



bitcoin
INCOGNITO

WHITEPAPER



bitcoin
INCOGNITO
Transactions with true anonymity.

The Environmentally Conscious and Private Bitcoin

Written by: Cari Brosious, MBA and Basil Kapsalis, MEng

June 30, 2018

Abstract

Bitcoin Incognito (XBI) is a cryptocurrency that takes Satoshi Nakamoto's original vision for Bitcoin and adds to the concept in a way that makes it both more environmentally conscious and private for its users. Bitcoin Incognito being Proof-of-Stake with Masternodes means that users are able to mint coins without using any more energy than a personal computer. Masternodes also make for fast, secure transactions and are inherently resistant to 51% attacks. Bitcoin incognito uses Zerocoin protocol to ensure that users will not be subjected to privacy invading analytics. The addition of the Incognito Masternode Pool (IMP) gives extra incentive to users to start and hold Masternodes even as the ROI decreases.



bitcoin
INCOGNITO
Transactions with true anonymity.

CONTENTS

1. Introduction.....	3
2. The Trouble with Bitcoin.....	4
3. The Solution for Excessive Energy Consumption.....	7
4. The Solution for Privacy and Safety Concerns.....	10
5. The Incognito Masternode Pool.....	12
6. Distribution.....	13
7. Conclusion.....	14
8. References.....	15



1. Introduction

When Satoshi Nakamoto wrote his original whitepaper for Bitcoin in 2008¹ he started a revolution that is still in its infancy. In the years since it has become more and more obvious that there were both some unforeseen circumstances in the original design and some vulnerabilities that were not originally intended. Though still early in the game, blockchain has the capability to change the world in many ways for the betterment of society. The most obvious way is to free private citizens from fiat currency that is under control of government entities that may not necessarily have their best interests at heart. Bitcoin was a great start, but it turned out to be lacking in the area of environmental consciousness (the unforeseen circumstance), and in privacy (unintended vulnerability). Bitcoin Incognito aims to fix both of these problems while building on Nakamoto's original idea. In addition, it has become clear in the ensuing years that community involvement is one of the most beneficial aspects of any cryptocurrency project, i.e. the more community involvement, the more successful a project will be. Bitcoin Incognito had a rough start with less than honest developers who abandoned the project, but the community saw value in keeping it alive and towards that end a new governance was begun. This governance is community driven and democratic, recognizing that all community members want to help make Bitcoin Incognito a successful project.



2. The Trouble with Bitcoin

Satoshi Nakamoto is the pseudonym for the anonymous creator of Bitcoin. All cryptocurrency as we know it started with his vision as it was laid out in the original whitepaper in 2008¹. The invention was for an electronic payment system based on cryptographic proof which is how the term cryptocurrency was coined. The creation of a “blockchain” was the method by which it would work.

