BitCash

BitCash Whitepaper v 2

What is BitCash?

BitCash is a cryptocurrency that helps consumers and businesses trade. By combining the benefits of decentralization with those of internet banking, BitCash makes spending and accepting cryptocurrencies as easy as other currencies, like dollars or yen. BitCash aims to be the world's most useable cryptocurrency, helping everyone enjoy faster, cheaper, and secure trading.

BitCash also powers our innovative PeerQ platform that aims to help facilitate adoption amongst the masses.

What is PeerQ?

PeerQ is a Quora-like platform that rewards users in cryptocurrency for answering questions and completing tasks.

What is BitCash's mission?

To become the world's most useable cryptocurrency so everyone can share in the rewards of decentralization.

How will BitCash deliver on its mission?

BitCash will help overcome the barriers that deter businesses and the general public from entering the cryptocurrency space. Specifically, BitCash will focus on the following key areas:

a) Usability
b) Stability
c) Simplicity
d) Mass adoption

PeerQ combines these four areas to create a familiar, easy-to-use platform that allows anyone to gain access to cryptocurrency.

Why does the world need BitCash?

The benefits of decentralized cryptocurrencies are well known: they include speed, privacy, security, efficiency, and lower fees. But so far, few people have enjoyed them.

While the market cap of cryptocurrencies has grown rapidly over the last few years, attracting widespread media attention, they have yet to seriously impact the way we exchange value today.

This is partly because consumers prefer the familiarity of credit cards and traditional currencies (fiat), bribed into maintaining the status

quo by incentives like reward points, insurance, and tap to pay. Just buying and storing cryptocurrency can be a technical challenge, and there are still too few places to spend it.

The challenge for businesses is a lack of tools. Cryptocurrencies offer huge advantages like zero chargebacks, faster settlement, and lower fees, but have yet to allow basic tasks like printing transaction statements, recurring payments, importing ledgers into accounting software, and so on – the very tools a business needs to run.

BitCash overcomes these challenges by helping consumers use BitCash as currency, while providing businesses with the tools they need to transact on a day-to-day basis. We aim to “borrow” the features of today’s fiat banking and combine them with the power of cryptocurrency. This will encourage mass adoption, and in turn, help more individuals and businesses enjoy the benefits of decentralization.

The PeerQ platform creates a peer-to-peer knowledge economy. It incentivizes participation, rewards the best answers, and provides real-world utility for the BitCash cryptocurrency.

Cryptocurrencies face an adoption challenge

Global adoption

Only a handful of businesses currently accept cryptocurrencies as a form of payment. Just over 13,000 venues in the world accept Bitcoin, for example (according to Coinmap's August 2018 figures). That's a drop in the ocean compared to the millions accepting credit cards.

Venues accepting cryptocurrencies grew by just 38% over the last year. At this rate, people could wait decades before being able to spend their cryptocurrencies as easily as using their credit cards.

Ease of Use

Buying cryptocurrencies is hard. You must download a wallet, navigate complex software, and keep track of passwords, transactions, and other data. At the moment, it's easier to buy a $1,000 couch online than it is to buy $1,000 worth of Bitcoin.

Unless we make buying and using cryptocurrency as easy as fiat, we'll never reach mass adoption and the rewards of decentralization will remain out of reach.

Tax reporting issues

Many Western Governments consider cryptocurrencies “intangible property”, subjecting them to capital gains or other similar taxes, depending on the jurisdiction.

So if you buy and then sell a cryptocurrency at a profit, you could be subject to taxation. Even if you make a loss, you might still have to report it to taxation authorities.

By this rule, every time you buy something with cryptocurrency – whether it’s a product or service – the transaction might be taxable. And at the moment, tracking cryptocurrency transactions is an absolute nightmare: you can’t print statements, there’s no accounting software support – you can’t even see what you spent your money on.

Can’t easily be integrated by online businesses

Once the general public starts filling their wallets with cryptocurrency, they’ll be looking for somewhere to spend it. Businesses that can’t accept cryptocurrency could lose out to others that can. The challenge is therefore ensuring cryptocurrencies adopt the tools of current banking systems, so every business can participate.

How will BitCash tackle the adoption challenge?

