2018

Carbon Zero Project

WHITE PAPER DRAFT - VERSION 0.3

Carbon Zero is a cryptocurrency project that offers a carbon neutral alternative to Bitcoin. The incremental reduction in greenhouse gasses from producing this alternative are issued as certified carbon credits[1] in the form of ERC-20 tokens. The proceeds from the sale of these carbon credits are disbursed to those that generated them – Carbon Zero Coin stakers and Masternode operators.

Introduction

Cryptocurrency

Cryptocurrency is a digital asset in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. It is designed to work as a medium of exchange, a source of income, and speculation. The purpose of this discussion is to solve a specific problem that exists with many cryptocurrencies. We're using cutting edge technologies to introduce new features to consumers, businesses, and governments that will provide tangible benefits well beyond security, privacy, and near-costless transactions for which cryptocurrency has become known.

Bitcoin

Bitcoin is a digital currency created in 2009. It follows the ideas set out in a white paper by the mysterious Satoshi Nakamoto, whose identity has yet to be verified. There are no physical bitcoins, only balances kept on a public ledger in the cloud, that – along with all Bitcoin transactions – is verified by a massive amount of computing power. Bitcoins are not issued or backed by any banks or governments, nor are individual bitcoins valuable as a commodity. Despite its not being legal tender, Bitcoin charts high on popularity, and has triggered the launch of other virtual currencies collectively referred to as Altcoins. [1]

Creation

On 18 August 2008, the domain name bitcoin.org was registered. Later that year on 31 October, a link to a paper authored by Satoshi Nakamoto[2] titled Bitcoin: A Peer-to-Peer Electronic Cash System was posted to a cryptography mailing list. This paper detailed methods of using a peer-to-peer network to generate what was described as "a system for electronic transactions without relying on trust". On 3 January 2009, the bitcoin network came into existence with Satoshi Nakamoto mining the genesis block of bitcoin (block number 0), which had a reward of 50 bitcoins. [2]

Who uses it

Many cryptocurrencies have come into existence in recent years, with Bitcoin the most prominent among them.[3] Although its short history has been volatile, the virtual currency maintains a core group of committed users. This paper presents an exploratory analysis of Bitcoin users. As a virtual currency and peer-to-peer payment system, Bitcoin may signal future challenges to state oversight and financial powers through its decentralized structure and offer of instantaneous transactions with relative anonymity. Very little is known about the users of Bitcoin, however. Utilizing publicly available survey data of Bitcoin users, this analysis explores the structure of the Bitcoin community in terms of wealth accumulation, optimism about the future of Bitcoin, and themes that attract users to the cryptocurrency. Results indicate that age, time of initial use, geographic location, mining

[1] Carbon credits is a generic term used to assign a value to a reduction or offset of greenhouse gas emissions. The standard representation of a carbon credit is equivalent to one ton of carbon dioxide equivalent (CO2-e)." [25]
[2] Satoshi Nakamoto is a pseudo-name used by the individual or collective that created Bitcoin. The real identity of Satoshi Nakamoto is not known.
[3] As of this writing, Bitcoin represents 57% of the total market capitalization of all cryptocurrencies worldwide [40]

status, engaging online discourse, and political orientation are all relevant factors that help explain various aspects of Bitcoin wealth, optimism, and attraction. [3]

Mining

All mining is intentionally designed to require a great deal of some resource. The problem being solved must be difficult enough so that the number of blocks found each day by miners remains steady. Individual blocks must contain a proof of something that is not easily produced but is trivial to check. The concept is identical to cryptography – one may create a public key if they possess the private key. It's also easy to check that the output of some combination of a private and public key are correct, but it's very difficult if not impossible to generate the private key if all you have is the public key. The primary purpose of mining is to allow cryptocurrency nodes to reach a secure, tamper-resistant consensus. Mining is also the mechanism used to introduce coins into the system: Miners are usually paid any transaction fees as well as a "subsidy"[4] of newly created coins. This both serves the purpose of disseminating new coins in a decentralized manner as well as motivating people to provide security for the system. When a node creates a block by solving a very difficult mathematical problem, a designated number of other nodes on the network can quickly verify the solution is correct. This allows people and their computers to conduct transactions with others even though they have no reason to trust them otherwise. The fact that trust between the parties is not required to complete a transaction is why this design is called "trustless". It has huge advantages over mainstream banking, which requires almost complete trust between parties where one party must always take a risk when initiating a transaction.

Proof of Work

Mining or minting of coins can take on several forms. The most widely used, and the type of mining that Bitcoin uses is called Proof of Work. A proof of work is a piece of data which is difficult (costly, time-consuming, computationally intense) to produce to meet certain requirements that are set forth in the coin's specification. It must be trivial to check whether the data satisfies said requirements. In other words, other nodes must be able to easily verify that the claimed solution is correct without the computational effort expended on providing the solution in the first place. Proof of Work is what we generally think of when we discuss mining. It is the consensus algorithm[5] used by Bitcoin and it's easy to understand and to prove the difficulty of the problems solved. That's because the resource used in a proof of work algorithm is simple to quantify – computing power, and therefore electricity. As computers become more advanced, the difficulty can be adjusted so that the requirement for computation power needed can outpace the rate at which technology advances and additional computing resources are added. The more computing power and electricity that is fed into the creation of bitcoin, the more difficult it becomes and the greater the demand for resources to create it – It's a perpetual cycle of increased power consumption. There is no other way to satisfy the requirements of a Proof of Work algorithm. The POW mining process is designed so that it will consume any amount of power put into it, without changing what it gives out.

Other Consensus Algorithms

Proof of Work may have been the first algorithm to create consensus in cryptocurrency, but it certainly isn't the only one. In fact, Proof of [enter word here] probably exists. For example, proof of *location*, proof of *platform*, proof of *capacity*, proof of *burn*, proof of *service*, proof of *authority*, proof of *elapsed time,* proof of *importance*, and proof of *storage* are all real consensus algorithms in use today. [4] [5] [6]. Some of them are so convoluted, they only make sense to the creator. Fortunately, most are experimental, but a few are simple and elegant enough to warrant consideration as a mainstream alternative to Proof of Work. As stated earlier,

[4] The subsidy is the amount given out by the coinbase as a reward each time a bock is completed this is the only mechanism by which new coins are introduced into circulation.

[5] A consensus algorithm is the mechanism by which several decentralized nodes can agree on something. In this case, other nodes MUST agree that the given solution is correct or it will be thrown out while additional solutions are calculated.

all these algorithms consume some type of resource, since that's what makes them effective. But that resource isn't always obvious – time is a resource, services are resources, platforms are a resource. Anything that can't be created quickly and easily (but not too easily) by a small number of individuals can be used as a resource for mining, although figuring out how to use a given resource for mining and the degree of security it can provide can be a little challenging. There are a few other consensus algorithms that are well developed enough to use in the mining process of cryptocurrency where the risks are real, and a well proven consensus mechanism is required. At the top of the list of alternative consensus mechanisms is Proof of *Stake*.

Proof of Stake

Like Proof of Work, Proof of Stake (PoS) is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS-based cryptocurrencies, such as Peercoin invented by Sunny King and Scott Nadal, the creator of the next block is chosen via various combinations of random selection and wealth or age. [7]

A Proof of Stake system combines randomization with the concept of "coin age", a number derived from the product of the number of coins multiplied by the number of days the coins have been held.[6] This assigns a number called a "coin weight" to each group of coins held in a wallet.

Coins that have been unspent for a set amount of time (staking maturity) begin competing for the next block. Older and larger sets of coins have a greater probability of signing the next block. However, once a stake of coins has been used to sign a block, it must start over with zero "coin age" and thus wait at least the maturity period before signing another block. Also, the probability of finding the next block reaches a maximum after a set number of days in order to prevent very old or very large collections of stakes from dominating the blockchain.

This process secures the network and gradually produces new coins over time without consuming significant computational power. [7]

The Problem

Six hundred trillion SHA256[7] computations are being performed by the Bitcoin network every second, and ultimately *these computations have no practical or scientific value; their only purpose is to solve proof of work problems that are deliberately made to be hard* so that malicious attackers cannot easily pretend to be millions of nodes and overpower the network. There is a problem: proof of work is highly wasteful [8] In the case of Bitcoin and other PoW coins, we are trading something of practical value (electricity) for something with no intrinsic value or practical use.

The Cost

Digital financial transactions using Proof of Work cryptocurrencies come with a real-world price: The tremendous growth of PoW cryptocurrencies has created an exponential demand for computing power. As

[6] This is a simplified version of how Proof of Stake works. In practice the algorithm is quite complex, but the computing power it uses is negligible comparted to Proof of Work.
[7] SHA256 is the specific algorithm used by Bitcoin. Other Proof of Work algorithms have been tried with the goal of making them "resistant" to newer hardware, thereby reducing difficulty and power consumption but they inevitable fall victim to hardware designed specifically for that algorithm. The processors created for this are called "ASICS". Therefore you will see newer algorithms advertised as "ASIC resistant", but this only holds true for a short time while the hardware is developed to defeat the algorithm.

bitcoin grows, the math problems computers must solve to make more bitcoin (the process called “mining”) get more and more difficult — a wrinkle designed to control the currency’s supply.

What is the cost of mining 1 Bitcoin? The short answer is around $6,000USD.

Just how much electricity is used to mine Bitcoin? It’s staggering.

Ever since its inception Bitcoin’s trust-minimizing consensus has been enabled by its Proof of Work algorithm. The machines performing the “work” are consuming huge amounts of energy while doing so. Digiconomist created The Bitcoin Energy Consumption Index to provide insight into this amount and raise awareness on the unsustainability of Proof of Work algorithm.

Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	73.12
Bitcoin's current minimum annual electricity consumption** (TWh)	54.41
Annualized global mining revenues	$4,750,974,177
Annualized estimated global mining costs	$3,656,073,069
Current cost percentage	76.95%
Country closest to Bitcoin in terms of electricity consumption	Austria
Estimated electricity used over the previous day (KWh)	200,332,771
Implied Watts per GH/s	0.155
Total Network Hashrate in PH/s (1,000,000 GH/s)	53,841
Electricity consumed per transaction (KWh)	898
Number of U.S. households that could be powered by Bitcoin	6,770,506
Number of U.S. households powered for 1 day by the electricity consumed for a single transaction	30.34
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.33%
Annual carbon footprint (kt of CO2)	35,830
Carbon footprint per transaction (kg of CO2)	439.89

[9]

What Exactly are the Miners Doing?

New sets of transactions (blocks) are added to Bitcoin's blockchain roughly every 10 minutes by miners. While working on the blockchain these miners aren't required to trust each other. The only thing miners have to trust is the code that runs Bitcoin. The code includes several rules to validate new transactions. For example, a transaction can only be valid if the sender actually owns the sent amount. Every miner individually confirms whether transactions adhere to these rules, eliminating the need to trust other miners. This "trustless" architecture is created by necessity.

It also means that you must get all miners to agree on the same history of transactions. So although every miner in the network is constantly tasked with preparing the next batch of transactions for the blockchain. Only one of these blocks will be selected to become the latest block on the chain. In proof-of-work, the next block comes from the first miner that produces a valid one, which takes about 10 minutes on average. Once one of the miners finally manages to produce a valid block, it will inform the rest of the network. Other miners check the transaction to verify the block is valid, they discard the work they have done, and the cycle starts again. The node that found the block first is the only one that receives a reward.

