



Cryptocurrency Whitepaper



GoByte Core Team

Hisyam

Muhammad Nabil . Mathieu Arbez . Antonio Moratti . Mohd Abdul Syafiq . Akif Rabbani

Advisers

Jarrad Williams . Brad Nickel . Logan Kugler . Massoud Gheysari

www.gobyte.network
www.github.com/gobytecoin/gobyte
www.twitter.com/gobytenetwork
[T.me/@gobytenetwork](https://t.me/@gobytenetwork)



This whitepaper is a living document and is improved and edited on a regular basis. The strategies and ideas you will read about will continue to be added to, revised, and improved as we move the project forward.

This whitepaper is divided in two parts ; the first is introducing GoByte as it currently is and as it will be. The second part is presenting the open source technologies we use as the core of GoByte and what we are doing to improve upon them to realize our vision.

Milestones	6
The GoByte Network	
Overview	8
Credits	10
What is GoByte?	11
- GoByte Pay	14
- Core features	15
- Future modules	22
- Miners, Masternodes, earning more GBX	22
- Anonymity	25
- Maximum supply	26
- Exchange and trading	27
- Roadmap	28
- Team	29
- Advisers	33
- Side team	35
- Strategy	38
- Target markets	41
- Distribution	46
- Strategy conclusion	53

Technical background

What is cryptocurrency?	56
- Different types of cryptocurrencies	58
- Main bottlenecks to Bitcoin	59
- Masternodes Network	68
GoByte Premine	85
Additional improvements	86
Security analysis	96
References	100

Milestones

16th Nov 2017	Genesis block mined
18th Nov 2017	First GoByte masternodes auction
19th Nov 2017	Second GoByte masternodes auction
19th Nov 2017	CoinsMarkets Listing
19th Nov 2017	Mnrank.com Listing
21st Nov 2017	Masternode.online Listing
21st Nov 2017	Masternodes.pro Listing
25th Nov 2017	Cryptopia Listing
04th Dec 2017	CoinExchange Listing
14th Mar 2018	Whitepaper Release
30th Mar 2018	GoBytePay Release
30th Mar 2018	HitBTC Listing
TBA	GoByte Core Soft Fork
TBA	Segregated Witness
TBA	Atomic Swaps
TBA	Quantum Resistance

The GoByte Network

Overview

Satoshi Nakamoto dreamed of creating a cryptocurrency that could replace our current financial system that has time and again caused suffering around the world. The idea was to create a platform of payments that was seamless, instant, secure, and powerful enough to free the poorest in the world from the oppression of fiat currencies by empowering them to break the cycle of financial dependency of banks. Nakamoto launched Bitcoin to the world in 2009, but 9 years later, the dream has still not been fully realized.

Cryptocurrencies are experiencing an amazing level of awareness growth when it comes to trading on exchanges, but the dream of a system of payments that was the foundations of the crypto revolution has not been achieved. While some spot locations around the world are using bitcoin and alternative cryptocurrencies for payments, the levels of adoption are so minuscule as to be statistically insignificant.

Our mission at GoByte is to fulfill the vision that cryptocurrencies were meant to usher in by creating a smart, powerful, and easy to use payment system that can be accessed and used by anyone on the planet. GoByte is the future of payments and will be the realization of the cryptocurrency revolution.

In November of 2017 a group of young developers from around the world got together virtually to create their own cryptocurrency. They took an existing currency called Dash with its foundations in Bitcoin and created a new coin and network called GoByte with the goal of changing how money transacts in the world. Now that the coin is launched, and the team has launched the GoByte Pay merchant payment system, the next step is to further advance the technology of the system making it easier and easier for consumers and merchants to use it on a daily basis. This will be achieved by launching a concerted business development and marketing strategy to get the product into the hands of merchants and consumers worldwide.

This document while extensively covering the technology upon which GoByte is based, will cover the plans for the product of GoByte as well as the plans for penetrating the market and getting GoByte to be an accepted form of payment with merchants and consumers worldwide. We understand the realities of the marketplace and the forces aligned against success, but we are determined to create a strategy that will result in adoption and user levels never before accomplished in the world of cryptocurrency.

The first part of this document details our strategy for market penetration for the GoByte currency and the GoByte Pay system. The second half of the document is a technical deep dive into the tech behind the network based upon its origins in Dash.

The purpose of this white paper is to introduce you to our products, our vision, and our strategy for dominating the world of payments. We welcome your thoughts and feedback and we invite you to join our community.

Thank You

Bitcoin, Dash, and the cryptocurrency world

Dear Reader,

Thank you for joining us on this journey towards a better financial system for the world. We want to start this document with the acknowledgement of our indebtedness to another cryptocurrency platform and the world of cryptocurrencies in general.

Without the initiative of Satoshi Nakamoto and the team that made Bitcoin real and their continued work to build upon that vision, GoByte and the currencies that came before it would not exist. We recognize the power of the original Bitcoin creation and we honor the spirit of open source and the financial revolution it embodies, by taking what exists and striving to make it better.

It is important for a reader of this white paper to understand the origins of the GoByte currency and the origins of much of the technical content of this white paper. GoByte is a hard fork of the Dash cryptocurrency and network. That means we took an existing open source licensed project and created a copy of it and then over time have been writing our own code to make the project what we envision GoByte needs to become to be the default method of payment in the world.

We must though, acknowledge our gratitude to the Dash team for the high-quality platform they built that has allowed us to launch and build the GoByte network. Without their tireless work and dedication to creating a powerful base upon which to build our vision, GoByte would have been much more difficult to accomplish.

We want to thank and recognize the Dash team for their work. While we are pursuing a different path technically and strategically, it is in the spirit of Open Source, that we share our code just as Dash shared theirs. All of us collectively in the cryptocurrency community are working toward a better future for the planet.

Thank you,
The GoByte Team

What is GoByte?

GoByte is an innovative, easy to use, and low fee cryptocurrency and digital payment system. It has everything a consumer needs to use digital currencies and everything a merchant needs to accept them.

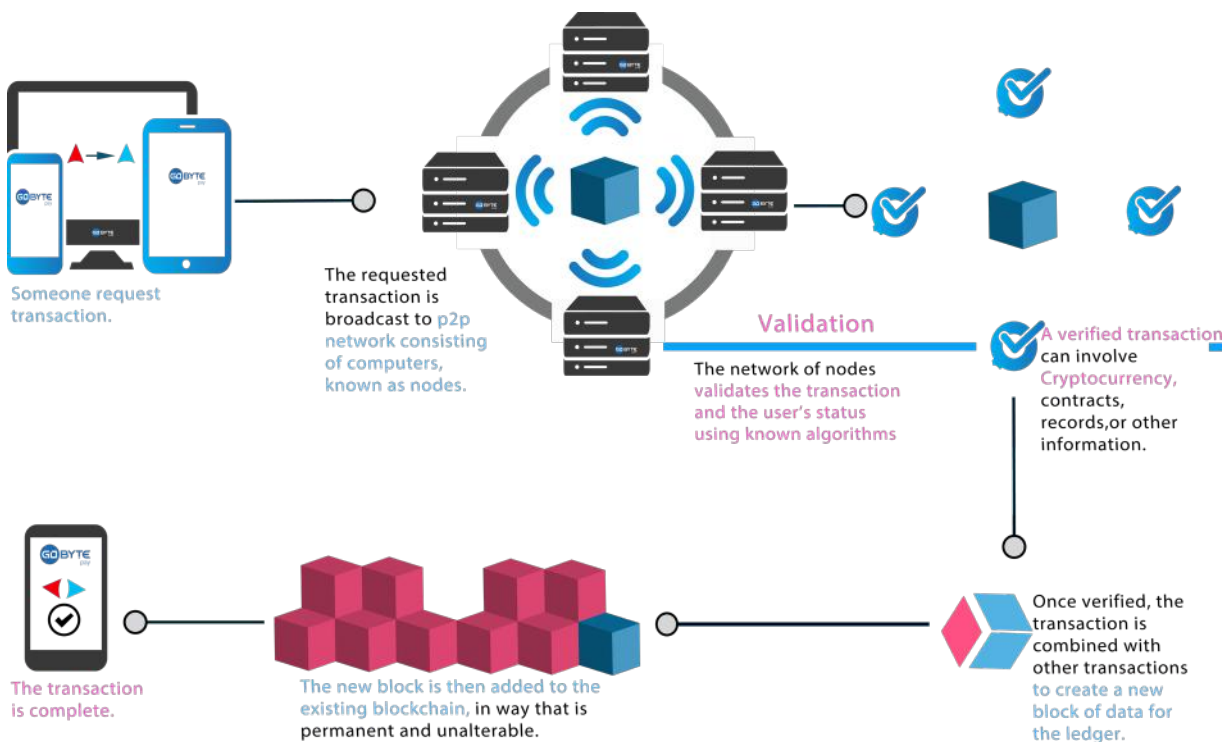
If you are new to cryptocurrencies, we encourage you to use the resource list at the end of this document to learn more about how they work and can be used.

