BYTECHCOIN

WHITEPAPER

CONTENTS

ABSTRACT

BytechCoin was created on January 1, 2019 by BytechCoin Developer Team.

BytechCoin is a global, open-sourced, blockchain-based, decentralized payment gateway and processing platform that anyone can use. BytechCoin ecosystem is open, so anyone can participate by maintaining the BytechCoin blockchain and implementing network services.

BytechCoin is based on the foundation of Cryptonote technology and forked from TurtleCoin.

The Cryptonote technology base allows users to transact with BytechCoin anywhere in the world with low network fees and speed without compromising on privacy. We chose this algorithm and base due to its stability and its ability to add future features, also to allow miners to be rewarded for assisting in maintaining a healthy and secure network with PoW (Proof Of Work).

CRYPTONOTE TECHNOLOGY

The CryptoNote technology has a similarly mysterious origin as Bitcoin. Initially emerging in 2012 and published on Tor, the author of the original whitepaper used a pseudonym Nicolas Van Saberhagen. The identity of the author is still unknown following the publication of a second version of the whitepaper under the same pseudonym less than a year later.

The original paper addresses the flexibility and privacy deficiencies with Bitcoin, particularly emphasizing traceability and linkability of transactions as well as enforcing Bitcoin's "one-CPU-one-vote" principle originally proposed by Satoshi Nakamoto. Referencing "we" in the paper, they present a new suite of advanced features for decentralized cryptocurrency networks predicated on mathematical analysis dubbed the CryptoNote Technology.

The CryptoNote Technology is built on the foundation of providing two fundamental properties that are needed to achieve full anonymity in a payment network:

- Untraceability
- Unlinkability

Untraceability refers to for all incoming transactions, all possible senders are equiprobable as the origin.

Unlinkability refers to the notion that it is impossible to prove that any two outgoing transactions were sent to the same person.

The original proposal has since been supplemented with several optimizations and improvements to keep the technology at the cutting-edge of innovation while still holding true to its original principles. A list of standards is maintained on the CryptoNote website as the specifications of the protocol. Currently, the primary features of the CryptoNote Reference Implementation focus on:

- Untraceable Payments
- Blockchain Analysis Resistance
- Unlinkable Transactions
- Egalitarian Proof of Work
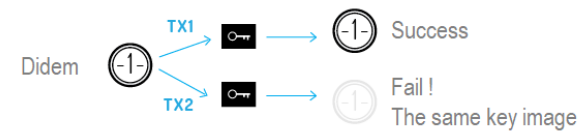- Double-Spending Proof
- Adaptive Parameters

CryptoNote achieves *untraceable payments* through its integration of ring signatures. Ring signatures are based on a group signature concept originally proposed by David Chaum and E. van Heyst that later evolved to the "Traceable Ring Signature" paper, which CryptoNote ring signatures are based on. Ring signatures use multiple public keys mixed together to muddle the true signer of a transaction without sacrificing the ability to verify that the transaction is valid. A further development of Ring Confidential Transactions (Ring CTs) is implemented in several CryptoNote cryptocurrencies today as an improvement on the original traceable ring signatures.


Ring Signature

Unlinkable transactions in CryptoNote are accomplished through the use of one-time keys. Even with a ring signature, all of the incoming transactions to a public key address can be observed on a blockchain. CryptoNote mitigates this by automatically generating one-time keys derived from the public key of the recipient for each transaction. By using an optimized version of the Diffie-Hellman Key Exchange — which allows for a cryptographically secure shared secret between two interacting parties –, the sender of a transaction hashes the recipient's public key with their own data to create a unique one-time key for that transaction. As a result, only the receiver can generate the private component of the transaction, thus being the only party that can release the funds once the transaction is committed.

Accomplishing a *double-spend proof* when the goal is to obfuscate transaction data comes with some clear challenges. CryptoNote cleverly employs a concept known as key images to ensure there are no double-spends even in an opaque blockchain ledger. Key images are unique markers designed to support linkability while allowing a signer to remain anonymous. For instance, if Didem creates more than one ring signature using the same private key, then this will indicate a double-spending attempt. To be able to identify this without revealing Didem's identity, a key image is generated when signing a transaction and subsequently retained by all users in the network. It is impossible to link a transaction to a public key and identify the signer of the transfer. Further, any transaction with a duplicate key image that is submitted is rejected outright by the network.