The process of producing a valid block is largely based on trial and error, where miners are making numerous attempts every second trying to find a valid block by incrementing a number called the "nonce". They are simply "guessing" and hoping the resulting completed block will match the requirements (as there is no way to

predict the outcome) The number of attempts (hashes) per second is given by your mining equipment's hashrate. This will typically be expressed in Gigahash per second (1 billion hashes per second).

As for the rewards the miners receive, they are usually sold immediately on the open market for fiat so the miners can pay for their electricity, cooling, and other costs. Because Bitcoin mining is a self-balancing system, the profit margins in mining it (and virtually all PoW cryptocurrencies are razor thin – sometimes as small as 1%. Holding onto the coins you produce isn't usually an option unless you like to gamble. This factor alone puts a constant downward pressure on the price of Bitcoin. Most of the minted supply goes into the market, increasing supply. The increase in supply by definition, causes inflation. No system can guarantee that newly minted coins don't constantly get dumped on the market, but there are other mechanisms that can be implemented in these networks that encourage owners to lock their coins into the network, making them temporarily unspendable, and getting rewarded for it. More about that later.

Security

51% attack refers to an attack on a blockchain – usually bitcoin's, for which such an attack is still hypothetical – by a group of miners controlling more than 50% of the network's mining hashrate, or computing power. The attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. They would also be able to reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins.

They would almost certainly not be able to create a create new coins or alter old blocks, so a 51% attack would probably not destroy bitcoin or another blockchain-based currency outright, even if it proved highly damaging. [10]

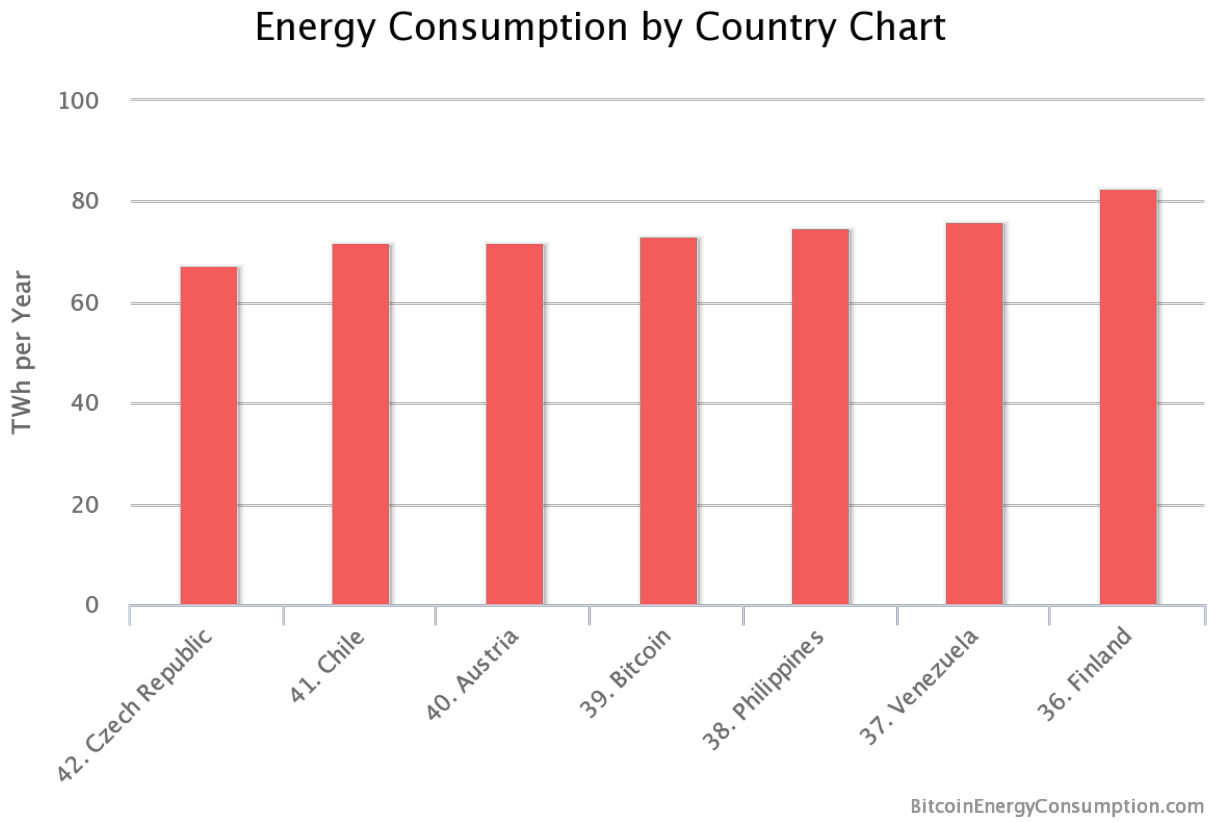
The only thing protecting Bitcoin from a 51% attack is the same thing that's destroying the planet – the hashrate has to continually outpace technology so that it is economically infeasible for an individual or group to effectively gain 5!% of the total hashrate being put into mining the coin. The very security that's preventing Bitcoin from being hacked is what causes it to devour so much of the world's energy. It's a catch-22 and it can't be solved with Bitcoin without leaving the network vulnerable to almost certain attack. The most vulnerable aspect of the security of Bitcoin is that someone mounting an attack on bitcoin doesn't have to own even a fraction of a Bitcoin to carry out the attack. There is no connection between the ownership of the coin and the process of mining it. It's easy to see why, with so much money at stake, there's a natural adversarial relationship between those that own bitcoin and those who want to hack it to steal it or even destroy it.

As you will see later, the Proof of Stake consensus mechanism – the means by which a Proof of Stake coin is created – is designed in such a way that your percentage of mining power compared to the whole is precisely the same as the percentage of the total coin circulation you own. It follows that at any given time if any person or group's ability to hack a Proof of Stake coin became feasible (which is unlikely because it would require owning 51% of the circulating coin), that hacking entity would also stand to lose the most in an attack. In other words, to mount this type of attack on a Proof of Stake coin would require owning 51% of the entire circulation. And if mounting an attack likely results in the demise of the coin… well such an attacker simply doesn't exist. Proof of Stake takes any incentive away from breaching the coins security because you would only be stealing from yourself – or worse destroying your coins while getting nothing in return.

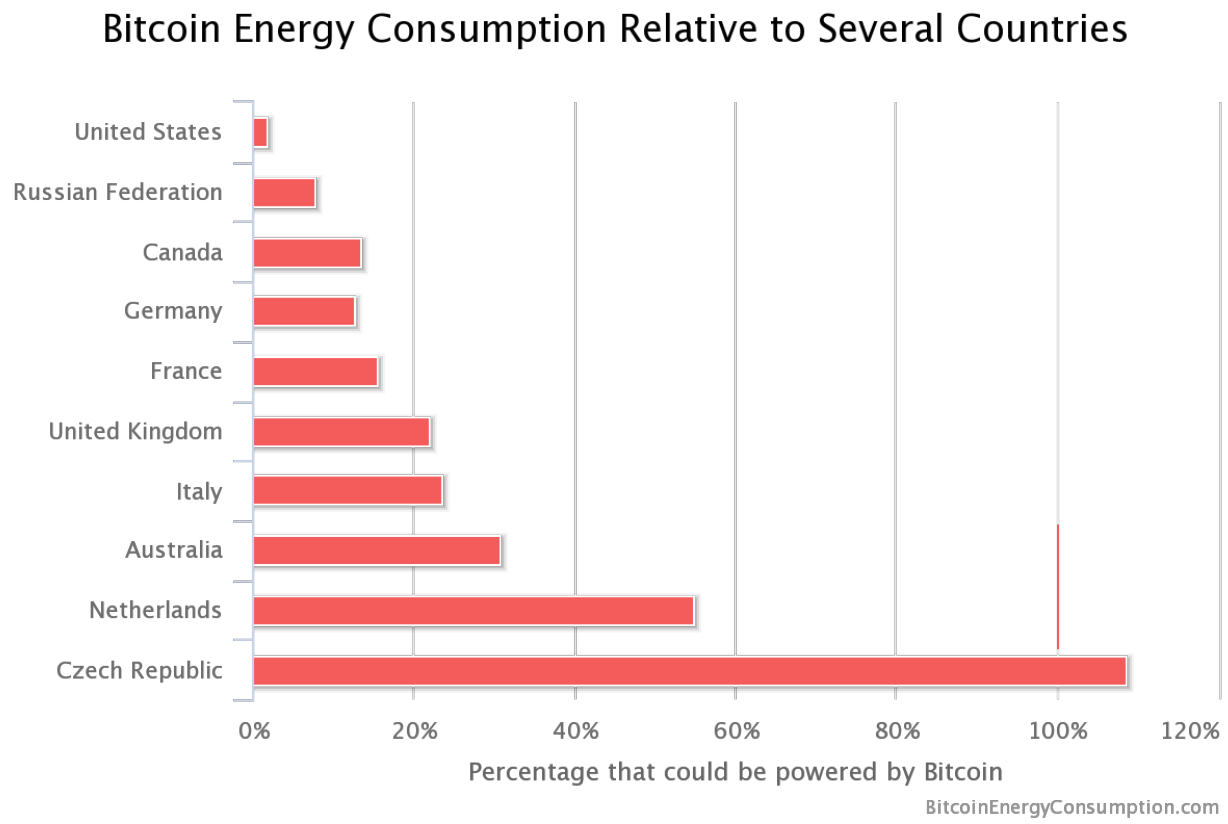
Sustainability

The continuous block mining cycle incentivizes people all over the world to mine Bitcoin. As mining can provide a solid stream of revenue, people are very willing to run power-hungry machines to get a piece of it. Over the years this has caused the total energy consumption of the Bitcoin network to grow to epic proportions, as the price of the currency reached new highs. The entire Bitcoin network now consumes more energy than a number

of countries, based on a report published by the International Energy Agency. [10] If Bitcoin was a country, it would rank as shown below.



Apart from the previous comparison, it also possible to compare Bitcoin's energy consumption to some of the world's biggest energy consuming nations.



