CROSTON COIN

A Peer-to-Peer Electronic Cash System

Croston Coin Developers
support@croston.io
https://croston.io

WHITE PAPER

INTRODUCTION

Croston Coin is the world's first integration of cryptocurrency's two foremost technological achievements — Bitcoin, and proof of stake consensus and the introduction of a backable cryptocurrency with Gold and other precious metals.

Today, Bitcoin core continues utilizing proof of work, a consensus algorithm that is slow, open to 51% attacks, costly to mine, harmful to the environment, and resistant to scalability. There are, however, many innovations unique to Bitcoin that require preservation, such as its 21 million token supply model and proven code-base developed by many of the world's foremost software engineers and cryptographers.

By combining Bitcoin's strongest assets with a highly efficient, scalable, flexible proof of stake consensus algorithm and brining an aged old idea of backing a currency with Gold, Croston Coin introduces a new paradigm for cryptocurrency utility.

Croston Coin does everything Bitcoin is currently able to do, while bringing new advances in blockchain technology onboard, and stability in cryptocurrency value thereby updating Bitcoin for the future. The value of Croston coin (CROS) will never drop but has great potentials of growth as mass adoption happens.

CRYPTOCURRENCY IS MONEY. WHAT IS MONEY THEN?

At its core, money represents value. For example, if I do some work for you, you give me money in exchange for the value I gave you. I can then use that money to get something of value from someone else at a future date.

Historically, value has taken many forms, and people used many materials to represent money. Throughout history, salt, wheat, shells, and gold have all been used as exchange methods.

However, for something to represent value, people have to trust that it is valuable and will stay valuable long enough for them to redeem that value in the future. Money was always represented by something until a century ago. Over the years, something happened that made us change our trust model from trusting something to trusting someone.

The invention of paper money came about as a result of people finding it too cumbersome to carry gold or other forms of money around the world.

In this system, a bank or government would take possession of one or more bars of gold, like one worth $5000, and in return give you receipt certificates, commonly referred to as bills, in the amount of $5000.

It was also easier to carry than gold bars, and you could buy a coffee for five dollars instead of cutting it into a thousand pieces. You could redeem your $5000 in bills, in this case, a gold bar, whenever you wanted to get your gold back by taking them back to the bank. Paper thus became an instrument of convenience and practicality when it began to be used as currency.

As time progressed and macroeconomic changes took hold, the bond between the gold receipt and its gold value broke down.

It is complex to explain what led us away from the gold standard but suffice it to say that governments told their people they would be responsible for the value of those paper money.

Rather than trade gold, we said, let's trade paper instead. So, people continued to trade receipts backed only by government promises.

Is there a reason that this continued to work?

Due to trust, of course. Since fiat money had no actual backing, people trusted the government, even though there was no actual commodity backing it.

By definition, fiat means "by decree." Dollars, euros, or any other currency are valued because the government orders them to be so. A coin or a banknote that is accepted as payment is known as "legal tender."

The value of today's money comes from a legal status that has been given to it by a central authority, in this case, the government. And so, the trust model has changed from trusting something to trusting someone, in this case, the government.

As a result, modern money acquires its value from the legal status it is granted by a central authority, in this case, the government. Consequently, trusting something has been replaced by trusting someone, in this case, the government.

Fiat money has two main disadvantages:

- Centralization: It is controlled and issued by a central authority. It's the government or central bank in this case.

- Second, it is not limited by quantity: The government or central bank can print money whenever necessary and inflate the money supply.

As a result of printing money, the value of each dollar drops, lowering your own money's worth. It is this effect that makes printing money so problematic.

Therefore, when you see prices rising over time, it's not because prices are going up so much; it's because your money has less purchasing power. As a result, you have to spend more money on something that used to "cost less."

MISSION

Currently, the world stands at a crossroads. The cryptocurrency revolution sparked by Bitcoin has yet to materialize for the masses, even though trust in financial institutions is at an all-time low. Over the years, most cryptocurrency projects have failed everyday users by over-complicating digital assets and under-delivering promises.

As Satoshi Nakamoto envisioned a bankless, financially independent, peer-to-peer electronic cash system, Croston aims to continue that vision. A secure cryptocurrency designed specifically for enterprise, payment, retail, and long-term investors, Croston is user-friendly, scalable, easy to adopt, and a great fit for millions of people in the world.

We are committed to making Croston the new standard by giving everyone an equal opportunity to manage and improve their financial security by providing an innovative, user-friendly, all-in-one platform.

We offer secure investments equivalent to gold and economic opportunities for those in communities where a capital market does not exist. We operate a community-focused, community-driven digital asset, fully decentralized.

Undoubtedly, blockchain technology is one of the most rapidly growing technologies in the world today. Croston is a digital currency that uses the proof of stake consensus mechanism of the Croston Blockchain.

As a result, we have built a network that is fast and secure at the same time, evenly distributed and does not lack integrity.

In this echo system, every coin is accounted for. The value of each coin is determined by the gram of Gold that backs it. As a result, your one Croston is equivalent to one gram of Gold. A new era of money is here. Welcome to the world where a time-tested proven commodity, GOLD, backs cryptocurrency.

WHAT IS PROOF OF STAKE?

A mining block must contain proof that the miner who generated it solved a computationally challenging task to achieve consensus in Bitcoin.

Due to its inherent self-destruction nature, the Proof-of-Work (PoW) base system is generally considered to be flawed. Unlike Proof-of-Work, Proof-of-Stake (PoS) relies on the staker who generates a block to prove that they have access to a certain amount of coins before the block is accepted.

Blocks are generated by sending coins to oneself, proving ownership. Similar to PoW, a difficulty adjustment process ensures an approximate, constant block time by specifying the number of coins to stake (also called stake).

Similarly to PoW, the block generation process will be rewarded through transaction fees and an underlying supply model, which is also the equivalent of an interest rate. A period of PoW mining is usually required to obtain the currency's initial distribution.

Croston works on the Croston blockchain; As of right now, our staking method is arguably one of the safest and most eco-friendly ways to earn passive income (for cryptocurrency). Investing and trading funds on this platform is quickly becoming a practice of staking to earn passive income.

Croston staking helps investors, including those needing more technical knowledge of cryptocurrencies, tokens, and coins, to receive rewards. A Proof of Stake is used for Croston staking, which is running on Croston blockchain. Croston offers exemplary staking services in addition to being the world's largest crypto exchange by volume.

Croston Staking ensures users' funds are safe by leveraging effective security measures and providing a Secure Asset Fund for Users (SAFU). With more individuals, including seasoned investors, understanding how profitable the crypto markets are, platform staking is quickly becoming a way to earn passive income by simply storing funds. As crypto staking has snowballed, various staking platforms have emerged that allow investors to collect staking incentives.