Double-spend proof (check)

Blockchain analysis has arisen as an interesting topic for research and innovation with some companies emerging for analyzing on-chain patterns. Developments at both the blockchain layer and network layer of cryptocurrencies have revealed methods to deanonymize users in a pseudonymous network like Bitcoin. Due to each transaction in CryptoNote having a unique one-time key, linking inputs and outputs through public addresses is not possible.
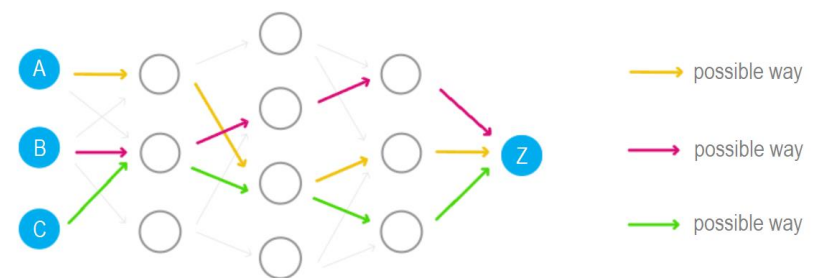
Blockchain analysis ambiguity

The focus on an *egalitarian proof of work* in the CryptoNote reference implementation stems from the centralization risk of Bitcoin with the development of powerful ASIC mining chips. At the time of the original CryptoNote paper, CPU mining in Bitcoin was

technically still feasible but was quickly becoming irrelevant due to the onset of specialized mining hardware. Especially considering the recently released Bitmain IPO prospectus that states Bitmain controls 37.1 percent of Bitcoin's mining hash power, CryptoNote's forward-thinking approach to ASIC dominance is largely corroborated in that 51 percent attacks may eventually be feasible, however unlikely.

Centralization of mining also permeates into off-chain governance decisions where it becomes even more complicated of a topic. Consolidation of mining power creates slower network upgrades but can also be a net positive considering Bitcoin's conservative approach to development. CryptoNote identifies that Bitcoin's SHA-256 mining algorithm does not sufficiently mediate the advantage that high-cost custom devices (like ASICs) have over standard CPUs. CryptoNote refers to the Pareto principle (valid at the time in the context of Bitcoin), where 20 percent of the system's participants control more than %80 of the votes, as the reason for promoting a memory-bound algorithm for the proof of work pricing function to distribute mining power.

The CryptoNight mining algorithm eventually implemented in Bytecoin and subsequently optimized for Monero is an excellent example of such an algorithm. CryptoNight effectively resists ASIC mining and only allows for CPU and GPU mining. However, with constant advances in mining chip hardware, remaining ASIC-resistant is difficult and required Monero to fork its protocol to maintain its status quo recently.

An interesting component of CryptoNote is the emphasis placed on adaptive parameters, also called adaptive limits. Hard limits refer to hardcoded parameters in a decentralized cryptocurrency network's protocol, such as block size and block difficulty. These limits can lead to polarizing dilemmas such as Bitcoin's block size debate and the eventual Bitcoin Cash hard fork. CryptoNote tackles hardcoded limits by setting automatically adjusting parameters for each block based on certain conditions.

Overall, the suite of features available in the CryptoNote Technology is built on some incredibly complex and innovative mathematical analysis. As an open-source protocol, CryptoNote is designed to provide the framework for a competitive environment of decentralized and privacy-oriented cryptocurrencies.

REASONS TO USE PAYMENTS WITH CRYPTOCURRENCY ON YOUR BUSINESS

Some controversy and challenges surround the use of cryptocurrency, but many business owners are embracing cryptocurrencies such as Bitcoin for transactions. One reason is that using the latest technology is a great way to stand apart from other businesses in the marketplace.