GoByte was born in November of 2017. It is a fork or copy of an existing cryptocurrency system called Dash. It is tested, secure, and powerful and has one of the fastest payment processing engines available.

It also has the ability to be anonymous if a user chooses to use that functionality.

GoByte can be used on ecommerce websites and in stores. The GoByte Pay module makes it easy for merchants to process payments from consumers in their store. A simple scan of a barcode and a transaction can be completed quickly and securely.

A modular network



Cryptocurrency

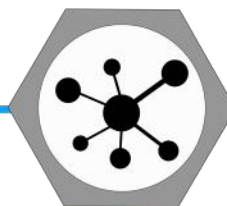
Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best know example.



Has no intrinsic value in that it is not redeemable for another commodity such as gold.



Has no physical form and exists only in the network.



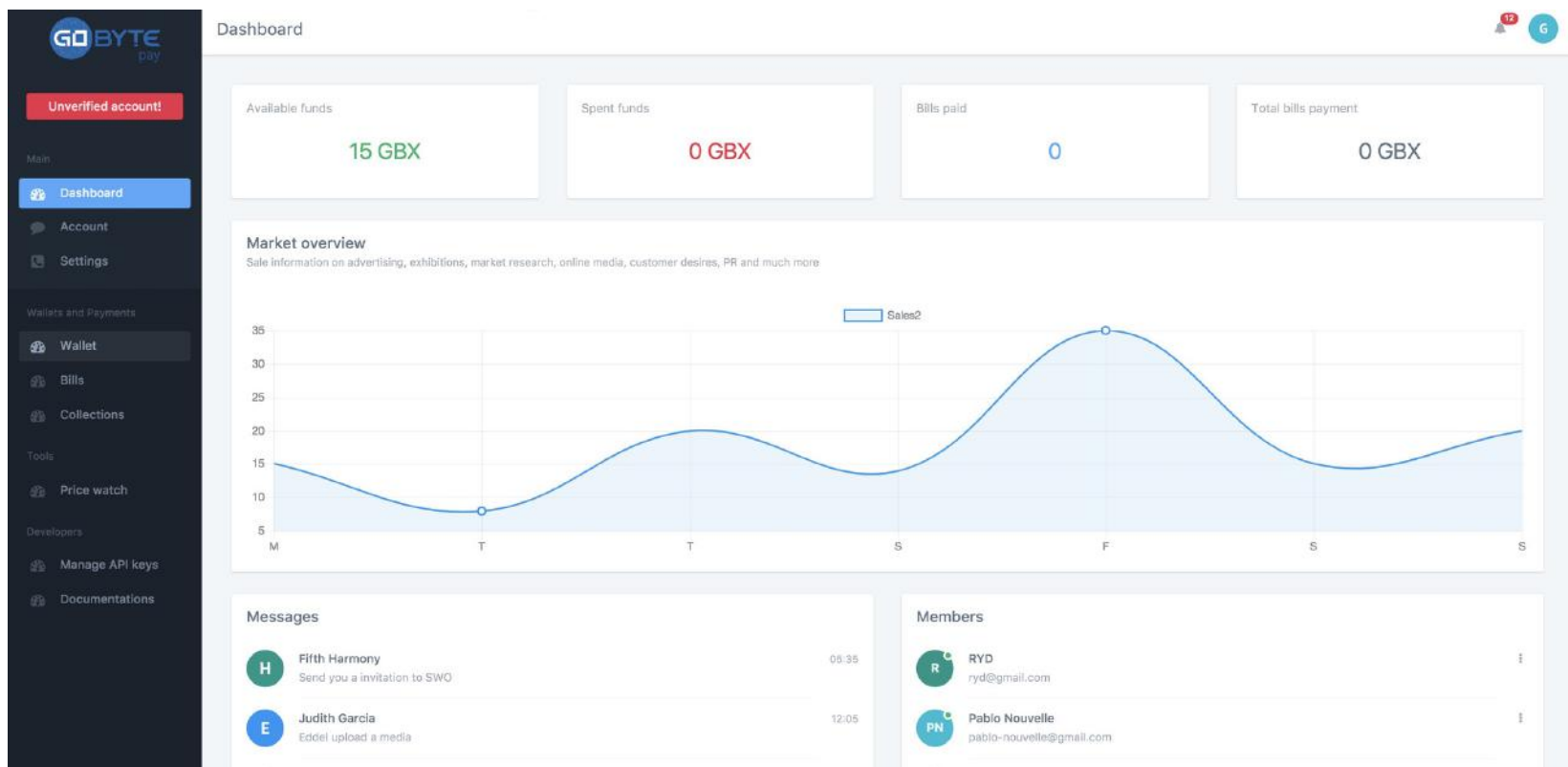
Its supply is not determined by a central bank and the network is completely decentralized.

The GoByte Network is a modular network based on a powerful blockchain technology. GoByte's modules are developed independently from the primary blockchain and work together to create a fast and secure network. The modular structure of the GoByte Network means that modules can be updated independently without causing errors or conflicts with other modules.

GoByte's developers are working tirelessly to create new and innovative modules to provide powerful new functionality for consumers, merchants, and developers. Every module is developed by an independent team lead by a senior developer. The modular design of the network gives developers a clean canvas upon which to build while they can make use of the powerful functionality of the network.

A "module" is a part of the GoByte Network created for a specific purpose and functionality. It assists the main network by reducing expansion to different domains of activity. This allows GoByte to have many functional capabilities and doesn't limit it to one central purpose. Where other cryptocurrencies focus on a specific capability like anonymity, transaction speed, or a vertical application, GoByte's modularity has no limitations. The GoByte network is growing at a very rapid pace adding up to 8 masternodes per day and assuring the security and anonymity of the chain. Thanks to the modularity of the system, the GoByte Network can maintain this growth rate for a very long time, which allows the development team to enable new technologies and capabilities and ensure the longevity of the platform.

GoByte Pay



What would a currency be if it couldn't be used to buy and sell things? While many cryptocurrencies are used to buy and sell things today, the process is difficult and often counterintuitive and wrapped in an unprofessional interface. GoByte Pay takes cryptocurrency payments to another level with a powerful and easy to use interface designed for technically challenged merchants and consumers on desktop, web, and mobile.

GoByte Pay is the first and most critical module of the GoByte Network. The GoByte Pay module interacts directly with the blockchain, allowing it to create and execute transactions which will later be confirmed by masternodes and miners. GoByte Pay is designed as the central pillar of the network. The GoByte Pay module is required to be fast, secure and easy to use and the development team dedicated to the module is determined to always improve it with every iteration.

Core features

- Send and receive GoByte (GBX) within seconds
- Built with payment gateway and web wallet integration so that a merchant can account for all of their transactions both on the web, in apps, and in stores
- Allows user to have multiple wallets in one account
- Will supports multiple currencies in a single account
- Supports 2 Factor Authentication(2FA) for logins, transactions and withdrawals to help users secure their coins
- Easy to use with professional interface
- Notifications with each payment and transfers
- Fund transfers within GoByte Pay network are free
- Mastercard third party issuer integration (TBA)

Although the GoByte Pay module was announced in Q1 of 2018, the development actually started at the same time as the main blockchain. In the first private tests of the GoByte Pay module it managed to create a billing address and receive and confirm a payment in under 10 seconds, thereby solving one of Bitcoin’s most significant problems – long transaction times. Thanks to the masternode network and the InstantSend feature, payments are completed from customer to merchant in less than 150 seconds.

Another recurring issue with Bitcoin and other cryptocurrencies is large transaction fees. GoByte Pay solves this problem by allowing \$0 transaction fees inside the module after a miner’s fee. All transactions inside the GoByte Pay module are done on the chain, not server side, increasing security and eliminating possible threats.

Fees

Account type	Transaction Fee	Withdrawal fee
Normal Merchant	Free	2% or 0.001 GBX, whichever higher.
Masternode Owners	Free	Free

The only fee that the GoByte Pay module subtracts, is the withdrawal fee for transactions to GoByte addresses outside the module, including exchanges, local wallets and 3rd parties. The withdrawal fee decreases up to 3% according to the user verification level and is completely removed when withdrawing to masternode addresses which have an ENABLED status.

The GoByte Pay module allows merchants to monitor and assign addresses to stores or franchises as desired and eases the tracking of payments or potential issues regarding bills or payments no matter the size of the merchant or company.

When a merchant owns a masternode, they enjoy \$0 fees for all transactions and withdrawals, because their transactions are confirmed by their masternode and as a reward for being a contributor to the security and transaction processing capabilities of the network.

At the time of this writing, the GoByte Pay module is capable of supporting more than 1,000,000 merchants with no impact on the transaction speed of the network because of the number of masternodes on the network. As we scale the masternode network, the number of merchants supported can be unlimited.

Apps

The GoByte Pay module also features a mobile app for IOS and Android which is directly linked to the accounts registered in the GoByte Pay module. These apps share the same capabilities of the desktop wallet which means they allow for \$0 fees and easy access to the wallets linked to a registered account.