BitCash solves the crypto adoption problem in three ways:

1. By making it simple to buy, mine, manage, and use cryptocurrency.
2. By giving businesses the banking tools, they need to accept cryptocurrency payments.
3. Through PeerQ, which is a Quora like platform that rewards users with BitCash for answers and completing bounties

We don’t believe cryptocurrencies will replace traditional currency (fiat). There’s enough room for both as each offers its own unique advantages. Instead, BitCash is designed to work alongside fiat to make everyday transactions faster, easier, and more secure.

Change takes effort. We often put off until tomorrow what we can do today, regardless of how persuasive the arguments. But as we all know, tomorrow never comes. BitCash is therefore designed to help the world move to a crypto-inclusive economy by making cryptocurrencies as easy to use as fiat.

What makes BitCash different to other cryptocurrencies?

To use most (if not all) cryptocurrencies today, you need a good amount of technical expertise. This complexity hinders mass adoption, as many people don't have the time, energy, or desire to learn how to use them.

Exchanges like Robinhood and Coinbase made it easy to buy and sell cryptocurrencies, but despite their popularity in the cryptocurrency community, they've have had little impact on mainstream adoption.

BitCash, on the other hand, is designed for mainstream adoption. BitCash is as easy to use, manage, and access as fiat money. That makes BitCash the only cryptocurrency working to deliver the benefits of decentralization on a global scale.

The PeerQ platform is easy-to-use and requires no technical experience. In order to achieve mainstream adoption it is vital that simplicity is always at the forefront.

What features does BitCash offer?

BitCash combines the convenience of the world's internet banking systems with the security, speed, and efficiency of decentralization. BitCash will be the world's first decentralized internet bank, and includes the following features and usecases:

- **PeerQ**

PeerQ is a social platform that rewards users for sharing knowledge. Users ask questions, offer bounties, provide answers, and complete tasks to earn BitCash.

- **Named accounts**

With named accounts, there is no more fiddling with messy blockchain addresses designed for geeks and crypto enthusiasts.

- **Stable currency feature**

BitCash Stable addresses the problem of price volatility when sending money to a third party, paying retailers, or storing value. BitCash Stable secures the value of BitCash for the short, medium, and long term, making it easier to integrate into the financial system.

- **Transaction references**

Buyers using BitCash can enter in a private record which is only visible to the buyer and seller - this creates stored transaction

records making it easy to see where your money went, manage your cashflow and plan for taxes.

- **Send coins via Twitter, Twitch and Instagram**

Tip anyone on Twitter, Twitch or Instagram.

- **Recurring payments**

Paying employees with crypto just became easier. Set and forget, you can now pay your staff with cryptocurrency just like you can with traditional banking software. Consumers can also now pay for their favourite subscription products using crypto.

- **Multiple accounts within one wallet**

Just like your normal online bank account, the BitCash wallet will allow users to create and label various accounts within the one wallet to help consumers and merchants organise their transactions.

- **Printable e-statements**

Your internet banking allows for easy statements, why shouldn’t your Crypto? With statements, both consumers and merchants can keep healthy records of their transactions.

- **BitCash payments to anyone**

Just like PayPal - you can send BitCash to anyone in the world, even if they don't have a BitCash address, nickname or wallet.

- **Pre-sending verification**

The BitCash wallet verifies that a BitCash address or Nickname exists before you can send to that address.

- **Stealth addresses Security**

Added security to ensure that your wallet is safe and secure.

- **One Click Mining**

Simply open your wallet and click "Start Mining" to earn BitCash. It doesn't get any easier than that.

What privacy features does BitCash have?

Stealth addresses

BitCash introduces a new kind of stealth address. Every time you send coins to a BitCash address, the coins will end up on another random stealth address. Also, every time you use the same nickname, the coins will end up on a new random receiver address.

BitCash uses the same stealth address concept as Monero. For more information, please read pages 7 and 8 of the Monero White paper.

Monero computes the destination key from the sender as follows:

$P=Hs(rA)G+B$

The receiver can compute the one-time public key as follows:

P’=Hs(aR)G+bG

The receiver can compute the one-time private key as follows:

X=Hs(aR)+b

In BitCash we additionally had a Master Public Key M and a Master Private Key m. We removed the Master Private Key with the hard fork on 23 July 2019. Since that time BitCash uses the public key from the transaction of block 1 of the Bitcoin blockchain as Dummy public key to replace the Master Public key. The assumtion is that nobody knows the private key for this public key.Also we only use one Public and Private Key for the addresses. So only A and a is used. B and b is not used.