Not sure what cryptocurrency is? Cryptocurrency is simply a digital currency that relies on encryption technology to transfer the value via the internet. This form of currency operates independently of a banking system and can be used in many countries like cash. The most common use of cryptocurrency is selling and buying goods or services online.

Cryptocurrency is another way businesses can accept payments from customers or pay vendors. Wondering if accepting cryptocurrencies is the right fit for your business? The answer depends on your business's needs, but typically, cryptocurrencies are advantageous for various reasons. Take a look at these reasons accepting cryptocurrencies can help your business grow and succeed.

It will save you Money

Over the years, U.S. merchants have paid over $78 billion in fees related to credit and debit card processing. Cryptocurrencies are decentralized, so they do not require a bank to verify every transaction. This means your business will eliminate those fees, saving 2 to 5 percent on each transaction. This is also the case with companies like PayPal and Stripe. No more sharing your hard-earned revenue with financial institutions.

One important thing to note is that many merchant wallets charge a flat fee of around $30. There are decisions all entrepreneurs will face, and usually those revolve around whether you're ready and willing to embrace change and the learning curve that comes with it.

Transactions will process quickly

It's frustrating to wait for funds to become available in your bank account. You don't have to wait with cryptocurrency transactions. In many cases, the transactions occur in real time or within a few minutes. There aren't various banks slowing down the payment process. High transaction speeds are a bonus; in today's world of instant gratification, no one likes to wait.

The currency works worldwide

There are a lot of benefits to an international currency, and it's especially helpful if your business exports services and goods or purchases materials from other countries. Cryptocurrencies help you avoid the expensive foreign transaction fees or exchange rates.

You will avoid fraud and chargebacks

Cryptocurrency is comparable to cash in that you either have the funds available or you don't. You should also know that all transactions are final when you use cryptocurrencies, because transactions are added to the blockchain via mining.

This system verifies funds and makes it next to impossible to spend more than you own. When paying with cryptocurrencies, both parties have to approve each transaction. As a result, there are no disputes to worry about and chargebacks will no longer happen.

You can acquire new customers

Cryptocurrencies have some major followers – more and more people are learning about it, embracing it and learn about investment solutions. As your customers become familiar with and

begin to use cryptocurrencies, it will really help your business if you accept digital currencies.

While this may still be a niche market, it won't be for much longer. The more payment options you offer your customers, the better. Not only will you attract a wider customer base and more shoppers, you'll also increase the chances that they all follow through with their intended purchases. According to a survey by Skrill, 28 percent of shopping cart abandonment is due to lack of the payment option the shopper wanted to use. Do what you can to shrink your shopping card abandonment rate so you can increase your revenue

Paper options will slowly become a thing of the past

Digital wallets and cryptocurrencies are growing steadily with the blockchain. This trend continued through 2017 and is anticipated to continue to grow as people become more familiar with digital currency.

While it may seem overwhelming for a small business, try to embrace this change. It makes a lot of sense for you and your business to become early adopters of cryptocurrencies so you can become familiar with it sooner than later. If you resist the change now, you'll just delay the inevitable. Set yourself apart from your competitors by welcoming fintech.

WHAT IS BYTECHCOIN?

BytechCoin was launched on January 1, 2019 and it is derived from four other open source projects; CryptoNote, Monero, Bytecoin and Turtlecoin.

BytechCoin is a global, open-sourced, blockchain-based, decentralized payment gateway and processing platform that anyone can use.

Features and Specifications

OWN BLOCKCHAIN
BytechCoin has a private blockchain, nobody sees your money except you.
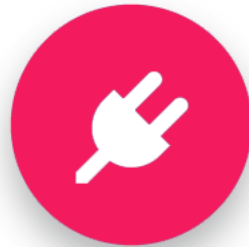
FAST TRANSACTIONS
BytechCoin is creating blocks every 120 seconds, as opposed to every 10 minutes. Your money travels 5x faster than on Bitcoin or BitcoinCash.

PRIVACY

BytechCoin has the same privacy features you'll find in Monero, Aeon and Turtlecoin. Every transaction is private, by default.