Both GoByte Pay apps feature 1-click payments to addresses in the user's address book, QR code scans to load GBX addresses faster, and in the future will incorporate fingerprint recognition and other biometric identity methods and technologies.

Terminal

Cryptocurrencies also suffer from a lack of adoption in retail stores. This is primarily because existing payment systems rely on software and hardware terminals that do not have cryptocurrency integrations. GoByte Pay will address this issue by providing an API to help existing terminals easily connect to POS Terminals developed by the GoByte Network or 3rd party developers. Integrations like this and others will connect with the GoByte Pay wallet and generate invoices as QR codes, which will be scanned by the customer using the GoByte Pay app and will confirm the transaction on the spot.

Existing payment processing terminals are often provided free of charge or inexpensively to merchants or offered on a payment basis and the GoByte network will utilize all of these methods to encourage adoption, especially as it relates to our geographically focused initial marketing targets covered in the Strategy section of this document.

The POS Terminals will be directly connected to the merchant account inside the "Pay" module, yet it won't be able to manage that account or bring any modifications to the account directly from the terminal. This way we want to prevent future token thefts from unauthorized persons. The terminal will be allowed only to generate new addresses for bills, inside the Pay module, and generate QR codes so the client can scan and pay with his "Pay" app.

The client scans the QR code and selects to pay the amount with a 0 fee, thanks to the “Pay” module. Once the transaction is broadcasted through the Masternodes, the POS Terminal will show a confirmed message.

Thanks to the customization capabilities of the POS Terminals, we can expand even further, by introducing our Crypto Debit cards which will allow multi-currency deposits. The debit card will work through the GoBytePay module, allows deposits, transactions and payments of other cryptocurrencies.

Technical specification for the terminals is available in the technology section of this

Ecommerce

GoByte Pay also comes with the ability to accept payments on the web in a shopping cart or in a simple website. It is a highly secure method of payment and all of the features of the GoByte Pay apps are available for online purchases.

The GoByte Pay Gateway is fast, transparent and secure. All transactions use a unique address to make it easy to find what you need and they are secured and heavily encrypted to stop hackers in their tracks. With GoByte Pay, you can provide your website customers with the same power that in-store customers enjoy.

The GoByte Pay Gateway has the following features:

- Supports multiple e-commerce applications out of the box with more upcoming
- An API is available, so you can integrate GoByte Pay with any other system
- You can charge users based on fiat currency like the US Dollar, so users can see the what they are paying without having to do the math
- All transactions are free of charge
- Get a payment confirmation in seconds
- Instant transaction for payments using the GoByte Pay wallet
- Merchants can save a small fortune over what merchant account gateways charge

The GoByte Pay module is at the center of all of our technologies because it enables us to build and grow a vast network of merchants and consumers using GoByte to save and succeed.

Future modules

The GoByte team is examining a number of potential options to speed adoption of the GoByte currency and will be announcing these as they make it onto our roadmap. One of the options currently in the research phase is GoByte Swap.

While more and more people have begun to invest in and adopt cryptocurrencies, the number of those currencies has made adoption for payment difficult. GoByte Swap will use the open source Atomic Swap technology as the basis for a system that will make it easy for consumers to swap out coins they already own in order to process a transaction on the GoByte network.

This serves a number of purposes.

1. It makes it easier for consumers to manage and use the cryptocurrencies they already have
2. It makes it easier for merchants to accept any cryptocurrency, without having to manage multiple currencies in their own wallets
3. It encourages merchant lock-in to the GoByte network and builds an infrastructure around the GoByte coin
4. Consumers will get more exposure to the power of GoByte and be encouraged to adopt it to make it even easier to buy and sell using GoByte
5. The swaps technology will also make it easier for GoByte to be traded on multiple exchanges, because a user can convert coins for buying and selling and sending on the fly and exchanges may make use of the technology for their own infrastructure
6. Increased liquidity means more trading volume and should have a positive impact on the value of GoByte coins

This is just one example of the many modules our development team is considering. Other modules will include integrations with other applications, markets, and ecosystems as well as specialized applications for specific vertical markets. In addition, our APIs will allow 3rd party developers to create their own modules for specific markets thus helping to increase adoption worldwide.

If you have an idea that would be a great addition to the GoByte network, please reach out to us on Discord or our other channels. We are a collaborative team and look forward to hearing your thoughts.

Miners, masternodes, earning more GBX

We've mentioned masternodes a few times in this document but haven't explained their purpose and we have yet to explain mining as it relates to the GoByte network. A much more technical explanation of both concepts is available in our Technology section, but for the rest of us, this section will explain their importance.

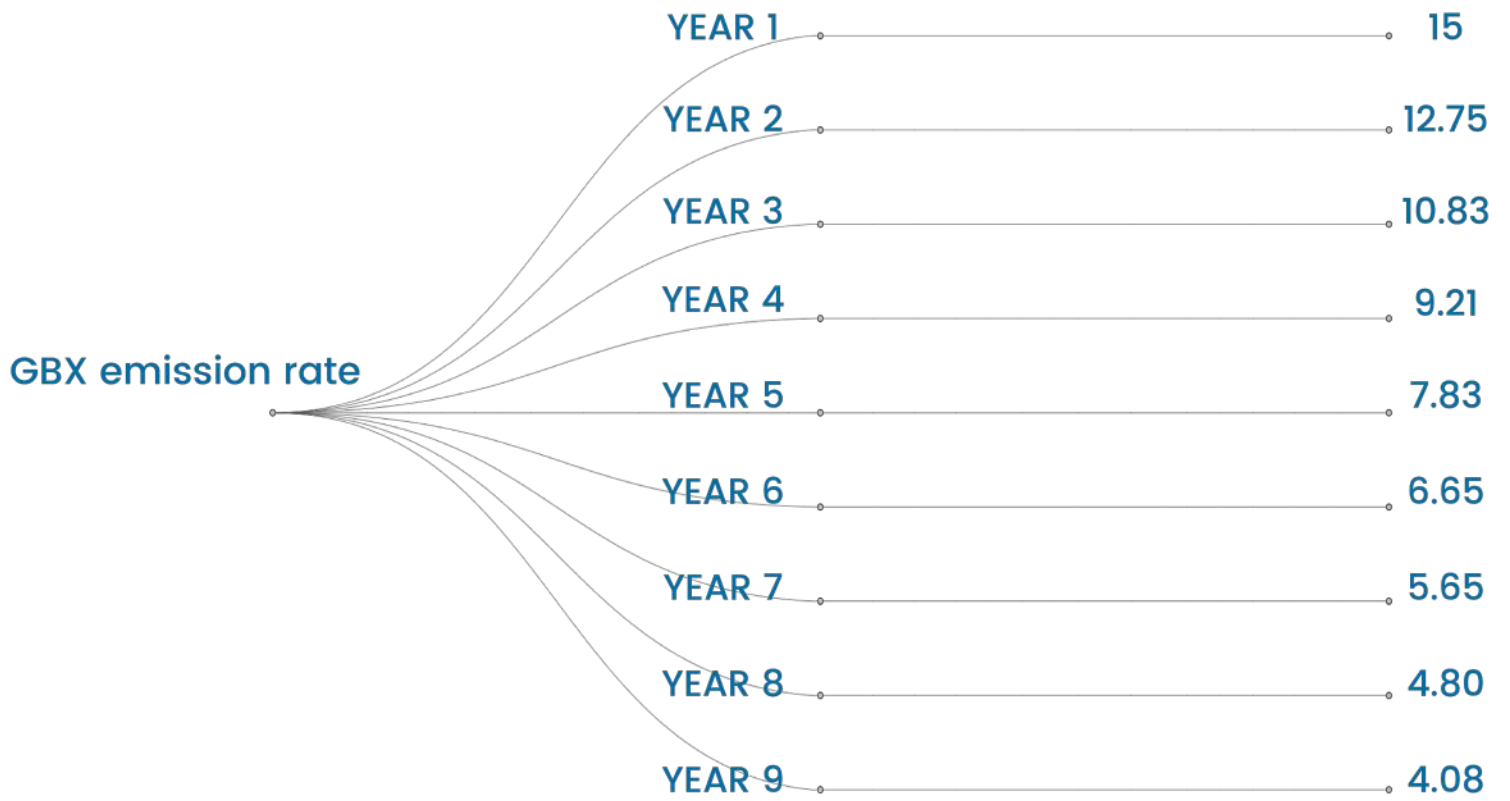
In order for cryptocurrencies to be powerful, fast, decentralized, and secure, they require a network of computers to provide processing power to the network. Satoshi Nakamoto foresaw as well, that these computers would need to be rewarded in some way for providing this power and so he created miners. Miners are computers that are tasked with solving a complex math problem in order to create a block on the blockchain where all transactions are stored in a virtual ledger (for an explanation of blockchains, please see the resources section at the end of this document). This ledger is duplicated from one block to the next ensuring that no "coins" can be spent more than once and that a record of all transactions is always available. A mining machine can require a great deal of processing power and therefore costs money and resources to build and run. For providing these resources every time a miner solves the mathematical problem first and records a block they are rewarded with coins associated with that block.