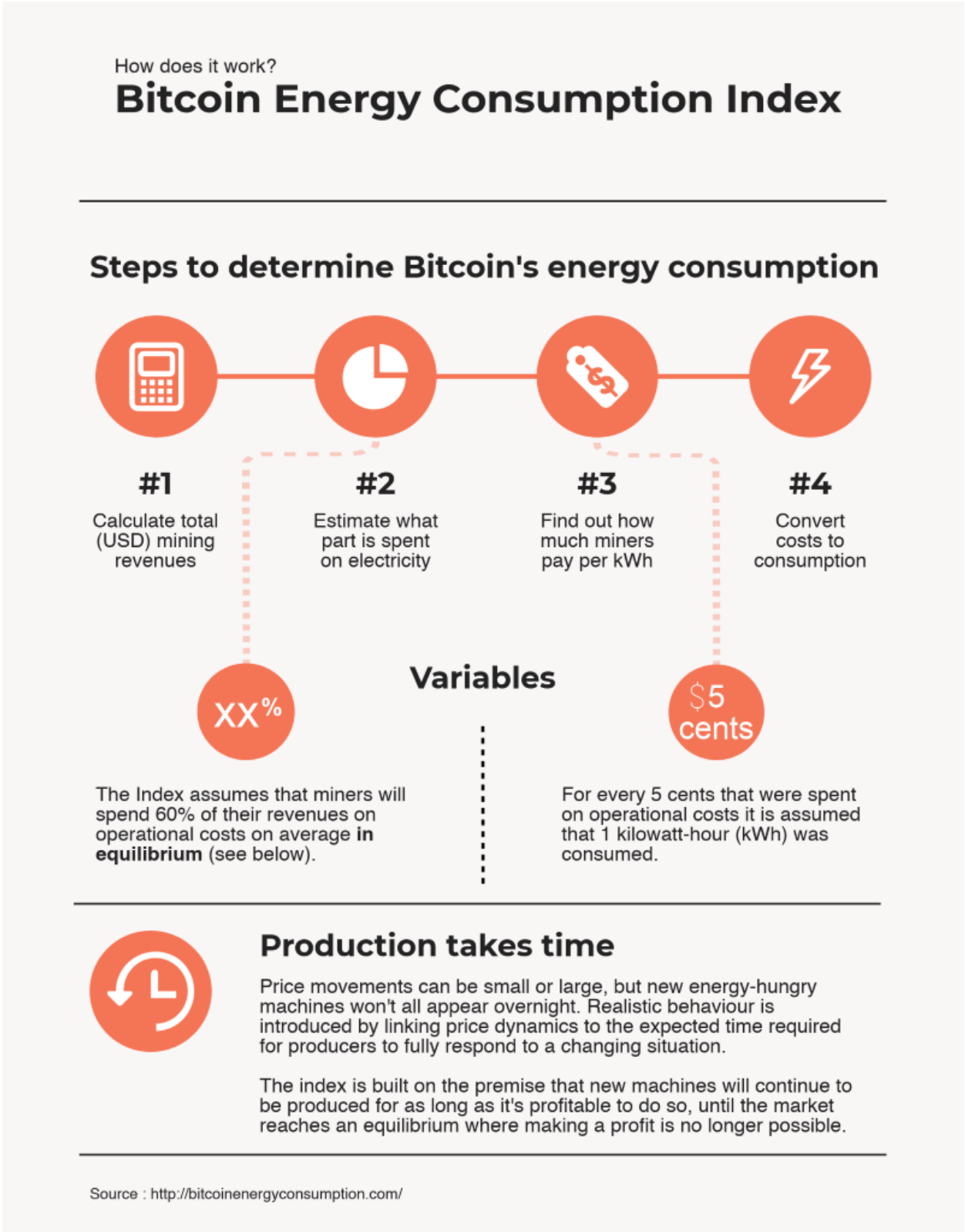
The Bigger Cost

Today, each bitcoin transaction requires the same amount of energy used to power nine homes in the U.S. for one day. And miners are constantly installing more and faster computers. Already, the aggregate computing power of the bitcoin network is nearly 100,000 times larger than the world's 500 fastest supercomputers combined. The total energy use of this web of hardware is huge — an estimated 31 terawatt-hours per year [11], about as much as Denmark. By the site's calculations, each Bitcoin transaction consumes 250kWh, enough to power homes for nine days. [12]. More than 150 individual countries in the world consume less energy annually. And that power-hungry network is currently increasing its energy use every day by about 450 gigawatt-hours, roughly the same amount of electricity the entire country of Haiti uses in a year. By February 2020, it will use as much electricity as the entire world does today. [11]

"By February 2020, it will use as much electricity as the entire world does today"

Global energy production obviously can't double in two years, and it would be an environmental disaster if it did.

The methodology used to create the Bitcoin Energy Index is illustrated below.


How does it work?
Bitcoin Energy Consumption Index
Steps to determine Bitcoin's energy consumption
#1
Calculate total (USD) mining revenues
#2
Estimate what part is spent on electricity
#3
Find out how much miners pay per kWh
#4
Convert costs to consumption
Variables
XX%
The Index assumes that miners will spend 60% of their revenues on operational costs on average in equilibrium (see below).
$5 cents
For every 5 cents that were spent on operational costs it is assumed that 1 kilowatt-hour (kWh) was consumed.
Production takes time
Price movements can be small or large, but new energy-hungry machines won't all appear overnight. Realistic behaviour is introduced by linking price dynamics to the expected time required for producers to fully respond to a changing situation.
The index is built on the premise that new machines will continue to be produced for as long as it's profitable to do so, until the market reaches an equilibrium where making a profit is no longer possible.
Source : http://bitcoinenergyconsumption.com/

[9]

Carbon footprint

Bitcoin's biggest problem is not only its massive energy consumption, but that the network is mostly fueled by coal-fired power plants in China. Coal-based electricity is available at very low rates in China. [13] This type of electricity has an emission factor of up to 1 kg CO2e per kilowatt-hour (KWh). Even with this conservative estimate, this results in an extreme carbon footprint for each unique Bitcoin transaction.

Alternatives

Proof-of-work was the first consensus algorithm that managed to prove itself, but it isn't the only consensus algorithm. More energy efficient algorithms have been in development over recent years. The one we will be discussing here is proof-of-stake, since this is the consensus algorithm used By CarbonZero. It is also the only other Consensus mechanism that has a proven track record in the world of cryptocurrency.

A Proof of Stake system does not require power hungry machines that produce as many hashes per second as possible to be profitable. Because of this, the energy consumption of proof-of-stake is negligible compared to proof-of-work. At the same time, a Proof of Stake network is very secure, partly because outside interests are not allowed to mine the coin as in Proof of Work. Creating new coins is tied to an existing ownership interest in that coin.

Security

In Proof of Stake the coin owners, not miners, create blocks. Anyone creating new blocks, and therefore earning rewards, must already have a vested financial interest in the network. Coins are mined by other coins – the greater one's holdings, the more they have at risk, and the less likely they are to become bad actors. In fact, there is generally no financial incentive in a properly designed Proof of Stake system to undermine the network – you would only be stealing from yourself. In a PoS network, the miner is limited to mining a percentage of the transactions that reflect his or her ownership stake. To carry out a 51% attack[8], which would only require 51% of the total hashing power on a Proof of Work network, to carry out a 51% attack on a POS network would require owning 51% of the total circulating supply of that cryptocurrency. And while it might be possible to assemble 51% of the hashing power of a PoW coin, with a PoS coin, the attacker would have to buy more than half of the target currency to stage such an attack. We can add more and more stakers and masternode owners over time without creating the huge demand for power. Our security can and will scale to a large degree higher than the existing Bitcoin code. A 51% attack is difficult and costly mount even on a small network. The network only grows stronger over time. Since it's common for well over 60% of coins to be locked in masternodes, a 51% attack would require AT LEAST ALL of the remaining 40% of coins in circulation. Not only is this possible, but if it were, then most of the network would be owned by the proposed attacker. And unless that attacker is one of the duller crayons in the box, he or she isn't going to attack a cryptocurrency of which they own over half. That's the beauty of requiring coin ownership to secure the network.

The Solution

There is one SHA256 alternative that is already here, and that essentially does away with the computational waste of proof of work entirely: proof of stake. Rather than requiring the prover to perform a certain amount of computational work, a proof of stake system requires the prover to show ownership of a certain amount of the cryptocurrency. [8] Doing so requires very little computational power. PoS is a consensus protocol that works

[8] A 51% attack can happen on PoW networks like Bitcoin IF someone or some group of individuals manages to get enough hashpower to be at least 51% of it. At that point, they would complete control over the network. What's scary about that is that this type of attack on bitcoin today would only take less handful of the most prolific bitcoin miners in the world to combine their forces. And on a PoW network, a 51% means you're done. The coin would likely become worthless. But before that's even noticed, the hacker would have made a huge profit.

smarter, not harder. It's not as simple as the brute force mechanism that defines Proof of Work, but when designed and implemented properly it carries with it some substantial benefits.

Etherium founder Vitalik Buterin openly supports [moving Etherium to Proof of Stake] by stating that not a single case has been seen of a Proof-of-stake network being hacked. https://t.co/gH2W03p3MM Honestly asking, has there even been a *single* instance of a PoS blockchain being 51% attacked? — Vitalik Buterin (@VitalikButerin) September 4, 2016 [14]

Under proof of work, miners may potentially own none of the currency they are mining and thus seek only to maximize their own profits. This disparity can raise security risks. Under proof of stake, however, those "guarding" the coins always own the coins, although several cryptocurrencies do allow or enforce the lending of staking power to other nodes. [7] CarbonZero does not allow such lending or proxy control of other's coins because we firmly believe it invalidates some of the most significant security mechanisms in place with Proof of Stake. Allowing someone to vote for you and stake for you in delegated proof of stake really makes no sense for the coin and the majority of it's owners, especially since it drives the network toward centralization of security. To take over the network, all I would have to do is convince 51% of the owners to allow me to stake their coins for them. It's difficult to visualize a use case where encouraging a more centralized architecture would make sense for anyone other than unscrupulous founders and, in any case, more decentralized=more secure. A Proof of Stake system that has a mechanism to consolidate staking inputs under fewer people makes no sense. I'm sure there are projects that say otherwise, but fully investigate why they are advocating a system that increases centralized control over the default. It is *very* important that you understand that before getting involved. Your rights as an owner are paramount to the PoS system and to other components that we'll introduce shortly.

Of course, this is a greatly simplified explanation about how Proof of Stake Consensus Algorithms work. The actual implementation and mathematics range from a bit more complex to an order of magnitude more complex for PoS versions 1 through 3 respectively. The next few sections will describe Carbon Zero's Proof of Stake V3 Protocol (CZPoSV3). It's a technical explanation of he our Proof of Stake Protocol works to perhaps encourage peer review, but it might not be of great interest to the average reader. If that's the case, feel free to skip over it. It will not affect your understanding of the Carbon Zero Project. But if you like this stuff, dig in!

Carbon Zero Proof of Stake V3 Protocol (CZPoSv3)

PoSv3's History

Proof of Stake V3 is not exclusive to Carbon Zero. Our implementation is adapted from the PoSV3 standard with additional features that provide additional security, checks, and balances. Proof of Stake has a fairly long history. We won't cover every detail, but explain broadly what was changed between each version to arrive at PoSv3 and ultimately CZPoSv3:

PoSv1 - This version of PoS is implemented in Peercoin. It relied heavily on the notion of "coin age", or how long a UTXO has not been spent on the blockchain. Its implementation would basically make it so that the higher the coin age, the more the difficulty is reduced. This had the bad side-effect however of encouraging people to only open their wallet every month or longer for staking. Assuming the coins were all relatively old, they would almost instantaneously produce new staking blocks. This however makes double-spend attacks extremely easy to execute. Peercoin itself is not affected by this because it is a hybrid PoW and PoS blockchain, so the PoW blocks mitigated this effect, demonstrating that it is still a viable protocol under certain circumstances.

PoSv2 - This version removes coin age completely from consensus, as well as using a completely different stake modifier mechanism from v1. The number of changes are too numerous to list here. All of this was done to remove coin age from consensus and make it a safe consensus mechanism without requiring a PoW/PoS hybrid blockchain to mitigate various attacks. [15]

PoSv3 - PoSv3 is more of an incremental improvement over PoSv2. In PoSv2 the stake modifier also included the previous block time. This was removed to prevent a "short-range" attack where it was possible to iteratively mine an alternative blockchain by iterating through previous block times. PoSv2 used block and transaction times to determine the age of a UTXO; this is not the same as coin age, but rather is the "minimum confirmations required" before a UTXO can be used for staking. This was changed to a much simpler mechanism where the age of a UTXO is determined by its depth in the blockchain. This doesn't incentivize inaccurate timestamps to be used on the blockchain and is also more immune to "timewarp" attacks where the time is changed to trick the system into assigning an older age to the coin. There are multiple checks in place so that several components of coin age must agree to consider a UTXO valid for staking. CZPoSv3 also added support for `OP_RETURN` coinstake transactions which allows for a vout to contain the public key for signing the block without requiring a full pay-to-pubkey script.