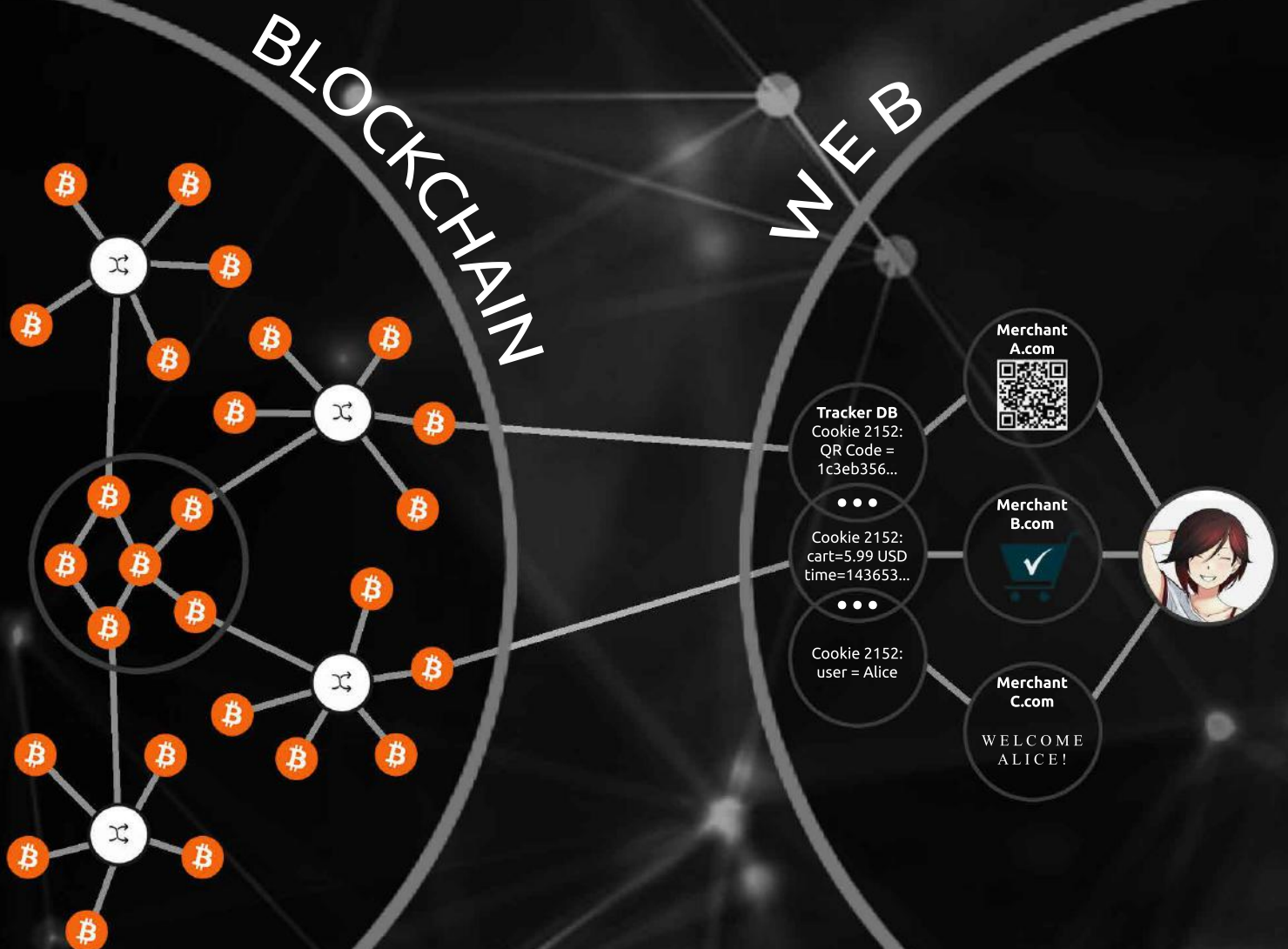
Blockchain is a global network of computers that work together to process transactions on an electronic ledger. Each computer is called a node. When a transaction occurs, it is transmitted throughout the blockchain so that the individual nodes can confirm that it is not a fraudulent transaction. Each transaction requires a certain number of these confirmations to be accepted. Blocks of transactions that are created during a certain time period are bundled together to be added to the ledger. Each block requires a difficult math problem, or hash, to be solved before it is added to the ledger. Individual nodes compete to be the first to solve this hash so that they can earn the transaction fees associated with it. This process is called mining, or Proof-of-Work, and it is where the first bit of trouble crops up.

In the original whitepaper, Satoshi Nakamoto acknowledged that it would be possible for a single user to defraud this system if they were able to control 51% of the nodes for a period of time. This type of fraud is now known as a 51% attack. It seems that Nakamoto had far more faith in humanity at large than is appropriate, for his original thoughts on this prospect were that: “If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.¹” The reality is that there have proven to be plenty of people who do not react as expected, and instead have no qualms about defrauding other users out of as many coins as they can. The good news for us is that this type of attack is really only feasible on Proof-of-Work coins, as it would be prohibitively expensive to control more than half of the nodes when the system is Proof-of-Stake or Masternodes or both.

There is another problem that is specific to Proof-of-Work coins and this is one that Satoshi Nakamoto apparently did not foresee. As mining difficulty got higher due to the number of miners working and the scarcity of coins, it forced individuals to need to find ways to increase their hashing power exponentially. This generally involves obtaining large amounts of hardware and having them run continuously. Originally this mining could be done with a personal computer, but now it requires specialized mining rigs that in some cases can fill an entire warehouse. There is also a large amount of heat released by these rigs, which can damage the hardware, so they require additional energy to keep them cooled. This results in a massive expenditure of energy that spans the globe and has the potential to damage the environment. In November 2017, the amount of energy consumed by Bitcoin mining annually was estimated to be 29.05TWh². This is 0.13% of the total energy consumption globally. That is more than the entire consumption of the country of Ireland. If this energy consumption continues on the same path, Bitcoin mining would consume all of the world's electricity by February of 2020. Think about that, it is less than two years away!

