Abstract

Conceptually, digital currencies and blockchain innovations are ground-breaking - but they are still in their early stages of adoption. As cryptocurrencies gain prevalent acceptance, they will create a huge potential for brand-new projects and development in the Fintech area, making them very appealing for startups and investors alike. Still, the cryptocurrency market is not totally realized - and the intricacy of trading (combined with security concerns and troubles with identity verification) can be a concern for many potential users. The future success of cryptocurrencies counts on their widespread usage. Mainstream adoption, in turn, pivots on the provision of a safe, integrated P2P exchange, which allows beginner users to safely trade and exchange their digital possessions. There is a strong and growing need for a well-structured, easy-to-use, safe cryptocurrency technology, which supports non-technical users, supplying them with the details, strategies, and skills required to enable them to take part in the cryptocurrency area.

A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. MicroBitcoin is an open source crypto-currency created in 2018, derived from the Litecoin 2011. MicroBitcoin features Scrypt Merged mining which allows 25x faster transactions than Bitcoin.

small Note: The whitepaper, documentation, designs are in research and development phase and subject to change.

1. Introduction to Cryptocurrencies

A cryptocurrency (or crypto currency) is digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrency is a kind of digital currency, virtual currency or alternative currency. Cryptocurrencies use decentralized control as opposed to centralized electronic money and central banking systems. The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency.

According to Jan Lansky, a cryptocurrency is a system that meets six conditions:

a. The system does not require a central authority, distributed achieve consensus on its state.
b. The system keeps an overview of cryptocurrency units and their ownership.
c. The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
d. Ownership of cryptocurrency units can be proved exclusively cryptographically.
e. The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
f. If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

In March 2018, the word "cryptocurrency" was added to the Merriam-Webster Dictionary.

Blockchain

The validity of each cryptocurrency's coins is provided by a blockchain. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Blockchains are secure by design and are an example of a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been achieved with a blockchain. It solves the double spending problem without the need of a trusted authority or central server.

The block time is the average time it takes for the network to generate one extra block in the blockchain. Some blockchains create a new block as frequently as every five seconds. By the time of block completion, the included data becomes verifiable. This is practically when the money transaction takes place, so a shorter block time means faster transactions.

**Timestamping**

Cryptocurrencies use various timestamping schemes to avoid the need for a trusted third party to timestamp transactions added to the blockchain ledger.

**Proof-of-work schemes**

The first timestamping scheme invented was the proof-of-work scheme. The most widely used proof-of-work schemes are based on SHA-256 and scrypt.[24] The latter now dominates over the world of cryptocurrencies, with at least 480 confirmed implementations.

Some other hashing algorithms that are used for proof-of-work include CryptoNight, Blake, SHA-3, and X11.

**Proof-of-stake and combined schemes**

Some cryptocurrencies use a combined proof-of-work/proof-of-stake scheme. The proof-of-stake is a method of securing a cryptocurrency network and achieving distributed consensus through requesting users to show ownership of a certain amount of currency. It is different from proof-of-work systems that run difficult hashing algorithms to validate electronic transactions. The scheme is largely dependent on the coin, and there's currently no standard form of it.

**Mining**

In cryptocurrency networks, mining is a validation of transactions. For this effort, successful miners obtain new cryptocurrency as a reward. The reward decreases transaction fees by creating a complementary incentive to contribute to the processing power of the network. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs running complex hashing algorithms like SHA-256 and Scrypt. This arms race for cheaper-yet-efficient machines has been on since the day the first cryptocurrency, bitcoin, was introduced in 2009. With more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest large sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash often does not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the enormous amount of heat they produce, and the electricity required to run them.

2.  Problem in Market

The number of digital currencies keeps increasing on a daily basis. For investors with little knowledge of these currencies, choosing the currency to invest in becomes hard

and complicated. Mostly, only a few currencies will be chosen such as Bitcoin, Ethereum, Dash, and Litecoin. However, there are hundreds of other currencies that are also a good investment that can bring good returns, and have little likelihood of collapsing. With little information, investors use a lot of funds and gain little from some of the assets in the market.

These are highly known currencies have a very high valuation, which increases daily. Therefore, their demand is very high. Nonetheless, the changes to the valuation cannot be highly controlled, and investors want to gain the best value. Therefore, the need to invest in more assets and stand a chance of gaining more returns arises. Moreover, there is little information available to the public about the cryptocurrency market index, which can be used to make investment decisions and also to track the market movements.