CZPoSV3 Structures and Rules

The core code in CarbonZero, just like almost all cryptocurrencies, is essentially Bitcoin Core. This means that we're starting out with all of the mature features and mechanisms that the Bitcoin Core team has developed over the last decade. Everything we develop for the Carbon Zero blockchain is built on a Bitcoin foundation. Therefore the actual mechanics of the blockchain are not a concern. Bitcoin code is very modular, which allows us to change out the PoW consensus mechanism with a PoS consensus mechanism without making too many changes to the core code that we know already works. Most of that changes is in the way the *kernel hash* is handled.

The kernel hash is composed of several pieces of data that are not readily modifiable in the current block. And because Proof of Stake miners do not have an easy way to modify the kernel hash, they cannot simply iterate through a large amount of hashes like in PoW.

Proof of Stake blocks add many additional consensus rules to realize its goals. First, unlike in PoW where the coinbase transaction (the first transaction in each block) must be empty and reward 0 tokens. Instead, to reward stakers, there is a special "stake transaction" which must be the *2nd transaction* in the block. A stake transaction is defined as any transaction that:

- Has at least 1 valid `vin`
- It's first `vout` must be an empty script
- It's second `vout` must not be empty

Furthermore, staking transactions must abide by these rules to be valid in a block:

- The second `vout` must be either a pubkey (not pubkeyhash!) script, or an `OP_RETURN` script that is unspendable (data-only) but stores data for a public key
- The timestamp in the transaction must be equal to the block timestamp
- the total output value of a stake transaction must be less than or equal to the total inputs plus the PoS block reward plus the block's total transaction fees. `output <= (input + block_reward + tx_fees)`
- The first spent vin's output must be confirmed by at least 720 blocks (in other words, the coins being spent must be at least 720 blocks old)
- Though more vins can used and spent in a staking transaction, the first vin is the only one used for consensus parameters.

These rules ensure that the stake transaction is easy to identify and ensures that it gives enough info to the blockchain to validate the block. The empty vout method is not the only way staking transactions could have been identified, but this was the original design from Sunny King and has worked well enough.

Now that we understand what a staking transaction is, and what rules they must abide by, the next thing is to cover are the rules for Carbon Zero PoS blocks:

- 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 its 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 its granularity
- The version of the block must be 7.
- A 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)

The details above are not very important to understand to understand the project or even the concept of staking. If you take away one concept from this technical section, it would be that what the effectiveness of PoS lies in the “kernel hash”.

The CZPoSV3 Kernel Hash

The kernel hash is used in a way that is similar to PoW (if hash meets difficulty, then block is valid). However, the kernel hash is not directly modifiable in the context of the current block. We will first cover exactly what goes into these structures and mechanisms, and later explain why this design is exactly this way, and what unexpected consequences can come from minor changes to it.

Carbon Zero uses Proof of Stake V3 to provide the fastest, most robust, and most secure network that can be built. Part of the creation of a block in PoS V3 requires the kernel hash to consist of specific data in a precise order.

- Previous block's "stake modifier"
- Timestamp from "`prevout`" transaction (the transaction output that is spent by the first vin of the staking transaction)
- The hash of the `prevout` transaction
- The output number of the `prevout` (which output of the transaction is spent by the staking transaction)
- Current block time, with the bottom 4 bits set to 0 to reduce granularity. This is the only thing that changes during the staking process

The stake modifier of a block is a hash of exactly:

- The hash of the `prevout` transaction in PoS blocks.
- The previous block's stake modifier (the genesis block's stake modifier is 0)

The only way to change the current kernel hash (to mine a block), is thus to either change your "`prevout`", or to change the current block time.

A single wallet typically contains many UTXOs. The balance of the wallet is basically the total amount of all the UTXOs that can be spent by the wallet. This is important because any output can be used for staking. One of these outputs are what can become the "prevout" in a staking transaction to form a valid PoS block.

So, if we were to show some pseudo-code for finding a valid kernel hash now, it would look like:

```
while(true){
    foreach(utxo in wallet){
        blockTime = currentTime - currentTime % 16
        posDifficulty = difficulty * utxo.value
        hash = hash(previousStakeModifier << utxo.time << utxo.hash << utxo.n <<
blockTime)
        if(hash < posDifficulty){
            done
        }
    }
    wait 16s -- wait 16 seconds, until the block time can be changed
}
```

Here's what this code means in English:

```
Do the following over and over for infinity:
Calculate the blockTime to be the current time minus itself modulus 16 (modulus is
like dividing by 16, but then only instead of taking the result, taking the remainder)
Calculate the posDifficulty as the network difficulty, multiplied by the number of
coins held by the UTXO.
Cycle through each UTXO in the wallet. With each UTXO, calculate a SHA256 hash using
the previous block's stake modifier, as well as some data from the the UTXO, and
finally the blockTime. Compare this hash to the posDifficulty. If the hash is less
than the posDifficulty, then the kernel hash is valid and you can create a new block.
After going through all UTXOs, if no hash produced is less than the posDifficulty,
then wait 16 seconds and do it all over again.
```

Now that we have found a valid kernel hash using one of the UTXOs we can spend, we can create a staking transaction. This staking transaction will have 1 vin, which spends the UTXO we found that has a valid kernel hash. It will have (at least) 2 vouts. The first `vout` will be empty, identifying to the blockchain that it is a staking transaction. The second `vout` will either contain an `OP_RETURN` data transaction that contains a single public key, or it will contain a pay-to-pubkey script. The latter is usually used for simplicity but using a data transaction for this allows for some advanced use cases (such as a separate block signing machine) without needlessly cluttering the UTXO set.

Finally, any transactions from the mempool are added to the block. The only thing left to do now is to create a signature, proving that we have approved the otherwise valid PoS block. The signature must use the public key that is encoded (either as pay-pubkey script, or as a data `OP_RETURN` script) in the second `vout` of the staking transaction. The actual data signed in the block hash. After the signature is applied, the block can be broadcast to the network. Nodes in the network will then validate the block and if it finds it valid and there is no better blockchain then it will accept it into its own blockchain and broadcast the block to all the nodes it has connection to.

Now we have a fully functional and secure CZPoSv3 blockchain. CZPoSv3 is what we determined to be most resistant to attack while maintaining a pure decentralized consensus system. To understand why we approached this conclusion however, we must understand its history.

To be clear, the detailed technical information regarding Carbon Zero's Proof of Stake Protocol can all be summarized with the term "Proof of Stake" without affecting your understanding of the project, how it operates, and what it aims to accomplish. So don't worry about plodding through the really technical stuff unless you

enjoy it like us! We have omitted some small but non-trivial pieces of the explanation to err on the cautious side of security. It doesn't change the ability to understand the processes we employ.

Masternodes

Carbon Zero PoSv3 protocol is half of what makes the CarbonZero network. Through the use of Proof of Stake – an incentive to people to hold coins in their wallet – it provides the first layer of the security to the network. Much in the way PoW provides security for a pure Proof of Work network, CZPoSv3 provides security by making the "mining" of blocks difficult, CZPoSv3 makes the creation of new blocks difficult through it's requirements for coin ownership to mine new blocks. Carbon Zero works a little differently from other Proof of Stake coins, however, because it has a two-tier network. Carbon Zero has an additional layer of security and premium network services provided by the second half of the network – masternodes.

Masternodes are the most important innovation of early Alt coins. It was introduced by Dash. [16] which is a PoW/Masternode coin. Users who run and maintain special nodes on the network called masternodes receive rewards similar to the rewards of miners in traditional Proof of Work (PoW) systems. [17] To run a masternode the user has to provide a predetermined number of the coin as collateral. The coins still belong to the user, but they must remain in place for as long as the masternode is operational. if the funds are moved or spent, the associated masternode will go offline and stop receiving rewards. Masternodes earn rewards for providing special services to the network like:

- InstantSend – feature that allows for near-instant transactions
- PrivateSend – enables users to send funds privately
- Governance and treasury – enables masternode owners to vote on budget and other proposals

In return, a percentage of the block reward and any transaction fees are given to the masternode when that block is created. For clarification, the terms created, minted, or mined have the same meaning in PoS and all refer to the process in which a new block is created, and the block reward is distributed.

The masternode system is referred to as Proof of Service (PoSe), since the masternodes provide crucial services to the network. In fact, the entire network is overseen by the masternodes, which have the power to reject improperly formed blocks from miners. If a miner tried to take the entire block reward for themselves or tried to run an old version of the Carbon Zero software, the masternode network would orphan that block, and it would not be added to the blockchain.

Masternode Payment Logic

Global list

Every masternode appears in the global list. Their position in this list is determined by their time since the last payment according to the network, not the blockchain. New masternodes joining the network and masternodes receiving payment are placed at the end of the list. Running, active masternodes which are restarted using the rpc commands 'masternode start' or 'masternode start-alias' are also placed at the end of the list. Using the new rpc command 'masternode start-missing' avoids restarting masternodes unnecessarily and falling to the bottom of the list – it only restarts the masternodes that are not being seen by the wallet. As masternodes are moved to the end of the global list, the remaining masternodes slowly migrate towards the top of the list. Once a masternode reaches the top 10% of the global list, it is eligible for selection from the selection pool.

Selection pool

The selection pool is the top 10% of the global list. Its size is determined by the total masternode count. As an example, if there are 4000 active masternodes, the top 400 masternodes in the global list are eligible for selection. Once in the selection pool, selection for payment is determined by block hash entropy. The block hash 100 blocks ago determines which masternode will be selected for payment. A double hash of the funding

transaction hash and index for all masternodes in the selection pool is compared with the proof of stake hash 100 blocks ago. The masternode with the closest numeric hash value to that block hash is selected for payment. Using an existing block hash as a component of the selection process provides randomness that is not easily achieved by a computer. Without an outside source of randomness, a CPU cannot truly create a random number.

Probabilities

Because selection is determined by block hash entropy, it is impossible to predict when a payment will occur. Once in the selection pool, payments become a probability. The longer a masternode has been in the selection pool, the higher the probability of it being selected to process the current block and receive the reward. The probabilistic process makes it impossible to know the exact order of masternode selection which provides a layer of security against certain types of attacks that require that information. [18]

Quorum Selection

InstantSend transactions, which transfer coins immediately without the need of waiting for confirmations, in Carbon Zero are secured using a consensus of deterministically selected masternodes. This set of masternodes is called a quorum and must be in a majority agreement, at least six out of ten, for a successful lock of the transaction inputs. Multiple quorums are self-selected for each input in an InstantSend transaction using the mathematical distance between the hash of each input and of the set of masternode funding transactions. [19]

All InstantSend inputs must be at least six blocks old or the transaction will be rejected. In other words, unconfirmed change and coins from transactions that are not confirmed yet are not available to send through an InstanSend transaction.

Each masternode receiving the InstantSend transaction lock request compares the hash of its funding transaction to the hash of the input requesting the lock. After validating the inputs are not spent, the ten masternodes furthest from this hash broadcast their acceptance of the lock. This locking insures that only a single transaction takes place with those coins and prevents double spending, even in a transaction that happens instantly.

