Civitas

Simul Autem Fortior Nobis

Whitepaper

—

2018

Success Will Come and Go, But Integrity Is Forever

www.civitascoin.com

Welcome To Civitas

A Coin Built By The Community... **For The Community!**

TABLE OF CONTENTS

The greatness of a community is most accurately measured by the compassionate actions of its members.

Abstract

WHAT IS CIVITAS?

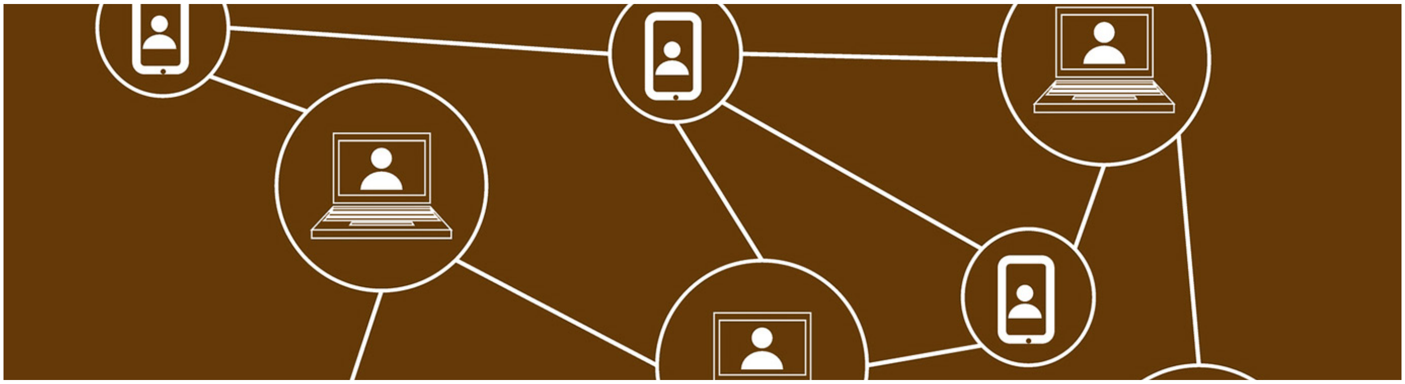
Civitas comes from the ancient Roman concept that community is not just the collective body of citizens, it is the contract that binds them all. The “together we are stronger” philosophy is the guiding force behind the Civitas coin.

Cryptocurrencies and blockchain technologies have given rise to new ideas and innovations that have reshaped the global financial landscape. Connecting people and resources in a speed never seen before, peer-to-peer decentralized networks have empowered citizens with the ability to exchange payment for goods and services without relying on traditional banking, FIAT currency, or creditors. A truly free society is being developed with instant, private transactions emboldened by the promise of blockchain technologies. Although Bitcoin has been the catalyst for this new movement, it lacks some key attributes that have been improved upon in several new cryptocurrencies. Our mission is to blend several of these elements to introduce the fastest, privacy-based coin with a community-based network of Masternodes (MNs) for security.

Small acts, when multiplied by millions of people, can transform the world.

- Howard Zinn

.



The cryptocurrency space has seen a plethora of innovations to address multiple issues that have arisen since the inception of the first blockchain based protocol, Bitcoin. Controversy regarding miner centralization and practical issues such as fungibility and privacy have been addressed. As the network grows, security becomes less of a factor while getting a consensus vote for implementing changes becomes increasingly difficult. The form of a voting system via MNs allows for a distributed group to vote on a continuous basis on matters pertaining to Civitas without giving up their right to vote to others. It is the community who will choose which problems Civitas seeks to solve as we move forwards in harmony with the ever changing blockchain environment.

As such, Civitas begins its journey by forking from the Pivx repository, a cryptocurrency based off Bitcoin's core 0.10x code base and running Blackcoin's Proof of Stake (PoS) 3.0 protocols. Maintaining the stable core code whilst adding the addition of MNs which will give resources for adding additional features such as governance, privacy, and faster transactions. Civitas was born as a Proof of Work (PoW)/PoS coin allowing both mining and staking. After a short time, it was discovered that the Zerocoin protocol would not support PoW and was terminated. Since then Civitas has been a PoS coin, meaning that the block rewards are split between MNs and staking wallets.

Communities and the internet have been synonymous since the first message boards sprang up in the 1970's. Now with the advent of cryptographically verifiable digital ledgers it has become possible for these communities to exchange value digitally, securely, and quickly.

