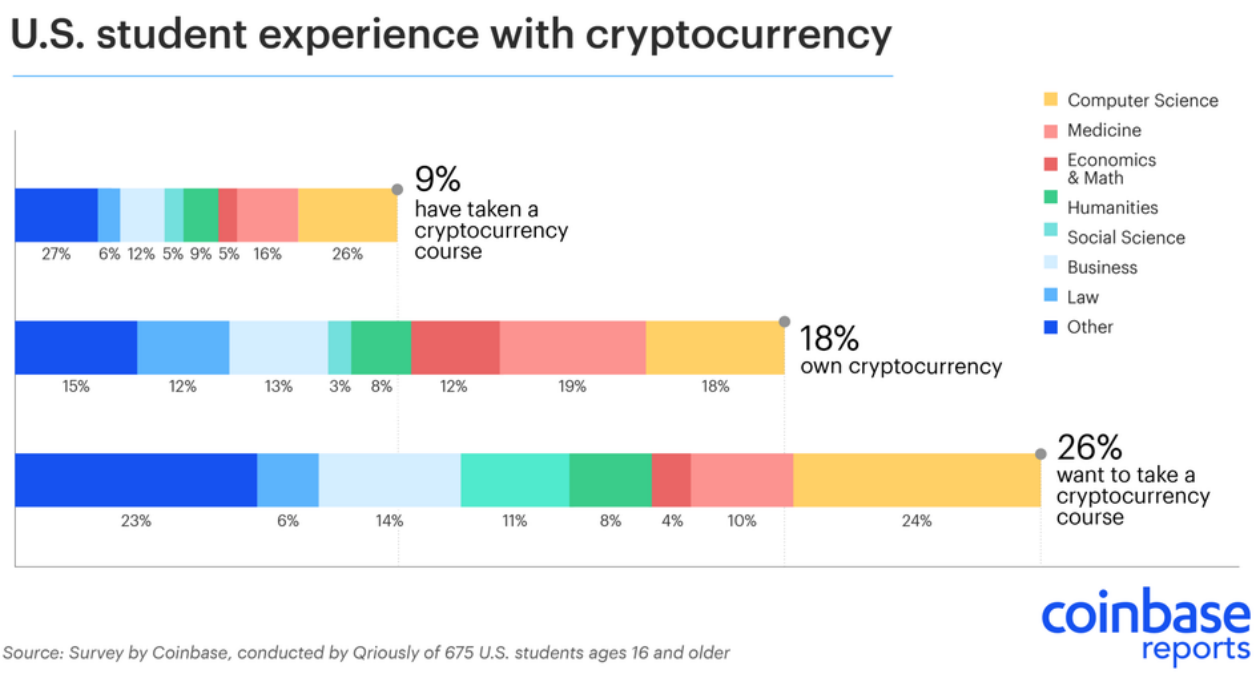
According to the chief executive of a top digital currency exchange, the entire cryptocurrency market will reach up to $ 1 trillion this year. There are more than 250 exchanges and around 4500 cryptocurrencies available on the market. Whereas the world is moving towards e-commerce, and its growth is 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.



Currently, the world is looking for a solution that combines the cryptocurrency and the 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. 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/*



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 that 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 attacks and to minimize the transaction fees, so everyone can easily access it.

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

FuturoCoin protocol introduces the number of benefits:

- Two-tier network - FuturoCoin works based on the principle of the 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 the 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 number of coins being sent.
- Governance model - In FuturoCoin, the block reward is divided equally.
- Advanced security - FuturoCoin's security system is inspired by solutions found in other cryptocurrencies, preventing all the latest known attacks.