Masternode Payments

The masternode payment schedule is setup in the initial software release. It is extremely important that the payment, or emissions schedule be delicately balanced between the creation of new coins and the prevention of runaway inflation. Most masternode coins fail because of extreme inflation – too many coins being created for the amount of demand that exists for those coins. The key to avoiding this is two-fold

1. Emissions schedule must pay out enough coins to provide adequate return
2. There should be a use or a purpose for the coin

However, our research has shown that the most successful coins are those that are intended to be adopted as a payment or trading mechanism. Knowing that the cryptocurrency market should be considered as an open, complex, stochastic, dynamic, controlled economic system with a number of inputs and outputs and that integration occurs between virtual and real sectors of the economy [20] it is possible to do both – to create a pure cryptocurrency that provides other significant benefits, but that doesn't rely on the outside benefits to succeed. The cryptocurrency should be made to be a viable method of payment with a value commensurate with its demand, and if additional benefits can be derived from it's use, those benefits can be distributed as rewards to those that support and use the coin, particularly those who support it financially and logistically by running masternodes. This way the coin has a dual purpose. The first is as a cryptocurrency which has intrinsic benefits over competing currencies (faster transactions, more secure, increased privacy, etc) and the second is to provide the secondary benefit through its existence (in this case, reducing power consumption, waste, and environmental damage). The second requires the first and only strengthens its position as a viable cryptocurrency – recognizing this and implementing the project accordingly is unique to Carbon Zero.

The first part of this equation is created by a sensible emissions schedule that can be sustained without outpacing demand for the coin. Given a stable price, the return of coins locked/coins minted on a masternode will typically decrease as the number of masternodes increases. This is because the rewards paid to masternodes are fixed on a per block basis and the target time per block is fixed – in this case at 60 seconds. So if one masternode exists, that masternode will receive all of the block rewards, which would be one per minute. If another masternode comes online, then each masternode will earn a block reward every other minute, cutting the return in half. At three masternodes, each will receive a payment every three minutes and so on.

Many projects address this by increasing the block reward substantially over time to create more coins. This will make the project look attractive at a high ROI on listings like masternodes.online, but this published ROI takes into account ONLY the number of coins received/coins locked and NOT the price of the coin. In other words, *published* ROI has nothing to do with *real* ROI when it comes to masternodes. For the published ROI to match the real ROI for a masternode the price of each coin would have to remain the same over time. What usually happens, however, is that as more coins are produced, the value of each coin goes down and while the published ROI appears to stay the same, the masternode owner is not realizing a profit. If you double the number of coins you receive as rewards in a week, but the value of each coin falls in half because of oversupply, you've made nothing. Creating a masternode coin whose only purpose is to create ROI isn't feasible because it's a zero-sum game. Coins created, and their reduced value offset each other.

This means that to have a chance of succeeding a masternode coin must have a reasonable rewards schedule – one that doesn't increase the circulating supply greater than demand. Under the right circumstances, the value of the coin will rise with time as it is adopted by more people. The key to a successful cryptocurrency is not attracting people with an artificially high published ROI, but to make the coin more practical as a cryptocurrency. Increasing the ease of use of the currency and it's acceptance in real life situations is imperative.

"The key to a successful cryptocurrency is not attracting people with an artificially high published ROI but to make the coin more practical as a cryptocurrency."

The Carbon Zero emission schedule has been designed for low inflation but with rewards high enough to attract support in the form of masternode owners. Because of the low rewards, the coin will remain scarce throughout its lifetime, so we're anticipating a stable to increasing price from release. For the purpose of anticipated return calculations, we will use what we feel is the worst case – no price appreciation. Since the code maintains the block time at one minute, we can accurately predict the amount of time to each change in the block reward. It allows us to provide a mathematically accurate picture of what the real range of ROI will be if we make a few simple assumptions based on history. In the table we assume that the network is starting with 100 masternodes (within 2 weeks or 20,000 blocks[9] – prior to this, return will be much higher for a short time, but not sustainable, so it is not reflected on the table. The make the estimates conservative, we assume 100 masternodes already exist at block 1[10]). We also assume that the price doesn't change from its initial price, and we assume that approximately half of the block rewards created will be directed back into creating additional masternodes, lowering the return for masternodes globally. In all, we've made the most conservative assumptions possible, so these numbers are expected to be minimums.

[9] 20,000 blocks for 2 weeks is calculated as 1 block per minute = 1440 blocks/day * 7 = 10,000 blocks per week.
[10] Presale will include 100 masternodes, but all will come online as they are sold after the genesis block. Therefore, all presale masternode owners will receive a benefit not reflected here.

OVERALL emission return on total circulation excluding price appreciation. As the ratio of masternodes to stakers varies, so do the returns awarded to each.

Collateral 1,000

Phase	Block Start	Block End	nSubsidy	Daily Added Circulation	Phase Added Circulation	Total Circulation	Phase Duration in Weeks	Total Weeks From Genesis (Block 0)	Daily Return	APR	Projected MN Count	MN Daily Return*	MN APR*
0	0	100,000	0.7	1008	70,000	160,000	10	10	0.63% - 1.01%	367.92% - 229.95%	100	80.64% - 0.81%	29433.60% - 294.34%
1	100,000	200,000	0.8	1152	80,000	240,000	10	20	0.48% - 0.72%	262.80% - 175.20%	140	0.92% - 0.66%	336.38% - 240.27%
2	200,000	300,000	0.9	1296	90,000	250,000	10	20	0.52% - 0.54%	197.10% - 189.22%	185	0.74% - 0.56%	270.31% - 204.56%
3	300,000	400,000	1	1440	100,000	350,000	10	30	0.41% - 0.58%	210.24% - 150.17%	235	0.62% - 0.49%	227.29% - 178.93%
4	400,000	500,000	1.25	1800	125,000	475,000	10	40	0.38% - 0.51%	187.71% - 138.32%	298	0.61% - 0.48%	223.66% - 176.67%
5	500,000	600,000	1.5	2160	150,000	625,000	10	50	0.35% - 0.45%	165.98% - 126.14%	373	0.58% - 0.46%	212.01% - 169.32%
6	600,000	700,000	1.75	2520	175,000	800,000	10	60	0.32% - 0.40%	147.17% - 114.98%	460	0.54% - 0.44%	197.54% - 159.97%
7	700,000	800,000	2	2880	200,000	1,000,000	10	70	0.29% - 0.36%	131.40% - 105.12%	560	0.50% - 0.41%	182.82% - 150.17%
8	800,000	900,000	2.25	3240	225,000	1,225,000	10	80	0.26% - 0.32%	118.26% - 96.54%	673	0.46% - 0.39%	168.94% - 140.68%
9	900,000	1,000,000	2.5	3600	250,000	1,475,000	10	90	0.24% - 0.29%	107.27% - 89.08%	798	0.43% - 0.36%	156.31% - 131.81%
10	1,000,000	1,100,000	3	4320	300,000	1,775,000	10	100	0.24% - 0.29%	106.90% - 88.83%	948	0.43% - 0.36%	158.17% - 133.13%
11	1,100,000	1,200,000	3.5	5040	350,000	2,125,000	10	110	0.24% - 0.28%	103.64% - 86.57%	1123	0.43% - 0.36%	155.32% - 131.11%
12	1,200,000	1,300,000	4	5760	400,000	2,525,000	10	120	0.23% - 0.27%	98.94% - 83.26%	1323	0.41% - 0.35%	149.84% - 127.18%
13	1,300,000	1,400,000	3.5	5040	350,000	2,875,000	10	130	0.18% - 0.20%	72.86% - 63.99%	1498	0.30% - 0.27%	111.28% - 98.28%
14	1,400,000	1,500,000	3	4320	300,000	3,175,000	10	140	0.14% - 0.15%	54.85% - 49.66%	1648	0.23% - 0.21%	84.24% - 76.57%
15	1,500,000	1,600,000	2.5	3600	250,000	3,425,000	10	150	0.11% - 0.11%	41.39% - 38.36%	1773	0.17% - 0.16%	63.81% - 59.31%
16	1,600,000	5,000,000	2	2880	6,800,000	10,225,000	340	490	0.03% - 0.08%	30.69% - 10.28%	5173	0.13% - 0.04%	47.44% - 16.26%

*Assumes 100 initial masternodes and 50% of all new coins being used as collateral for new masternodes. This is only likely if early investors use emissions for additional masternodes.

*Total circulation discounts the relatively small premine held by the devs, which are effectively locked for the first two years.

*Min/Max APR are theoretical based on every circulating coin competing for rewards. For that reason, return will be higher than what is shown here for Masternode Owners.

*The earliest investors will see an extraordinarily high rate of return which will settle down to "normal" return as the presale progresses to the end.

Emissions are spread out over many years. There will be only 3,425,000 coins at about 3 years. This is a coin with a very low supply. The max circulation figure of just over 10 million is reached in ~ 10 years

*All numbers are subject to change. Should we detect an oversupply situation, we may adjust with a collateral increase. We've spent many hours coming up with the emissions schedule and do not anticipate such a problem.

The emission schedule shows the coins that will be created in the first 7.5 years. Even with such small rewards, the total circulation at the end of that period is just over 40 million coins. This is additional evidence that a more aggressive block reward structure is not sustainable for any coin with a maximum supply of under 50 million. If there is an increase in price, real returns will be substantially higher. This table does NOT include dividends received from Carbon Zero ERC-20 Tokens (Carbon Zero Token), which are disbursed equally among masternodes and will be discussed separately as an income component. The above table ONLY represents the annual returns based on block rewards from the Carbon Zero Coin.

The Bigger Solution

At this point, we've covered the potentially catastrophic problems that could be brought about by Bitcoin and other PoW cryptocurrencies over the next few years. We've drilled down into the data to the point where we feel that the data and the cited references make an overwhelmingly solid case against the sustainability of Proof of Work consensus mechanisms and Bitcoin in particular. We've also built the foundation on which the ultimate solution will be built – a practical solution that could help end the impending energy crisis, that rewards all parties involved, in a streamlined and practical way. Our idea is not to simply throw away Proof of Work, replace it with Proof of Stake, congratulate each other and walk away. That will never happen. The POW mechanisms would take several years to untangle from our current networks, and let's be honest with ourselves – Bitcoin isn't going to disappear. But what we can do is create a Carbon Neutral Bitcoin Alternative that offers the same features (and more), faster transaction times, more modern algorithms and consensus mechanisms, as well as a slew of additional exciting features. We can have a cleaner cryptocurrency that works better, is over 10x faster, is more private, with lower fees, and a decentralized system of governance BUILT INTO the software to allow the currency and it's support system to exist as a completely decentralized organization and in a way that you haven't seen before.

Why would we want to do this? Are we environmentalists?

We love the environment and the earth, and we like the climate the way it is, but we're not activists of any kind. We are certain that Bitcoin as it is now is having a generally bad impact on our lives and literally the lives of everyone around us. And it's not negligible. But it's not clear that this emotional desire to save the planet or better utilize resources is enough to drive a project of the scope and breadth of what we intend to do. It might work, but it would require an extraordinary amount of marketing and a bit of luck. That's not good enough – not if we can do better. *We intend to prevent at least 36 million kt of CO2 from making its way into the earth's atmosphere every year.* There are hard ways to do that, which are costly and difficult to implement, and there are smart ways to do it. With the specific skillsets of the Carbon Zero team, we've spent the last 2 years coming up with a smart way to do just that and we've devised products and a process that incentivizes all those

involved (and many not yet involved) with long term participation in the project. The greatest thing about success is that in its success everyone wins. This is also one of the primary reasons the project will succeed. Our goals are ambitious, but so is our plan. In fact, with a successful first 18 months Carbon Zero will have arrested the growth of Bitcoin difficulty and therefore the accelerating increase of its consumption permanently. After that, the project will begin reversing the need for Bitcoin emissions until there are none. It's important to note that the success of the financial and other project goals can be achieved independently of the other desired goals. In other words, if it takes us 24 months to arrest the acceleration of Bitcoin Energy consumption, it doesn't affect any of what we are doing. The environmental reasons are both a reason for doing what we're doing and a by-product of the process. Once we explain the components of the Carbon Zero Project, you'll understand why.