A man's value to the community primarily depends on how far his feelings, thoughts, and actions are directed towards promoting the good of his fellows.

- Albert Einstein

Section 1: Bitcoin Core Fundamentals

"Well, I think it is working. There may be other currencies like it that may be even better. But in the meantime, there's a big industry around Bitcoin.—People have made fortunes off Bitcoin, some have lost money. It is volatile, but people make money off of volatility too."

- Sir Richard Branson

THE FIRST TO OFFER A CHANGE

The legacy of Bitcoin will always be established in the fact that it was first to publish this amazing new technology. A pioneer of its time, the solutions that the cryptocurrency offered are revolutionary. Allowing buyers and sellers to create commerce without a trusted third party to conduct their transaction. Changing the dynamic of conventional payment systems from a trust-based model to one that requires cryptographic proof begins to eliminate fraud and corruption. Timestamps provide chronological order of transactions, while digital signatures verify them and their contents.

Nodes are an integral part of the blockchain network. Not only do they verify transactions but they also verify the outputs of other nodes, thus maintaining the networks integrity. As the digital ledger continues to grow, so does the memory requirements to store it. As such, lite nodes serve to function on small memory devices such as phones which contain only the parts of the blockchain that they require. They then query a full node for verifiability. Full nodes refer to nodes with the complete blockchain on it, yet in some cases this does not need to be the case.

Bitcoin utilizes a 1 tier incentive structure to secure its network. Miners operating full nodes are also able to spend computational and electrical power in tacking another block to the blockchain, thus confirming all the transactions sent by the nodes. This process mints a new coin rewarding the miners for their contribution to the network.

Section 2: Dash Masternode Theory

Dash was the first cryptocurrency that incentivised coin holders with the idea of the MasterNode (MN). The MN operator helps to validate the superfast transactions (InstantPay) and provides the anonymity for the coins on the network.

- Dreamminers

MASTERNODING THE CHALLENGES

Looking to reward full nodes, Dash introduced a second tier to their system known as Masternodes (MNs) in 2014. This second tier allowed for additional features such as privacy and faster transactions to be performed on the network with MNs being incentivized by receiving a portion of the block reward for performing these tasks.

While in a 1 tier system, only the miners are incentivized to committing computational and electrical power to securing the network. In a sense, they are voting for code changes in the form of updating their node software. In a 2-tier system such as Civitas, its incentive structure is split between MNs and traditional (PoS) staking wallets. MNs require 10,000 Civitas collateral and a minimum downtime of 1 hour per day connectivity. They receive 65% of the block reward for their contribution. The remaining 35% of the block reward goes to traditional staking wallets. These two tiers are treated different when it comes to incentives, based on resources needed to participate.

This type of structure allows rewarding network participants based on their contribution of resources to the network, while at the same time sets an inherent cap based on diminishing returns. Meaning, if too many MNs are built, the remaining 35% of the reward becomes greater if 10,000 Civitas is staked rather than being used to build a MN.

Masternodes facilitated by the PoS 3.0 framework offer a more robust network to build upon making the incorporation of other features easier; be it governance, privacy, security, or further decentralizing the network. MNs at present only facilitate voting and are intended to allow advancement of the project in the future. This network structure allows Civitas to implement additional features to keep up with development as well as implementing additional features should the community vote in favor of them.

Deeper Dive

2.a Governance

Governance takes the form of nodes/users submitting propositions which are voted on by MN holders each super block (approx. 1 month). MN holders either reject or accept submissions regarding changes in protocol, brand or, direction of the project. Developers retain the right to veto any change that is technically not possible or if the technical solution is alternate to the proposed statement voted on.

2.b Faster Transactions (SwiftTx)

Another benefit of utilizing this form of network is that users can send and receive instant, irreversible transactions. Once the MNs reach consensus on a transaction, the inputs of that transaction become locked and become non-transferable elsewhere on the network. The process takes about four seconds and is a decentralized means in allowing near instant payment for real world commerce as well as peer-to-peer exchanges.

Section 3: PIVX/ Zerocoin Privacy

Pivx was the first PoS cryptocurrency to use and improve upon the Zerocoin public repository. Pivx is a protocol created by academic cryptographers that allows users on the network to interact with zero knowledge proofs, thus minimizing the amount of data transmitted with a transaction. This protocol protects both the sender and receiver by only sharing information pertaining to the amount that was sent, known as the value.