The above features of FuturoCoin show 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 the 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 describing the algorithm where no secret key is exchanged. The message can still be appropriately 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):

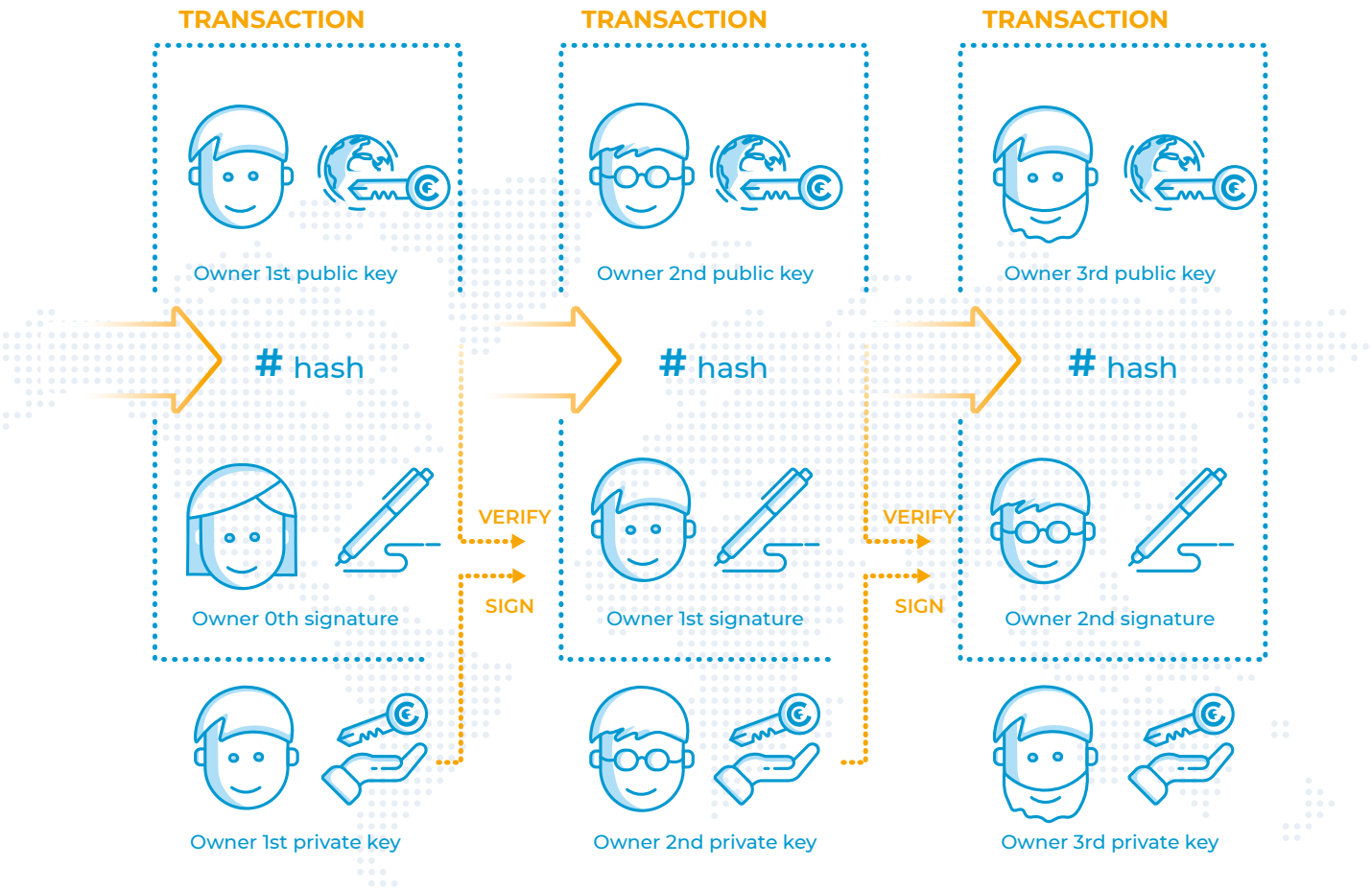
- Every public key originates from its corresponding private key.
- A random 32–bytes number can be assigned as a private key.
- FuturoCoins are allocated to a public key.
- The holder of a public key is the person who controls the corresponding private key.
- The owner of FuturoCoin needs to use their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

Transaction

Cryptocurrency is a digital currency that 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 needs to digitally sign a hash of the recent 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. Santoshi described it in the following manner:

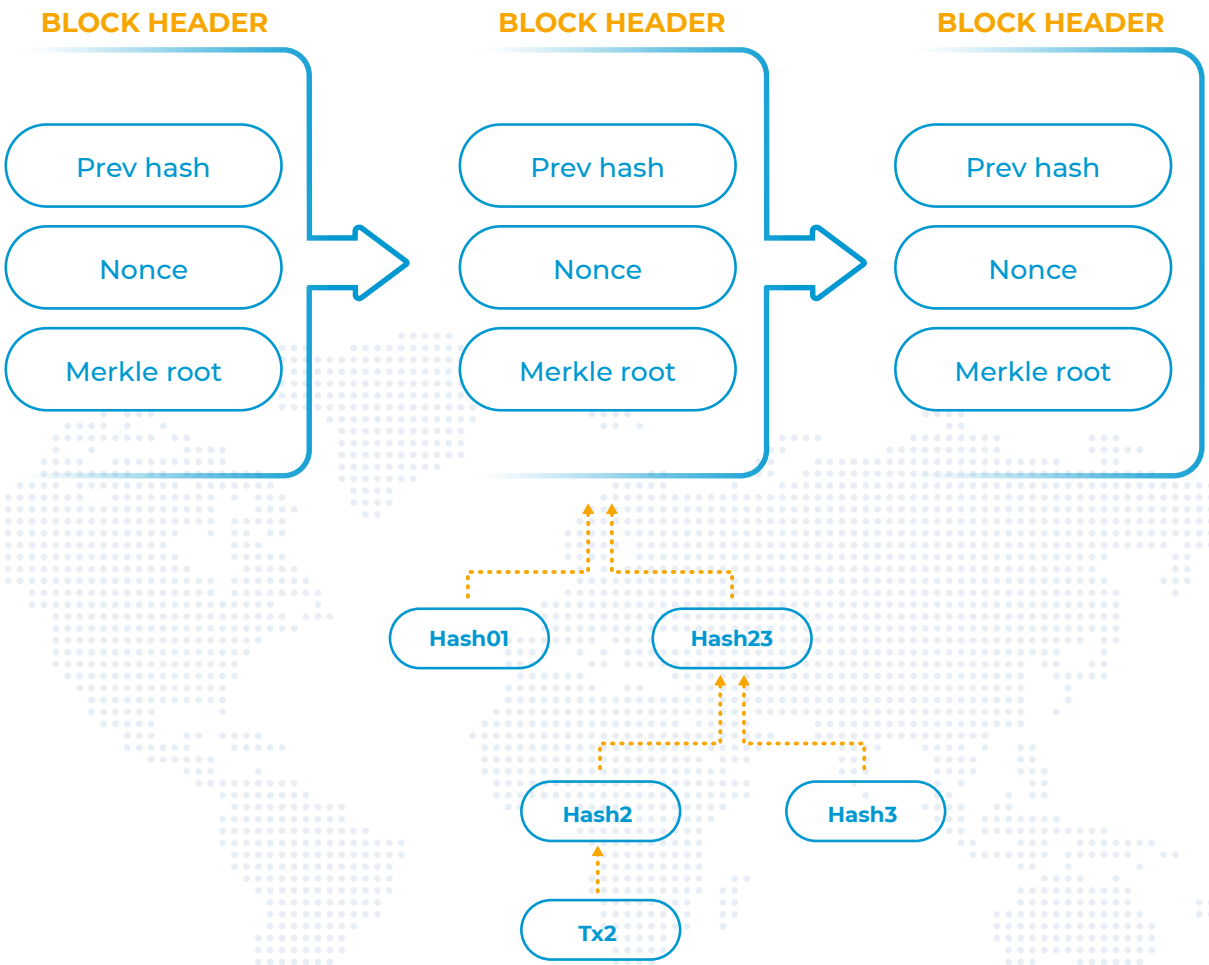
This process is neither time nor power consuming and assures the receiver that the sender is the true possessor of coins and can perform transactions. But this process does not provide the solution for the double spend attack. The owner of the coin can send the same coins twice or more times. In the 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 to get rid of double-spend attacks. Mining is also a process by which transactions are authenticated and affixed to the public ledger. The proof-of-work also establishes representation in the majority of decision making. Within the 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.

