# Micro Bitcoin

A Peer-to-peer Microtransaction Payment Platform

www.microbitcoin.org

Draft Version 2.1
March 2018

# Table of Contents

# Abstract

Micro Bitcoin (MBC) is a decentralized peer-to-peer (P2P) payment platform for the micro-economy. It is intended to be a means-of-payment coin, created (forked) from the Bitcoin (BTC) blockchain, and is designed to be used as a fast, flexible and acceptable method of payment which can be used between peers and between traditional businesses and their customers. Satoshi Nakamoto's original plan for creating Bitcoin was to provide a decentralized system of payments which was not under the control of any centralized fiat-rendering organization. However, Bitcoin has found limited application for micro-payments because of the problems of scalability, slow transaction times and high transaction costs. An effective blockchain-based payment solution has to be cheap to use and provide near-instant settlement of transactions for value to be delivered. This is where Micro Bitcoin comes in. The vision of the team behind Micro Bitcoin is to fulfill Nakamoto's original vision of creating a true Peer-to-Peer electronic-cash system for the micro-economy.

The forking process allows it to retain usage of a distributed ledger, while still providing the flexibility that is required to perform transactions at the micro-level without the hurdles of expensive fees and slow confirmations. We believe that Micro Bitcoin would be a beneficial complement to the Bitcoin blockchain and thus the cryptocurrency realm. It is not designed to replace Bitcoin, but to create a variation that can complement Bitcoin and rely on its strong foundation to support a specific purpose in the cryptocurrency community.

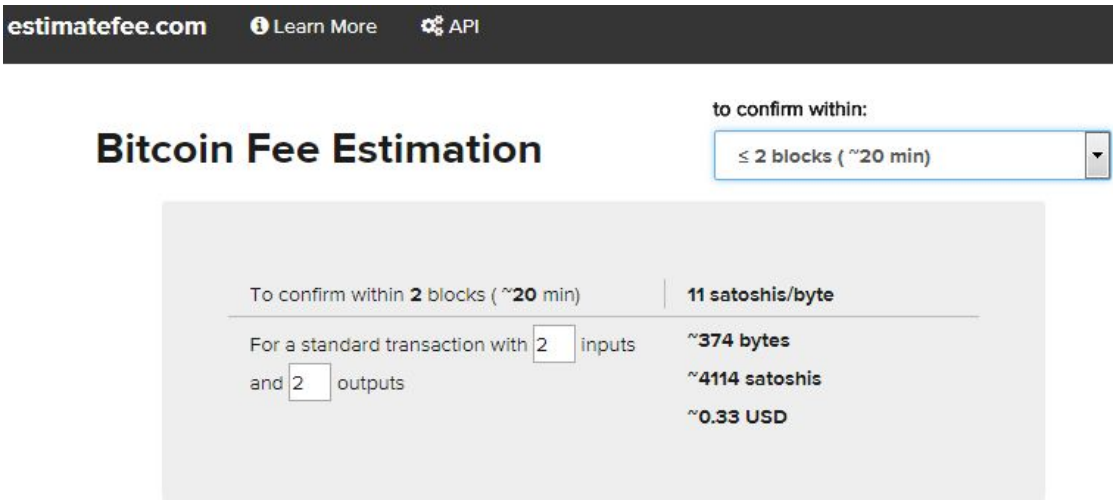
Keywords: Micro Bitcoin, MBC, peer-to-peer, open source, decentralized, "ASIC-resistant, micro-economy, microtransactions, micropayments.

# Introduction

Bitcoin and other cryptocurrencies began to witness a surge in interest from early 2016, about two years after the collapse of the Mt.Gox exchanges caused investor panic in the market. 2017 saw the price of Bitcoin soar from around $800 to a peak at almost twenty thousand U.S. Dollars. This move led to a dramatic surge in Bitcoin purchases, Bitcoin trading activity as well as trading activity in other altcoins. This massive user growth by mostly retail investors also led to an increase in the number of transactions on the Bitcoin network. This led to a stretching of the capacity of the network to handle the rapidly rising volumes, leading to an increase in confirmation fees and slower transaction confirmations.