Bitcoin was designed in part to protect user's personal privacy. It was theorized that since there was no identity connected to an individual wallet, each transaction could not be traced to a particular person. This is fine in theory but in actual practice it turns out it doesn't work as well³. The Bitcoin ledger is open source and available for anyone to see, including prying government eyes. If someone wanted to track a particular payment, they could track it to an individual wallet and in turn track other payments to or from that wallet. This means it only takes one instance where a name is attached to a transaction from that wallet to reveal the identity of the entire wallet. Think about it, how many times have you paid for something online and not considered that issue? What about when you used one of those exchanges that required KYC?

Bitcoin has its uses, and it doesn't appear to be going away any time soon, but being the first doesn't always mean you are the best. This has been especially true with technology which seems to grow and change at an almost alarming rate. Developers of new cryptocurrency projects have found new ways to deal with the shortcomings of Bitcoin, and there may still be more and newer innovations ahead. Bitcoin Incognito aims to be a project that will stay on top of these innovations.



3. The Solution for Excessive Energy Consumption

What leads to excessive energy consumption in other Crypto Currencies?

The current estimate for Bitcoin's energy consumption is 71 TWh per year⁴, sufficient to power 6.5m typical US households. This high level of energy consumption is driven by two closely linked factors inherent to Bitcoin's and other Proof of Work Cryptocurrencies implementations:

1) The nature of the proof of work algorithm and increasing difficulty: In order to keep the rate of block generation constant, Bitcoin adjusts the level of difficulty of the hashing algorithm based on the overall network hash rate. Miners respond to this and to intense competition from other miners by deploying ever increasingly powerful hardware. This has seen miners progress initially from CPUs, onto GPUs and now more commonly custom ASICs. This has increased the typical power rating for mining nodes from perhaps 600W for a reasonably powerful server, then with an additional 250W per additional GPU. And now ASIC mining nodes are often rated for 1300W. Whilst on paper these higher rated ASIC miners are technically more efficient, doing more work for the given energy consumption, overall, they draw more power and are deployed in ever larger numbers to meet the competition.

2) The way that Bitcoin reaches consensus: The major power inefficiency with Bitcoin, which is also at the root of the arms race, is associated with the way it reaches consensus. A new block is created on Bitcoin's Blockchain approximately every 10 minutes, with the reward going to the first miner to produce a valid new block that can be verified by the other miners. This process means once a winner is found, all the previous work of all the other miners on that block is discarded. It has also been known for some miners to send out fake blocks for verification order to waste the resources of their competitors. This intense competition for the block reward leads to massive duplication of effort and drives the arms race identified above.



How Bitcoin Incognito solves this challenge

Bitcoin Incognito takes a different approach, one that is designed to offer greatly enhance energy performance, whilst offering the rigorous security afforded to Bitcoin holders. XBI uses a consensus mechanism to ensure the integrity of its BlockChain, but instead of using an expensive proof of work algorithm to distribute the block reward to miners based on a winner per block, it instead uses Proof of Stake to reward for the community for both staking coins and for running Masternodes.