Users of the Civitas network can choose to convert their normal Civitas (Civ) coins into a denominated amount of zCiv coins, thus dissociating any of their wallet information from the transaction ID. This allows for a verifiable asset transfer to occur anonymously through the network.

Zerocoin protocol functions by “burning” the zCiv transactions at these denominated values with other user’s transactions. A zero-knowledge proof is then executed to mint new coins that are sent to the correct addresses. The process is quick and respects both the privacy of the sender and receiver as well as removing any unwanted histories associated with the received coin.

The benefits of privacy in cryptocurrencies are that they become fungible and safer to use. This protects the community’s balances from prying eyes whilst still maintaining the option to send a fully transparent transaction, should one be required.

Summary

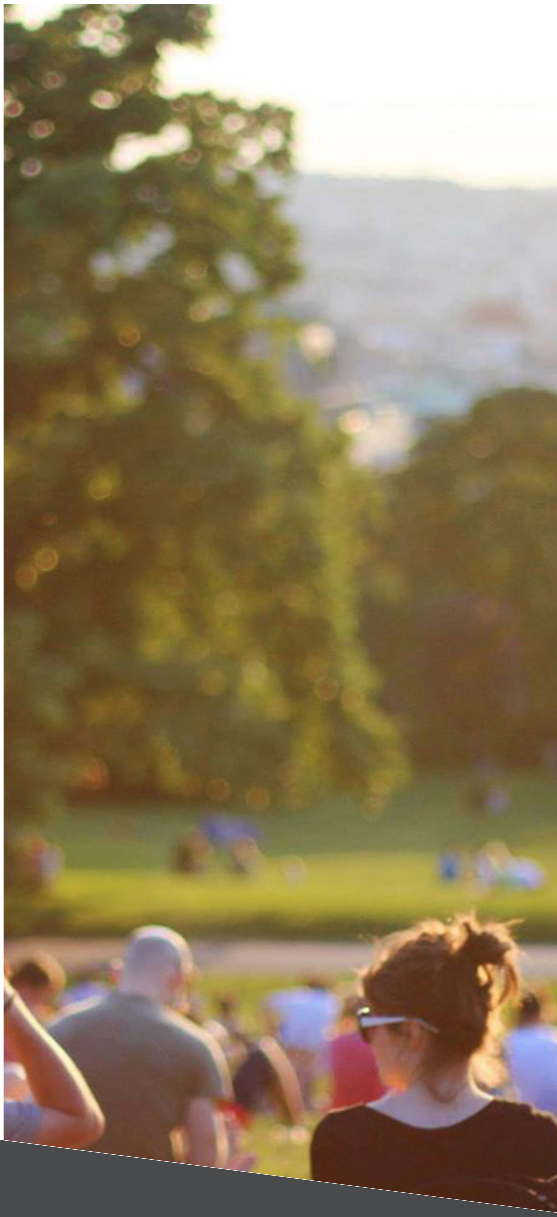
As cryptocurrencies move out of their infancy and begin to embody one of their first definitions, namely decentralization, digital autonomous organizations become a natural part of this process. Civitas seeks to empower its network by starting from a robust framework (Masternodes), removing previous made additions, and allowing the network users to vote and choose which protocols they want to see or problems they want addressed by the project.

