BitCash

BitCash Whitepaper

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.

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) Accessibility
c) Simplicity
d) Mass adoption
e) Acceptance by world's governments

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.

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.

Reputation for criminal activity

Digital currencies like Bitcoin and Monero are infamous for their use in illegal activities, especially on the Dark Web. It is not uncommon to hear of cryptocurrencies being used to launder money or purchase illicit items.

While privacy is one of cryptocurrencies’ many benefits, total anonymity encourages the use of privacy coins for illegal activities. Attempts to grant anonymity without risking criminal misuse have, so far, failed.

Push back by governments and legislators

Cryptocurrencies have an image problem.

Since cryptocurrencies make it easy for people to hide money or conduct illegal activities, governments and legislators are reluctant to accept them into their societies. In some countries, they want to ban or discourage the use of cryptocurrencies altogether.

Nevertheless, cryptocurrencies aren't responsible for criminal behavior, and with the right security mechanism, might even reduce crime by leaving an indelible transaction history underwritten by the blockchain.

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, manage, and use cryptocurrency.
2. By giving businesses the banking tools they need to accept cryptocurrency payments.
3. By assuring users' privacy while still deterring criminals.

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.

We believe that privacy is a basic human right. However, we don't believe in enabling illegal activity via cryptocurrency. This is why BitCash is private to the general public, but open to world governments and law enforcement when necessary.

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.

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 will include the following features:

- Named accounts
- Transaction references
- Record-keeping
- Recurring payments
- BitCash Master-Key
- Multiple accounts within one wallet
- Printable e-statements
- BitCash payments to anyone

- Pre-sending verification
- Privacy
- Security
- Importable transactions
- Accounting software support

Is BitCash a privacy coin?

Yes and no. Your day-to-day transactions and wallet balance are **completely private and anonymous**. However, law enforcement agencies can request a BitCash "Private Master Key" to view transactions made using a particular BitCash wallet. This is similar to internet banking whereby it is completely private, but if absolutely necessary, law enforcement agencies are allowed access to deter bad actors and criminals.

How does BitCash offer privacy but remain government compliant?

Today's privacy cryptocurrencies are doing more for criminals than law-abiding people. Not only do criminals have a glut of black markets eager to use their ill-gotten cryptocurrency, but they tarnish the reputation of an otherwise legitimate and world-changing technology.

The right to privacy is generally accepted across the world, but when exploited by ill-meaning individuals or organizations, it puts the welfare of everyone at risk. With few alternatives, governments and exchanges are increasingly forced to ban privacy coins altogether.

BitCash is therefore the world's first decentralized privacy coin to work with the law, not against it. Through a newly-invented technology, BitCash grants the right to privacy while still being able to reveal the evidence law enforcement needs to prosecute criminals (should they request it). The same applies to your bank account.

With BitCash, your day-to-day transactions and wallet balance are completely private and anonymous, however law enforcement agencies can request and receive a BitCash "Private Master Key" to view transactions made using BitCash.

This deters bad actors and criminals while still providing you with the privacy you need. We believe it's the best of both worlds and will enable mass adoption of cryptocurrency.

Although we can't predict specifically how law enforcement will work with us, we have nevertheless enabled the technology for them to do so. While we have some ideas of how to enable an open dialogue and transparency, we are open to exploring ideas and initiatives that foster what we call "Safe Privacy".

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. BitCash adapts this concept so the real receiver address can be calculated and description lines decrypted by anybody who knows the Private Master Key.

The Private Master Key will remain a secret known only to the developers of BitCash. But if needed to fight illegal activities, the BitCash team will provide authorities with access to a special password-protected blockchain explorer which uses the Private Master Key to show the real receivers of a transaction.

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 have a Master Public Key M and a Master Private Key m.

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.

BitCash computes the destination key from the sender 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

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.

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?

BitCash uses the Cuckoo Cycle algorithm.

Cuckoo Cycle is a new graph-theoretic proof-of-work design that's cost effective, energy-efficient, and can be run on slower computers.

It's the first proof-of-work algorithm that can scale memory with instant verifiability, and where memory latency dominates the runtime.

Barring any memory-time trade-offs, this makes Cuckoo Cycle a near ideal memory-bound proof-of-work algorithm. It could also greatly benefit the decentralization of mining by allowing more miners to take part.

BitCash uses a fixed value for the graph size of 2^{27} (27 edgebits).

For more information, please read the Cuckoo Cycle White paper.

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?

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

Both the premine and block reward go to the BitCash team fund, which we'll use to hire more developers, list on large, reputable exchanges, and on marketing, joint ventures, and partnerships.

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.

Most importantly, the block reward gives the team a fund for attracting the best talent in the industry. The more valuable BitCash becomes, the more the team can do with the rewards.

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.

What is on the development roadmap for BitCash?

Q3 2018

- ✓ Launch the BitCash network and make it available to the public

- ✓ Create the blockchain explorer
- ✓ Create the BitCash wallet for Windows and Mac
- ✓ Integrate reference-line and record-keeping functionality into the BitCash wallet
- ✓ Allow users to create accounts with nicknames to send and/or receive coins (nicknames replace wallet address)
- ✓ Allow users to send BitCash to anyone, even if they don't have a BitCash wallet
- ✓ Create the Paper Wallet
- ✓ Create the BitCash Private Master-Key
- ✓ Launch the new website
- ✓ Implement the difficulty retargeting algorithm
- ✓ Add the verify-before-sending feature
- Create GPU Miner
- Integrate the GPU miner into the BitCash wallet
- Announce BitCash on Bitcointalk

Q4 2018

- Establish a reliable mining pool
- Launch Light Wallet
- Build our own exchange to support community trades
- Allow users to create various accounts in one BitCash wallet
- Allow users to print statements from their BitCash wallet
- Integrate recurring payments within the BitCash wallet
- Integrate BitCash in 1000s of online stores

Q1 2019

- List BitCash on major exchanges
- Release a mobile wallet for Android with all BitCash features
- Release a mobile wallet for iOS with all BitCash features
- Market BitCash to the world (press releases, influencers, Youtubers…)

Q2 2019

- Build support for various accounting software (XERO / Intuit)
- Build partnerships with ecommerce platforms (Magento, BigCommerce, Shopify)
- Build partnerships with banks and/or accounting software firms

How can you get involved in BitCash?

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

1. Mine BitCash using your computer
2. Buy and sell BitCash
3. Join the various BitCash social media groups
4. Reach out to the BitCash team to ask how you can help grow the community
5. Spread the word
6. Write and post useful articles and blogs about BitCash
7. Share your ideas with the BitCash team

Additional Information about BitCash

Supply and emission

Total supply: 100,000,000 Coins

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: Cuckoo Cycle (Proof-Of-Work)

Block time: 60 seconds

Join the discussion & community…

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

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

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

Bitcointalk = *tba*

Reddit = *tba*