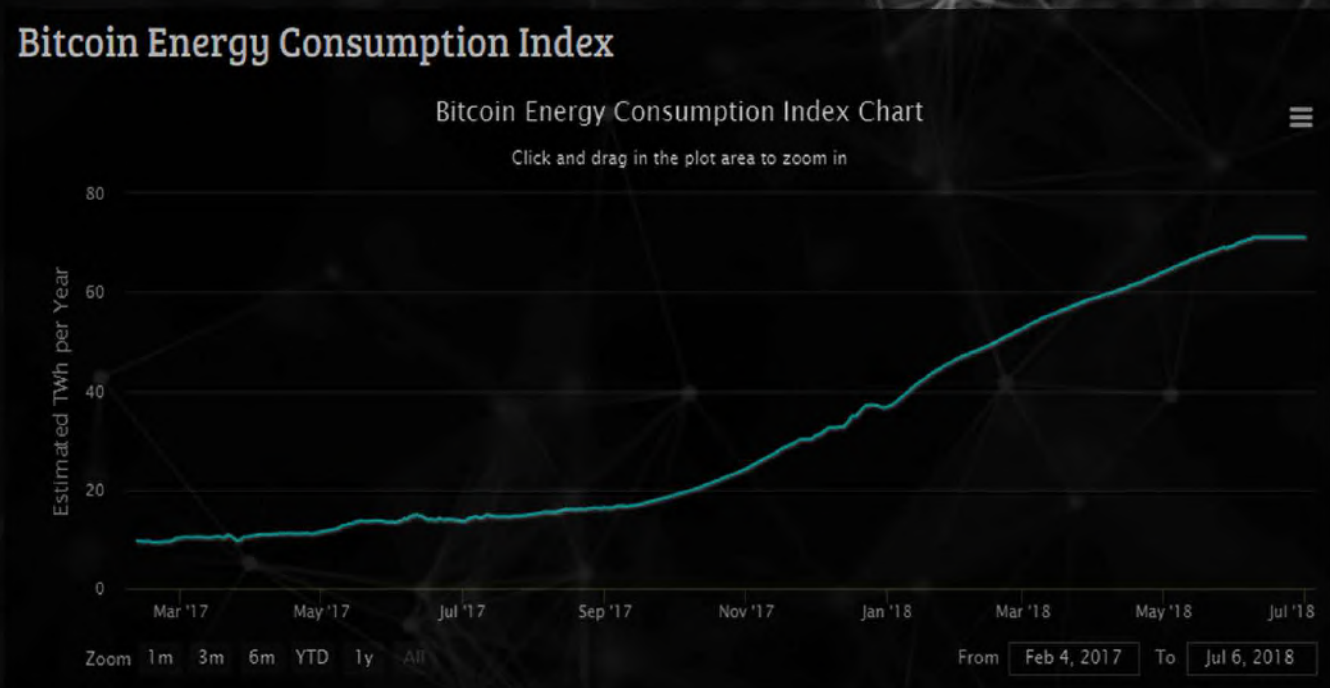
To run a MasterNode, it is necessary to stake coins against a wallet address linked to the MasterNode key and with proof of the deposit through the transaction hash and index. The stake required per MasterNode is constant across the network and is set at **3,000 XBI**. This means community members with more coins are directly incentivised to run more MasterNodes if they wish to increase their share of the overall reward. This offers fairness and proportionality in relation to both the overall stake held by the member and the amount of resource they offer to the network.

This fairness of this mechanism eliminates the competitive and increasingly inefficient arms race present in other coins, whilst incentivising the running of master nodes to help build and secure the network. Of course, like any Crypto Currencies, XBI does require Hashing, and this is based on the Xevan algorithm which uses a unique combination of dual X17 algorithms with a 128 bit headers. Xevan can be performed efficiently on standard PC servers, and so the cost of entry for new entrants is low, which helps increase the vitality of the XBI network and community.

Over the life of XBI, the balance of the reward scheme will shift both in terms of the number of coins and the ratio of reward between the Masternode and the Staked Coins. This is summarized in the table below:

Block Timeline	Coins Per Block	Block Reward	Total Blocks	Coins Mined/Block	XBI Circulation
Revised Block Data Post Fork		In % MN/S	3,057,580	Max 21,000,000	per block period
	10,500 (Premine)	Premine	200	21,000,000	2,100,000
0 - 200	1	PoW Phase	4,800	4,800	2,104,800
201 - 5,000	30	75 / 25 22.5 / 7.5	20,000	600,000	2,704,800
5,001 - 25,000	20	80 / 20 16 / 4	114,760	2,295,200	5,000,000
25,001 - 139,760	10	85 / 15 8.5 / 1.5	870,000	8,700,000	13,700,000
139,761 - 1,009,760	5	85 / 15 4.25 / 0.75	1,068,120	5,340,600	19,040,600
2,077,881 - 3,057,580	2	85 / 15 1.7 / 0.3	979,700	1,959,400	21,000,000
Total			3,057,580	21,000,000	21,000,000

Bitcoin Energy Consumption Index



4. The Solution for Privacy and Safety Concerns

Bitcoin Incognito uses Zerocoin protocol⁵ to ensure privacy for its users. Zerocoin protocol achieves anonymity through cryptographic operations applied to the Zerocoin minting process and separately to Zerocoin spend transactions.

By minting a Zerocoin from XBI, a user generates a random serial number that is then encrypted and then converts this into Zerocoin through use of a second random number. The Zerocoin is then added to a cryptographic accumulator in the Masternode pool and at the same time, an amount of XBI equal in value to the denomination of the Zerocoin is added to a Zerocoin escrow pool.