The advantage of mining for the GoByte network over many other networks is that it is ASIC resistant. That means it can use a graphical processing unit to mine for the network rather than very expensive ASIC processors that require even greater electrical resources and are out of reach of common computers. GoByte has always been about making it easier to use and to earn and that is reflected in our mining requirements.

On the other side of the processing and computing power equation are masternodes. Masternodes require less computing power, but also help secure the network and record transactions. Masternodes are less resource hungry, because they represent an investment by a coin holder in the GoByte network. Every masternode owner is required to hold 1000 GoByte coins and store them on their masternode server.

Then, on a regular basis (determined by the overall processing capabilities of the network) they too earn more coins for validating transactions on the network. Masternodes help keep the network fast and secure and so masternode owners are rewarded for their investment in coins and processing with more coins being delivered to them on a regular basis.

Currently the block reward or the number of coins created and distributed for every block recorded is 15. This means that the miner receives 7.5 coins for every one they mine and the chosen masternode is rewarded 7.5 GoByte coins. The number of coins rewarded drops by approximately 15% annually and a new block is created approximately every 150 seconds.



Masternodes and mining are a great way to contribute to the GoByte network and to be rewarded for that contribution. We provide extensive help on our website for those that would like to take part in mining or own a masternode.

Anonymity

GoByte payments can be if needed, completely anonymous using PrivateSend. This is done by breaking up a payment into multiple parts and combining the parts with other transactions. Most cryptocurrencies while they do provide a layer of simple anonymous capabilities, can eventually be traced. This is true of Bitcoin and most of the major altcoins, but GoByte takes anonymity to a very deep level providing complete protection from detection. A detailed description of PrivateSend is available in the technical section of this document.

Maximum supply

The maximum number of coins that will ever exist for GoByte is approximately 31.8 million. This means that after all coins are created, no more coins can ever be made. This stands in stark contrast to fiat currencies, that are inflationary and are printed “as needed” by the US Central Bank which creates a destabilizing effect on the value of the US Dollar and has led to a number of financial crises.

GoByte (GBX) is celebrated by supporters and admonished by skeptics because of its finite supply. There are only approximately 31.8 million GBX that can ever be mined, regardless of the earth’s population and its corresponding demand for GBX. Once all 31.8 million have been mined, there will never be any new GBX (unless a change to the protocol is made to increase the supply).

It is estimated that mining will continue for approximately 243 years and provide an extended time period as an incentive to miners and masternode holders to continue to secure the network and process transactions.

Exchange and trading

Cryptocurrencies are speculative, highly volatile and very risky. They may also be illegal where you live. We encourage you to consult a licensed financial advisor and legal counsel before investing in cryptocurrencies of any kind and do your own research. GoByte coins are readily available for purchasing and trading on multiple exchanges and will become more available as we continue to advance our network reach.

At the time of this writing, GoByte is available for purchase and trading on the following exchanges and typically trades under the symbol GBX:

- Karsha Exchange
- Cryptopia
- Crypto-Bridge
- BarterDEX
- CoinExchange
- Stocks.Exchange

Roadmap

- 🚀 WhitePaper (In Progress)
- 🚀 Mobile Wallets (In Progress)
- 🚀 Web Wallet (In Progress)
- 🚀 Payment Gateway - GoBytePay (In Progress)
- 🚀 Payment Gateway - Apps (In Progress)
- 🚀 Get listed on Exchanges [1/3]
- 🚀 Attract Merchants

Q1 2018

- 🚀 Start dev. of POS Terminals
- 🚀 Testing GBX payments on vending machines
- 🚀 Development of the "Overwatch" module (Start)
- 🚀 Development of the "Mint" module (Start)
- 🚀 Start building the mining farm. Share profits among MasterNode owners
- 🚀 Hardware wallets for GoByte tokens
- 🚀 Attract Merchants

Q3-Q4 2018

Q4 2017

- 🚀 Launch Website
- 🚀 Window, Mac and Linux Wallet Release
- 🚀 Get listed on Exchanges [4/4]
- 🚀 Get listed on Coinmarketcap
- 🚀 Get listed on Masternode Monitor Website
- 🚀 Get listed on Whattomine

Q2 2018

- 🚀 Electronics Shop
- 🚀 Market Module - GoByte Market(Start)
- 🚀 Exchange Development (Start)
- 🚀 Marketing and Awareness campaign
- 🚀 Hiring PR team
- 🚀 Attract Merchants

Q1 2019

- 🚀 Smart Contracts
- 🚀 Development of the "Social" platform (Start)
- 🚀 New MasterNode feature
- 🚀 Attract Merchants

We have already accomplished a great deal of innovation on the GoByte network in a very short period of time and we are adding to our development team on a regular basis, so we can roll out even greater functionality to serve the needs of our users and the goal of being the dominant global payment solution.

The following represents our planned innovations, but please be aware that development timelines can be fluid and so while we provide some estimates of delivery, these release dates can be delayed.

Team

The GoByte team is truly international. Our team members work virtually to create the powerful platform and cryptocurrency you have available for your use today. Every member of the team shares a core vision of making commerce easier and leveling the playing field of finance for every participant in the world.

We can be reached via the following channels and welcome your feedback, ideas, and community involvement. Without you we don't really have a reason to exist, so please dive in with us.

Discord: <http://discord.gobyte.network>

Reddit: <https://www.reddit.com/r/GoByte/>

Bitcointalk: <https://bitcointalk.org/index.php?topic=2442185.0>

Website: <https://www.gobyte.network>

Medium: <http://medium.com/@gobytenetwork>

Telegram: [T.me/@gobytenetwork](https://t.me/gobytenetwork)

Hisyam (LowKey)

Location: Malaysia

Position: Chief Executive Officer, Lead developer

One of the four founders. He is the lead core developer and the project manager. Hisyam worked for years as a system administrator & network security specialist. He is on those cryptocurrency enthusiasts, exciting coders and men of vision, who can push things to the next level.

Muhamad Nabil (mnfikri)

Location: Malaysia

Position: Chief Information Officer, Senior developer

One of the four founders. Graduated as a Network Engineer, he is working as a hardware engineer and a senior core developer. Nabil is a perfectionist leading our quality test processes in order to find and fix bugs and security issues.

Antonio Moratti

Location: Bucharest, Romania

Position: Chief Marketing Officer

One of the four founders, Antonio is the brand's face, and the person you have to contact regarding GoByte. He is in charge of the marketing and brand awareness. Antonio is also in charge of merchant relations and applications.

Linkedin: <https://www.linkedin.com/in/antonio-moratti-7792a7156/>

Twitter: <https://twitter.com/AntonioMoratti1>

Mathieu Arbez (hewwo)

Location: Paris, France

Position: Designer, Senior Marketing Assistant, Public Relations, Tech Support

One of the four founders. Mathieu is a cryptocurrency enthusiast interested in the relations between the blockchain technology and the western world utopias. He is in charge of the public relations and community management. He is also helping on design, tech support and strategy.

Linkedin: <https://www.linkedin.com/in/mathieu-arbez-hermoso-a9b98383/>

Twitter: <https://twitter.com/MAH51323118>

Mohd Abdul Syafiq (0PC0de)

Location: Malaysia

Position: Designer, Senior Marketing Assistant, Public Relations, Tech Support

Syafiq is in charge of the public relations and the community management. He is also helping on design, tech support and marketing strategy.

Linkedin: <https://www.linkedin.com/in/mohd-abdul-syafiq-said-92377729/>

Twitter: <https://twitter.com/syafiq6191>

Akif Rabbani

Location: Malaysia

Position: Chief Technology Officer, Lead developer of the GoByte Pay module, Head of R&D Department

Akif is the lead developer of the GoByte Pay module. He leads a team of six Senior and Junior developers who can work on different modules for GoByte. Akif is a great leader and has the resources needed to lead the R&D department.

Linkedin: <https://www.linkedin.com/in/akif-r-393575a4/>

Twitter: <https://twitter.com/akifrabbani>

Advisers

Jarrad Williams

Location: USA, Miami, FL

Position: US General Manager

Jarrad is in charge of brand awareness in the United States. Jarrad is also in charge of merchant applications in the United States.

Linkedin: <https://www.linkedin.com/in/jarrad-williams-43912919/>

Logan Kugler

Location: USA, Miami, FL

Logan is a serial entrepreneur who has built six companies and a vast network of world-renowned business leaders. He has written about advances in technology, including cryptocurrency, for dozens of national magazines including Popular Science, Forbes, PC Magazine and Computerworld.

Linkedin: <https://www.linkedin.com/in/logankugler/>

Twitter: <https://twitter.com/logankugler>

Brad Nickel

Location: USA, Miami, FL

Brad Nickel has been in the startup world as a founder and adviser since 1997. He founded one of the first SaaS providers, designed the core tech for network printing, and has been a digital marketing executive for companies large and small.

