With Gratitude; *The Progressive Realization Of A Worthy Ideal...*

Bitocoin

WHITEPAPER

Table of Contents

ABSTRACT

First, to the reader: we would like to express our heartfelt gratitude in advance for thoughtfully spending time familiarizing yourself with the project. This Whitepaper defines the perpetual goals, inspired vision, and the WHY of Bitocoin. We conduct a thorough assessment of the current ecosystem of cryptocurrencies by describing the blockchain innovations which back up this new cryptocurrency. It also presents how Bitocoin seeks to solve the flaws identified within the current system by implementing our latest technology.

A peer-to-peer crypto-currency design derived reverently from Satoshi Nakamoto's BTC. Proof-of-stake replaces proof-of-work to provide most of the network security in Bitocoin blockchain ecosystem. Under this hybrid design proof-of-work mainly provides initial minting and is largely non-essential in the long run. Security level of the network is not dependent on energy consumption in the long term thus providing an energy efficient and more cost-competitive peer-to-peer crypto-currency.

Bitocoin (BTO): A Transparent, Scalable, Organic, Lightning Fast Blockchain

OVERVIEW

COMPLETELY SECURED

LIGHTNING FAST

MORE PRIVACY

The concept of decentralized digital currency, as well as alternative applications like property registries, has been around for decades. The anonymous e-cash protocols of the 1980s and the 1990s, mostly reliant on a cryptographic primitive known as Chaumian blinding, provided a currency with a high degree of privacy, but the protocols largely failed to gain traction because of their reliance on a centralized intermediary.

In 2009, a decentralized currency (Bitcoin) was for the first time implemented in practice by Satoshi Nakamoto, combining established primitives for managing ownership through public key cryptography with a consensus algorithm for keeping track of who owns coins, known as "proof of work".

Currently, Bitcoin (BTC) is the dominant cryptocurrency, despite the fact that it is experiencing inherent flaws. Most fears in the crypto-world are not only exacerbated by wild price fluctuations, but also lack of security and privacy of the crypto-investors. Our point of the argument lies in the elucidation of what is lacking in Bitcoin and other major cryptocurrencies such as Ethereum, Litecoin, and Ripple, and how Bitocoin seeks to solve these issues.

INTRODUCTION

Cryptocurrencies are fast gaining in value as the world becomes more digitalized. To alleviate the problems of traditional physical systems, everything is going towards digitalization.

Bitocoin seeks to become a premier hybrid cryptocurrency that guarantees privacy and anonymity of its users by introducing innovative blockchain technologies and improving the current state-of-the-art. The development has integrated the latest privacy standards into Bitocoin's technology stack.

It is our belief that no one should have their finances or identity scrutinized by financial authorities, Government entities or any other individual or group because privacy is an inherent right. We are working to offer the latest technology that will protect the user's privacy.

CURRENT PROBLEMS IN CRYPTOCURRENCY

Privacy and anonymity

BTC is built upon an immutable blockchain, SHA-256 bit encrypted that is publicly available and distributed over a decentralized network supported by wallet users and miners. In situations where a human identity is linked to a wallet address through a commercial vendor or a crypto exchange, it is compromised irrevocably with regards to privacy. The anonymity of a user can never be retrieved without generation of a new one and loss of the remaining BTC linked to the same address. This can be compared to having a public record of your bank statement indicating all available transactions that can be seen by everyone.