3. About MicroBitcoin
    a. General Information

       MicroBitcoin is a highly secure peer to peer decentralized MicroBitcoin cryptocurrency using the Scrypt PoW/POS (Hybrid) Algorithm with a self-regulated financial system which allows users to earn MicroBitcoin through Mining, Staking and by buying with Bitcoin, Ethereum and Bitcoincash during the pre-sale phase and then via BTC only once the main investment portal is live. A sophisticated method of difficulty that re-targets every block. This currency is like the Dollar, but it is only available in the digital world. The concept may sound like Bitcoin and is actually not much different from bitcoin. A total of 25.2 Million MicroBitcoin coins will be minted. This is done via natural supply and demand and through general market fluctuations the price will rise and fall accordingly, but obviously, the more the demand, the more the coin will rise in price, giving all those holding MicroBitcoin an incentive to Stake from their wallets 10% per year on average.

    b. Our Vision

       Our vision is to create a cryptocurrency which gives high rewards to all users but stays alive after the high-POS phase and keeps on improving all the time. We truly believe that high-pos coins can have a future and that they are not damned to die soon as the high-pos ends.

       Ours Goals:

       • Creating a strong and responsible community.

- Creating a high-pos coin with a clear future
- To achieve all our visions as set in the road map
- To create an environment to support the cryptocurrency and avoid future disputes.
- To make it open source and decentralized for its wide spread adoptions
- The users can be completely anonymous and don't need to share their identity for their transaction or holding MicroBitcoin.

4. Technology

a. Proof of stake

Proof of stake, or PoS, is a type of Algorithm by which a crypto currency Blockchain network aims to achieve distributed consensus. In PoS based crypto currencies, the creator of the block is chosen via various combination of random selection of wealth or age.

In contrast, the algorithm of proof-of-work based cryptocurrencies such s bitcoin uses mining; that is the solving of computationally intensive puzzle to validate transaction and to create new blocks.

b. Proof of Work
Proof of Work, or POW, is the original consensus algorithm in a Blockchain network. This algorithm is used to conform transactions and produce a new block to the chain. The miners compete against each other to complete transactions on the network to get rewarded. A decentralized ledger gathers all the transactions on the block to the chain. The main working principle are a complicated mathematical puzzle and a possibility to easily prove the solution.

c. Scrypt Algorithm

In cryptography, Scrypt is a password based key derivation function created by Colin Percival. The algorithm was designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012, the algorithm was published by the IETF as an internet draft intended to become an informational RFC, but a version of Scrypt is now used as a proof of work scheme by cryptocurrencies like MicroBitcoin. Scrypt is a memory hard key derivation function, it requires a reasonably large amount of Random Ac-cess Memory to be evaluated. This makes implementation in special purpose custom hardware (ASICs) require more VLSI area, which would make it unprofitable to

build for the purpose of mining Viacoins. The requirement of Scrypt algorithm is a large array of pseudo random bits to be held in memory and a key that is derived from this. The algorithm is based on TMTO (Time-Memory Tradeoff). ASIC advantage in Viacoin is reduced by a factor of 10 compared to Bitcoin.

Scrypt uses the following parameters to generate a derived key:
- Passphrase: String of characters to hash
- Salt: Random string provided to Scrypt functions
- N: Memory/CPU cost parameter
- P: Parallelization parameter
- R: Blocksize parameter
- dkLen: Intended length of the key derived key in bytes
kd = scrypt(P, S, N, P, R, dkLen)

5. MicroBitcoin

   a. Overview

   Micro Bitcoin is powered by the most scalable and advance Blockchain technology the power instant and private payments. Use Micro Bitcoin to make instant, private payments online or in-store using our secure open-source platform hosted by thousands of users around the world. Micro Bitcoin is open-source and accessible to all. With Micro Bitcoin, you are your own bank. Only you control and are responsible for your funds. Your accounts and transactions are kept private from prying eyes.

   b. Coin Information and Distribution

   General Specification of MicroBitcoin

   Algorithm: Scrypt

   Type: PoW/PoS

   Coin Name: MicroBitcoin

   Coin Abbreviation: MBC

   Coin Supply: 25200000 MBC

   Premine: 1260000 MBC

   Address letter: M

RPC port: 33014

P2P port: 33013

PoS percentage: 10% per year

Block reward: 57 coins

Coinbase maturity: 20 blocks

Target spacing: 64 seconds

Target timespan: 1 block

Transaction confirmations: 6 blocks

Seednode 1: 207.148.77.109

Seednode 2: 207.148.77.122

c. Premine

The pre-mine coins will be used for ICO sales, bounties and airdrop for the community. The total pre-mine coins to be sold during the ICO will be 2,50,000.00 MBC

d. ICO

An initial coin offering (ICO) or initial currency offering, a type of crowdfunding using cryptocurrencies, is a means of raising capital for development and future improvements required to sustain the project and also promote the awareness of MicroBitcoin through different channels of efforts by the team.