Linkedin: <https://www.linkedin.com/in/bradnickel/>

Twitter: <https://twitter.com/clickbrain>

Website: <https://blacknox.com/>

Masoud Gheysari

Location: United Arab Emirates

Masoud Gheysari registered Karsha Business & Technology Inc. as a legal corporation on November 2011. He started expanding this automatic exchange system, accepting newly introduced cryptocurrencies and being one of the very first Bitcoin service providers.

Linkedin: <https://www.linkedin.com/in/khashmeshab/>

Twitter: <https://twitter.com/khashmeshab>

Website: <https://karsha.biz/>

Side team

Azlan Shah

Location: Malaysia

Status: Contract on going

Azlan Shah was hired at the end of December 2017 to develop and release the mobile apps of the GoByte “Pay” module. Azlan is a young developer with a lot of potential and knowledge regarding the mobile platforms and an excellent partner for us . Azlan is in charge of both IOS and Android apps for the “Pay” module.

Yugaindiran Marimuthu

Location: Malaysia

Status: Contract on going

Yugaindiran is a Junior Developer in the GoByte “Pay” development team that is lead by Akif Rabbani. Thanks to his knowledge, Yugaindiran is a Senior Hardware Engineer at the R&D department lead by Akif Rabbani. Yagaindiran is a key member for the further development and research of the POS Terminals that will be connected with the GoByte “Pay” module.

Long-term health

- 1 Larger and faster blocks. GoByte relies on a block size of 2MB and a block time of 150 seconds.
This effectively allows GoByte to handle a transaction volume 8x greater than Bitcoin's.
- 2 Masternodes. The GoByte network constitutes a 2-tier architecture, where the first tier is the protocol level, mining and staking and the blockchain itself. The second layer is its masternode array, being a large network of high availability dedicated servers operated by users. These users provide enhanced services to the network (such as faster transactions,

Masternodes require a collateral of 1,000 GoByte to operate in order to ensure that launching malicious nodes is too costly for a potential attacker, and nodes are paid in GoByte for their services. Since these are dedicated and powerful servers, they can better handle the increasing load of a larger chain than an average desktop machine or smartphone.

Architecture and operation of the GoByte network

The architecture and operation of the GoByte network can be summarized as follows:

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work solution to recover its block.
- When a node finds a proof-of-work solution, it broadcasts the block to all other nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent. This critical step ensures that a double-spend attack cannot occur.

Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash. Given that cryptographic hashing functions are computationally infeasible to reverse, a hash match confirms that the new block refers to the exact current state of the entire blockchain.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work solution is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach a sufficiently large number of nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realize it missed one.

Strategy

There is no point in putting in thousands of man hours to create a strong cryptocurrency if you have no way to establish market dominance. The growth of cryptocurrency interest in an investment context and the hyperaware levels of consumer interest in them, means right now is the time for us to launch a strong strategic push into the market. No brand in cryptocurrency has captured payments and none is as well positioned GoByte to do so.

That said, this is not an easy task. We will be using multiple strategies, tactics, and targeting mechanisms in order to grow our brand and it will require a strong base of talent and community enthusiasm to continue the growth we've already begun. We are determined to make GoByte the number one choice for cryptocurrency payments worldwide and we are ready to invest in the marketing and team needed to succeed.

Our goal to establish a strong presence in the payments market means we have multiple sides to the market we must target and reach.

- Merchants
- Consumers
- Agents
- Merchant Franchisers
- Merchant Headquarters
- Investors
- Money transfer locations

To do that, we have to build interest and excitement about GoByte. We generally believe that the fastest way to drive consumer adoption is through a presence in merchants and through other online consumer promotions. We must have both sides of the equation if we are going to succeed.

In order for that to happen, we have to build enough of a base of merchants in order to have consumers see the presence of our brand in multiple retail locations. This need to create two-sided demand means that in order for merchants to stay with us, they will have to have enough customers using GoByte Pay to make it worth it to keep using and promoting it.

Our approach to this is multi-pronged

- Geographic concentration targeting starting with South Florida and moving northward to other locations in the United States and worldwide.
- Geographic targeting in hub countries with a high influx of travel and business connections to South Florida. This will include Brazil, Colombia, Costa Rica, Dominican Republic, Venezuela, Argentina, Spain, and other European countries.
- Merchant agent targeting in our geographic target and nationally across the United States to have agents offering GoByte to their credit card processing clients
- In store marketing and promotions to get consumers to try and use GoByte
- Promotions targeting GoByte merchant customers and fans on social media with promotions and offers to drive consumers into stores to use GoByte
- Further promotions for transfers of funds via GoByte from South Florida to family and friends in other countries
- Aggressive and highly sophisticated US and International online advertising and growth tactics to encourage buying and using GoByte in a variety of situations, including money transfers, purchases, import and export and much more

Every consumer that signs up needs if possible to have more than one use of GoByte within their daily life. That can be either multiple merchants with whom they do business in person or online or other methods of use including funds transfers across borders and being an investor in GoByte on an exchange, as a masternode owner, or as a miner. Our goal is to be able to reach new users with marketing communications for them to be introduced to other ways of using GoByte. This is a critical component of our strategy and will be a part of every introduction we do to customers with “How You Can Use GoByte” type messaging at every brand exposure.

Part of the strategy is to connect with every new GoByte user by providing an incentive to connect with the GoByte community, signup for a newsletter or get more involved in what we are doing every time they use GoByte in a transaction.

We also will work with our merchants to provide incentives for them to offer discounts and coupons for using GoByte. This becomes an easier task, because transactions are free or have extremely low fees. Our merchants are already saving significantly with the use of GoByte, so they have more margin with which to play for GoByte-based purchases and the low-cost of the network means it is in their best interest to encourage more customers to use it. On average they are paying about 3% per transaction and in many retail businesses, 3% can be the difference between surviving and profitability.

In addition, encouraging consumers to recommend merchants in return for rewards means that we will be completing the multiple merchant per consumer strategy that will help drive repeat use of GoByte.

Target markets

We have two primary market segments for GoByte in broad general terms being merchants and consumers, but those targeting objectives are too broad in these early days of building out our network, so we are going to use targeting and testing strategies to identify our best early payment adopters.

As we progress through our marketing strategies, we will narrow our specific market segment targets of both consumers and merchants by building out a series of marketing messaging and advertising tests that will help us identify our most likely early adopters for payments.

Merchants

In order to grow the use of GoByte, we will have to grow the number of merchants available to take payments from consumers. Our success as a currency depends on our ability to grow both sides of the market simultaneously and that is why we are taking a multi-pronged approach to the growth of our merchant network.

Our targeting for merchants will be geographic, vertical, and mass market. We will use sophisticated marketing techniques, referral programs, and networks of referral partners and agents to grow our based of merchants.

Geographic

1. We have a business development, marketing and investor team in the area and a beginning base of merchants to grow upon
2. The area is a global travel, e-commerce, and industry hub.
3. The international nature of the area is perfect for spreading GoByte around the world.
Millions of dollars are transferred into and out of South Florida to relatives, friends, and ecommerce daily and the fees those transfers cost mean a GoByte transfer option can be very attractive.
4. Much of the transfers of funds in and out of Miami happen in small retail outlets, so we can target locations where immigrants currently frequent, but where currently no funds transfer capabilities exist
5. South Florida is an international banking and finance hub. Numerous import and export businesses operate in the region and the ability to transfer large sums of money with very low-cost fees using GoByte will be a natural progression from consumer use in the area.
6. Florida is also a tourist destination with the potential to also spread GoByte to other regions of the country and the world by targeting tourist retailers to help them and consumers save.
7. As we progress through our strategy, we will ascertain other regions where GoByte is seeing increased adoption and will pick a few targets for our next geographic expansion.
8. We will also expand geographically through north Florida and into the Atlanta, Georgia region and then upwards throughout the United States.

Vertical

There are a number of verticalized currencies in the market today. These currencies are meant to solve a problem for a specific industry, but when it comes to consumer payments for things like cannabis treatments, healthcare, and other specialized products and services, these currencies will likely struggle, because they do not serve a consumer in any other scenario. So, while some currencies will succeed in those markets, most will not generate the level of demand necessary to sustain a market.

GoByte's approach is very different. We will target vertical markets for payments, but these will only be as an initial adoption segment to get GoByte into consumers hands and to get them used to using digital currencies. Once we have a consumer using our currency, we will then encourage them to use it at other local, national, and ecommerce merchants. We will build into our apps the ability to locate other merchants in the area that accept GoByte Pay, as well as online sites.

We will also use advertising to drive customers to these vertical markets, because we can more easily target them online with advertising and merchants will appreciate that we are driving customers to their stores.

It is critical to have consumers see a currency as usable in multiple locations. It cannot be just one store or for one type of item they buy. Adoption by consumers for everyday use will be dependent upon adoption by merchants where they shop.