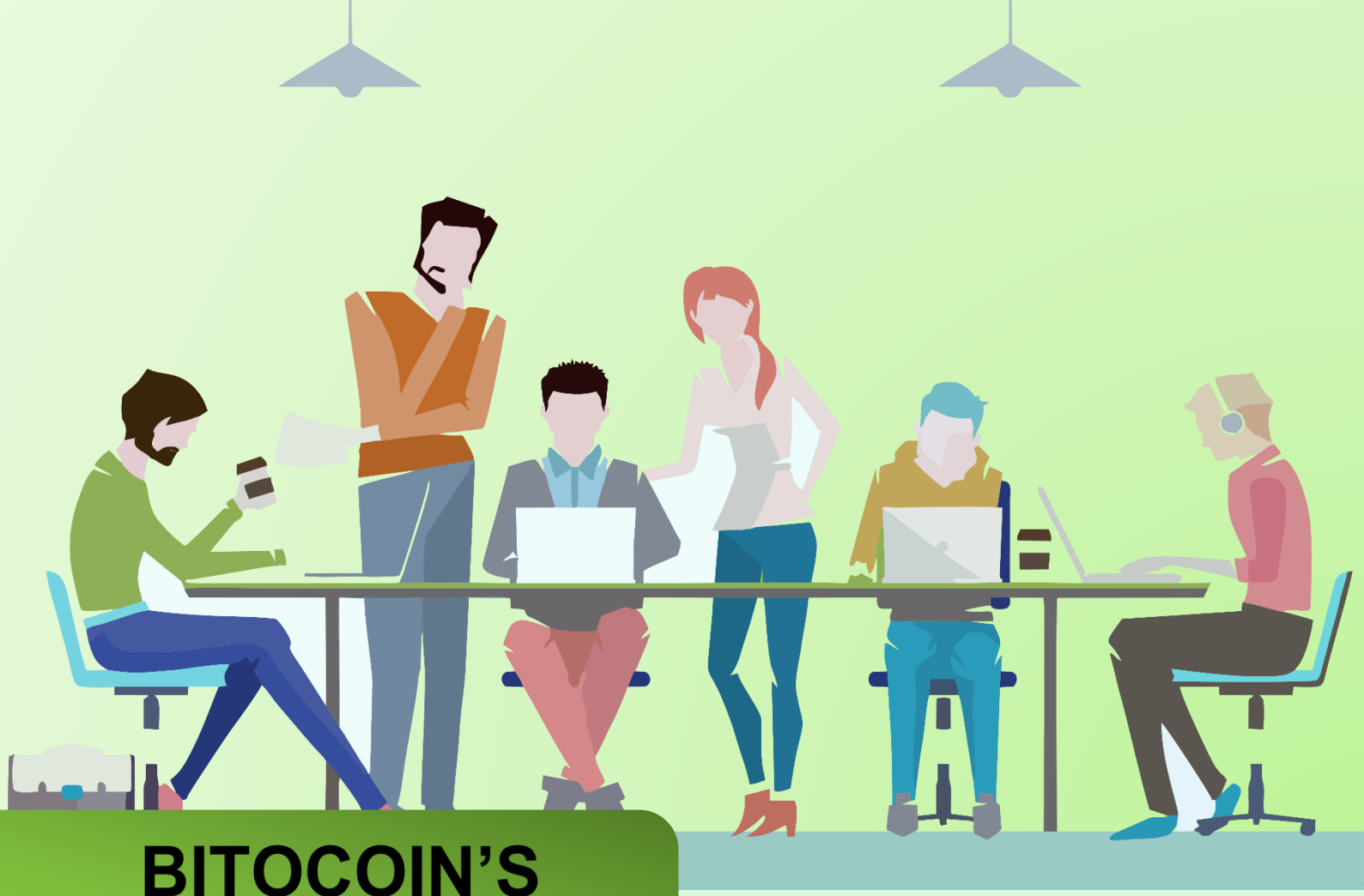
Your BTC address that was once anonymous is now linked irrevocably to your personal identity. This implies that the exchange is in a position to exactly verify the number of BTC you have in all the addresses (i.e. your newly created address and your once anonymous BTC address). Furthermore, they can verify to whom you are receiving or sending BTC. In circumstances where the BTC is required to share the details of their customers to Government bodies or law enforcement agencies, then they also get to know your identity as well as the number of BTC you have in your wallet. The same applies to the addresses of the persons you have been interacting with over the past transactions.

For most businesses, this could be catastrophic and perhaps one of the primary reasons major institutions haven't adopt BTC because privacy is a fundamental principle when it comes to financial operations. (Actually, it is information that is mandated in several jurisdictions). Therefore, there is clarity in the fact that the level of privacy adopted by BTC makes it fully inadequate for mass adoption. We can now make our conclusions on the "anonymous" nature of Bitcoin that is quoted often to be a fallacy in the eyes of its users

Scalability and Speed

BTC demands that all previous blocks within the blockchain are verified cryptographically by all nodes on the network. This requires significant storage space and computing power in regards to the blockchain size. It also requires a significant amount of time that would allow processing of the entire chain. BTC solely relies on the SHA-256 based x13 proof of work (PoW) to mint new coins and process blocks.

There is also a speed limit on how the transaction takes place which is proportionate to the difficulty currently configured by the design. A single block at present has a high degree of variability and has a confirmation time of 350 minutes. Most services often require a minimum of 6 confirmations for verification. This means that to send or receive a payment, you are likely to spend at least 35 hours which rules it out as a perfect payment system in the modern world.



BITOCOIN'S VISION

Bitocoin guarantees privacy and anonymity of its users by introducing the novel blockchain technologies and improving the current state-of-the-art. The development has integrated the latest privacy standards into Bitocoin's technology stack. It is our belief that nobody should have their finances or identity scrutinized by financial authorities, Government entities or any other individual or group because privacy is an inherent right. We are working to offer the latest technology that will protect the user's privacy

The key innovation of Bitocoin is it's invention of proof-of-stake, an alternative consensus protocol to Bitcoin's proof-of-work. Proof-of-work blockchains are secured by proving the consumption of a costly limited resource: electricity. Proof-of-stake replaces this expensive security protocol by utilizing an organic alternative scarce resource: time.