The MicroBitcoin project will get funded with the premine coins sold during the ICO The raised funds will be used for improved marketing, exchange listing fee or to pay the team.

e.  Features of MicroBitcoin

The peer-to-peer payment system is electronic money transfers made from one person to another through an intermediary, typically referred to as a P2P payment application. P2P payments can be sent and received via mobile device or any home computer with access to the Internet, offering a convenient alternative to traditional payment methods. BitherCash has the built-in functionality of peer to peer payment that would facilitate the users to send and receive their earned amount directly into their e-wallets without having to worry about massive surcharges implemented on traditional payment methods.

Peer-to-peer itself means BitherCash runs without having a central server. The storage server is decentralized and distributed-divided into various servers run by each user connected to the network.

i.  Instant Peer to Peer Transfer

MicroBitcoin coin supply will only have 25.2 Million coins worldwide, this resembles an economic system based on deflation and with increasing supply coin, MicroBitcoin coin prices tend to rise, when demand is high and the number of coins that remain is not increased.

ii.  Limited Number of Coins

Just like Bitcoin, it can be sent anywhere in seconds, whenever and wherever you want. Money transfer with MicroBitcoin can happen only with a smartphone's internet connection.

iii.  Transactions are Anonymous

All the transactions we have done can be seen, but we do not know who the owner of the MicroBitcoin address is if the owner does not tell it. Each MicroBitcoin user can actually choose whether or not his name will appear, but even if the user wants to keep his identity secret, all of his transactions are still recorded and can be monitored through blockchain.

iv.  Transfer Made easy

You can transfer MicroBitcoin to anywhere in the world as long as it is connected to the internet. MicroBitcoin will be deposited into the Wallet.

v.    Low Transaction Fee

MicroBitcoin using scrypt algorithm as their consensus mechanism allow the efficiency to provide low or no transaction fee for transaction on the blockchain network compared to the centralized and other transaction modes available.

vi.    Decentralized

Since MicroBitcoin makes use of the Blockchain database, it means it is not controlled by a third party but is so open to the public that it is impossible for someone to forge transactions in Blockchain. All transactions are recorded live, transparent, and spread across multiple servers. Those who want to change or falsify MicroBitcoin transaction data must hack multiple servers at the same time.

vii.    Transactions are fast and Easy

MicroBitcoin uses Scrypt algorithm which allows it to have faster 25x transactions than Bitcoin and it is easy to send money using any of the available wallets. Users do not require register when using the QT wallet.

viii.    Open source

Microbitcoin is open source and it is available to public to participate in the community for development and bugs fix required in the system to support the currency of future - MicroBitcoin

ix.    Community

Microbitcoin is been developed from popular cryptocurrency – Bitcoin and Litecoin providing the community an easy understanding and less efforts to create adoption on a mass level.

f.    How we are different from Bitcoin

In the world of cryptocurrencies, Bitcoin and MicroBitcoin coin are not much different, the difference is the opportunity as well as price. To have one Bitcoin, you have to get ready for more than $7000. You have a better opportunity of acquiring MicroBitcoin coins because the price is still very cheap and you have a chance for the price of the ICO which is certainly something you can't get in bitcoin before.

Our reason for making use of Blockchain

**Decentralization**

A lot of people know blockchain as an innovative technology introduced together with its first use case – Bitcoin, a decentralized peer-to-peer cryptocurrency. However, blockchain technology has since also been used for business and organizational purposes, either with a cryptocurrency of its own as a public blockchain or without one as a private blockchain. While aspects of the technology are seen as something that could be useful for such purposes, there are some concerns as to why a business would want decentralization at all, leading some too, incorrectly, dismiss blockchain technology as a hyped-up trend and nothing more.

Below are a few business benefits attributed to decentralization with blockchain:

**Security:** Since records are distributed across multiple areas and are updated as each block is created, there is always a high level of availability of the data. So, even if a large number of nodes fail or are shut down by an attack, the data is still available for people to access. In addition, since the system is regularly updated with the latest block, accessing any of the active nodes means acquiring the latest data, even in the event of a DDoS attack – a highly-desirable trait for network security.

**Distributed Processing:** In addition to being able to access the latest block from an active node, the system can also continue to process additional data and add more blocks into the blockchain. So, not only is the data accessible, the system can continue operating as long as there are active nodes in the system. Thus, if an attacker wants to shut down the system to halt processing, they would need to shut down every node on the blockchain, making it even more restrictive to achieve.