We are working through a number of potential vertical markets and have begun the process of building partnerships with merchant account agents and others in particular segments.

Our goal is to work through vertical markets while we are using geographic targeting and will attempt to coincide expansion into those geographic areas in parallel.

Consumer to merchant promotion

We also will work to have our consumer clients that use GoByte help us to promote to other merchants in their area, market, and on sites where they make purchases.

We will use rewards to encourage consumers to promote GoByte Pay to merchants that they frequent in the form of prizes, GoByte coins, and other incentives.

We will launch an easy to use and manage rewards system tied to the GoByte Pay app to manage the rewards we will offer.

Mass market

While being very specific in our targeting both vertically and geographically, we will also be promoting and marketing our solutions for merchants on a national and international level. We will use targeted advertising, social media, content marketing, public relations, and events to recruit merchants.

Consumers

We can book as many merchants as we want, but if we don't have consumers to use the GoByte network, then we will not be able to grow or sustain it.

Our consumer targeting will be based on specific demographics of current users, community members, and supporters, but we will also begin testing marketing campaigns to new market segments.

Demographic targeting

As we engage with more and more users of GoByte, we will work to establish a “persona” for consumers to be most likely to use our service so we can target them with digital marketing. We need not only early adopters, but also adopters willing to spread the word to other consumers in return for rewards.

We will use existing targeting metrics in social media to cross identify current cryptocurrency exchange users and target them with our payment messaging. In addition, we will be working to test messaging across social media and other digital channels to determine what will work best for attracting and converting users.

Currently those most likely to invest in and use cryptocurrencies are younger men and some younger women and so those will necessarily be some of our initial targeting metrics, but we will seek to determine other demographics likely to adopt and use our system via testing both online and through merchants.

Geographic targeting

Just as we are launching initial south Florida targeting in the United States for merchants, we will also do the same for consumers. For specific strategies and justifications for this approach, please see the geographic section under Target Markets/Merchants.

Distribution

GoByte is currently a small organization and in order to grow our payments market share, we will necessarily need to make use of partnerships to increase our market penetration and distribution to merchants and consumers.

In this section we detail our strategies for going to market via partnerships that have customers we want to target with GoByte and GoByte Pay.

ISO / Agents ISOs or Independent Sales Organizations and Agents offer merchant account or credit card processing services to retail and online stores. For every merchant they sign up for processing services, they retain a small percentage of all processing charges that a merchant pays out of each transaction.

These organizations and sales people create recurring revenue streams for themselves that can last for years. In order for GoByte to be able to utilize these same networks for our services, we will need a rewards system that also equates to significant revenue and will be using coin and masternode incentives to help them see the value of GoByte over other forms of payment. The more the network grows, the more value they will see in their coin rewards and so in turn, the more they will want to offer GoByte Pay to merchants. Over time the value will far outstrip the revenue from credit card transactions, but there is no reason they can't sell both.

In recent years, the prospects for credit card processing revenue have begun to dwindle for these sales and agent organizations, because companies like Stripe and Square and others have begun to gain market share with simpler pricing and no middlemen. This has resulted in less commissions and recurring revenue. This means these sales people are nervous about the future of their business and the GoByte system can provide an amazing opportunity for them to earn more.

We will also target service providers that work with merchants and provide them an incentive to offer GoByte, include point of sale products, merchandising services, and much more.

Integration

One of the benefits of building a system for payments and a cryptocurrency is the ability to integrate that system with any other system that would be compatible. We will examine the market for point of sale systems, accounting, and other business-related systems that would be a strong fit for integrations. In the early stages we will provide the integrations with major providers of systems that would be of value and provide rewards to product and service providers that promote GoByte to their clients.

We will also offer an API for developers to make it easy to connect to the GoByte payment system from their apps and website.

The goal is to make it as simple as possible for application developers and systems with existing companies to be able to make use of the GoByte Pay system and to help increase consumer adoption.

Referral partners and consumer advocates

GoByte will establish a full consumer and partner referral program to provide a series of rewards for signing up merchant adopters as well as consumer users. We will market the system heavily in order to grow our user base and build a larger community of users and advocates.

A similar program will also be available to businesses, consumers, and professionals to refer merchants for signup.

Marketing and PR

We will be mounting an aggressive marketing and PR program to grab market share in our geographic targets and worldwide.

Community / Social media

We have already developed a very strong community following for GoByte and we plan to leverage that community to help us grow the brand. Each member of the community has a vested interest in seeing us succeed and many have already offered to support us as we launch our coordinated marketing strategy. Now that we have the tools that consumers need to succeed, we are confident they will assist in our effort to grow.

Our current community is very investment oriented and while that has sustained us when things were difficult, we also must begin to expand our community to other demographics. For example, most purchasing in the United States is handled by females and targeting females for cryptocurrency spending can be difficult. In this case, we will work to build community first around younger females that are more likely to be willing to give GoByte a try. That targeting means that we need to build a different type of community around the demographic and social networks that will be our best targets. These campaigns will not only be organically driven, they will also be advertising driven with the exception of Facebook.

One of the initial communities we build around our network will be one oriented to people that would like to earn more money by referring GoByte to merchants and other consumers. It will be critical though that we create the network where they already are involved with communities including social networks and chat related applications.

All of this requires us to use strong content and social aggregation tactics to reach each target demographic's attention while providing a strong reason for each to become involved. Again, this requires testing and strong data analysis in order for it to be a success.

Just as we are planning geographic targeting in general, we will also use social geographic targeting to increase the opportunity for consumers to use GoByte for transactions

We also need to build a community for merchants. This will require a different type of social strategy, but one that will be needed anyway.

We will require strong social media professionals and community managers to help us grow our presence and as we grow the network and revenues, we will be able to staff teams to make that possible. We will also identify strong social communicators

Event marketing

Because we are taking a geographically centric approach to marketing, we will also make use of event marketing in our initial markets to build brand awareness and to drive signups. Festivals, fairs, business conventions and more will all be part of the overall strategy to drive adoption.

We will also use our own created events in partnership with our merchants, that will be fun to attend and will encourage existing GoByte users to bring their friends.

Content marketing

Content marketing is the single most cost-effective type of marketing available to digital marketers and we will use it in every facet of our strategies. From advertising great content, to social promotion, we will work to constantly connect with merchants and consumers by providing them with high quality, educational, and entertaining content. Content marketing allows you to establish a relationship with consumers over time, so they become comfortable with your brand, expertise, and capabilities.

We will generate written, video, audio (podcast), and graphical content to catch the attention of our target markets. Most of the content we develop will be educational or entertaining. Educational content allows us to establish ourselves as experts and as a company that provides value to merchants and consumers while entertaining content pushes our brand into the minds of consumers and makes it recognizable and positive. Both can have a great deal of impact.

The key to successful content marketing is creating a connection with potential customers. That connection can be via social media on their wall or via automated bots or it can be email drip campaigns of courses or entertaining materials. The priority is to make a connection and then to continue to generate value for them.

Merchant content marketing

Most of our merchant targeted content will be educational. Retailers are constantly looking for ways to improve their bottom line and we will provide content that captures that desire. Everything from marketing to accounting to operations will be tested and when we find content types that result eventually in conversions to GoByte Pay merchants, we will double down on those targets and content types.

We will also create content that profiles our merchants to other merchants to show how GoByte has made them successful and to consumers to help them connect with more customers to use GoByte. Profiling our early adopter merchants will also allow us to establish a stronger bond and loyalty with them and increase our ability to gain referrals from other businesses.

Consumer content marketing

Our consumer content marketing will be a pretty even mix of entertainment and educational. The educational content will be around the types of things that interest our market whether it be crafts and cooking or wine and technology. Again, we will use demographic targeting to determine our best bet and then provide them the content that has the greatest impact in longer term conversions.

We may also use our merchants to provide educational content to consumers. If we discover that wine lovers will adopt GoByte, then we will provide a series of courses on wine tasting and wine regions. We may hold in-store events that are educational as well.

Advertising

Online advertising can be very cost effective, but if you don't know what you are doing, it can be very painful. We will be working with the best in social, search, and display advertising to target and capture consumer interest. Most of our consumer advertising will drive consumers to engaging content and our merchant advertising will drive them to educational content about business.

We will also test campaigns to drive people straight to signups. Learning what search terms and social interactions will drive conversions will be very important.

Effective advertising is all about data and we will be constantly analyzing our returns over time to hone in on campaigns that are driving the most signups and eventually revenue.

Public relations

Public relations is no longer about press releases. Today it is about getting great stories written in targeted publications and we have a number of strategies we will pursue using a professional PR agency.

- Stories about our merchants published in trade websites and magazines around their vertical market with an emphasis on how they are making more money using GoByte or some other angle that has a tie-in to GoByte.
- Stories about or quoting our executive team.
- Stories about consumers that are helping to drive GoByte adoption.
- Speaking gigs at business shows to attract merchants in specific verticals or things like larger city chambers of commerce where we can teach attendees about cryptocurrencies while also letting them know how they can use GoByte to jump into the market, make more revenue, and reduce fees and expenses.