To redeem the Zerocoin back into XBI (preferably to a new public address) the owner of the coin needs to prove two things via a zero-knowledge proof. A zero-knowledge proof is a technique by which one party can prove to another that a given statement is true, without conveying any additional information. The first proof is that they know a coin that belongs to the set of all other minted Zerocoins without revealing which coin it is. In practice, this is done simply by use of a one-way accumulator that does not reveal the members of the set. The second is that the person knows the random number that along with the serial number corresponds to a Zerocoin.



Expenditure of Zerocoins is supported by posting the proof and serial number as a Zerocoin spend transaction, this allows confirmation that the proof and the serial number have not been spent previously. After verification, the transaction is posted to the blockchain, and an amount of XBI equal to the Zerocoin denomination is transferred from the Zerocoin escrow pool. Anonymity in the transaction is assured because the minted coin is not linked to the serial number used to redeem the coin.



bitcoin **INCOGNITO** *Transactions with true anonymity.*

Specifications	<i>bitcoin</i> INCOGNITO	 <i>bitcoin</i>	 BitcoinCash	 DASH	 litecoin
Network Consensus	PoS	PoW	PoW	PoW	PoW
Maximum Supply	21,000,000	21,000,000	21,000,000	18,900,000	84,000,000
Block Size	2MB	1MB	8MB	2MB	1MB
Avg. Block Time	1 min	10 mins	10 mins	2.5 mins	2.5 mins
Max. Transactions	75 tx/s	7 tx/s	61 tx/s	28 tx/s	56 tx/s
Minimal Fees	✓	✗	✗	✗	✗
Masternodes	✓	✗	✗	✓	✗
InstantSend	✓	✗	✗	✓	✗
PrivateSend	✓	✗	✗	✓	✗

Bitcoin Incognito Comparison Chart



5. The Incognito Masternode Pool



The Incognito Masternode Pool is a unique idea conceived by the Bitcoin Incognito team. It presents a way that holders of XBI have an additional incentive both to start running a masternode and to keep it running even as the daily reward (measured in XBI) decreases as the coin matures and grows in fiat value over time.