EASY TO USE

We support almost every OS, you can make a secured paper-wallet for free, and get started with BytechCoin in under 5 minutes.

EASY TO MINE

BytechCoin comes with its own basic CPU miner, but you can also use any Monero mining software you're used to if you'd rather use GPU's or mining pools.
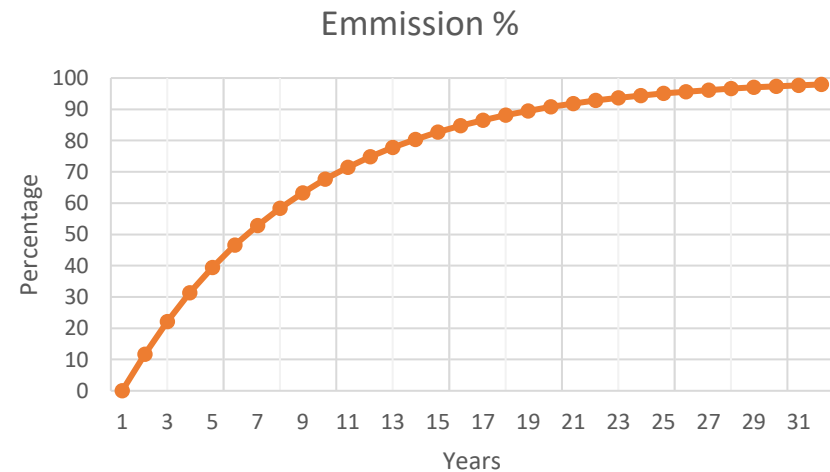
COMMUNITY

BytechCoin community is very welcoming to all users and developers. Please join us in our Discord Chat.

BytechCoin Technical Specs

Ticker	BYTC
Max Supply	1.000.000.000.000
Decimals	2
Block Time	120 seconds
Algorithm	CN Lite V1
Premine	0

BytechCoin Emission

Emmission %

BytechCoin Mining

BytechCoin uses Cryptonight Lite v1 algorithm and anyone can mine BytechCoin with its own basic CPU miner or you can mine with Monero's XMR mining softwares (CPU/GPU) on our **Official Pool**.

Roadmap

Q1 – 2019

– Paper Wallet
– GUI Wallets
– Official Pool
– Expand Our Community

Q2 – 2019

– First Exchange Listing
– Web Wallet
– New Developers to Join Our Team
– Setting up New Releases

Q3 – 2019

– More Exchanges
– Android App
– iOS App
– Setting up new releases

Q4 – 2019

Next Year Plannings

– Setting up New Updates of all apps for next year.

BytechPAY

Contactless has become a typical way of transacting but there are lots of concerns about security and privacy. The purpose of BytechPay is to ensure that users' data is kept private and their transactions remain secure during contactless transactions.

Smartphones occupy an important place in our lives and BytechPAY will be an application that can be install on to their phones. Users will be able to use BytechPAY on smartphones to make payments with ease but maintaining the aspect of privacy and security.

People that have no access to smartphones can also pay and get paid using the QR code feature to interact with BytechPAY users.

Payment terminals will be modified to allow the use of BytechCoin. BytechCoin is easily obtained by establishing relationships with large businesses to ensure that it is accepted as a payment method.
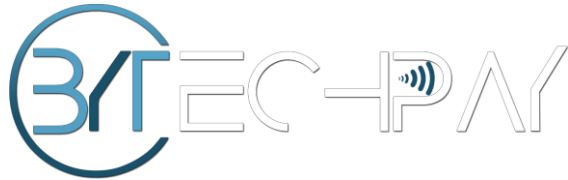
BYTECHCOIN COMMUNITY

Social /Community

Website	Github	Twitter	Discord
Facebook	Telegram	Linkedin	Instagram

SOURCE

1 "What is CryptoNote Technology?"
https://blockonomi.com/cryptonote-technology/
https://cryptonote.org/inside
2 "6 Reasons Your Business Should Accept Cryptocurrency"
https://www.business.com/articles/6-reasons-to-accept-cryptocurrency/
3 BytechCoin
http://www.bytechcoin.com