A Proof of Stake is used for Croston staking, which is running on Croston blockchain. Croston offers exemplary staking services in addition to being the world's largest crypto exchange by volume. Croston Staking ensures users' funds are safe by leveraging effective security measures and providing a Secure Asset Fund for Users (SAFU).

With more individuals, including seasoned investors, understanding how profitable the crypto markets are, platform staking is quickly becoming a way to earn passive income by simply storing funds.As crypto staking has snowballed, various staking platforms have emerged that allow investors to collect staking incentives.

Benefits of Staking

Staking in crypto has many advantages, including receiving block rewards and fees paid by blockchain users who want to prioritize their transactions before others as a reward for staking your coins or tokens.

You sometimes hear a validator in the POS system generating block rewards called “minting.” Since block rewards are not issued for solving puzzles (or “mining”), you may hear this described as “minting.”

Here are the benefits of cryptocurrency staking:

- It's an easy way to earn interest on your cryptocurrency holdings.
- You don't need any equipment for crypto staking like you would for crypto mining.
- You're helping to maintain the security and efficiency of the blockchain.
- It's more environmentally friendly than crypto mining.

PROBLEMS OF BITCOIN CENTRALIZATION

You shouldn't fix something that isn't broken, as the saying goes. While many Bitcoin proponents might argue that Bitcoin isn't broken, that view quickly evaporates when framed in the context of the future.

Bitcoin's current electricity-based miner-dependent design encourages the centralization of mining resources. Electricity and the mining hardware that runs on it are costly resources. Additionally, mining Bitcoin requires that one possess those resources, or ongoing access to them, in high supply.

Bitcoin PoW Creates Dependency on Electricity

Of all the resources most highly prized by Bitcoin miners, electricity correctly belongs at the top of any miner shopping list. But unfortunately, access to electricity is rare across all nations and regions.

Thus, some geographic areas are more likely to have electricity bottlenecks than others due to lower or higher prices per kWh. [2]

This allows miners in regions with cheap electricity to monopolize the Bitcoin mining industry. Monopolization is also called centralization, which Satoshi Nakamoto promised would be conquered in the original Bitcoin whitepaper.[3]

Governments exacerbate the problem in countries with high electricity costs, not recognizing and legitimizing Bitcoin mining in any way, which means tax write-offs and subsidies will not be available.

In light of the fact that governments have no interest in subsidizing electricity costs in order to benefit the decentralization of Bitcoin technology, there is no way to subsidize electricity costs for Bitcoin technology.

China is home to the most significant number of mining cartels in the world - and most of them profit from the practice. (4)

As a result of its dependence on electricity, Bitcoin rewards centralization instead of averting it. Since proof of work algorithms are based on the concept of proof of work, the mining outfit with access to cheap electricity typically outperforms, outmines, and benefits more financially than smaller global mining outfits.

These same miners were, once upon a time, the hope of creating a decentralized alternative to the current financial system.

“Now, the network is finding creative ways to tackle problems of mining centralization. With an aim to break the mining hardware monopoly and bring much-needed competition, Bitcoin Core contributor BtcDrak began a mining project, setting up an ASIC chip manufacturing company. While some strongly oppose it, a new initiative for the Blockchain Defensive Patent License is put forward as a way to counteract the AsicBoost patent monopoly that blocks competition, without jeopardizing the pristine protocol. Opportunities for the use of renewable energy are emerging as a way to decentralize mining. The idea is to take the excess capacity from
solar and hydro energy production and use them to mine bitcoin.” [5]

Although there is a shift in paradigm evident in the above quotation, electricity continues to be a significant energy source, albeit from alternative sources. It will, therefore, result in more of the same.

Bitcoin PoW Mining Hardware Centralization

The centralization of Bitcoin mining around Chinese regions is only one half of the centralization issue. Concurrent with it is the fact that the largest Bitcoin mining hardware suppliers are all Chinese, with titans of the industry like Bitmain and Canaan within those ranks.

What are the sizes of these organizations? In today's market, Bitmain is backed by world-renowned investors like Softbank and Tencent, and is valued at or near $15 billion USD. (6)

With backers like these, Chinese mining hardware suppliers can continue providing the crypto-mining industry with virtually unimpeded hardware.

Therefore, mining hardware and inexpensive hydroelectric power are plentiful in Sichuan, where Bitcoin hash rate dominance is primarily achieved.

By December 2019, 54% of Bitcoin's total hash rate came from the Sichuan province alone [7], creating an ethical quandary for Bitcoin supporters, developers, and users.

After years of competing with China, the US seemed poised to challenge it for mining supremacy or hash rate redistribution, but Chinese import tariffs, including those on mining hardware, dashed those hopes. Consequently, no attempt is presently being made to challenge the incumbent's hold on hash rate.

> *"The centralization of hashrate threatens the ultimate promise of cryptocurrency networks: that no one party or group controls the ledger or flow of transactions," said mining expert Kristy-Leigh Minehan to Crypto Briefing. "Any number of natural disasters or state-level threats could introduce network turmoil, whether through increased block times, transaction costs, or transaction censorship at the state-level."[8]*

Bitcoin's network and all its value are at risk due to the fact that most of its hashrate is concentrated in a few geographical areas. While there may not be a central bank or government at the head of Bitcoin, mining conditions within the regions that dominate Bitcoin hold real and troubling influence over the world's largest virtual currency.

The Bitcoin Proof of Work creates a massive strain on the environment

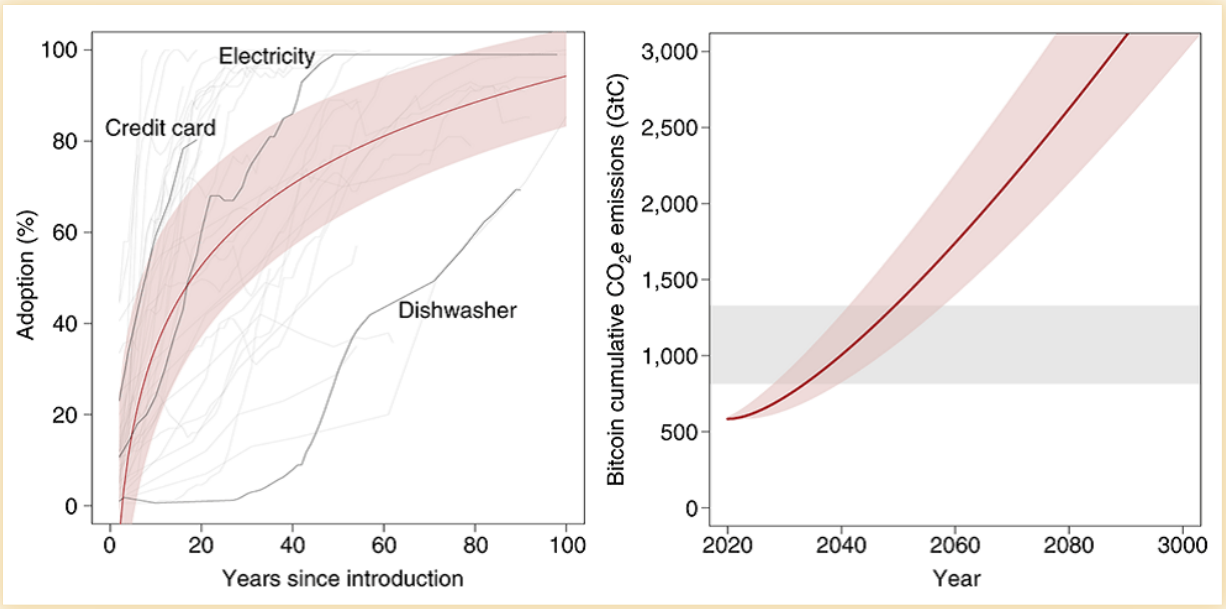
A centralized mining effort would be an enormous tax on the environment and be a significant contributor to climate change; as a result, global warming occurs.