Carbon Zero Coin

The first part of the project includes creating a Proof of Stake/Masternode coin with its own blockchain. The Carbon Zero Coin will provide the initial funding for the project AND auxiliary benefits based on it's production. To understand why and how this works requires a short explanation of a few important items that make it possible. The first of those factors is the Kyoto Protocol.

The Kyoto Protocol

The Kyoto Protocol is an international agreement linked to the United Nations Framework Convention on Climate Change, which commits its Parties by setting internationally binding emission reduction targets. Recognizing that developed countries are principally responsible for the current high levels of GHG emissions in the atmosphere because of more than 150 years of industrial activity, the Protocol places a heavier burden on developed nations under the principle of "common but differentiated responsibilities." The Kyoto Protocol was adopted in Kyoto, Japan, on 11 December 1997 and entered into force on 16 February 2005. The detailed rules for the implementation of the Protocol were adopted at COP 7 in Marrakesh, Morocco, in 2001, and are referred to as the "Marrakesh Accords". [21] It doesn't necessarily apply directly to modern carbon emission projects in developed countries, but it's a necessary foundation. Without the Kyoto treaty, these programs probably wouldn't exist today. It also gives us a basic framework for how to measure greenhouse gas emissions and how to put a value on them.

Kyoto Mechanisms

Under the Protocol, countries' actual emissions have to be monitored and precise records have to be kept of the trades carried out. [21] The mechanisms include:

- Registry systems track and record transactions by Parties under the mechanisms. The UN Climate Change Secretariat, based in Bonn, Germany, keeps an international transaction log to verify that transactions are consistent with the rules of the Protocol.
- Reporting is done by Parties by submitting annual emission inventories and national reports under the Protocol at regular intervals.
- A compliance system ensures that Parties are meeting their commitments and helps them to meet their commitments if they have problems doing so. [22] [23]

The Kyoto Protocol and its mechanisms have set forth the framework for setting and meeting emissions targets for countries, encouraging and assisting with adaptation, and rewarding those who meet or exceed their targets for the reduction of their carbon footprint. Not every carbon emission reduction project is subject to the Kyoto Protocol, but it has sparked many other carbon reduction initiatives, a carbon reduction industry, and even a Global Carbon Economy. Since Cryptocurrency and blockchain is blind to international borders, we will take the explanation of the Carbon Zero Project to where it will be operating – the Global Carbon Economy.

The Carbon Economy

The Global Carbon Economy exists because of the commoditization of carbon emission reduction. To get to a point where this could happen, some unit representative of greenhouse gas emissions had to be created. This unit became known as a carbon credit. A carbon credit is a permit or certificate allowing the holder to emit carbon dioxide or other greenhouse gases. The credit limits the emission to a mass equal to one ton of carbon dioxide. The issuance of carbon credits aims to reduce the emission of greenhouse gases into the atmosphere. [24] Specifically we will be using what's called a "cap-and-trade" CO2 program as an example. This isn't the only way carbon credits are acquired or traded, but it's an easy example to understand.

Under a cap-and-trade or emissions program, a company emitting less than its capped limit may sell unused credits to a company exceeding its limit. For example, Company A has a cap of 10 tons but produces 12 tons of emissions. Company B also has an emission cap of 10 tons but emits only eight, resulting in a surplus of two credits. Company A may purchase the additional credits from Company B to remain in compliance. Without the purchased carbon credits, Company A would face penalties. When the fines exceed the cost to buy, the company will favor purchasing the credits. However, sometimes the price to acquire the credits exceeds the fines. As a result, some companies accept the penalties and continue operations and the emissions of hydrocarbons. [24] As you can see by this example, under a certified program, carbon credits gain intrinsic value based on the alternative cost – the penalties for exceeding carbon emissions. There are many other scenarios, including voluntary programs, that give value to these credits.

The Carbon Zero Project has a negligible carbon footprint even if we're considering the entire network. Therefore, we don't approach any kind of regulated cap on emissions, which means that any reduction in carbon emission credits we create would be surplus. There are many types of carbon credits. For example, a country may sell its surplus credits to a country that does not achieve its Kyoto level goals through the Emission Reduction Purchase Agreement under the Kyoto Protocol while the separate Clean Development Mechanism for developing countries issues carbon credits called Certified Emission Reduction (CER). A developing nation may receive these credits for supporting sustainable development initiatives. The trading of CERs is on a separate marketplace. [24]

Carbon credits created in different ways will not usually be different in what they represent – the standard carbon credit unit is equal to the abatement of 1 ton of Carbon Dioxide, but they are traded on open markets – essentially Carbon Exchanges – and the monetary value on the open market of a carbon credit will be proportional to the "quality" of that carbon credit. Just like other traded instruments, some carbon credits are considered sub-prime, others are considered prime, but there are many different, although somewhat arbitrary, classifications for carbon credits based on whether they are certified or not, the certifying organization, the mechanism, etc. Carbon credits don't have to be certified – there are also voluntary programs, but certified carbon credits are usually worth more. Climate exchanges have been established to provide a spot market in allowances, as well as futures and options market to help discover a market price and maintain liquidity. Carbon prices are normally quoted in Euros per ton of carbon dioxide or its equivalent (CO2e)[11]. [25]

There are carbon credit pricing models which have buyers committed to buying credits that meet certain criteria for a fixed price. It's one of the easiest ways of selling carbon credits because the demand is already there, but

[11] "Carbon dioxide equivalent" or "CO2e" is a term for describing different greenhouse gases in a common unit. For any quantity and type of greenhouse gas, CO2e signifies the amount of CO2 which would have the equivalent global warming impact. A quantity of GHG can be expressed as CO2e by multiplying the amount of the GHG by its GWP. E.g. if 1kg of methane is emitted, this can be expressed as 25kg of CO2e (1kg CH4 * 25 = 25kg CO2e). "CO2e" is a very useful term for a number of reasons: it allows "bundles" of greenhouse gases to be expressed as a single number; and it allows different bundles of GHGs to be easily compared. [41]

it also pays the least. This model, called Fairtrade[12], calculates a minimum price that ensures the average costs of the projects will be covered. However, in the Fairtrade model a buyer also pays an additional premium on top. to fund activities that help them adapt and become more resilient to an already changing climate. Here is example of this pricing model (in the project classification of Carbon Zero):

Energy Efficiency – 8.20€/tCO2e + 1€ Fairtrade premium

So, for now, we'll use this *8.20€ ($9.50) figure as the minimum value per surplus carbon credit for a project that seeks to provide improved energy efficiency*. This minimum carbon credit value is guaranteed for a Projects Registered with Gold Standard. [26] There are many registries similar to this that offer different levels of certification for carbon credits. The more stringent the certification criteria, the higher the value of each credit. This method of transacting carbon credits sacrifices some of the potential revenue per credit in exchange for not being exposed to the volatility of a Carbon exchange. In the case of Carbon Zero, we've designed a system that will be extremely lucrative regardless of the price received for the Carbon Credits we produce. The reason we're using this low estimate for the value of Carbon Credits in our calculations is that the disbursement of credits should be as simple as possible. The process must be sustainably decentralized so that it can exist regardless of the involvement of any one or any group of individuals. Anything above the fixed Fairtrade price will be additional profit. We can use the Fairtrade price in our calculations and be confident that our profit estimates are conservative.[13]

Carbon Zero's Role

Carbon Zero Coin uses a minting process involving Masternodes and PoS staking. This will be the mechanism for the carbon reduction that the entire project achieves. To create carbon credits from a mechanism, that mechanism must do the same thing as an alternate inefficient process. The difference between the inefficient process (PoW and Bitcoin specifically) and the Carbon Zero process is represented by the difference in the amount of CO2 output of each. Since Carbon Zero's minting methods do NOT use a significant amount of computing power, the electricity it uses, and therefore it's carbon footprint, are negligible. That means we can use nearly 100% of the alternative method's carbon output as the baseline for the relative reduction in carbon output and the number of carbon credits being issued by the project.

ERC-20 Token

ERC-20 is a technical standard used for smart contracts on the Ethereum blockchain for implementing token creation and distribution. ERC stands for Ethereum Request for Comment, and 20 is the number that was assigned to this request. The clear majority of tokens issued on the Ethereum blockchain are ERC-20 compliant. As of 2018-07-26, a total of 103,621 of ERC-20 compatible tokens are found on Ethereum main network, according to Etherscan.io. [27] Among the most successful ERC20 token sales are EOS, Filecoin, Bancor, Qash, and Bankex, raising over $70 million each. [28] [29].

ERC-20[14] was proposed on November 19, 2015 by Fabian Vogelsteller. It defines a common list of rules that an Ethereum token must implement, giving developers the ability to program how new tokens will function within the Ethereum ecosystem. The ERC-20 token standard became popular with crowdfunding companies working on

[12] The Fairtrade minimum price defines the lowest possible price that a buyer of Fairtrade products must pay the producer.

[13] Not all carbon credits are certified by an authoritative body. There are Voluntary carbon credit programs which allow the trade of carbon credits without certification of their validity. Naturally, this type of carbon credit is of lower quality and value. We haven't considered these for Carbon Zero, but they are a very "easy" alternative.

[14] ERC-20 is a technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. ERC stands for Ethereum Request for Comment, and 20 is the number that was assigned to this request. The clear majority of tokens issued on the Ethereum blockchain are ERC-20compliant.

initial coin offering (ICO) cases due to the simplicity of deployment, together with its potential for interoperability with other Ethereum token standards. [27]

In the last 8 months of 2017, the total amount gathered by ICOs[15] exceeded 4 billion US$ and overcame the venture capital funneled toward high end tech initiatives in the same period. A high percentage of ICOs is managed through smart contracts running on the Ethereum blockchain, and in particular to ERC-20 Token Standard Contracts. [30]

There's no doubt that ERC-20 tokens are among the highest volume cryptocurrency derivatives on the market. The reason for this is that they are not cryptocurrencies in the traditional sense. They are tokens that reside on the Ethereum Blockchain and are created using (comparatively) simple smart contracts. These smart contracts allow for the creator of the token to issue tokens as necessary without relying on the "mining"[16] of the coins. The tokens are simply minted by the administrator of the Token and distributed. In fact, the entire maximum supply of the token can be minted in one block and then held in an ERC-20 Token compatible wallet and sold at any time. The logic for doing this can be placed into the smart contract and the process can be automated. The aspect of Tokens that makes them largely ineffective as a cryptocurrency on their own – no control over the blockchain, no inherent restraints on the number produced, and many other characteristics, make them a great candidate as a representative token of some underlying utility, value, access, functionality, etc. Therefore, unlike a blockchain based cryptocurrency (coin), if a Token[17] represents a particular asset, the tokens can be minted precisely in proportion to the assets backing the token, much like a government does (or used to do) for fiat money. A good example of this is USD Tether.