The Master Public Key is known to the public, but m is not known by the public.

The sender calculates a shared secret through a Diffie Hellman exchange with the receiver as follows:

S=rA

The receiver can calculate the same shared secret as follows:

S=aR

This shared secret is used by the sender to encrypt the random data r with AES encryption. This encrypted version of r can later be decrypted by the receiver with the shared secret as password.

The sender computes the destination key as follows:P=Hs(rM)G+A

The receiver can compute the one-time public key as follows:

P’=Hs(rM)G+aG

The receiver can compute the one-time private key as follows:

X=Hs(rM)+a

The owner of the Master Private Key can compute the one-time public key as follows:

P’=Hs(mR)G+A

BitCash also stores 2 bytes of the real public key of the receiver in without any encryption. This enables BitCash to find potential matching transactions much faster. Before we introduced this, the stealth addresses were very slow.

The sender of a transaction can reveal r to prove that he sent the transaction and to enable any person to check decrypt the stealth address and the description line.

Addresses with viewkey

BitCash uses addresses with a viewkey for the web wallet and the mobile wallets. The web server can store the view key to recognize incoming transaction. The web server is however not able to spend any coins with only the view key.

These addresses are longer and contain two full public keys, like the Monero addresses.

V is the public viewkey and v is the private view key.

If the addresses with viewkey are used the shared secret S is calculated with the viewkey as follows:

The sender calculates a shared secret through a Diffie Hellman exchange with the receiver as follows:

$S=vA$

The receiver can calculate the same shared secret as follows:

$S=aV$

This enables the receiver who knows the viewkey private key V to decrypt the encrypted random private key r.

Then the real address can be decrypted:

$P=Hs(rM)G+A$

Non privacy addresses

BitCash also provides a special address format for non privacy transactions. These addresses are mainly intended for the exchanges. These addresses are faster to compute than the stealth addresses. If a wallet contains thousands of addresses it is preferable to use non privacy addresses.

For the non privacy address the shared secret S is calculated as usual. But it is then only used to encrypt the description line, but not to encrypt the real address.

Description line

BitCash introduces an AES-encrypted description line field for all transaction outputs.

A shared secret T is calculated and is used to encrypt and decrypt the description line with AES encryption.

The sender and receiver can calculate the shared secret as follows:

T=rM

The owner of the private master key can calculate the shared secret as follows:

T=mR

This way the description line can be decrypted by the receiver and the owner of the Private Master Key.

Stable currency feature

The BitCash Stable feature, like other stable coins, was created to address the problem of price volatility when sending cryptocurrency to a third party, paying retailers, or storing value. BitCash Dollar secures the value of BitCash for the short, medium, and long term, making it easier to integrate into the financial system. With the new BitCash stable feature, there are now two currencies stored on the blockchain, BitCash and the BitCash Dollar. One account is the BitCash account and the other is the BitCash Dollar account.

The BitCash Dollar account has its own address with “dollar@” in front of the nickname or address. So for e.g. dollar@JohnDoe would send to the BitCash Dollar account and @JohnDoe to the BitCash account. Also, there will be two send functions, one function to send from your BitCash account and one to send from your BitCash Dollar account.

BitCash → BitCash

BitCash → BitCash Dollar

BitCash Dollar → BitCash

BitCash Dollar → BitCash Dollar

BitCash Dollar = $1 USD.

when you hold your money in a BitCash Dollar account, the value will always remain the same. Keep in mind, you can send the money from one BitCash Dollar account to another BitCash Dollar account. You can also make payments in BitCash Dollars directly and there will be no price risk for the merchant.

The benefits of BitCash Stable are groundbreaking. With this feature, you can send US$1,000 to someone across the globe and they would receive it in less than a minute with minimal fees, no conversion fees on each end, no middle man, no hefty transaction fees for both parties, and no having to wait days for funds to clear.