Bitocoin is capable of allowing any network connected computer to participate in the blockchain's security process. This efficiency strengthens Bitocoin by growing the number of security providers and ensuring that security can be sustained over the long-term.

QUARK ALGORITHM

How Is Quark Different?

The way Bitocoin mines is fundamentally completely different than BTC. This is because instead of mining on SHA-256, which is the algorithm that BTC is mined with, Bitocoin is a Quark-based cryptocurrency.

When cryptocurrencies are produced via a process of hardware mining as a result of a method called Proof-of-work, there are a number of ways in which they can be instructed to do so. Quark is a method that comes from 2013, a little later than the earlier forms of mining which is how cryptocurrencies such as Bitcoin and Litecoin are produced.

The first difference between SHA-256 and Quark is that Quark uses 9 different hashes (formula combinations) to mine a single Bitocoin block vs. SHA-256 which uses 6 hashes. Further, whereas SHA-256 is an actual algorithm (equation) in and of itself, Quark is not. Instead, Quark is a word for a broader system that represents 6 separate algorithms (Grøstl, Blue Midnight Wish, Keccak, JH, Skein and Blake) all running at the same time, solving the 9 hashes that is used to create a block on Bitocoin's Blockchain.

ENERGY EFFICIENCY

The effect of these changes is that Bitocoin is a lot more secure to mine than BTC is, while at the same time requiring a lot less power to mine. Under our design even if energy consumption approaches zero the network is still protected by proof-of-stake. We call a crypto-currency long-term energy-efficient if energy consumption on proof-of-work is allowed to approach zero.

Proof-of-Work blockchains are proven to be far superior in terms of price performance with respect to store-of-value of digital coins.

Proof-of-Stake blockchains are popular with a wide number of people, the coins tend to never appreciate much in value as so many coins are always flooding the market.

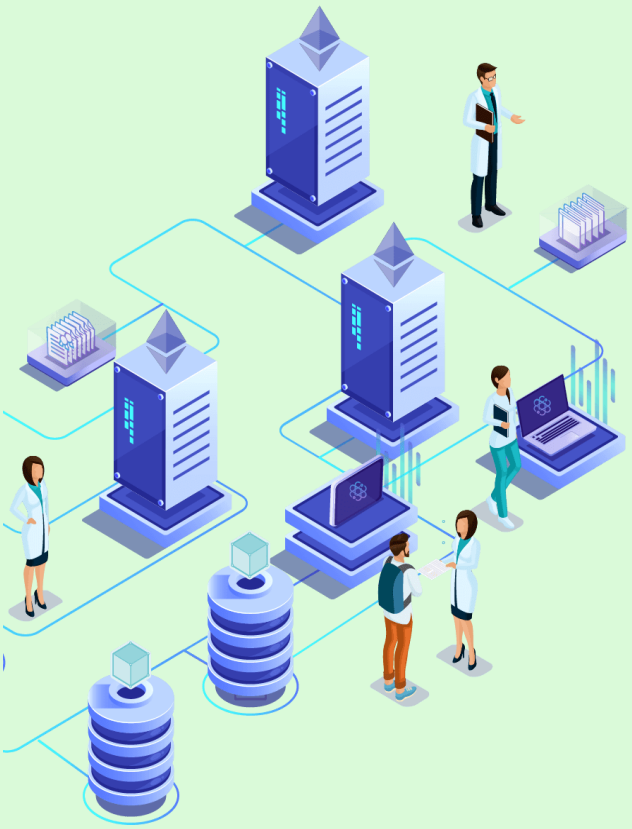
Quark algorithm fortifies the PoW method of mining making 50%+1 attacks effectively impossible too, so it's the best of all worlds!

Advantages of Hybrid PoW+PoS Blockchain

By adopting the Hybrid PoW+PoS censuses mechanism, Bitocoin can maximise user engagement, benefiting both parties. In future Bitocoin holders and miners can participate in decision making by voting, allowing users to determine the direction of Bitocoin as a company and as a technology, for example, implementing certain technologies or protocols, determining whether the development team should apply certain functionalities, whether existing code should be activated, and how to spend allocated budgets. If the updates are approved, the fork will be automatically conducted without a need for intervention by developers. In short, this means Bitocoin can truly embody the meaning of decentralisation.

PoW miners are responsible for producing and submitting new candidate blocks. PoS stakeholders confirm that a candidate block should be appended to the blockchain by voting. A network node can be either a PoW miner, a PoS stakeholder, or both at the same time. Therefore, the PoW and PoS have an equal importance in the consensus mechanism.