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



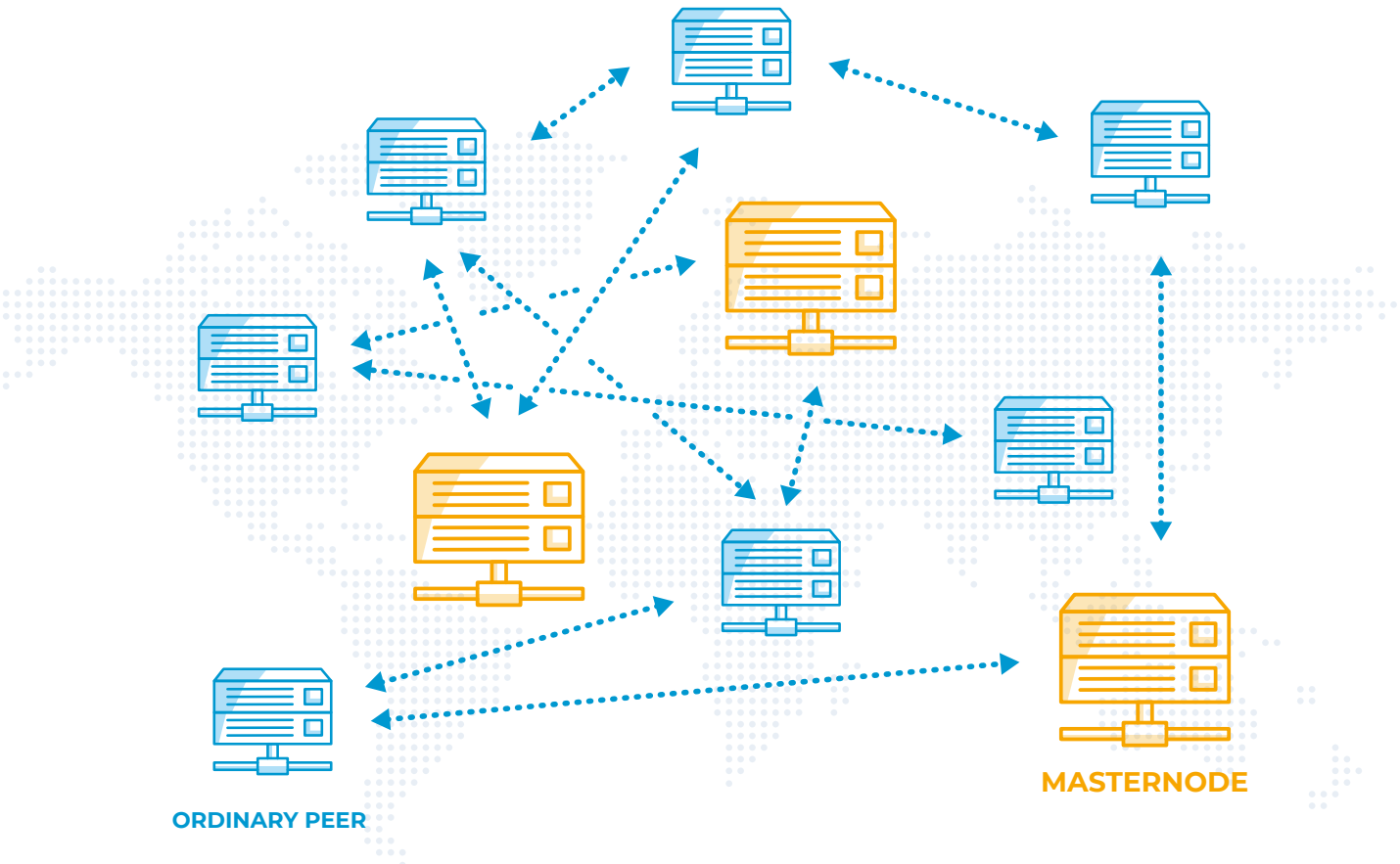
Two-tier network

Bitcoin uses a single-tier network where processes are executed through nodes. At the same time, FuturoCoin, on the other hand, utilizes a two-tier network. Masternodes act as a second layer. They are responsible for maintaining numerous network services. The servers are connected to mining and all other passing nodes and are always on.