The BitCash Stable feature makes it feasible for an online merchant who may be interested in accepting cryptocurrency as a payment because they can now accept BitCash Dollar without having to sell instantly. Instead, hold the coins in their BitCash Dollar account until they're ready to sell. This will help entice more online merchants to accept BitCash and/or BitCash Dollars.

How the stable feature works

BitCash stores 3 price pairs at the end of the block header. Each price pair needs to signed by one of 14 private keys. BitCash checks if all 3 price pairs are signed by a different of the private keys. Each of the 3 price pairs consists of one price which will be used to convert BitCash into BitCash Dollars and another price which will be used to convert BitCash Dollars into BitCash.

BitCash will then take the average of the two prices which are closed together to calculate the effective price for the block. It will calculate one effective price for the exchange from BitCash into BitCash Dollars and one for the exchange from BitCash Dollars into BitCash.

BitCash stores one additional byte with the target currency for every transaction output. At the moment two currencies are supported.

0 = BitCash and 1 = BitCash Dollar.

BitCash checks if the price is converted correctly (using the effective block price), if the transaction inputs are in another currency than the transaction output.

All transaction inputs need to have the same currency. The transaction outputs can have different currencies.

BitCash uses two fields to store the value of the transaction output. One stores the value in the currency of the transaction inputs (nValueBitCash). And one stores the value in the currency of the transaction output (nValue). nValue can change until the transaction

has been mined into a block. Therefore nValue is not included into the transaction hash.

How is BitCash mined?

Mining BitCash is simple. It's a CPU-mineable cryptocurrency, so anyone with a computer can start mining BitCash in as little as four steps:

1. Download the BitCash wallet for your operating system.
2. Install the BitCash wallet.
3. Open the BitCash wallet.
4. Click "Start Mining"

As the project develops, BitCash will release a GPU miner to allow miners to direct their GPUs to BitCash, which will strengthen and grow the BitCash network.

We'll embed the GPU miner into the BitCash wallet so that non-technical users can mine with the click of a button, without needing any batch files or code.

What Proof-of-Work algorithm does BitCash use?

Initially, BitCash utilized the Cuckoo Cycle algorithm. However, as the network grew, some individuals were able to manipulate this algorithm and gain an unfair advantage over others in the network.

As a result, on 23 February 2019 12:00 UTC, BitCash forked over to the well known and proven X16R algorithm.

X16R is a hashing algorithm, which is based on the classic X11. It uses sixteen chained hashing algorithms in an effort to thwart the move to ASIC mining

For more information on the X16R algorithm, please the x16R bitcoinwiki page.

Because there now is an ASIC miner available for X16R, we will be moving from X16R to X16RV2 soon.

We are adding the algorithm Tiger into three seperate parts of the current X16R algo. The Tiger hash is performed before the algorithms Luffa512, Keccak512, and SHA512.

How does BitCash handle difficulty retargeting?

BitCash uses a new algorithm for difficulty retargeting called Virtual Timespan Retargeting (VTR).

For Bitcoin and other cryptocurrencies, difficulty retargeting happens after a fixed number of blocks (2,016 for Bitcoin). To set the new difficulty, Bitcoin compares the time it took to mine these blocks with the target time (2,016 blocks x 10 minutes). Since the difficulty stays the same for all 2,016 blocks, the time between these blocks can be compared easily.

However, the BitCash VTR algorithm examines the time it took to mine the last 24 blocks and changes the difficulty after *every* block. The problem with retargeting after every block is that the difficulty constantly changes, so it's not enough to simply compare the time it took the mine these 24 blocks with the target time (24 blocks x 1 minute).

Other cryptocurrencies have invented algorithms like DarkGravityWave (Dash) and Kimoto Gravity Well to try to solve this problem, but they still don't calculate the correct difficulty. If a single miner mines 20 blocks, the difficulty is too low, but the algorithm will then try to compensate by making the difficulty too high, delaying discovery of the next block. The difficulty can fluctuate for some time.

BitCash's VTR algorithm offers a simple solution to this problem.

First, we take the time it took to find the next block for every of the 24 previous blocks, and then adjust that time to the difficulty of the latest block. This means multiplying the timespan between two blocks by the latest difficulty, and then dividing it by the difficulty of the block in question.