BTC could play a significant role in breaching the 2-degree Celsius threshold with enough growth, according to a 2018 report in Nature on Bitcoin's contribution to climate change.[9]

While the world focuses on reducing emissions, there currently needs to be plans for creating a more environmentally friendly algorithm or making adjustments to PoW to alleviate environmental damage.

"The estimated emissions produced by Bitcoin last year alone is 69 million metric tons of CO2. Mora calls the numbers mind-blowing. "That is the source of concern for us. If this [technology] is so insignificant and the footprint is so big, can you imagine if this thing were to take off? " As Bitcoin gains popularity, it's energy demands increase dramatically. "We don't have a single thing–not agriculture, not transportation–that we can think of that in two decades would be enough to warm the planet by two degrees. But Bitcoin can."[10]

Bitcoin's adoption levels are still very low compared to major fiat currencies. Because of its immense environmental impact, a growing adoption of this technology will also have terrible consequences due to its dependency on guzzling electricity.



Source: Nature.com

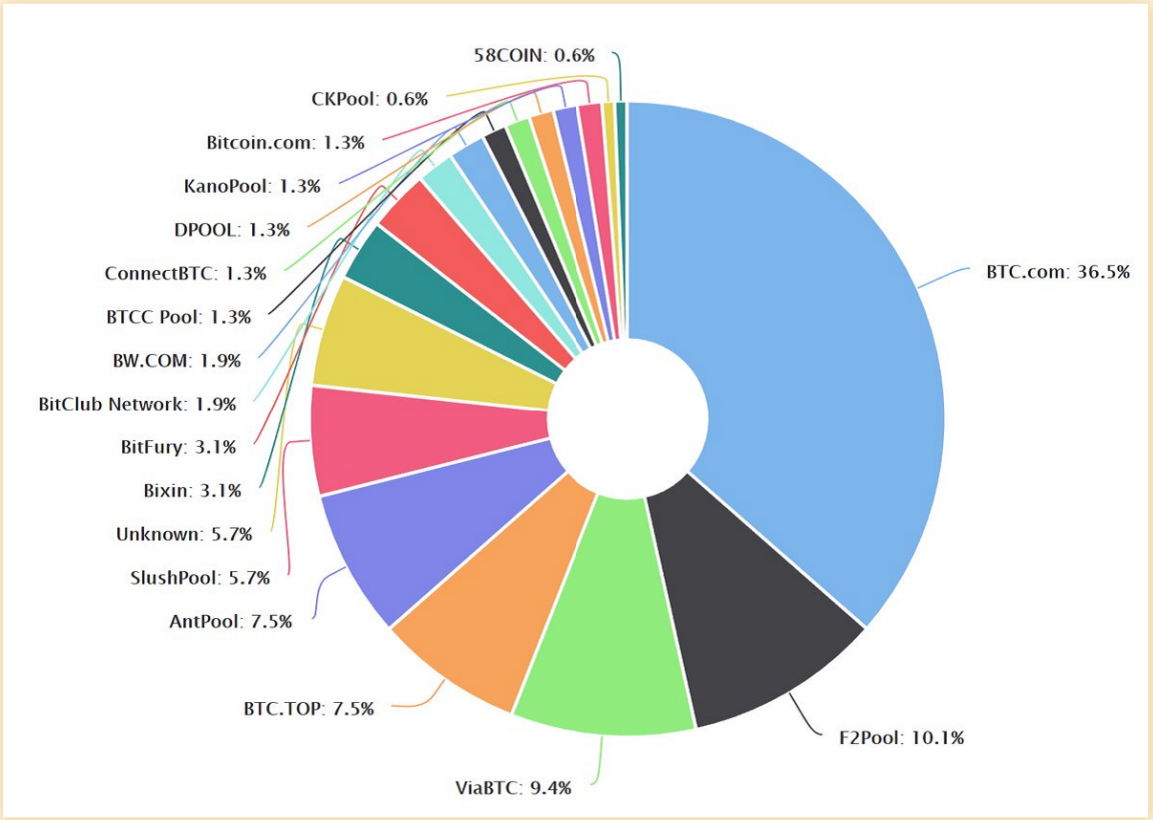
Currently, the Bitcoin network consumes 66.7 terawatt-hours of electricity due to its proof of work algorithm, which would power the entire Czech Republic. In other, more recent measures, Bitcoin is even outperforming Switzerland in terms of energy consumption and is on equal footing with medium-large countries. [11]

The irony in Bitcoin is that while it is a digital currency, it does not require paper, thus saving trees, but it is powered by a source that has a real impact on the environment.

A 51% attack is possible with Bitcoin PoW centralization

As if the proof of work algorithm wasn't already inherently flawed, security is another primary concern with Bitcoin's centralization. Since proof-of-work mining is centralized, it creates an unnecessarily concentrated locus of power for the network. It is unlikely that Bitcoin's gathered resources will survive a forceful or sophisticated event, whether it is natural, criminal, or otherwise. There is a high likelihood of the infamous 51% attack taking place.

Basically, a 51% attack refers to a group concentrating a majority of Bitcoin's hashrate, thus controlling the network and having the power to validate transactions fraudulently. Due to the financial resources required to perform a 51% attack on the BTC network (billions of USD, fluctuating with BTC value), it is unlikely but not impossible. A 51% attack is possible if the heads of different mining organizations band together and pool their hashrate, effectively crippling the network.