Bitcoin's payment network offers a high level of censorship resistance, which is dependent on the continued decentralization of the system. This is an expensive event, as the cost of full node operations tends to rise with increasing number of transactions on the network. As block space usage has spiked, so also has the cost of using up blocks for transaction confirmations. Users are now essentially in a bidding war to have their transactions prioritized for processing. This bidding war has driven up costs of processing transactions to levels where businesses operating at the level of the micro-economy will find it unprofitable to accept payments with Bitcoin.

To get a proper view of the situation, a popular online Bitcoin fee estimator shows that as at the time of writing this white paper, the cost of confirming a transaction within 2 blocks or less (equivalent to 20 minutes or less) was about 33 cents.




When compared with traditional payment methods, P2P micropayments done using Bitcoin at an average of 33 cents per transaction would be too expensive. Then there

is also the problem of preservation of value. If a small business were to receive 2BTC worth of payments on April 1st 2018, would these retain their dollar value in a month given the price volatility in the Bitcoin market? This chart clearly shows that there is a severe depreciation risk involved.


A number of solutions have been developed and are still undergoing development to combat these challenges. Some of the solutions include previous hardforks such as Bitcoin Cash and Bitcoin Gold, implementation of SegWit and the ongoing development of the Lightning Network. The Lightning Network was initially believed to be a workable solution to many of Bitcoin's shortcomings, but this initial optimism is now coming under intense scrutiny. There are many who believe that the Lightning Network would cut out the miners who maintain the network as well as compromise the element of anonymity that Bitcoin is known for. There are even fears that the routing structure of the Lightning Network renders it vulnerable to DoS and DDoS attacks.

Furthermore, the adoption of the Lightning Network would mean that an integral characteristic of Bitcoin would have to be sacrificed; the distributed ledger system. Distributed Ledger is one of Bitcoin's most important components, ensuring that trustless transactions can be confirmed by various parties using a consensus mechanism.

In the light of these challenges, we are proposing a new platform that makes transactions faster, cost-effective and easy to use for the micro-economy without sacrificing the essential elements of the parent Bitcoin network. Transacting parties on the network will, therefore, derive the benefits of a truly decentralized network without having to sacrifice the beneficial elements of Bitcoin. Our solution will instead, assist in the advancement and application of the technology and ecosystem in general.

An additional application of our solution is an incentive mechanism that will promote the incoming of pioneers and developers who will use their skills to drive the advancement of the technology. The incentivized mechanism will also promote adaptation of our solution by peers and in the real world micro-economy. It will also provide for a better store of value, and not be subject to the wild variations in price that Bitcoin has been subjected to over time. This is very important for holders of the coin, who need to be sure that the value of their coins will not be suddenly halved or quartered in a few days of price volatility. This is presently a significant challenge for Bitcoin holders, who have had to endure repeated onslaughts from speculators who cause prices to move in wide ranges on a day-to-day basis.

Utility is a word that is being used quite often in the space, and we believe that an ecosystem of pioneers with ideas for the application of the technology and understanding of the benefits of a trustless system will help bridge the gap and pave the way. In order for such talent to excel, a technology that is easy to use out of the box, such as a plug-n-play kit, can be provided by a community of developers and incentivized if need be.

Ideas can be proposed and for such an event to be seen in motion that eventually leads to an end user also educating that such an ecosystem is in place, is priceless. We hope to help build such an ecosystem for a community that works together and towards a common goal, peer-to-peer payments.

# Technical Specifications

Presented below are the proposed technical specifications that will be implemented for the initial phase of the hardfork. With progression and adaptation, we believe an open and talented community will continue to contribute toward the technological improvements of the platform.