**Partnerships and Consortiums:** While partnerships and consortiums are usually created with the best intentions and with all of the necessary legal agreements in an attempt to protect all parties involved, there still lingers the concern of trust, especially in cases when the parties involved are in competition in other areas. Because of the decentralized nature of blockchain, the issue is significantly mitigated as trust is not needed in terms of processing data as well as storing it. Verifying that one has the same information that another party has is relatively easy to do without the need for additional trust among the parties involved.

These are just a few of the benefits businesses can have when using blockchain technology due to its decentralized structure. With the increasing number of businesses looking into solutions that blockchain can provide, we're sure to find even more benefits of decentralization in the near future.

The original Scrypt algorithm was created by Colin Percival, for an online backup service called Tarsnap. The technical definition of the Scrypt algorithm is that it's a 'password-based key derivation function', which means that it derives a secret key from a password. Percival deliberately designed the algorithm to be computationally intensive to perform, requiring a large amount of memory to perform. The purpose of this was to make brute force attacks more expensive to perform. The idea behind this is that a person who knows their password would be required to pay the computational cost of performing the mathematical operation once, which would be negligible, but a person trying to guess someone's password would have to pay the computational cost many times, significantly adding to the cost and difficulty for the attacker.

g.   How secure is MicroBitcoin

Blockchain, the distributed ledger technology underlying MicroBitcoin coin, may prove to be far more valuable than the currency it supports. But it's only as valuable as it is secure. As we begin to put distributed ledger technology into practice, it's important to make sure that the initial conditions we're setting up aren't setting us up for security issues later on. To understand the inherent security risks in blockchain technology, it's important to understand the difference between public and private blockchains.

MicroBitcoin coin relies on a public blockchain, a system of recording transactions that allows anyone to read or write transactions. Anyone can aggregate and publish those transactions, provided they can show that a sufficient amount of effort went into doing so, which they can demonstrate by solving a difficult cryptographic puzzle. The process by which a network of nodes confirms the record of previously verified transactions, and by which it verifies new transactions, is known as a consensus protocol. In the MicroBitcoin coin system, because no user is implicitly trusted to verify transactions, all users follow an algorithm that verifies transactions by committing software and hardware resources to solving a problem by brute force (i.e., by solving the cryptographic puzzle). The user who reaches the solution first is rewarded, and each new solution, along with the transactions that were used to verify it, forms the basis for the next problem to be solved.

This decentralization and relative freedom of access has led to some unexpected consequences: Because anyone can read and write transactions. Because the consensus protocol is energy consuming, the majority of users operate in

countries with cheap electricity, leading to network centralization and the possibility of collusion, and making the network vulnerable to changes in policy on electricity subsidies. Both of these trends have led to an increased interest in private blockchains, which could ultimately give businesses a greater degree of control.

Primarily used in financial contexts, private blockchains give their operators control over who can read the ledger of verified transactions, who can submit transactions, and who can verify them. The applications for private blockchains include a variety of markets in which multiple parties wish to participate simultaneously but do not fully trust one another. For example, private blockchain systems

fully trust one another. For example, private blockchain systems supporting land and physical asset registries, commodities trading, and private equity distribution are all being tested. As these systems develop and evolve, they, too, may encounter unexpected consequences, some of which will have repercussions for the security of the system and the assets it manages or stores. As in software and product development, considering security at an early stage alleviates the difficulty of making fundamental changes to a product to address a security flaw later on.

h.  Privacy and Security

When privacy is mentioned in association with cryptocurrencies, the chances are that anonymity is meant instead. The sending of coins from one wallet to another via the blockchain is considered "Private because your personal information is not sent during this transaction. However, the fact that a transaction has been made makes the transaction itself "Public" but without any identifying details. Due to the transparency needed for most cryptocurrency blockchains, information on all transactions within it—traceable to its origin— is publicly available online.

Another point worth mentioning is many HYIP sites will conduct their "Exit Strategy" by claiming they have been hacked. We have spent many thousands of dollars ensuring the integrity of our site and have hired external trusted parties to attempt to attack it or find vulnerabilities and we are proud to say our site is as safe as it can possibly be.

We will also operate with hot and cold wallets to ensure the majority of the investors' money is insecure multi-sig cold wallets should an attack ever takes place. 2FA will be mandatory for our users. We also respect user's privacy, the only identifying information we will receive from you will be your wallet addresses and email address, keep in mind that if you take part in the referral

program, there may be other users who have access to your email address so it is advisable to use a separate or dedicated email address for not only this site but most Crypto sites.