Strategy conclusion

Thank you for taking an interest in GoByte. We are excited about the opportunity and we would be honored to have you join us as we take over the world of payments. We believe we have the network, applications, and the strategy to make GoByte a dominant payments provider worldwide and we are getting ready to do much more to make that possible. Every time another person joins our worldwide community, our network grows stronger. Please feel free to reach out to us if you have any questions. We are here to make it easier for you to be empowered by cryptocurrency through the GoByte network.

Technical Background

This section of the white paper is intended for readers with a strong technical background and some experience with blockchain technologies and cryptocurrencies.

What is a cryptocurrency?

Standard definition

A cryptocurrency is a medium of exchange that uses hash-based algorithms or cryptography to provide more secure transactions and a better protocol as a medium of exchange. Most currencies are peer-to-peer and utilize decentralized communication between networks. They run with a proof-based algorithm that makes the network possible.

The usefulness

Cryptocurrency is useful in a number of ways, including but not limited to:

- More profitable
- Transactions are faster and more secure
- Less prone to inflation
- Gives users more control over currency due to less government interference

How does mining work?

Cryptocurrency mining uses a computer's processing power to verify blocks, secure the network, and lower the hash difficulty targets. This means that the computers within the mining network are processing the transactions and verifying a chain more rapidly, resulting in faster payment processing and greater network stability.

- Most miners have a block erupter system built-in
- ASIC & Cryptonote based currencies typically rely on the number of CPU cores and the quality of the central processor
- Non-ASIC currencies, like GoByte, are more GPU based and are mostly multi-threaded hashes.

How does trading work?

Trading cryptocurrencies means buying and selling. The values of cryptocurrencies change rapidly. This is especially true because many cryptocurrencies use different algorithms and the rate at which the price changes is dependent upon market demand and other influences. Most exchanges allow users to trade between cryptocurrencies and the best traders use tools that show price fluctuations in the market and buy and sell utilizing this information.

Different types of cryptocurrencies

ASIC based cryptocurrencies

- Primarily Proof of Work(POW) or mining-based
- BTC Cash, Litecoin, etc.
- May utilize ASIC based mining more in the future
- Mining BTC Better utilizes ASIC (Application-Specific Integrated Chips)

NeoScript cryptocurrencies

- Anonymity
- Egalitarian PoW
- Memory bound functions
- Utilizes GPU cores for mining
- Defined as utilizing an application layer protocol

Non-ASIC cryptocurrencies

While more ASIC-Resistant than other coins, Non-ASIC cryptocurrency revolves around an entirely different concept. Most utilize miner's GPU or graphical processing unit for mining. GPU accelerated computing is also an option since it is closer to analyzing algorithms that are multithreaded. Some Non-ASIC cryptocurrencies utilize smart contracts like Ethereum.

Main bottlenecks to Bitcoin

1. Centralization
2. Network capacity (transactions per second)
3. Sustainability
4. Governance

Any decentralized payment system that wishes to achieve universal adoption and solidify itself as a viable global currency must be built in such a way that its very infrastructure addresses and solves all bottlenecks early on.

Economically speaking, the recent exponential price appreciation of Bitcoin from under \$0.01 to over \$10k as of writing this paper clearly demonstrates an increasing global market demand for the solution that Bitcoin offers, however, we believe that until a comprehensive solution arises that fully answers the challenges faced by the Bitcoin network, a full capitalization of the global multitrillion-dollar financial industry cannot be reached.

With this philosophy and unmet market demand in mind, we have decided to create GoByte (GBX). GoByte is a community driven, open source and fully autonomous cryptocurrency that places a strong emphasis on the very building blocks required to create a complete payment system: it is secure, anonymous, trustless, scarce and fungible with a very low-cost transaction pro le. It is designed to embody all that Bitcoin as well as more advanced cryptocurrencies have grown to become as well as to capture the economic value that is thus far inhibited by the systemic constraints outlined above.

We will expand on these 4-main adoption and growth barriers and outline how GoByte's unique architecture seeks to resolve them.

Centralization

A network is considered centralized when either vast or absolute decision-making power is vested in the hands of few individuals. We believe that in recent years, the Bitcoin network has taken on a path of evolution that is incompatible with its founders' original vision.

The first is the question of mining. Mining is the process by which individuals dedicate computational resources to solving difficult mathematical problems. Upon solving the aforementioned, a new block is found on the blockchain and with it newly pending transactions are confirmed and cleared through. This process is known as Proof of Work (or PoW) as it forces the miner to prove that they have done the necessary work to verify the block, and the first miner to find a new block is compensated for their efforts. This introduces an element of economic competition between miners and prevents the network from being attacked as attacks become too costly and thus, economically unviable.

Unfortunately, the Bitcoin protocol has introduced a mining algorithm that allows for ASICs (Application-Specific Integrated Circuit) devices that can create a very large number of hashes per second. This has created an unfair status quo whereby those who can afford to purchase ASIC devices have a clear upper hand and those who cannot are effectively excluded from participating in the network. Since every bitcoin protocol enhancement needs to be approved with a 95% majority of miners, the top X% of miners who own 95% of the mining power can either accept or veto any suggestion that is brought before the community. This effectively overrules the democratic nature that a decentralized network should be characterized by and creates a disproportionate centralization of decision-making power. In order to prevent such an occurrence, GoByte utilizes an advanced and fair hashing algorithm known as NeoScript. NeoScript is well known for being a lightweight algorithm that can be mined with very modest hardware devices.

This ensures that anyone can participate in the GoByte mining, whether they own a smartphone or a supercomputer. As the name suggests, NeoScript is a further development of Script as described in Percival. It is aimed at increased security and better performance on general purpose computer hardware while maintaining comparable costs and requirements., which makes the development of a dedicated ASIC device specifically designed to produce a large number of hashes per second virtually impossible. This property is known as ASIC-resistance, and with it, we seek to eliminate any barrier to entry for the average GoByte end user in terms of network governance and promote absolute decentralization and democracy.

Network Capacity

Abstract

We outline an initial scaling mechanism for GoByte. After deployment and activation, GoByte will be able to handle double the transactions it can currently handle. This means that GoByte will be prepared for eight times the traffic of Bitcoin.

Motivation

Peer to peer electronic cash systems rely on the fact that they can be used with little to no trust in a third party. We have also seen scaling issues have dramatic effects on the usability of these systems. The current state of the GoByte network requires users to trust that developers will deliver a scaling solution when needed. Implementation of DIP1(Dash Core) allows users to actively participate in increasing the capacity of GoByte.

In addition, scaling solutions take time to roll out. As such, developers are tasked with rolling out scaling solutions four or five months before they are needed. Forecasting network traffic growth is an impossible task. However, there are outside factors that could accelerate this estimate. For example, a chain fork which is being discussed for bitcoin may drive users to alternatives. Also, market actors can have a profound impact on the use of GoByte, and do not necessarily announce their intentions for proprietary reasons.

One more motivation is that adopting this proposal serves as a proof of concept of GoByte's governance system. It shows that proposals voted on by masternodes do actually have real world results. It removes the need for users to trust in GoByte's proposal system.

Conventions

- 0x20000000 is the bit sequence 00100000000000000000000000000000 and is the current version of dash blocks.
- 0x20000002 is the version used to signal acceptance of a consensus change rule. A miner should use this version to signal acceptance of the miner and the masternode for the block of a consensus rule change.
- We use % as it is used in C++. It is the remainder on division. So $7 \% 3$ is 7 modulo 3 and is equal to 1.

Quadratic hashing challenge

Currently Dash has a size limit of 1MB per block. With this limit a miner could include a transaction that takes around 3 minutes to verify on a moderate CPU.

However, GoByte, with a 2MB block size means an attacking miner could include a transaction that takes around 12 minutes to verify. If an attacker successfully gets an attacking block in the chain then all nodes in the future will need to verify this block when syncing. This attack is even more dramatic as block size increases. Paradoxically, this attack could get so bad that it becomes impossible because propagation would force an attacking block to be orphaned. Even if an attacking block is not included in the main chain, trying to verify attacking blocks can have negative transient effects.

This attack is quadratic with respect to transaction size. As such, limiting transaction size makes this attack impossible. Currently, transactions over a size of 100kB are nonstandard and dropped by the network. A quadratic hashing attacking transaction of size 100kB would take around 2 seconds to verify. Since transactions are processed in parallel, a 2MB block full of 100kB attacking transactions would take from 4 to 8 seconds to process. For this reason, GoByte changed consensus rules so that blocks with a transaction over 100kB are ruled invalid and orphaned.

Consensus protocol changes

- A block over 1MB is invalid.
To allow the network to scale we replace this rule with the two rules:
- A block over 2MB is invalid.
- A block with at least one transaction over 100kB is invalid.
Note the 100kB cap on transaction size will not necessarily be satisfied by old blocks. For this reason, this new rule must only be enforced on blocks after activation of the protocol change.