To avoid confusion, we should mention that although USD Tether considers themselves a "proof of…" cryptocurrency, they claim to be a "Proof of Funds"[18] type of system [31], what you would notice on close inspection is that it isn't actually a proof of anything. As you've already learned, a Proof of Something is a technical term used in cryptocurrency to indicate that it's a proof used to describe a type of consensus mechanism. So if you look more deeply into USD Tether, just understand that it's not really a "Proof of Funds" cryptocurrency since there is absolutely no automated mechanism that provides consensus on whether or not there are backing funds available. In a "Proof of" cryptocurrency methodology, the proof of that something must reside in the blockchain. The logic in the blockchain must know when it begins, when it ends, and what happened in the middle. "Proof of" and "Probably have" are vastly different in meaning. USD Tether is a "Probably have" currency, meaning there's no proof of anything that can be examined externally. The only thing there is proof of is that they minted and sold the tokens.

What USD Tether is, simply, is a currency in the form of a token in the sense of a typical currency. Tether claims that "…every tether is always backed 1-to-1, by traditional currency held in our reserves. So 1 USD₮ is always equivalent to 1 USD" [32]. For our purposes we will assume this is true[19], so that having a USD Tether Token is the same as having a US Dollar Bill. For every USD Tether Token in circulation, there is a US Dollar locked away in a vault somewhere. As the company acquires more dollars, they issue more tokens – one for each dollar they put away in their vault. Assuming everyone has been honest, this means that if all USD Tether were suddenly redeemed for US Dollars, the company would be able to pay everyone and remain solvent. This is quite a bit different from regulated banks which are only required to keep a portion of the backing asset in

[15] ICO – Initial Coin Offering is named after and operates like the equities markets' IPO – Initial Public Offering
[16] The Ethereum Blockchain does currently run using Proof of Work algorithms, which will change in the future, but a token on the Ethereum blockchain produces no additional PoW overhead.
[17] The terms "Token" and "Coin" are often incorrectly interchanged, even by projects. They are distinctly different and a Token should never be called a Coin and vice-versa. It's the source of a great deal of confusion for many.
[18] "Proof of Funds" does have a legitimate implementation on the blockchain, but this is not it.
[19] In general, this has been accepted as a true assumption, but because of the lack of oversite, it isn't necessarily true. We really have no way at this point of knowing whether they have $1 backing each USDT or if it's $0.50. They tell us it's $1, we believe them, and because we believe them USDT is worth $1, just like fiat. Hopefully that will change.

reserves. This makes the idea of issuing tokens to represent an asset very simple – x number of tokens per x amount of an asset – The token can represent ownership in something in a fixed amount since the administrators[20] have control over how much of that token is issued. That doesn't mean every token is backed by something of intrinsic value. A token can represent your access to a platform, or it could represent your ability to pay for a service, where if the platform or service went away, the token would be useless. The Carbon Zero Token model is much closer to the former than the latter. Carbon Zero Tokens will be backed by something with a specific value and only issued in proportion to the acquisition of the underlying asset. In fact, since the carbon credit is an output of part one of the project and the input to the second part, it's easy to audit. It's completely transparent. The blockchain, which was the mechanism for creating the carbon credit is openly explorable from day one of the project.

Carbon Zero Token

As we said above, the Carbon Zero Token is most similar to the USD Tether token in that it represents an underlying asset, but it's not fiat money. The Carbon Zero Token contract is being written so that one Carbon Zero Token has the value of one carbon credit. Not only does it have the value of a carbon credit, it IS the carbon credit.

The Carbon Zero Token is yet another component of the Carbon Zero Project and it's what makes it revolutionary as a cryptocurrency and even more so in the world of masternode coins. If the Carbon Zero Coin is the cake, then the Carbon Zero Token is the icing, the ice cream, the baking pan, and your own kitchen.

"Not only does it have the value of a carbon credit, it IS the carbon credit."

As we discussed earlier, a carbon credit is a something that represents the removal or prevention of one ton of CO2 in the earth's atmosphere. But what IS a carbon credit really? Well, it can take many forms. Quite often it's just a number on an order book on a carbon credit exchange. Just like many representative instruments being traded, it's all done electronically. There isn't one particular form of carbon credit that physically exists. A carbon is concept that can be can be represented by anything that prevents two different entities from claiming the same credit at the same time. The agreement among the parties in a carbon credit transaction using a given type of carbon credit from a certain source determines the characteristics of those carbon credits, such as value and ownership – they usually have to reach "consensus" outside of the blockchain. But we already know what the master of consensus is – *the blockchain*. Quite elegantly, the mechanism for creating the carbon savings that can be automatically polled by the Carbon Zero Token Minting and Generation Protocol (The Carbon Zero TMaG™ Protocol) The carbon credits in the Carbon Zero project are certified credits in the form of a Token! The amazing thing about using an ERC-20 token for this purpose is precisely that it can ONLY be owned by one entity at a time. If the administrative entity is issuing the credits only when the project has eliminated or prevented 1 ton of Carbon Dioxide from being in the atmosphere, an ERC-20 Token Carbon Credit (Carbon Zero Token) happens to be the ideal way to represent carbon credits (its ingenious). Our TMaG™ protocol guarantees that the that the distribution of the carbon credits through an ERC-20 contract is auditable by ANYONE, and that the mechanism that is producing the carbon savings and therefore the credit is 100% automated and auditable by ANYONE[21]. *The Carbon Zero Project plans to be offering the highest quality carbon credit in the world in the form of an ERC-20 token*. There is not another project of which we are aware that provides such a clear and auditable path from the mechanism of the Energy Savings all the way

[20] Administrators of a token are the individuals or entities that have control over minting and distributing the token, usually the original developer of the smart contract.

[21] It could easily be audited by using the Carbon Zero and Ethereum Blockchain together. Both offer an immutable record of every transaction on their respective networks.

through to the issuance and ownership of the carbon credits. This alleviates the most challenging problem with carbon credits – they are typically very difficult to certify and audit. The Carbon Zero Project eliminates those obstacles completely. This is amazing and it's exiting, and it makes so much sense that we expect an extraordinary amount of demand for the token. As we mentioned earlier, we will be using the worst case "Fairtrade Price" of $9.50 per carbon credit in our calculations. We're doing this to keep our estimates conservative. The Investopedia Inc investment dictionary defines a carbon credit as a "permit that allows the holder to emit one ton of carbon dioxide … which can be traded in the international market at their current market price". [25] and the market price of a high quality carbon credit has an average value of over $30 each.

But it gets a lot better.

Putting it Together – The Carbon Zero Project

The Beginning

In 2016-2017 we saw the Carbon Zero Coin and the Carbon Zero Token as two separate projects. Our initial thought was that it would be difficult to combine both a masternode/PoS blockchain coin and an Etherium based ERC-20 token. But we also knew that both had to exist for us to create the carbon savings and represent those savings in a tangible carbon credit – something that would have value based on the underlying mechanism from which it came. Each project would be profitable on its own – with the low inflation emission schedule creating scarcity in the coin, masternode owners can realize tremendous sustainable returns, while the project continues to appeal to investors, and while attracting newcomers all the while maintaining an attainable and sustainable inflation-controlled economy. We've mapped out the entire schedule over 7 years[22], so we know that even being conservative, we'll not only see adoption, but price appreciation. We also know that creating a carbon credit in the form of an ERC-20 token is something not being done anywhere in the industry of carbon offsets – anywhere in the world. And we know that an ERC-20 has all the characteristics for creating one of the highest quality carbon credits on the market. So we knew that both the Carbon Zero Coin and the Carbon Zero Token will be profitable to extremely profitable ventures, while also doing what's right for the environment.

Success to the early supporters of the Carbon Zero Coin can be all but guaranteed.

In early 2018, with development of the individual projects nearly complete, some changes in our development team presented us with an unexpected opportunity and something we had not given serious thought to previously – combining the two projects so that they can not only provide value to each other, but provide additional value to be people that funded them. With a coin alone, developers are often unable to guarantee success and returns to their earliest supporters. At the same time, out of pocket money to invest in the issuance of a new token can be a high risk endeavor, since the management of such contracts are often, by necessity, more centralized than a coin on it's own blockchain with it's own masternodes.

Project Value

It occurred to us that we could provide a tremendous value to our initial supporters while sharing the profit from BOTH projects with them. After all, those supporting the Carbon Zero Coin Project are responsible for the carbon offsets the project produces, so if we can capture those credits (which we are doing in the Carbon Zero Token) and give a portion of them back to the projects original supporters, we can create a much higher probability of a lucrative environment for everyone. Most masternode coins fall victim to extreme inflation due to the abundance of the coin because masternode owners and stakers are dumping huge amounts of the cryptocurrency so they can reclaim their profit. However, if those same people can be helped to see over the

[22] We can increase the duration of minting past 7 years if it makes sense and if a proposal for that is voted into place by the masternode owners.

horizon, that problem disappears. Success to the early supporters of the Carbon Zero Coin can be all but guaranteed. there will be a very persuasive reason to attract new people to the coin, and instead of having some type of sale or offering on the Token, we can simply award those tokens to those that have held the coin over time as dividends.

"The blended return on the Carbon Zero Project has the potential to be astronomical."

That's how the Carbon Zero Project became one project. We've uncovered huge benefits to having the projects exist together rather than separately. It also creates a much easier path going forward for both projects. When the Carbon Zero tokens start being issued in 2019 it will be based on the first month of the Carbon Zero Projects Carbon reduction efforts, and once it begins, Carbon Zero Tokens will be issued every month thereafter. We've decided that 50% of those tokens will go to existing masternode owners as dividends for them supporting the network. So when the Carbon Zero Token smart contract goes live, masternode owners will receive the carbon credits in the form of Carbon Zero ERC-20 tokens in a proportion to be determined through the project registration project. As we mentioned earlier, coal-based electricity is available at very low rates in China. [13] This type of electricity has an emission factor of up to 1 kg CO2e per kilowatt-hour (KWh). With on Bitcoin transaction consuming an average of 898Kwh, we fully expect to be generating at least one carbon credit (Carbon Zero Token) per Carbon Zero Coin created, including those coins that are created for the presale. That means a presale purchase of 1 masternode will immediately be worth a carbon dividend of at least 500 Carbon Zero Tokens. At the Fairtrade price (the lowest price) of $9.50 each, that's an INITIAL carbon credit dividend value of approximately $4,750 (up to $15,000 on the high side). When these dividends are issued, you will have the choice of receiving the $9.50 equivalent BTC through the automated clearing of the carbon credits, or taking possession of the Carbon Zero Tokens yourself and selling them on the secondary market it one exists for the tokens[23]. We will at least allow you to choose your method of receiving dividends on a per masternode basis, so if you have more than one masternode you will be able do diversify your method of dividend receipt (MODR). We may add the ability to further divide the MODR as a percentage of your masternode holdings, but that will not be immediately available upon release.

The estimated electricity saved will be calculated per transaction because a transaction that takes place on the Carbon Zero network is a transaction that is not occurring on the Bitcoin Network. The average amount of power consumed for each bitcoin transaction is 898KWh which produces approximately 440kg of CO2. If we assume the minimum of 1 transaction per block on the Carbon Zero Network, that's about 1 metric ton of CO2 saved per 2 Carbon Zero blocks. At 10,000 blocks per week, that means that approximately 5,000 carbon credits will be produced weekly. At $9.50 per carbon credit, that would mean a disbursement of $47,500 worth of carbon credits per week. For 100 masternodes, that's an additional $475/week ($24,700/year) per masternode, and more if there is more than 1 transaction per block. We expect that to be the case at some point, but remember, these are estimates and we have no way of knowing what the actual number of transactions per block will be until we have some history behind us. Any credits we produce is independent of the creation of Carbon Zero Coins, so it has no direct impact on inflation.

While we are on the topic of inflation, there is a very simple equation that many coin creators either don't read, or don't understand before releasing a coin. The monetarist explanation of inflation operates through the Quantity Theory of Money, which applies strongly to coin generation and particularly. Masternode based coins/blockchains.