Masternodes use several protocol expansions such as the Masternode ping message. The Masternode announces and disperses the message around the network. Regular peers and masternodes are typical in their connection behaviour. They form a classic P2P network. FuturoCoin ecosystems are responsible for fast transactions and management or administration with low and consistent transaction fees. In the future, we will describe this calculation.

Instant payments

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



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 an 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 a "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 FuturoCoin, no additional fee is needed for this kind of operation as all transactions are instant.

Low and constant transaction fees

With FuturoCoin, we have introduced the flat rate for all transactions. The fee model depends completely on the number of inputs applied in a transaction. Most commonly, this number is less than ten. To prevent a flood attack, we need to introduce certain security measures. When the number of inputs exceeds 10, the base fee is multiplied by 2, and so on. This 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 does not depend on the amount of coins being sent. Base minimal fee can be modified or altered by the spork functionality.

Reward distribution model

Masternodes grant some essential functions, which are not present in other cryptocurrencies.

In FuturoCoin, 50% of the block reward is given to miners, and 50% goes to masternodes. Masternodes are naturally distributed and secured autonomously by every owner.

Every user who would like to set up his masternode can do it freely. All that is required is to install the node, possess 10.000 FTO and configure the node to work as a masternode.

FuturoCoin uses a similar kind of enhanced strategies that are available in some cryptocurrencies. Amongst them are Multi-Phased Forks ("sporks"), which are related to global variables that can be altered by the developers' team.

An example of such a variable is a transaction fee. Transaction fees are modifiable by FuturoCoin developers and are dependent on many economic and technical parameters. The purpose is to have the most competitive transaction fee on the digital currency market.

Advanced security

FuturoCoin introduces refined solutions to numerous types of attacks that take place in the cryptocurrency world. 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 has all mitigations safeguarding the network from these kinds of attacks.

Instant transactions

FuturoCoin is a digital currency that makes transactions instant. Consensus is achieved through masternodes, which lock the inputs and validate transaction correctness.

Big and growing community of supporters

FuturoCoin's community's rapid growth helps us building a broad audience around the world. Apart from having a strong team of developers, it is essential to emphasize the vision and plans for FuturoCoin. These features make FuturoCoin exceptional and increase its scope.

PrivateSend functionality

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

Economics

Total coin emission

Since the start of FuturoCoin every block was rewarded by 13.31811263 FTO and the increase of FTO was linear. New version developed in March 2020 introduced a halving mechanism. Every two years supply of new FTO will be halved by two. After reaching 1.66476407875 per block, FTO protocol will switch into tail emission and stay on that amount.

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

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

Emission rate

Dark Gravity Wave algorithm is used in the case of difficulties retargeted. On average, new blocks will be mined every minute. Rewards started from 13.31811263 FTO and after introducing halving mechanism in March 2020 the reward will be halved every two years till reaching 1.66476407875 FTO. After this the protocol will switch into tail emission.

Block reward allocation

FuturoCoin divides every block reward in half:

- 50% goes to the winning miner,
- 50% goes to a masternode network. Masternodes can be are freely deployed by every node owner who possesses 10.000 FTO

Flat fee for all kind of transactions

One of the aims FuturoCoin was created for is to guarantee instant transactions with fixed fees at a competitive level and resolve scalability issues available in other cryptocurrencies.

Conclusion

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

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

FuturoCoin has terrific potential for development and growth. The World is ready for a cryptocurrency like FuturoCoin.

With a significant and growing community of supporters, we are confident about our vision and plans for FuturoCoin. We believe FuturCoin will play a crucial role in the world economy.


FuturoCoin