## 1. Total Supply

The supply of Bitcoins is presently pegged at 21 million coins, out of which 80% have already been mined. Any crypto coin to be used as a supplement to transactions in the micro-economy must be able to guarantee a vastly increased supply of these coins. An increased total supply would lower the value of integers, also known as "Satoshi," as well as the cost of transaction fees. Micro Bitcoin, to be known as MBC, would see the creation and deployment of 210,000,000,000 coins, or 10,000 times the number of BTC that can ever be mined.

210,000,000,000 MBC

*Increased ratio 1 BTC :10,000 MBC*

Increasing the total supply of MBC by a ratio of 1:10,000 to that of Bitcoin will lead to transactions of lower values attracting lower fees. This is in keeping with the intended idea for lowering transaction costs of micropayments made using the platform.

## 2. Proof-of-Work

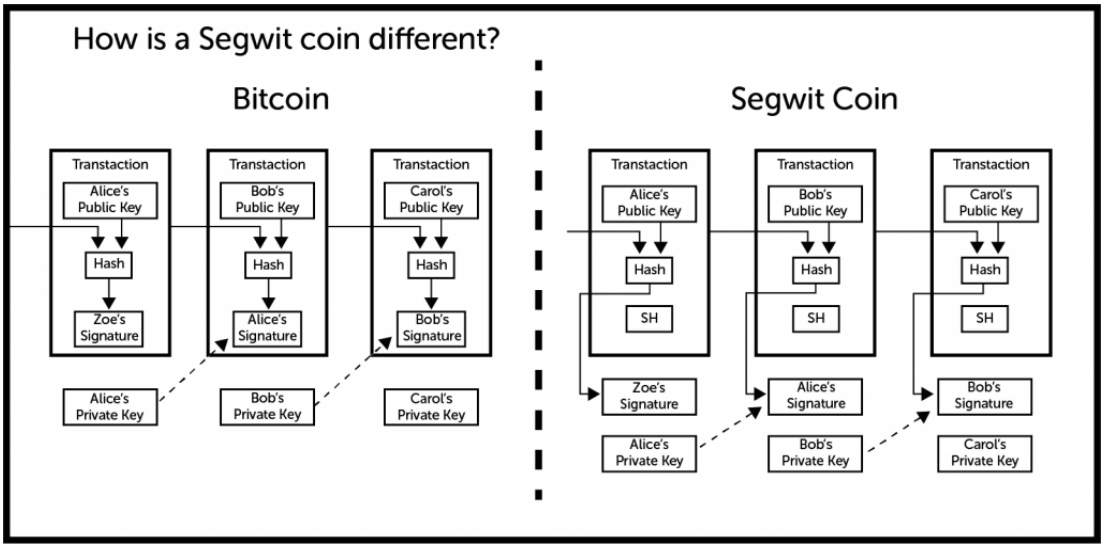
Issues regarding the current Bitcoin proof-of-work algorithm have been raised after significant improvements were made to mining equipment. These new mining equipment, commonly known as “ASIC Miners” (Application-Specific Integrated Circuits), became the latest generation of mining equipment and have supplanted the CPUs and GPUs that preceded them. Their incredible processing speeds and lower power consumption have made them the mainstay of the mining market, but their emergence has slowly led to a "centralized" mining structure. Due to the inequality of access to these ASIC miners, only those who could afford them and had the infrastructure to support their use could have access to these equipment. If you lived in a resource-deprived country where power cuts are the norm and not the exception, then the guys with the ASIC miners were already in an advantageous position.

Mining has to be kept decentralized so that it does not become skewed to suit those who had the muscle to afford ASIC mining equipment. This is why the "ASIC-resistant" mining equipment have been developed. Micro Bitcoin will implement the "ASIC-resistant" proof-of-work algorithm known as "Grøstl" that was developed by the team at Groestlcoin.

Full specifications related to mining will be listed on the official Micro Bitcoin Github repository. Link can be found via the official website.