Source: bitcoin.com

Binance Academy's statement on 51% attack states that in the case of one being performed against the Bitcoin network, the following would probably happen:

> *Going further, let's imagine a scenario where a malicious entity is not motivated by profit and decides to attack the Bitcoin network only to destroy it, no matter the costs. Even if the attacker manages to disrupt the network, the Bitcoin software and protocol would be quickly modified and adapted as a response to that attack. This would require the other network nodes to reach consensus and agree on these changes, but that would probably happen very quickly during an emergency situation. Bitcoin is very resilient to attacks and is considered the most secure and reliable cryptocurrency in existence."[12]*

The position presented here is misleading. What happens when network nodes are compromised as well?

The assumption must be that an attacker who has enough wealth, resources, and influence to pull off a 51% attack could also coerce other nodes into standing by or disrupting the response enough to delay and render it ineffective.

China accounted for 74% of Bitcoin's hashrate in November 2019. Since tariffs have been imposed in recent years, the likelihood of that hashrate concentration increasing is high, despite no reason to believe that number has changed.[14]

CROSTON SOLVES BITCOIN'S CENTRALIZATION PROBLEM

The preceding sections have described many problems associated with Bitcoin's centralization. As an alternative to Bitcoin proof of work, Croston Coin introduces a new solution by replacing Bitcoin proof of work with Croston proof of stake.

The four problems associated with proof of work that combine to create an unnecessary centralized cryptocurrency are eliminated when we replace Bitcoin's PoW with PoS.

Due to its lower cost, lower barrier to entry, and less reliance on electricity, Croston is more appealing than other cryptocurrencies, decentralized and easily accessible, eco-friendly due to its gentle use of electricity, and more excellent resistance to 51% attacks because of its decentralized architecture.

Croston reduces our electric consumption by 99%

Looking at energy consumption worldwide, we are at a significant crossroads. A cleaner economy demands a better way to finance if we are to design the future of currency, and that way must meet the needs of a cleaner economy and a cleaner world.

Thus, Bitcoin is in dire need of an update, namely a proof of stake consensus algorithm. PoS reduces energy consumption by 99%, a figure that the Ethereum team has confirmed. Ethereum's discovery has accelerated the move away from PoW and towards PoS, that PoS reduces its dependence on electricity. Blockchain energy consumption is projected to be reduced by at least 99% using the proof of stake algorithm [13], leaving those still using PoW algorithms in the dark.

A reduction in the need for electricity allows network validation to take place on a more level playing field. On the Croston network, network validators do not have to worry about finding an electricity source that is cheap. Lightweight hardware requires only a minimal amount of electricity for PoS validation.

The amount of electricity needed to run a laptop is sufficient. However, in a PoS network, validators, called stakers, can delegate staking to a pool.
As a result, stakeholders can validate the network without running hardware themselves; nevertheless, their stake remains in their wallet, as usual, thereby circumventing the centralization of mining pools, too.

Croston Makes Staking Easy

A proof of work network requires miners to have access to cheap electricity and costly hardware mining rigs. By contrast, Croston requires no mining rig since proof of stake networks are lightweight and don't place a heavy burden on stakeholder hardware.

Stakers only need to create consensus around each transaction, whereas miners must solve complex algorithmic equations. As a result, they are rewarded according to the stake they hold.

It allows for true decentralization by reducing the material threshold for participating. Users can stake using regular hardware, such as laptops or desktop computers, or delegate their stake to a mining pool while retaining their staked Croston coins.

A key goal of the Croston design is to reduce the burden on network participants. As staker demands decrease, participation increases, and the network becomes more decentralized and flexible.

The paradigm for participation will only lead to the hoarding of resources that already exists if it requires the actor to have immense resources globally.

> Is blockchain for the 1% or everyone?

We must ask ourselves this question. Can blockchain be seen as an attempt to widen participation in the opposite direction?

We are fundamentally in favor of the latter approach, and we designed Croston to promote widespread participation.

Croston Is Eco-Friendly

We are the ones who will shape the future.
Everyone who cares about the future must also participate only in networks that understand the consequences of using environmentally destructive technologies such as PoW.

So, the Croston team is committed to making Croston green in order to improve blockchain technology. The only green aspect of Bitcoin speculation was its profits.

With the addition of proof of stake to the network, investors, speculators, and participants in the network alike can now rejoice in the fact that this is a digital currency that reduces the impact of blockchain.

The reason for proof of stake's environmentally friendly by design quality is described succinctly by Marc Blinder of the Harvard Business Review:

> *"While Bitcoin, Bitcoin Cash, and Ethereum all depend on energy inefficient cryptographic problem-solving known as "Proof of Work" to operate, many newer blockchains use "Proof of Stake" (PoS) systems that rely on market incentives. Server owners on PoS systems are called "validators" — not "miners." They put down a deposit, or "stake" a large amount of cryptocurrency, in exchange for the right to add blocks to the blockchain. In Proof of Work systems, miners compete with each other to see who can problem-solve the fastest in exchange fora reward, taking up a large amount of energy. But in PoS systems, validators are chosen by an algorithm that takes their "stake" into account. Removing the element of competition saves energy and allows each machine in a PoS system to work on one problem at a time, as opposed to a Proof of Work system, in which a plethora of machines are rushing to solve the same problem. Additionally, if a validator fails to behave honestly, they may be removed from the network — which helps keep PoS systems accurate."[15]*

The architecture of proof of stake is also elegantly simple. As an algorithm becomes increasingly difficult, instead of requiring unfathomably complicated machinery, The only thing stakers need to put up for validation is their skin in the game, a stake in the network's token. As a result of the simplicity of the proof of stake, fewer errors can occur than with more complex systems, and fewer resources are needed that strain the environment.

Croston Is More Secure Against 51% Attacks

Cryptocurrency advocates, investors, speculators, and network participants are concerned about security.

What person wants to lose everything because of a bug in the system?