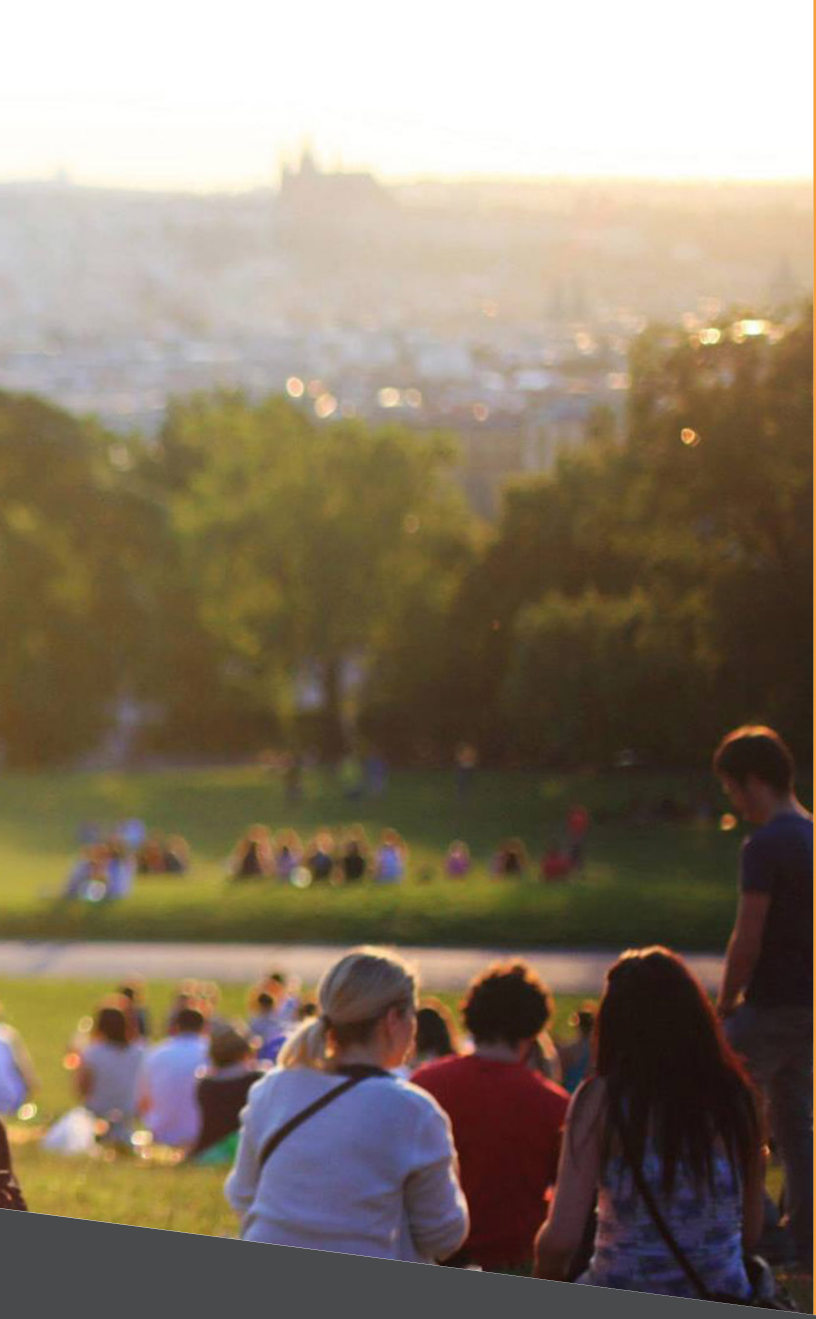
Utilizing the above-mentioned protocols, Civitas seeks to enhance its network users whom it sees as not merely passively investing in this fintech space but are actively participating in the network. This is accomplished by using the technology and helping form what cryptocurrencies will become in the future.

“Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it’s the only thing that ever has.” Margaret Mead (1982)

“Never doubt that a small group of thoughtful, committed citizens can change the world; indeed, it’s the only thing that ever has.”

- Margaret Mead (1982)





Technical

Algo: Quark

Block Time: 60 Seconds

Difficulty Retargeting: Every Block

Max Coin Supply (PoW Phase): 30,000 CIV

Max Coin Supply (PoS Phase) Infinite

Premine 400,000 distributed as such:

100,000 coins:

AIRDROPPED to the Community on launch day

100,000: Given to Community members for Masternode securing of the network

100,000 paid to pre-launch development team

100,000 BOUNTY coins for services and utilities.

Written using the Quark algorithm

Total supply: 8,716,000 for phases 1-3, phase 4 adds 525,600 CIV per year

speed per block: 60 Seconds

This is a full proof of stake coin.

POS phases 1-4 rewards allocated at 65% Masternodes 35% Stakers

coins per block each POS phase 1: 10 CIV phase 2: 5 CIV phase 3: 2 CIV phase 4: 1 CIV

Resources

Githubs

Dash: https://github.com/dashpay/dash
PivX: https://github.com/PIVX-Project/PIVX
Zerocoin: https://github.com/Zerocoin/libzerocoin
Blackcoin; https://github.com/CoinBlack/blackcoin

Whitepapers
Blackcoin Pos 3.0
https://bravenewcoin.com/assets/Whitepapers/Blackcoin-POS-3.pdf

Dash Whitepaper
https://github.com/dashpay/dash/wiki/Whitepaper   Dash About

PivX Whitepaper
https://pivx.org/what-is-pivx/white-papers/