CAPITAL WHITEPAPER

Revision 1.0 24 March 2018

I. Abstract

"*The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A."*
Milton Friedman - 1999

The development of a decentralized digital currency after the creation of the internet was not a possibility, it was an inevitability. Before the genesis block for Bitcoin was mined in 2009, numerous e-currencies were planned, but most failed or never came to fruition.

One of the earlier attempts was BitGold, which aimed to become a non-tangible version of gold by replicating its core properties of scarcity, fungibility and decentralization.It arguably has given lots of influence to the structural framework seen in Bitcoin today. One such example, is the adoption of the POW consensus mechanism, which uses computational power to solve increasingly complex cryptographic hashes.This helped in creating a secure solution to the Byzantine General's issue, as there was too much of a disincentive to control the network because of the electricity costs expended in splitting hash power to turn nodes rogue. The BitGold e currency fell short due to the fact it was unable to solve the double spending issue without compromising the aspect of decentralization. Bitcoin built on this by using the Proof of Work consensus to direct hashing power towards determining whether funds had been spent or not. The process works by bundling transactions into 10 minutes slots and allocating a 12.5BTC block reward randomly to the mining entity that helps in solving the hashes. After verification, each transfer has 6 confirmations, making it impossible to reverse the transaction.

Bitcoin transformed the way cryptocurrencies were viewed because it was able to maintain its decentralized aspects, while solving key issues that are necessary to produce a stable means of exchange using blockchain technology.

II.The State Of Cryptocurrencies

Recently, there has been a multitude of digital currencies created solely for speculative purposes. On CoinMarketCap there were over 1500 listed as of March 2018 ,and this neither includes dead projects or coins that do not have the sufficient trading volume required for addition.

The rapid rise in the creation of new cryptos can be attributed to the altcoin boom of 2017, which gave inspiration for a myriad of developers and influencers to start projects of their own. Even in the years preceding the 2017 bull run, new coins were still appearing everyday despite prolonged periods in a bear market .The vast majority of these projects have severely fallen short of expectations due to:

Overfunding - ICOs asking for obscene amounts of money. Not only does this disincentivize the developers to work, but also grossly inflates the market cap above the token/coins intrinsic value.

Inefficient distribution models - Developers locking a huge % of the total premine, creating room for wild price volatility as speculators attempt to time the influx of these new coin/tokens into the market.

Vaporware - The technology advertised in the whitepaper is not realistically achievable with the resources available.

III.Introduction

Capital is a privacy coin that utilizes masternodes to create an ultra secure network.

The underlying ideological principles for the coin are exactly what got people into cryptocurrency in the first place. CAP values individual rights, freedoms and decentralization over coercion, collectivization and power being concentrated in the hands of governmental institutions. In the early days of cryptocurrency, anarcho-capitalists, cyberpunks and libertarians were the majority of users, but the overwhelming majority of new money has not entered the space for ideological reasons. The mania that caused the exponential gains of 2017 was not just a consequence of market immaturity, but a reflection of the participants lack of understanding in blockchain technology and the potential impacts it will have on wider society.

If cryptocurrencies want to increase adoption, then there must be more awareness on the benefits it can provide to the masses. Capital does this by utilizing a multifaceted chain that maximizes privacy and provides an efficient governance system where power is transferred to the people.

IV.Staking

To promote distribution of the coin, POW consensus was used alongside POS from block 1-1440. From block 1441 onward, CAP was made pure POS. The reasoning behind this choice was because of the major advantages it has over POW.

Electricity Consumption: POW is very inefficient in this respect. Over time, the algorithms used to solve blocks become harder, thus the equipment to solve the hashes must be more powerful and have the capable hardware to compete. The sustainability of POW is also questionable in both scaling and time. The longer the chain is active, the faster difficulty increases, meaning hardware becomes obsolete more quickly. Unless there is a massive reduction in the number of miners, it would be difficult to see POW surviving in the longer term. This is especially the case in industries where the hardware would end up comprising a large proportion of the variable costs, like healthcare for example.