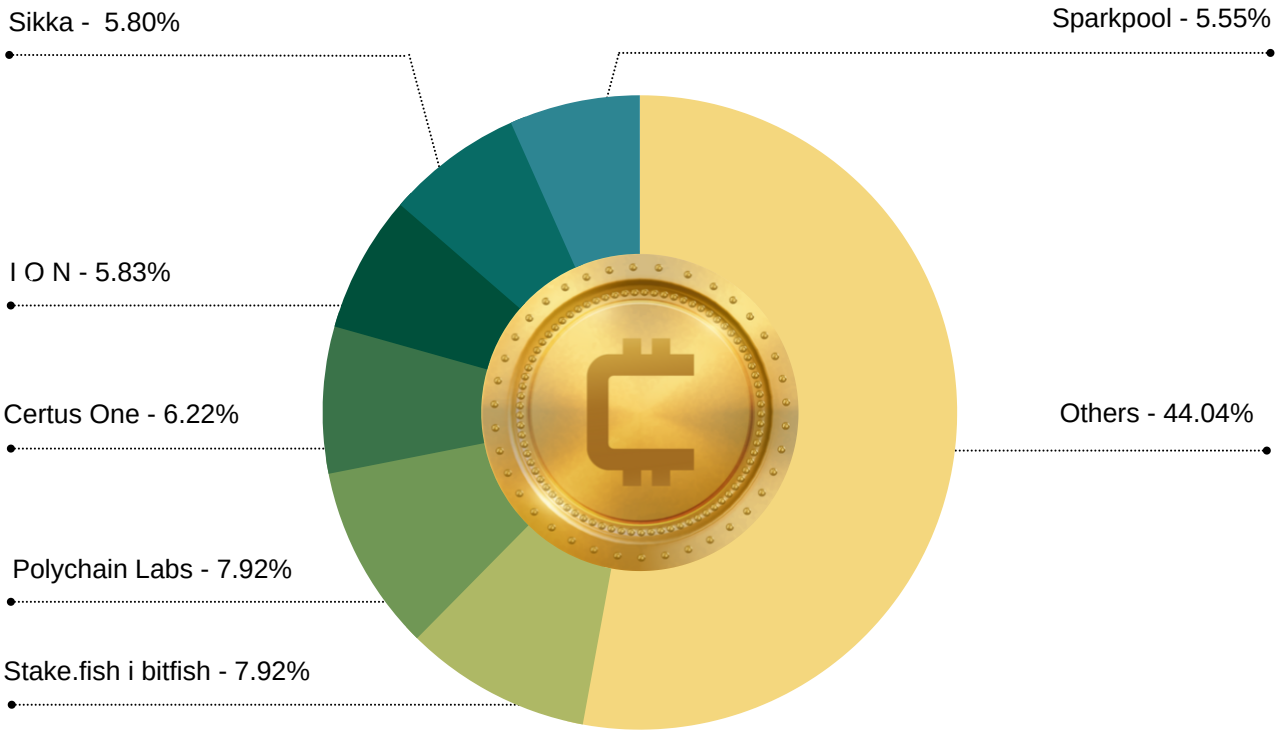
There is a flaw in Bitcoin, which is called centralization. A 51% attack becomes possible when mining creates a paradigm of centralization. The entire network, worth billions of dollars, would be at risk if an attack of this kind occurred. In such a scenario, the Bitcoin network would be destroyed.

Through its elegantly simple design, Croston uses only proof of stake and avoids the possibility of a 51% attack. For Croston, an attacker would need to control at least 50% of the token supply in order to attack the network, as opposed to 51% of the network hashrate for Bitcoin.

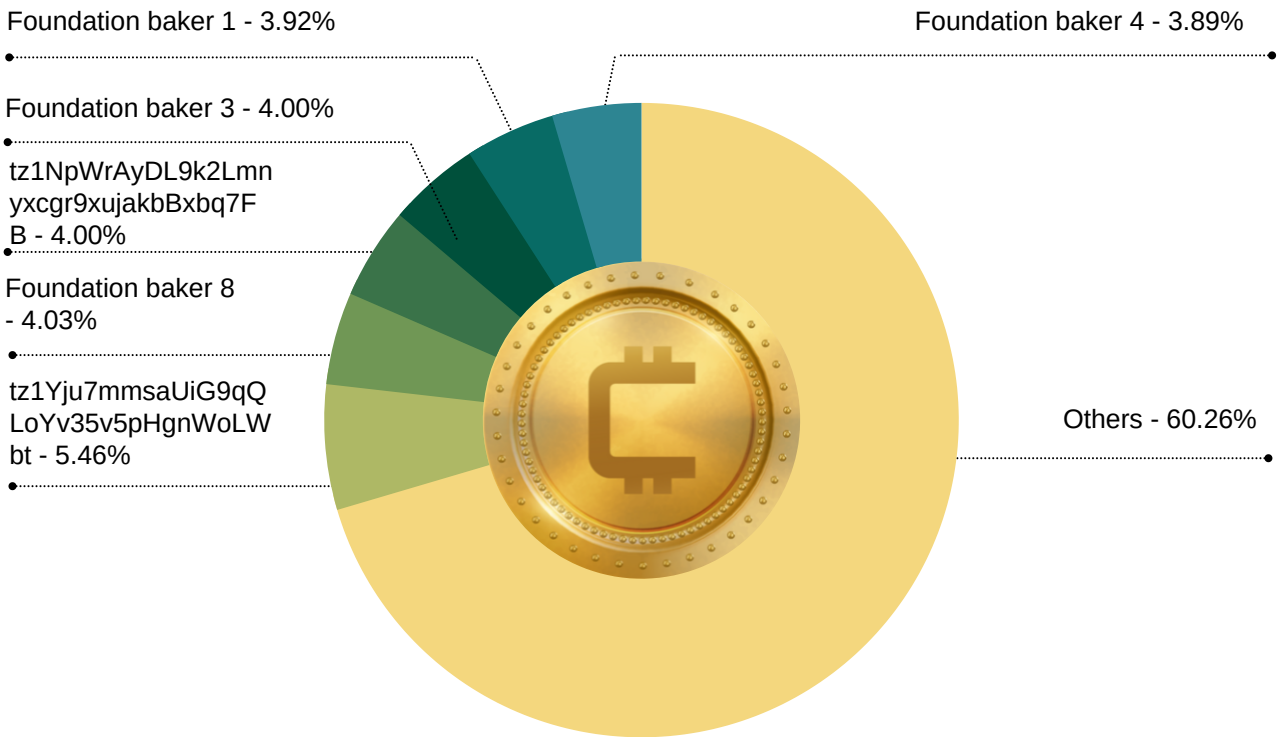
The importance of recognizing this difference cannot be overstated. It is possible to consolidate hashrate by establishing common interests among the heads of significant mining cartels. However, a token network cannot be consolidated by the same method since its members are spread across a larger cast of actors with varying aims, interests, and values. To convince token holders to sell or contribute their stake would be exceedingly difficult, if not impossible, and therefore not considered a threat to the Croston.

The use of stake pools within the proof-of-stake ecosystem has been accused as a potential source of centralization, despite their benefits for delegating stake and reducing technical knowledge. Staking pools, however, don't possess the tokens in a saleable form because they aren't required to hold the tokens being staked. As a result, 51% network attacks are less likely to occur not only in Croston but in all proof of stake networks

Voting Power Distribution Across Proof of Stake Cryptos (June 13, 2019)



Cosmos Voting Power



Tezos Voting Power

Source: Longhash.com

CROSTON ARCHITECTURE

Bitcoin's updated codebase forms the foundation of Croston. There is, however, a significant difference in the consensus algorithm. As opposed to proof of work, Croston relies on proof of stake to establish consensus.