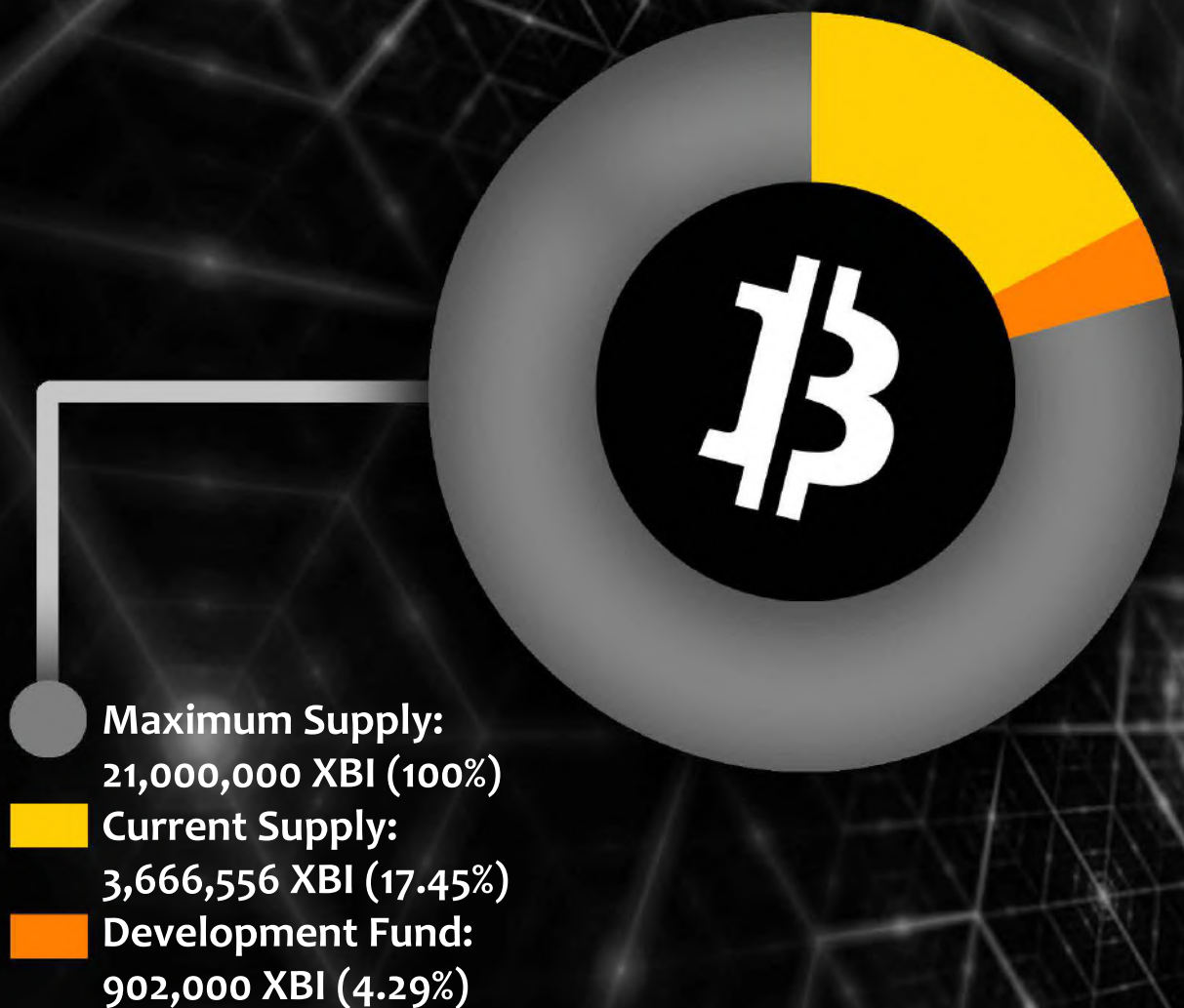
Masternode currencies in general offer strong incentives through daily rewards paid in coins. These can either be accumulated to run additional nodes or liquidated if the holder wishes. Early in such projects, when additional nodes are added and while the project is gathering momentum, the fiat value of the incentive may be low. Later in the project, as it reaches maximum supply, in this case 21 million coins, the daily reward and associated ROI would end. Under normal circumstances this would leave little incentive for Masternode holders to continue with their node. The Incognito Masternode Pool is the solution to this problem.

The Incognito Masternode Pool allows the community to suggest and vote through referenda on masternode and other lucrative coin projects for the pool to obtain and run. Masternodes rewards and at certain times stakes from these projects could then be liquidated into XBI or other high liquidity coins and split among all Bitcoin Incognito Masternode holders. The intention is for most of the process, beyond the decision of which Masternodes to purchase or liquidate, to be automated so that there is no question of fairness or opportunity for fraudulent activity. In effect the long term aim of the Bitcoin Incognito Project is to build a Digital Autonomous Organization (DAO) to manage high income cryptocurrency investments.



6. Distribution

The Bitcoin Incognito project is a community takeover, and thus coins are already in distribution, so there will be no ICO or other sale which could potentially risk a loss of value of purchased coins. Instead, XBI is already available on exchanges for purchase from other individuals at the market price. Like the original Bitcoin, the maximum supply will be 21 million coins. There is an existing Development Fund which will be used for Incognito Task Force operations, bounties, exchange fees, and project upkeep.



7. Conclusion

Bitcoin Incognito set out to create a coin which was an answer to the shortcomings of the original Bitcoin. Toward that end, it started out with the same maximum supply, but changed the technology to be more energy conscious and to increase privacy for its users. In addition the Incognito Masternode Pool creates additional demand for the coin.

The Bitcoin Incognito team is devoted to maintaining a project that stays on top of available technology. To ensure this, there may be updates to protocols and additional features or uses added as the project moves forward. As a community coin, suggestions in this area are welcome and will be considered.

8. References

1. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. URL: <https://bitcoin.org/bitcoin.pdf>
2. Power Compare. Bitcoin mining now consuming more electricity than 159 countries including Ireland & most countries in Africa. 2017. URL: <https://powercompare.co.uk/bitcoin/>
3. MIT Technology Review. Bitcoin transactions aren't as anonymous as everyone hoped. 2017. URL: <https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/>
4. Digiconomist. Bitcoin energy consumption index. 2018. URL: <https://digiconomist.net/bitcoin-energy-consumption>
5. Zcoin. Privacy enhancing technology, Zerocoin protocol. 2017. URL: <https://zcoin.io/tech/>