# 3. Segregated Witness (SegWit)

Segwit is a protocol upgrade that has been designed to make Bitcoin more scalable without increasing the size of blocks. All Bitcoin input transactions require the sender to use the private keys to digitally sign off on the transaction. By segregating the signature block (which takes up the chunk of data size of each transaction), up to 60% reduction of the data size is achieved, reducing the transaction time and cutting transaction costs. Micro Bitcoin will fully implement SegWit.




*Source: Peter Rizun*

SegWit has proven to be a success in increasing the speed of transactions and Micro Bitcoin should continue with this advancement of the tech to provide the necessary transaction speeds for everyday usage and maximum speed of adoption in the micro-economy.

# 4. Block Size and Interval

To increase the number of transactions per second or "TPS," an increase in block size would supplement the many transactions happening on the network. Adoption of the SegWit protocol as mentioned previously will lead to a block size gain of four megabytes per block. More transactions can then be handled per block, at lower costs.

Furthermore, the interval between the creation of new blocks will be lowered to one minute to facilitate near-instant transaction confirmations for micropayments. So you can expect to walk into a pizza shop and pay for your pizza with MBC within the same time frame it would take to run your credit card on a PoS machine.

# 5. Block Reward

The ratio of the increase in total MBC supply in relation to existing BTC supply will be applied to block rewards. With Bitcoin transactions currently being done at 12.5 BTC per block (at an interval of ten minutes per block) we can formulate that:

$$(12.5 \times 10{,}000) / 10 = 12{,}500 \text{ MBC per block}$$

*(BTC Reward x Ratio) / Block interval ratio = Micro Bitcoins per block*

So miners would get more rewards of MBC in relation to BTC for each block mining cycle.

# 6. Replay Protection

Replay Protection is the generalized term used in describing techniques for prevention of replay attacks. Replay attacks are defined as fraudulent or malicious duplication or delay of validly transmitted data within the blockchain. If you have a main chain and a forked chain, it exposes the data transmitted on one chain to fraudulent duplication on the other chain. But replay protection makes such transactions only valid on the chain that the sender intended and renders invalid any malicious duplication of such data on another chain. In other words, data validly sent on chain X will not be valid on chain Y and vice versa. As this is an essential security measure, it’s a necessary implementation going forward.

In addition to implementing replay attack protection, Micro Bitcoin will use its own unique address formatting system as an added measure to secure transactions within its network.

# Pre-mine Distribution

There is a lot of negative perception about pre-mining in the cryptocurrency realm. Many see it as an opportunity for the developers and team members to make undue profits at the expense of the latter investors who come in at the Initial Coin Offering (ICO) stage. However, as you can see from the breakdown of pre-mine distribution funds below, all of the funds will be allocated to the development and sustainability of the Micro Bitcoin project. There are no "bonuses" or "payouts" for the core team and developers during this period.

It must be pointed out that the team also intends to provide support for startups and other blockchain-based projects that will be operating using the platform. This is being done to deepen and expand the ecosystem.

Out of the total supply 210,000,000,000 of Micro Bitcoin (MBC) coins, only 5% of them will be allocated at the pre-mining stage. The exact breakdown of the pre-mine allocation is detailed below:

## 1. Contributors

By contributors, we are referring to the team that will work on this project prior to the hard fork. The coming together of a team to volunteer to contribute toward the core development of the Micro Bitcoin platform is vital. It is only fair that team members who have put in their time and effort be duly compensated. To this end, 11% portion of the pre-mine allocation will be granted to them.

This project is to be open-sourced and should continue to have community support for further development and adaptation. The core contributors will continue to work to build a better community for a sustainable ecosystem.

## 2. Backers

Apart from the initial development that is carried out by the contributors, there are others in the background who provide financial support as well as support in invisible areas. 15% of the pre-mine portion will be distributed to those who have backed this project in good faith.