It is important to note that Croston is not a Bitcoin chain fork. Instead, it is an original implementation of the Bitcoin codebase with several performances and consensus improvements that make Croston a superior choice for financial applications such as payments, allowing vastly improved network scalability.

Staking Prerequisites

The staking process involves holding funds in a cryptocurrency wallet to support its operation using blockchain technology. The goal is to receive rewards by locking cryptocurrencies.

For staking Croston, the following requirements must be met:

- Staked coins must be mature; that is, the unspent outputs (UTXOs) in the main chain must have a depth of at least 500 blocks (which is the coinbase / coinstake maturity)

- Coins staked must have incompatible addresses/transaction types
  (This document was written when the following was true, only P2PK and P2PKH are supported)

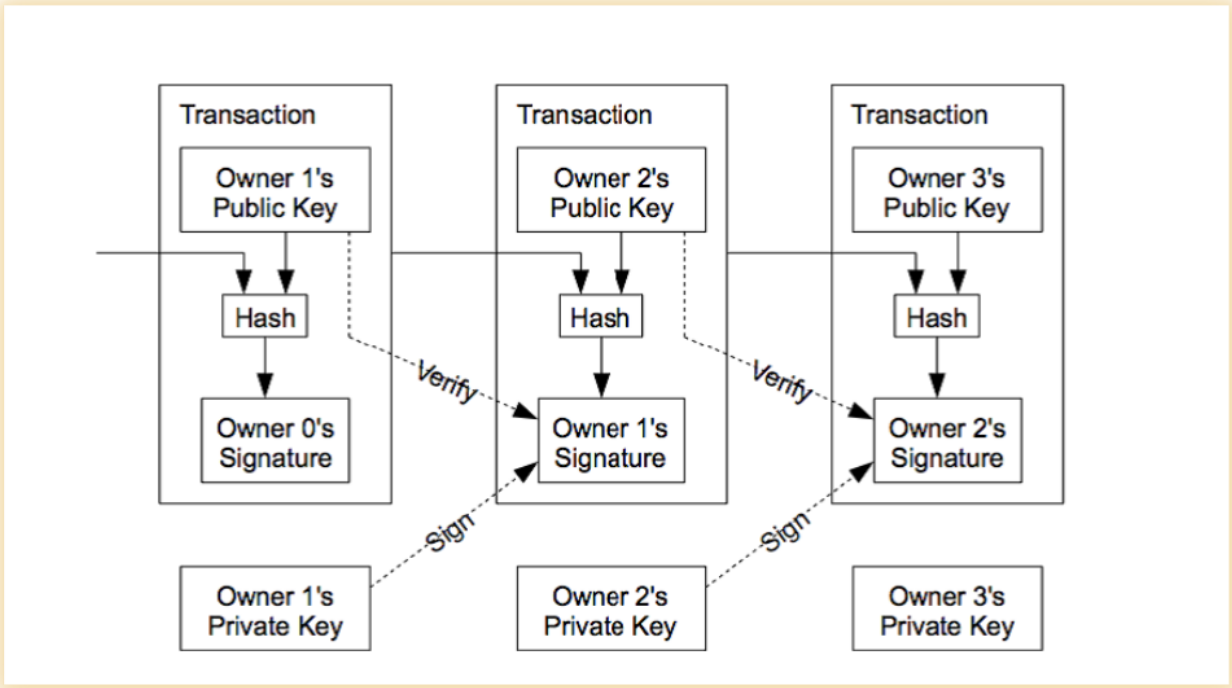
BLOCK STRUCTURE

Croston uses PoS V3 as consensus algorithm. The blocks must abide by these rules:

- Must have exactly 1 staking transaction
- The staking transaction must be the second transaction in the block
- The coinbase transaction must have 0 output value and a single empty vout
- The block timestamp must have it's bottom 4 bits set to 0 (referred to as a "mask" in the source code). This effectively means the blocktime can only be represented in 16 second intervals, decreasing it's granularity
- The block's kernel hash must meet the weighted difficulty for PoS
- The block hash must be signed by the public key in the staking transaction's second vout.The signature data is placed in the block (but is not included in the formal block hash)
- The signature stored in the block must be "LowS", which means consisting only of a single piece of data and must be as compressed as possible (no extra leading 0s in the data, or other opcodes)
- Most other rules for standard PoW blocks apply (valid merkle hash, valid transactions, timestamp is within time drift allowance, etc)

TRANSACTIONS

Like Bitcoin, Croston transactions function on the basis of public and private key signatures wherein a public key is verified, and the sender signs a private key



Double spending is discouraged in non-proof-of-stake blockchain networks because there is no incentive to stake every fork. Staking every fork is encouraged by proof of stake networks like Croston.

Do PoS systems increase the likelihood of double-spend transactions?

The answer is no.There are several drastic assumptions made in the above scenario, which, in reality, are nearly impossible. It is commonly referred to as the "nothing at stake" problem. Staking every fork is among those assumptions that are egregious since every staker is likely to stake every fork no matter how far-fetched it may seem.

The logistics and costs of motivating stakeholder support for a damaging fork are prohibitive since an attacker (or group of attackers) would need to reward them en masse.

That isn't the case with Bitcoin's proof of work algorithm. A mining cartel does not hold delegated coins, nor do they represent the interests of other parties. The fact that they possess unjustifiably high amounts of hashrate makes it possible for a double-spend attack to occur.

Double-spend attacks are, therefore, impossible with Croston transactions, and they retain the basic Bitcoin transaction infrastructure known and loved by users.

MUTUALIZED PROOF OF STAKE (MPOS) CONSENSUS

There are many types of proof of stake consensus algorithms. In addition to delegated proof of stake systems, such as EOS, there are also BFT PoS systems, such as Cosmos. When it comes to the latter, dPoS will add undue complexity to an already elegantly simple concept. Further, dPoS algorithms promote increased network centralization and don't create enough cost for attackers.

In addition, the Croston blockchain has implemented the Mutualized Proof of Stake consensus function, which further prevents the possibility of an attacker disrupting the blockchain.
In a nutshell, MPoS creates an impossibly high-cost barrier for malicious actors that is theoretically impenetrable.