POS does not involve solving complex mathematical problems. Consequently, the resources used to maintain the network are a fraction of what is needed for POW.

Decentralization: The distribution of hashing power for POW becomes more top heavy over time, as early miners are able to reap the benefits of decreased competition and higher block rewards, allowing them to purchase more resources and efficient hardware. In the end, economies of scale are used to create a technical monopoly where a few holders are in control of the whole network. The mining company Bitmain have gained over [1]$4 billion profit in 2017 alone. These colossal profits have been used to develop patented ASICs that have up to a [2]20% efficiency boost over their closest competitor*

**Please be aware that the efficiency boost does not apply to Bitcoin since the integration of Segwit has rendered the ASICs unusable. However, it can be used on its controversial substitute, Bitcoin Cash [BCH]*

Incentive - When it comes to miners in POW, it's a race against time to get a return on investment because of the rate at which the equipment depreciates. Consequently, miners have a tendency to immediately sell over the highest buy order, which ends up hurting the price long term. In addition to this, there are no monetary incentives to hold the coins that have been mined. This contrasts to POS where more coins being staked in the network would result in greater weighting given to the participant, enabling them to earn a higher frequency of rewards. The longer term impact is that a greater % of the circulating supply will be locked using the POS consensus, in turn, leaving less coins free on the exchange to be sold.

V.Masternodes

One of the most vital features in maintaining the CAP network is the implementation of masternodes. Our abandonment of the seesaw mechanism in favor of a fixed rate 80/20 block reward split, demonstrates the importance of the role they play when providing security, privacy and many of the core features utilized in the wallet.

Masternodes work by running the wallet software on a VPS server and they add value to the network by performing various tasks.

To summarize, they contribute by:

Anonymizing transactions - interacts with accumulators in the zerocoin spending process.
Increasing transaction speed - using a quorum of masternodes to lock transactions. This prevents double spending when using the Swift Tx. feature.
Transaction Validation - confirms the latest transactions.

The prerequisites for running a masternode are 10000 CAP coins, a VPS server and the latest wallet for their operating system. For a masternode to function, the collateral must always remained locked, deeming the funds unspendable. If the coins are unlocked and spent at any time, the node is broken.

For Capital, we have maximized the monetary incentives for early investors by giving healthy masternode gains through high block rewards. Our model is based on slow reductions in the total block reward over monthly periods, which will help in mitigating against long term price drops by curbing the inflation rate.

Our block reward scheme also has the added twist of superblocks. These appear approximately every 60 days and deliver 1000% higher rewards than the average block. The purpose of these blocks is to not only reward current investors, but also generate additional interest on our social media platforms. There are reasons to suspect an increase in selling temporarily, however, the gain in liquidity and interest in the long term trump any immediate price depreciation.

VI.Zerocoin Protocol

Freedom of the individual was one of the key points elucidated in the introduction section. To achieve true freedom, there should be no external constraints from the state or any source of central authority. In principle, this is done by removing any traceability of what a person does with his/her money.

The adoption of zerocoin protocol is a solution to making a Capital a completely anonymous cryptocurrency. The process can be broken down into 2 main stages, the minting and spending phase. All minted zerocoins are referred to as zCAP.

The minting of zCAP begins by burning the old coins. This stage is important because it severs any connections that could have been made between sending addresses. The process continues by the conversion to zCAP using whole number denominations ranging between 1-5000. A single denomination is used to maximize privacy, however, by incorporating this protocol the network is placed under heavy load. The utilization of 8 denominations can be considered an optimal amount that does not stretch the network capacity, while still being able to maintain the all important privacy aspect. Once the funds have been sent, the user should see a decrease in his coin balance by x amount of coins and an increase in his zCAP balance by x. The coins are now minted.

All of the coins are kept track in an accumulator secured using RSA 2048 encryption. Masternodes play a vital role in interacting with the accumulators to ensure they are secure, as well as to confirm any transactions that take place once the coins are sent. To determine an owner of coins in the accumulator, a unique serial key is assigned to each zCAP balance. A zero knowledge proof is then sent out to the blockchain using the serial number. By doing this, funds can be transferred without anyone knowing information about the transaction. Once the ledger has verified the serial number, the funds are then converted back to normal CAP and transferred to the recipient.