# 3. Bounty

Apart from standard contributions that are performed in any crypto project such as code updates, another component of contribution comes from spreading the word to the public, finding and fixing flaws in the software, assisting with promotional content, and many more. Rewarding those who can contribute in areas that go beyond the core team's mandate is a proper way to go. From community care providers to bug finders, all support team members bring an edge to broaden exposure and further progress the initial development phase. 4% of the pre-mine coins will be allocated to the bounty program.

Details on the bounty program will be announced via the official communication channels listed on the project website.

# 4. Initiative Costs

These are costs that are incurred in a blockchain project, which are vital to the initiation and running of the platform. Some of these initiative costs include miner fees, costs of setting up exchanges, developing coins and mining pool setups. The ecosystem is comprised of both miners and users of the platform. Miners keep the network running and secure. Their work demands significant investments in hardware and utilities. A marketplace incentive will be allocated to this group. Some of the expenses that this project will incur may be spent on the expansion of exchanges and mining pools to improve the ecosystem. 5% of the pre-mine will be used to cover these initiative costs.

# 5. Foundation

One of the largest hurdles in the progression of a sustainable ecosystem of creators and users is the availability of funds to maintain the growing community and the underlying technology infrastructures on which the ecosystem is built on. A substantial part of the pre-mined amount will be kept aside for future development of the platform, its ecosystem, and addition of new product lines such as incubators. This process will be managed by the Micro Bitcoin Foundation, which will be allocated 65% of the pre-mine.

To avoid abuse and misuse, the funds will be locked in a multi-signature wallet that the core contributors and other leaders will have access to. It is in the interest of the

project, and the entire ecosystem that funds raised are used in good faith and in the interest of the project.

# Contribution

It is envisaged that the project will be built by human resource pooled from outside the initial builders of this project. As such, the team is open to new contributors, who will put in their quota toward developing the network and community. Like Bitcoin, an open and transparent platform will be put in place. Contributors with skills that are relevant to the development of the future products that will run on this platform are highly encouraged to join the team. This project has been developed to accommodate future spin-offs, which will need a more substantial number of capable hands to handle.

As contributors and communities develop, a need for better consensus and contribution mechanisms may need to be in place in order to avoid malfunctions and abuse of the available resources. Peer-to-peer review systems have proven to be effective and potentially improve the governing ecosystem down the line. These will be incorporated into the project.

# Ecosystem

An excellent example of the use of Micro Bitcoin (MBC) in the micro-economy is when one can simply pay for a cup of coffee at his or her favorite coffee shop. Technology advancements have made customer experiences satisfactory by refining practices through the years. The same has to happen with new business models that are developed via the use of cryptocurrencies in real-world applications. There are many "Pioneers" with potentially great ideas but who lack the resources to develop simple payment solutions for their businesses.

One example many may relate to is how Steve Jobs was able to take Steve Wozniak's innovations and bridge the gap between us and personal computers [6]. The example shown helps to illustrate that there needs to be a team with various skills to have a working solution.

It is our intention to encourage open source development, creative ideas, user communities, utility and smart applications. Therefore, ours will be a community platform where fellow pioneers can access easy and ready-to-use technology and implement their ideas for people to have access to. It will also be a place where such ideas can be shared and built upon for the propagation of micropayments. This is the vision for Micro Bitcoin.

As further development is carried out, examples of use cases and applications will be written for others to be able to adapt in ways that best fit their environment.

# References

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf

[2] CoinMarketCap, “Historical Snapshot - December 17, 2017”, https://coinmarketcap.com/historical/20171217/

[3] Grøstl, “Grøstl – a SHA-3 candidate”, http://groestl.info/

[4] Bitcoin.org, “BIP-141”, https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

[5] Jimmy Song, “How Segwit2x Replay Protection Works”, https://bitcointechtalk.com/how-segwit2x-replay-protection-works-1a5e41767103

[6] Investopedia, "Steve Jobs and the Apple story," https://www.investopedia.com/articles/fundamental-analysis/12/steve-jobs-apple-story.asp