MPOS EXPLAINED

Goals

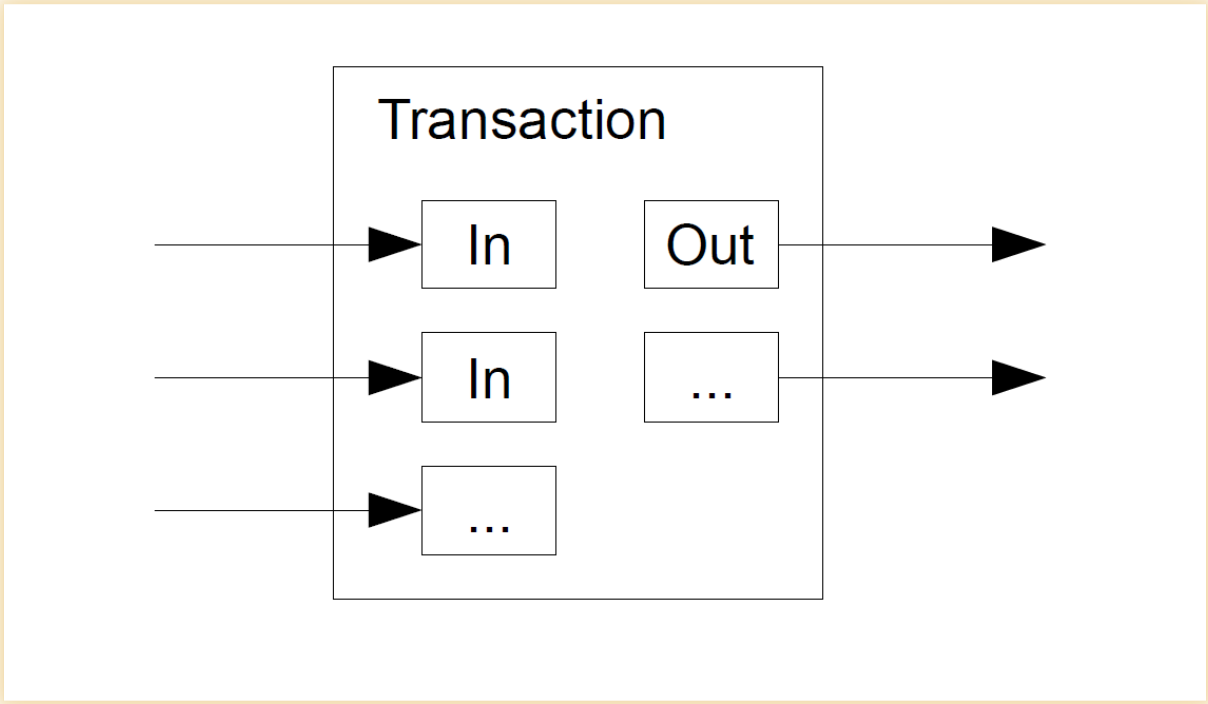
- Prevent malicious miners from attacking the network for free by constructing expensive to validate blocks, and then receiving all of the fees back to themselves through the mining process
- Help to make it more difficult and expensive for an attacker to DoS the network
  Procedure
- When a staker mines a block, he receives only a small portion of the PoS reward and fees. The rest of the reward and fees are shared with 9 other people.
- When a staker mines a block, his stake script (staketx.vout[0]) is registered to receive a share of the reward, lasting 10 blocks, 500 blocks from when the block was mined
- Thus, every block there will be 10 reward recipients. The creator of the block, and 9 "mutual stakers".
- 4. After 9 blocks of shared rewards, the staker's script will be removed, and another will be added to replace it
- If a stake script has mined more than 1 block in a 10 block period, then there can be a case where he receives 2x the share. However, once the earliest stake script instance exceeds 510 blocks from it's mined block, it is dropped and the reward drops to normal. Identical stake scripts should not be combined into a single UTXO, the rewards should be duplicated

MPoS prevents attackers from spamming the Croston network with fees. Rather than the entire fee going to a single block creator, all network participants share the fees. A spam attack becomes irrelevant with fee sharing in place and a rotation of stakeholder participants.

Moreover, because we have already deployed MPoS at scale on our test network, under widespread use, its success has already been demonstrated.

Stake Aggregation

As a means of eliminating practices like transaction flooding when staking with a high number of transactions (fan-out), Croston combines several inputs. First, it is a stake transaction (fan-in), which tries to increase the stake of the block. As a countermeasure to the unwanted effects of this input reduction mechanism, where large transaction outputs may result, if the stake exceeds a certain threshold, it will also be split into several outputs.



Croston Payments

The largest and most in-demand use case for cryptocurrencies is payments.

Digital payments powered by similarly digital currencies are gradually taking over cash as the world transitions to a paperless world.

Bitcoin cleared the way for this reality but has stumbled in several major categories.

- Bitcoin cannot scale to the needs of millions — or billions — of worldwide users.
- Bitcoin can't be easily integrated into existing payment rails and point-of-sale devices.
- Bitcoin confirmations take far too long, making it inefficient for real-time payments.

While some solutions, such as the Lightning Network, have been proposed and worked on, they are as yet missing from the space and have adoption issues of their own.

Croston has several advantages in the payments space. It is designed expressly for integration with existing payment systems, networks, and point-of-sale devices for a seamless cash-to-crypto experience. Wise design factors aid this transition.

- The small block size of Bitcoin systems is a scaling liability. Proof of stake blockchains such as Croston, reduce block times to handle more transactions per second, making them fast enough to handle the speed of real-time business.
- Block finality in Croston is improved over Bitcoin, which creates a major advantage for retailers and retail users as payments are settled nearly instantly and with finality.
- Whereas proof of work scaling solutions take network activity off the main chain and onto side chains,Croston high throughput capabilities mean scaling is handled on the same chain without relying on third-party solutions.

Croston Coin Supply

Croston coin is not designed to compete with Bitcoin. As a result, it will replace Bitcoin. This is due to the superior consensus algorithm, easy payment facilitation, vastly reduced power consumption requirements, and the fact that it is 100% backed by Gold to the ratio of 1:1.

Given these design goals, it is important to adhere strictly to the Bitcoin coin supply fundamentals, as Croston Coin pushes for strict adherence to Satoshi Nakamoto's original vision of a cashless, bankless, and third-party-free financial experience.

MAXIMUM COIN SUPPLY — 21 MILLION CROSTON COIN (CROS)

Croston Coin Block time

With a block time of 30 seconds, Croston Coin is many times faster than Bitcoin and can handle 20 times as many transactions as Bitcoin. A block difficulty algorithm based on exponential adjustments is used to calculate the difficulty, and it adjusts every block. Using this algorithm makes block times more predictable and less prone to big spikes.

The rewards for the blocks are split the following way:

- blocks 1 to 100 have a reward of 209,900 CROS (pre-mine)
- blocks 101 to 100000100 have a reward of 0.0001 CROS

The blocks from 0 to 10000 are proof of work blocks, pre-min is done by the founder; a portion of these funds will be allocated for continued development and maintenance of Croston Project.

Apart from under-the-hood differences in consensus making and a vastly improved performance, the look and feel of Croston Coins are strikingly similar to Bitcoin and will make the transition for Bitcoin users simple.