Our site will store cookies and may record your IP as part of our antifraud procedures, but no other than the aforementioned no identifying information about you will be held by us, however, in saying that you need to ensure you have secured both your site password, your email address used to sign-up and your wallet should be encrypted and backed up, we take no responsibility for your failure to take standard security precautions when it comes to Crypto Currencies.

i.    MicroBitcoin Team

We know we are going to take a hit here for this, but we believe it is still viable for us and our investors to do so. We believe that the individuals have right to conduct business without any approval in the crypto world so we are not providing our identities to the General Public to avoid for any negative attention towards ourselves or our families. Tax is other implication, we would fall under the jurisdiction of some of our developer's Countries as what could be deemed as "Business Owners", therefore we choose to exercise our right to privacy. It may take some cost to pre/post launch, then so be it, we would rather out of pocket than in Prison on charges of "Operating as a financial institution without a license" etc.

Another reason we are not providing our identities to the General Public, as true believers in crypto we believe that individuals has a right to conduct business without anyone approval so we do not want any negative attention towards ourselves or our families.

MicroBitcoin is not associated with any scams or investment schemes. It is being designed and developer to be the cryptocurrency for tomorrow and the easy and cheapest mode for transaction for the unprivileged people who do not have bank account. It is being designed to get attention from community to migrate themselves from the centralized and heavily charged currency transaction methods.

j.    Our Team of Developers

Our coin creation team has been in the business for many years. We have spent a considerable amount of our own time and money refining our site, both front and back end and our user interface to ensure we provide you with a working, easy to use a sustainable product that will be here for the long term. We are more than aware of the scams, the BS, and the likelihood of attempted attacks on our site. Our Dev team for MicroBitcoin are professionals in the space and have been in the industry for many years, so we know how to overcome this and still provide a working product to our clients.

k. Roadmap

MicroBitcoin team has made its vision and path for future clear to support the network and the users participating in the community. We have planned and created our roadmap with aspects considering it to be the future of digital currency and decentralized.

Feb 2017 – Launch of the Idea
March 2017 – Implementation & Development of planned
April 2017 – Market Framework planned
June 2017 – Core Strategic Team with Executive team
August 2017 – Core Development team started development
December 2017 – Blockchain implemented on livenet
January 2018 – Pre ICO started
February 2018 – Marketing and PR
February 2018 – Test net implemented
February 2018 – Wallet Launch
June 2018 – Listing on Exchange
May 2019 – Support and Partnership use case
December 2019 – Integration with leading Hardware Wallet Provider
January 2020 – Launch of Debit Card

l. Resources

   i. Website and Wallet Software

     MicroBitcoin has developed and maintained its website to store and make all the data available for the users in the community. Users can also download the wallets available on the website to create and make transactions anonymously.

     Website: https://www.microbitcoin.co

Wallet: https://microbitcoin.co/my_wallet/


    ii.   Development Repository

MicroBitcoin is open source and the source code is been made public on the Github repository for interested developers to provide with their inputs and allowed to create their own branches/repository to modify and push the code after testing on the livenet.

GitHub: https://github.com/digixhub/MicroBitcoin

    iii.   Block Explorers

Microbitcoin also had a block explorer hosted to keep their blockchain alive and on live to track on the various factors and transactions on the network.

Block Explorer: https://blockexplorer.microbitcoin.co


    iv.   Social Media

MicroBitcoin is active on multiple social media channels to get the attraction and easy community access to achieve the vision to create "Digital Money for Payments".

Facebook:
Instagram:
Twitter:
Youtube:
Reddit:
Quora:
Bitcointalk:
Telegram:
WhatsApp:

6. Conculsion

Firstly, we would like to thank you for taking the time to read whitepaper document about MicroBitcoin, unless you just skimmed through it to the payment amounts and we

hope that you use this Whitepaper as a guide to make an informed decision on whether or not to invest in MicroBitcoin.

As mentioned we have our vision and roadmap planned to keep the coin sustainable for the long run and for those who invest to have peace of mind. We have a good marketing and PR teams working together to strive hard and achieve the success we have decided for MicroBitcoin. Furthermore, we will be spending a lot of time to search for teams to join us and create utility with MicroBitcoin for mass adoption.

And one final word that we would like to leave you with is, that if you are reading this in 2018, remember you are even now, in this day, still only a very small percentage of the population who "Get" Crypto. We believe Blockchain and Cryptocurrency will soon be part of everyday life for Generations to come.