Then we add the times of all 24 blocks together to create a "virtual timespan". This is an estimate of how long it would have taken to mine these 24 blocks if all had the same difficulty as the last block.

Now we can compare these virtual timespans with the target timespan (24 x 1 minute) to calculate the new difficulty.

This algorithm will adjust the difficulty within a short number of blocks to the right difficulty without overcompensating in either direction. We could even adjust it for large changes in mining power (by a factor of 10) within 5 to 10 blocks.

How is the BitCash team funded to grow and promote BitCash?

The BitCash project has no physical offices or any employees. The network is coded, designed, and run by volunteers from all around the globe, and anyone is welcome to contribute. No ICO or fundraiser of any kind ever took place. All code is given away and published as open source.

BitCash was launched with a 9.7% premine and has an ongoing 10% block reward.

PeerQ is a very strong asset for the BitCash project, as it is a seamless entry point into BitCash and can help facilitate mass adoption. With that being said, the block reward is used to redistribute BitCash into PeerQ bounties to allow for those who do not mine or trade a fair way to gain access to BitCash.

The remaining BitCash from the block rewards is used to fund our discord bots. This allows for us to reward our community members for being active on our community platforms.

Why are the premine and ongoing block reward important?

The premine and block reward recognize the BitCash team's hard work and incentivize them to keep making BitCash the best it can be. The team worked tirelessly on developing BitCash for over a year before the official release date, and they plan to continue developing BitCash long into the future.

It is also vital that the block reward remains so we can create unique entry points into crypto and BitCash (PeerQ).

What makes the BitCash team uniquely qualified to deliver on the promises described in this White Paper?

The BitCash team comprises the best talent from cryptocurrency, blockchain, and other technology industries. Together, we have over 50 years of software development, web development, SaaS (Software as a Service), ecosystem building, and marketing experience.

We know how to build incredibly easy-to-use software and then put it in the hands of millions of end users, as well as how to build and maintain a global brand. Our expertise and experience place BitCash far ahead of other cryptocurrencies in our mission to create the most useable cryptocurrency on the planet.

While we've decided to remain anonymous, we plan on pricing our skillset and experience through our product, as well as the community we build and nurture on our way to becoming the well-known brand that helped cryptocurrencies go mainstream.

We hope you'll join us on this incredible journey.

How can you get involved with BitCash?

Below are just some of the ways you can get involved in BitCash:

1. Mine BitCash using your computer
2. Sign up to PeerQ and post questions and/or answers
3. Trade BitCash on exchanges
4. Join the various BitCash social media groups
5. Reach out to the BitCash team to ask how you can help grow the community
6. Spread the word
7. Write and post useful articles and blogs about BitCash
8. Share your ideas with the BitCash team
9. Keep a lookout for ongoing bounties on PeerQ

Additional Information about BitCash

Total supply: 100,000,000 Coins (before release of stable feature)

Coin symbol: BITC

Coin Units:

1	BitCent = 0.00000001 BITC
10	BitCent = 0.0000001 BITC
100	BitCent = 0.000001 BITC
1000	BitCent = 0.00001 BITC
10000	BitCent = 0.0001 BITC
100000	BitCent = 0.001 BITC
1000000	BitCent = 0.01 BITC
10000000	BitCent = 0.1 BITC
1	BitCash = 1 BITC

Hash algorithm: x16R (Proof-Of-Work) changing over to X16RV2

Block time: 60 seconds

Join the discussion & community…

Website: https://www.choosebitcash.com/

https://www.peerq.com

Twitter: https://twitter.com/ChooseBitCash

Discord: https://discord.gg/7P4YcXU

Telegram: t.me/chooseBitCash

Medium: https://medium.com/@BitCash

GitHub: https://github.com/WillyTheCat/BitCash

Bitcointalk: https://bitcointalk.org/index.php?topic=5106123.0

Explorer: http://explorer.choosebitcash.com

Exchanges: https://www.choosebitcash.com/exchanges.html

Mining Pools & Miners:
https://www.choosebitcash.com/poolmining.html

Mac Wallet:
https://wallet.choosebitcash.com/downloads/bitcash.dmg

Windows Wallet:
https://wallet.choosebitcash.com/downloads/bitcash-setup.exe