VII.Technical Roadmap

This section will expand upon the roadmap provided in the ANN.

Exchanges - The team firmly believes in quality over quantity when it comes to exchange additions.To provide a steady flow of liquidity, Capital has listed to TradeSatoshi and CryptoBridge exchange. We believe that fundamentals create more value in a coin than the exchanges it lists on. In other words, the weighting placed by most investors on exchanges is overestimated and the technology tends

to be undermined in the short term. After the implementation of Zerocoin Protocol, mid-tier exchange listings with $10 million + volume will be considered.

Masternode Ranking Sites - Masternodes.Online is the most popular tracking site. There are plans for listings to Mntop and Masternodes Pro, giving users a wide variety of choice in where they want to track their investments.

Blockfolio - Once CryptoBridge provides an API that can be used for Blockfolio, investors will be able to track the price and their holdings. Until then, the team will make an effort to get CAP listed on the most popular alternative – Delta.

CMC Listing - To get on CoinMarketCap, the coin needs to consistently get $100,000 volume on a daily basis.

Superblocks - Enhanced block rewards are given out in 100 block batches every 2 months.

Block Reward Reduction - After the end of a superblock cycle, the total block reward decreases. This takes place in 2 coin increments until the stage 9 is reached where each block is only worth 10 coins.

Zerocoin Protocol - Integration of an advanced privacy protocol that will grant the user anonymity when making transactions across the chain.

Mobile Wallets - The release of lite wallets that can be stored conveniently on a mobile device, as the space taken up from installing the software is significantly lower than that of a normal PC wallet.

VIII.Marketing

The recent actions of Facebook, Twitter and Google banning cryptocurrency advertisements, shows increasing hostility towards the blockchain industry. The implications of this being that traditional online campaigns are no longer viable, however, market saturation has decreased as a direct result of the bans.

The CAP team has formulated a marketing plan that aims to penetrate the general population and crypto enthusiasts alike.

1) **Video Platforms** - incentivizing video creators to produce objective and unbiased content on Capital coin. We plan to achieve this via pooling 1% of premined coins to those that produce videos meeting our minimum requirements for quality and view count.

2) Blogging - a separate campaign will run for Korean, Chinese, Japanese and English articles. We feel that many coins underestimate the impact Eastern influence can have on a coin. CAP itself has garnered a lot of interest from the Chinese community and we have no plans to slow down in this area.

3) **Masternode Ranking Sites** - Masternodes.Online, Mntop and Masternodes.Pro are some of the MN ranking sites we have planned for CAP listing. Not only does this generate exposure within the Masternodes community, but also allows existing investors to follow the relevant statistics for tracking purposes.

4)**Banner Advertising** - despite the fact most major ad providers have done a widespread ban on anything cryptocurrency related, there still exists the possibility of custom arrangements that can be made between the owners of specific sites and the CAP team. Only 10% of the advertising budget has been allocated to banners because of the large variation in conversion rates.

5) **Chinese Bounty Program -** as explained above, the blogging bounty has been partitioned into 4 different languages.

The rest of the bounty program has been also been separated, but only between English and Chinese. The underlying tasks are similar for both the English and Chinese bounties, however, changes have been made in the Chinese program to reflect cultural differences, such as differing social media platforms (e.g. Wechat and QQ groups versus Facebook and Twitter).

6) **Bounty Site** - an interactive webpage is in the process of being built to help run the program effectively. It has been structured to maximize engagement through an

attractive GUI and gives the opportunity to repeat bounties after a certain fulfillment period. The user is able to accumulate points through completing the tasks provided, which can be converted to real Capital coins later on.

IX.Sources

[1] CNBC, https://www.cnbc.com/2018/02/23/secretive-chinese-bitcoin-mining-company-may-have-made-as-much-money-as-nvidia-last-year.html
Evelyn Cheng, 23rd February 2018

[2] The Merkle,
https://themerkle.com/what-is-asicboost/
JP Buntix, 9th April 2017