MV=PT

[23] While we do guarantee exchange listings for the Carbon Zero Coin, there is no way for us to guarantee a secondary market for the Carbon Zero Token, which is why we will offer the automated exchange to BTC. Be sure to consider this risk if taking possession of the tokens and use your best judgement when deciding what to do.

Where M is Money Supply, V is Velocity of Circulation, P is Price level and T is Transactions or Output. As monetarists assume that V and T are determined, in the long run, by real variables, such as the productive capacity of the economy, there is a direct relationship between the growth of the money supply and inflation. [33] All of these factors must be taken into account when creating the emission schedule, the block time, and other coin specifications.

Incremental Technologies

Block Time

The target block time of Bitcoin is 10 minutes. That means that a new block is created about every 10 minutes and the transactions waiting to get on the blockchain are added at that time (unless there is no room in that block, in which case the transaction may have to wait one or more additional 10-minute periods just to get onto the blockchain. Subsequently, confirmations for that transaction take about 10 minutes each[24]. This means you can expect a Bitcoin transaction to take a minimum of 30 minutes (assuming the recipient requires only 3 confirmations.

Carbon Zero has a block time of 1 minute. That means a new block is almost always less than a minute away. Carbon Zero blocks are also larger than Bitcoin blocks, so they can accommodate many more transactions, preventing the Bitcoin bottleneck by allowing all waiting transactions to be included in the upcoming block. Confirmations also occur every minute – 10 times faster than Bitcoin confirmations.

SwiftX

Instant Transactions: SwiftX transactions are confirmed and spendable within seconds, guaranteed by the network of masternodes, with no need to wait for multiple confirmations in order to be confident in the validity of the transaction. [34]

Governance and Budgeting

Carbon Zero has a built-in system for making proposals and voting on them. Any masternode owner can make a proposal on the blockchain, and if other masternode owners vote for that proposal, the proposal budget is entered into the final budget and paid out as set forth in the proposal. The Carbon Zero Treasury sets aside 10% of the block reward, from which it makes payments to the approved project.

Conclusion

First and foremost, Carbon Zero intends to be a great cryptocurrency. Our ultimate goal is to supplant Bitcoin as the leading cryptocurrency which means becoming the most used and best-known cryptocurrency in the world. We don't know when/if that will happen because it really isn't up to us. We can give it the best chance any cryptocurrency has of achieving this, and we think we have. We use Bitcoin at the Carbon Zero Core and we add to that, among other things:

1. 1-minute block times vs 10 minute BTC block times
2. Bigger Block Sizes (eliminating the primary bottleneck in BTC)
3. Faster transactions
4. Lower fees. No fees in some cases
5. Increased Privacy
6. Proof of Stake vs Proof of Work
7. Virtually no carbon footprint
8. Masternodes for special transactions

[24] New blocks built on top of an existing block are considered "confirmations". So when there are three additional blocks added after a transaction, that transaction is said to have three confirmations.

9. Instant send
10. Zerocoin Protocol
11. Built in immutable proposal and voting system for decentralized management
12. A budget and Treasury to set aside and assign minted coins for projects proposed by and approved by the community.

What we do know is that whether we achieve that goal or not, Carbon Zero will be a tremendous success. It's the first ever combined masternode coin/ERC-20 project, and it's the first cryptocurrency project that seriously addresses the environmental impact of PoW coins and does something about it. It's the first crypto project that is confident enough to publicly state the goal of achieving parity with Bitcoin.

That's where we're headed, and we'd like a few select people to join us on the starting line to come along for this exciting ride. If you do decide to join us early, we hope that you'll get involved in our "early adopter" discussions to help shape the future of Carbon Zero. Having been involved in a handful of cryptocurrency projects, it's become clear that the early adopters are the best source for ideas, and the most sincere and impassioned feedback. We treat early adopters as advisors because they are one of the best resources we have to succeed. They will quickly find a level of dedication and transparency that is rare in today's crypto markets. We'll get there together, with you.

The blended return on the Carbon Zero Project has the potential to be astronomical. *However, just like all cryptocurrency projects, there are risks, including the risk of losing all or some of your investment. While we have a vested interest in making the former happen, we can't guarantee it, so please only invest what you can afford to lose. The same is true of any investment in cryptocurrency.*

References

[1] "What is 'Bitcoin'," , . [Online]. Available: http://www.investopedia.com/terms/b/bitcoin.asp. [Accessed 10 9 2018].

[2] "History of bitcoin," , . [Online]. Available: http://en.wikipedia.org/wiki/History_of_bitcoin. [Accessed 10 9 2018].

[3] J. . Bohr and M. . Bashir, "Who Uses Bitcoin? An exploration of the Bitcoin community," , 2014. [Online]. Available: http://ieeexplore.ieee.org/document/6890928. [Accessed 10 9 2018].

[4] Z. . Wang, L. . Bian and X. . Hang, "Algorithm based on time-window for mining sequential patterns in relational database," , 2001. [Online]. Available: http://adsabs.harvard.edu/abs/2001spie.4556...33w. [Accessed 10 9 2018].

[5] "Why Blockchain Needs 'Proof of Authority' Instead of 'Proof of Stake'," , . [Online]. Available: https://cointelegraph.com/news/why-blockchain-needs-proof-of-authority-instead-of-proof-of-stake. [Accessed 10 9 2018].

[6] Killjoy, "The Different Proofs of Crypto Currency," Steemit, 2017. [Online]. Available: https://steemit.com/cryptocurrency/@killjoy/the-different-proofs-of-crypto-currency. [Accessed 15 September 2018].

[7] "Proof-of-stake," , . [Online]. Available: http://en.wikipedia.org/wiki/Proof-of-stake. [Accessed 10 9 2018].

[8] V. . Buterin, "What Proof of Stake Is And Why It Matters," , . [Online]. Available: https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/. [Accessed 10 9 2018].

[9] "Digiconomist," [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[10] "Key World Energy Statistics 2017," 19 September 2017. [Online]. Available: https://webstore.iea.org/key-world-energy-statistics-2017.

[11] E. Holthaus, "Bitcoin could cost us our clean-energy future," 5 December 2017. [Online]. Available: https://grist.org/article/bitcoin-could-cost-us-our-clean-energy-future/.

[12] "Bitcoin's Carbon Footprint," 7 December 2017. [Online]. Available: https://digiconomist.net/bitcoin-carbon-footprint.

[13] "Average electricity prices around the world: $/kWh," March 2015. [Online]. Available: https://www.ovoenergy.com/guides/energy-guides/average-electricity-prices-kwh.html.

[14] . . superadmin, "Proof-of-Work vs Proof-of-Stake: merits and disadvantages," , . [Online]. Available: http://www.coinfox.info/news/reviews/6417-proof-of-work-vs-proof-of-stake-merits-and-disadvantages. [Accessed 10 9 2018].

[15] P. . Vasin, "BlackCoin's Proof-of-Stake Protocol v2," , . [Online]. Available: http://www.blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf. [Accessed 11 9 2018].

[16] M. . Opačić, M. . Veinović and D. . Adžić, "A Short Introduction Into Innovative World of Masternode Coins," , 2018. [Online]. Available: https://singipedia.singidunum.ac.rs/izdanje/42895-a-short-introduction-into-innovative-world-of-masternode-coins. [Accessed 14 9 2018].

[17] "Dash Official Documentation," [Online]. Available: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146943/Masternodes. [Accessed 14 September 2018].

[18] "Masternode Payment & Logic," Dash, [Online]. Available: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/8880184/Payment+Logic. [Accessed 15 September 2018].

[19] "Quorum Selection," Dash, [Online]. Available: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/58523665/Quorum+Selection. [Accessed 15 September 2018].

[20] V. G. Soslovskyi and I. O. Kosovskyi, "CRYPTOCURRENCY MARKET AS A SYSTEM," , 2016. [Online]. Available: http://fkd.org.ua/article/view/91065. [Accessed 15 9 2018].

[21] U. N. F. C. o. C. Change, "Kyoto Protocol - Climate Change Newsroom from the UNFCCC," , 1997. [Online]. Available: http://unfccc.int/kyoto_protocol/items/2830.php. [Accessed 11 9 2018].

[22] "Kyoto Protocol Reference Manual On Accounting of Emissions and Assigned Amount," , . [Online]. Available: http://unfccc.int/resource/docs/publications/08_unfccc_kp_ref_manual.pdf. [Accessed 16 9 2018].

[23] "The Mechanisms under the Kyoto Protocol," , . [Online]. Available: http://unfccc.int/kyoto_protocol/mechanisms/items/1673.php. [Accessed 16 9 2018].

[24] "Carbon Credit Definition | Investopedia," , . [Online]. Available: http://www.investopedia.com/terms/c/carbon_credit.asp. [Accessed 12 9 2018].

[25] "Carbon credit," , . [Online]. Available: http://en.wikipedia.org/wiki/Carbon_credit. [Accessed 16 9 2018].

[26] "Gold Standard," [Online]. Available: https://www.goldstandard.org/project-developers/our-project-registry. [Accessed 11 September 2018].

[27] "ERC-20," , . [Online]. Available: http://en.wikipedia.org/wiki/ERC-20. [Accessed 16 9 2018].

[28] . . etherscan.io, "Etherscan Token Tracker Page," , . [Online]. Available: https://etherscan.io/tokens. [Accessed 16 9 2018].

[29] "Token Data," , . [Online]. Available: https://www.tokendata.io. [Accessed 16 9 2018].

[30] G. . Fenu, L. . Marchesi, M. . Marchesi and R. . Tonelli, "The ICO phenomenon and its relationships with ethereum smart contract environment," *arXiv: Computers and Society,* vol. , no. , pp. 26-32, 2018.

[31] "Proof Of Funds - POF," , . [Online]. Available: http://www.investopedia.com/terms/p/proofoffunds.asp. [Accessed 10 9 2018].

[32] "Home Page," Tether, [Online]. Available: https://tether.to/. [Accessed 16 September 2018].

[33] "Monetary inflation," , . [Online]. Available: http://en.wikipedia.org/wiki/Monetary_inflation. [Accessed 17 9 2018].

[34] "Features," PIVX, [Online]. Available: https://pivx.org/features/. [Accessed 16 September 2018].

[35] I. Stewart, "Bitcoin Wiki," Proof of Burn, [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_burn. [Accessed 10 September 2018].

[36] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2," [Online]. Available: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf. [Accessed 9 September 2018].

[37] W. i. B. Mining?, "Everything you need to know about Bitcoin mining," , . [Online]. Available: https://www.bitcoinmining.com/. [Accessed 10 9 2018].

[38] X. . Wu, V. . Kumar, J. R. Quinlan, J. . Ghosh, Q. . Yang, H. . Motoda, G. J. McLachlan, A. F. M. Ng, B. . Liu, P. S. Yu, Z.-H. . Zhou, M. . Steinbach, D. J. Hand and D. . Steinberg, "Top 10 algorithms in data mining," *Knowledge and Information Systems,* vol. 14, no. 1, pp. 1-37, 2007.

[39] "Masternode vs Mining," Dash, [Online]. Available: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/56655894/Masternode+vs.+Mining. [Accessed 14 September 2018].

[40] "Charts," CoinMarketCap, [Online]. Available: https://coinmarketcap.com/charts/. [Accessed 16 September 2018].

[41] M. Brander, "Greenhouse Gases, CO2, CO2e, and Carbon: What Do All These Terms Mean?," Ecometrica, 2012.