The PoS mechanism then also encourages Bitocoin holders to keep their coins in wallet rather than on an exchange where it is ready to be traded, and also has a positive impact on Bitocoin ecosystem as people will focus on the application of Bitocoin technology rather than short term price fluctuations. The adoption of Hybrid PoW+PoS guarantees the price of Bitocoin from the PoW side, due to the relatively stable cost of mining. This is because miners will not sell the BTOs earned at a lower price than what it cost them to mine. Additionally, the increasing cost of computing power will support the price of Bitocoin, alleviating the centralisation problem of a purely PoS mechanism. Regarding security, PoW progress needs to be approved by PoS, therefore, PoW miners cannot change the rule by themselves which prevent the chance of 51% attack. This helps the network remain secure.



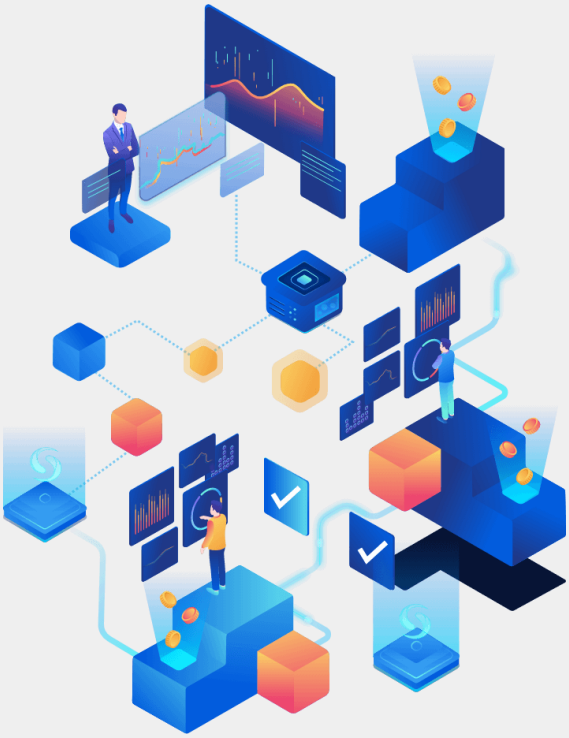
Benefits

As noted, the hybrid system's PoS mechanism requires wallet software to run constantly so that the stakeholder's chance of voting isn't missed. Further, since block rewards are distributed across PoW miners and PoS stakeholders, hybrid PoW mining is typically less profitable than pure PoW mining. Therefore, participating nodes tend to invest less in gaining hashpower, thereby lowering the barrier to entry for new PoW miners. Both of these factors help to encourage greater network participation. Finally, due to the potentially reduced total investment in hashpower, the network's energy consumption may be relatively lower than pure PoW.

What about Masternodes?

It may be some crypto full node which underpins the network by facilitating complete duplicity of the coin's record in genuine time. In exchange, the Masternode will get crypto coins as compensation. It may be an awesome alternative to mining.

First, PoS and Masternode technology have two things in common: staking coins for passive income and keeping the network secure. However, Masternodes don't usually create new blocks, they only have the power to reject blocks and verify transactions; Masternodes are a way to enhance a network based on a PoW or PoS protocol.



Running a Bitocoin Masternode requires 25k BTO coins as collateral. Masternode participants are rewarded at a slightly higher level as compared to just staking through the PoS protocol due to their importance across the network. There's no restriction in being an active participant of the network, staking, or becoming a Masternode. In fact, there is a guaranteed reward for everyone involved.

Value Proposition

Exclusive Benefits to the users

Highly-secure

Another extremely essential issue in today's environment is security. Users are always anxious about their data and transactions. Bitocoin provides a secure payment gateway to its users.

Bitocoin provides greater protection against majority attacks by requiring PoW miners and PoS validators to depend on each other.

FastSend

Time is the key value of every business and its processes. Companies and individual users are experiencing delays due to a lack of existing money transaction speed, particularly when it comes to financial transactions. Bitocoin provides the solution to such problems and offers a fast gateway of transactions.

Enhanced Scalability

Bitocoin is benefitting its users with enhanced performance than its counterpart Bitcoin. Its more enhanced scalability is putting Bitocoin on top of other cryptocurrencies. Potentially greater network stability via collateral benefits, such as incentives for maintaining always-online nodes.

Obfuscation

Bitocoin has the ability to make anonymized transactions using coin mixing Technology to protect the senders' identity.

Better energy efficiency.

Due to the potentially reduced total investment in hashpower, the network’s energy consumption is relatively lower than pure PoW.