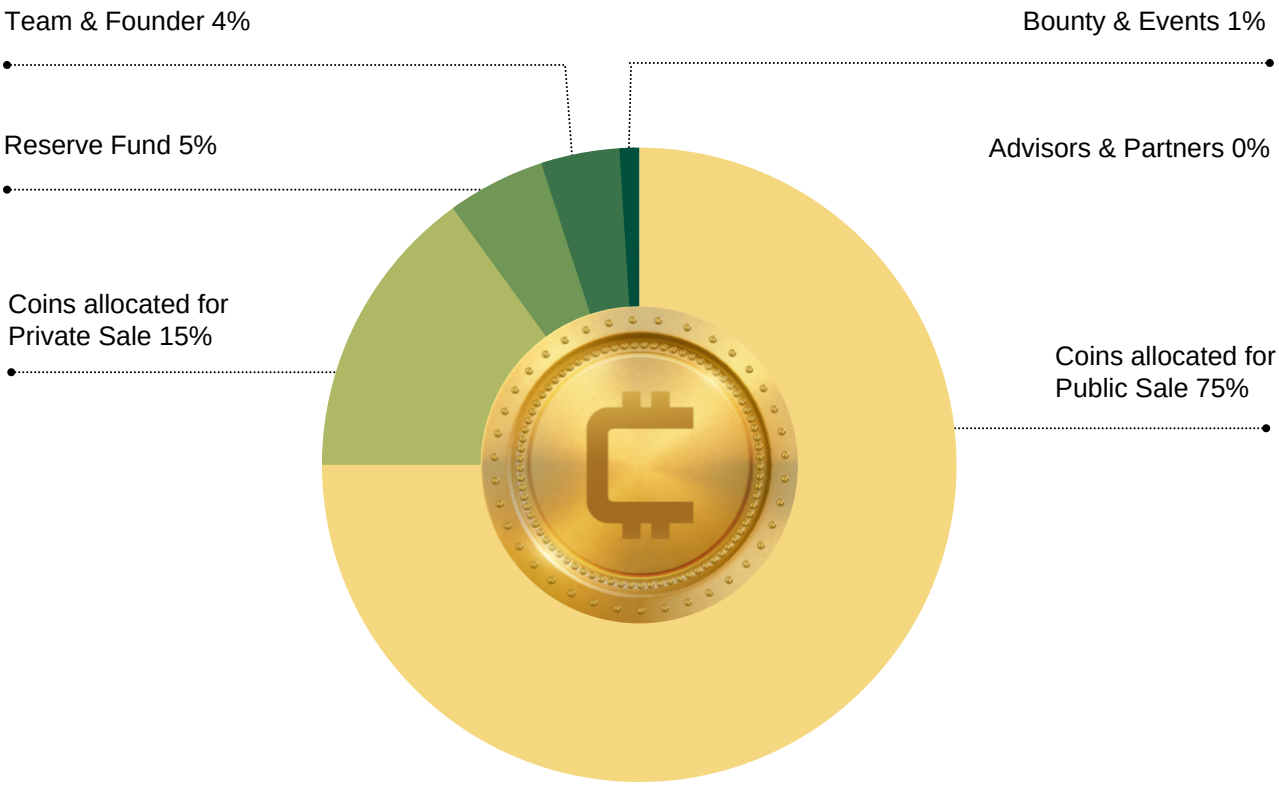
Proof of stake offers rewards to stakers according to stake size. Just as with Bitcoin proof of work mining, where rewards go to the miner who solves the block (known as block rewards), Croston Coins rewards also go to the staker but are split into ten equal rewards (using the MPOS algorithm); the chance of minting a block is proportionate to the stake size, meaning the higher the stake, the higher the chance is for the staker to mint a block before anyone else.
Croston Coins rewards stakers for securing and validating the network with fees collected from transactions.

Source: Ledger Academy

In order to accomplish proof-of-work mining, a great deal of energy must be expended, large amounts of money must be spent on hardware, and technical expertise is required. Croston Coin, on the other hand, can be staked in the background of other tasks, allowing you to earn passive income as a staker.

COINOMICS

- Coins allocated for Public Sale 75%
- Coins allocated for Private Sale 15%
- Reserve Fund 5%
- Team & Founder 4%
- Bounty & Events 1%
- Advisors & Partners 0%



ROADMAP FOR CROSTON COIN (CROS)

Q2 2022

Designing of the Platform and conducting technical demonstration

Q3 2022

Real time scanning. In-house testing of functional Prototype published and linked to Blockchain with real time scanning. Securing Physical Gold assets

Q4 2022

Launch for global sales Conducting the launch press tour Opening global sales of Croston Coin. Listing at various exchanges. Establishing Croston in other countries.

Q1 2023

Croston Pay
An all-new payment system that will allow retailers to accept Croston Coin (CROS), bitcoin and Ethereum. User can use CROS for travelling. Partnerships with Travel Industry players, Influencers, and service providers.

Q2 2023

Smart wallet capability
Multi-cryptocurrency wallet with smart wallet technology to store all currencies in just one wallet and pay without converting them.

Q3 2023

Croston will start offline crypto education centers with community collaboration.

Q4 2023

Croston will launch its own cryptocurrency exchange.

REFERENCES

- https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf
- https://www.eia.gov/energyexplained/electricity/prices-and-factors-affecting-prices.php
- https://bitcoin.org/bitcoin.pdf
- https://www.forbes.com/sites/youngjoseph/2019/12/12/new-report-shows-china-dominates-bitcoinmining-is-this-a-sign-of-worry
- https://bitcoinmagazine.com/articles/op-ed-challenge-mining-centralization-unveils-bitcoins-elegantdesign
- https://cointelegraph.com/news/bitmain-hits-15-billion-valuation-with-recent-backing-from-uberslargest-shareholder
- https://cryptobriefing.com/bitcoin-mining-centralization-record-levels-majority-china/bid.
- https://www.nature.com/articles/s41558-018-0321-8
- https://www.forbes.com/sites/andreamorris/2018/10/29/bitcoin-predicted-to-be-the-nail-in-thecoffin-of-climate-change/#47a1917e745e
- https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculationcambridge-index-cbeci-country-comparison
- https://www.binance.vision/security/what-is-a-51-percent-attack
- https://cointelegraph.com/news/the-dangers-of-mining-pools-centralization-and-security-issues
- https://bitcoinist.com/ethereum-pos-blockchain-cut-energy/
- https://hbr.org/2018/11/making-cryptocurrency-more-environmentally-sustainable

CONTACT US

+1 909 929 1235

+1 310 951 0644

info@croston.io

@CrostonFintech

facebook.com/Crostoncoin

@crostonfintech