Observation

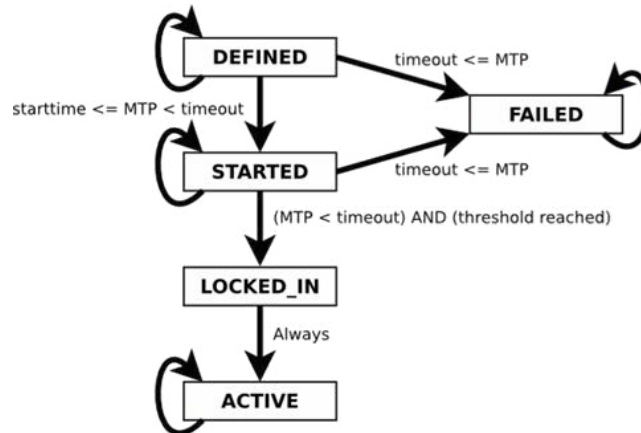
100kB transaction limit

This subsection is to only point out a possible efficiency of the 100kB transaction size limit. Currently, transactions in the mempool already verified to be standard and thus satisfy the size limit. It should then be possible that only transactions not seen by the node would need to be checked to satisfy the 100kB limit. However, checking if a transaction is in the mempool might take as long as verifying the size.

BIP 009 inspired activation (Bitcoin Core)

To ensure a coherent network roll-out we employ BIP9(Bitcoin Core) signaling adjusted for GoByte. We reserve the last bit in the version to signal for DIP1(Dash Core) activation. A DIP0001(Dash Core) enabled miner will broadcast block version 0x20000002 only if the masternode selected for that block is also DIP1(Dash Core) enabled. We model the 2016 block difficulty adjustment period in BIP9(Bitcoin Core) with a 4032 block round. This length of a round should allow for a representative sample of masternodes to be taken.

As a block is mined the version number is determined by the miner who mined it and the masternode that is selected for that block. Note that blocks mined by non-upgraded miners will broadcast version 0x20000000 without regard for the DIP1(Dash Core) acceptance of the masternode selected.



Above, MTP represents the median time past as in BIP113(Bitcoin Core). The variables starttime and timeout are particular integers that represent the time in the current epoch. Here, threshold reached, is a particular Boolean we will define below, and denote without the space, threshold reached, in code.

The state of every block is determined by the algorithm below:
 The state of the Genesis block is DEFINED as in BIP009.

```

State GetStateForBlock(block) {
  if (block.height == 0) {
    return DEFINED;
  }
}
  
```

All blocks in the same round have the same state.

```

if ((block.height % 4032) != 0) {
  return GetStateForBlock(block.parent);
}
  
```

Otherwise, the next state depends on the previous state:

```

switch (GetStateForBlock(GetAncestorAtHeight(block, block.height - 4032))) {
  
```

We remain in the DEFINED state until we either pass the starttime or the timeout. GetMedianTimePast in the code below refers to the median nTime of a block and its 10 predecessors.

```

case DEFINED:
  if (GetMedianTimePast(block.parent) >= timeout) {
    return FAILED;
  }
  if (GetMedianTimePast(block.parent) >= starttime) {
    return STARTED;
  }
  return DEFINED;
  
```

After a period in the STARTED state, if we're past the timeout, we switch to FAILED. If not, we tally the bits set, and transition to LOCKED_IN if a sufficient number of blocks in the past period have bit1 set to 1.

Note that a block's state never depends on its own nVersion; only on that of its ancestors.

```
case STARTED:
    if (GetMedianTimePast(block.parent) >= timeout) {
        return FAILED;
    }
    if (thresholdreached) {
        return LOCKED_IN;
    }
    return STARTED;
```

The protocol change is only in force when the first block is in an ACTIVE state.

Selection of parameters

For values of starttime and timeout, we implemented as follows:

- starttime= 1508025600-- turned off Oct 15 at midnight
- timeout= 1539561600-- 52 weeks later

The selection of a round consisting of 4032 blocks is made based on masternodes not being randomly selected, rather they are in a queue. As such it can't treat the sample of masternodes as a simple random sample. At current time 4032 masternodes would consist of a sample of around 87% of masternodes. This number is small enough that the sample of masternodes are unique. If this number were larger then there would be a chance that some masternodes would be sampled twice while others aren't sampled at all. This property is maintained as long as the number of blocks in a round is under 90% of all masternodes. The number 4032 also has the property of being equal to about a week of blocks.

Calculation of thresholdreached

Determination of thresholdreached

Given a block with $\text{block.height} \% 4032 = 0$

we can calculate thresholdreached. thresholdreached is determined by bit1 on each version of all blocks in the previous round. Note the current block is not considered to be in the previous round. We define thresholdreached to be true when and only when, $(\text{sum}(\text{bit } 1) \geq 3226)$.

This sum is over $(\text{block.height} - 4032)$ through $(\text{block.height} - 1)$.

This translates to 80% of the DIP1 flags.

Expected activation conditions

Given that bit1 will be 0 if mined by a non-DIP1 miner this actually targets activation in the following cases.

- $\geq 80\%$ of mining power and 100% of masternodes
OR
 - $\geq 89.5\%$ of mining power and $\geq 89.5\%$ of masternodes
OR
 - 100% of mining power and $\geq 80\%$ of masternodes
- In any case, activation is highly unlikely without at least 80% of miners and 80% of masternodes.

Copyright

Copyright (c) March 25, 2015 - 2017 Dash Core Team. Licensed under MIT License

Copyright (c) November 16, 2017 - Present GoByte Core Team. Licensed under MIT License

MasterNodes network

Full nodes are servers running on a P2P network, that allow peers to use them to receive updates about the events on the network. These nodes require significant amounts of traffic and other resources that carry substantial cost. As a result, on the Bitcoin network a steady decrease in the amount of these nodes has been observed for some time and as a result block propagation have been upwards of 40 seconds. Many solutions have been proposed such as a new reward scheme by Microsoft Research and the Bitnodes incentive program.

Masternode reward program - cost and payments

Much of the reason for the decrease of full nodes on the Bitcoin network, is the lack of incentive to run one. Over time the cost of running a full node increases as the network gets used more, creating more bandwidth and costing the operator more money. As the cost rises, operators consolidate their services to be cheaper to run or run a light client, which does not help the network at all.

Masternodes are full nodes, just like in the Bitcoin network, except they must provide a level of service to the network and have a bond of collateral to participate. Collateral is never forfeit and is safe while the Masternode is operating. This allows investors to provide a service to the network, earn interest on their investment and reduce the volatility of the currency.

To run a Masternode, the node must store 1,000GBX. When active, nodes provide services to clients on the network and in return are paid in the form of a dividend. This allows the users to pay for the services and earn a return on investment. Masternodes are all paid from the same pool of money, approximately 50% up to 80% of the total block reward is dedicated to this program.

Due to the fact that the Masternode rewards program is not a fixed percentage and the Masternode network nodes are fluctuating, expected Masternode rewards will vary according to the current total count of active Masternodes and current block reward distribution. Payments for a standard day for running a Masternode can be calculated by using the following formula:

$$(n/t)*r*b*a$$

Where:

- n is the number of Masternodes an operator controls
- t is the total number of Masternodes
- r is the current block reward (presently averaging about 15 GBX)
- b is blocks in an average day. For the GoByte network this usually is 576.
- a is the average Masternode payment (50%-80% of the average block amount)

Return on investment for running a Masternode can be calculated as $((n/t)*r*b*a*365) / 1000$

Where variables are the same as above.

The cost associated with running a Masternode creates a hard and soft limit of active nodes on the network. Currently with X (where X = Current GoByte coins in circulation), only Y nodes (where $Y = X/1000$) could possibly be running on the network. The soft limit is imposed by the price it costs to acquire a node and the limited liquidity on exchanges due to usage of GoByte as a currency and not merely an investment.

Deterministic ordering

A special deterministic algorithm is used to create a pseudo-random ordering of the Masternodes. By using the hash from the proof-of-work for each block, security of this functionality will be provided by the mining network.

Pseudo Code, for selecting a Masternode:

```
For(masternode in masternodes){
    current_score = masternode.CalculateScore();
    if(current_score > best_score){
        best_score = current_score;
        winning_node = masternode;
    }
}
CMasterNode::CalculateScore(){
    pow_hash = GetProofOfWorkHash(nBlockHeight); // get the hash of this block
    pow_hash_hash = Hash(pow_hash); //hash the POW hash to increase the entropy
    difference = abs(pow_hash_hash - masternode_vin);
    return difference;
}
```

The example code can be extended further to provide rankings of Masternodes also, a “second”, “third”, “fourth” Masternode in the list to be selected.

Trustless quorums

Currently the GoByte network has ~705 (as of March 2018) active Masternodes. By requiring 1,000 GBX collateral to become an active Masternode, we create a system in which no one can control the entire network of Masternodes. For example, if someone wants to control 50% of the Masternode network, they would have to buy 352,500 GoByte coins from the open market. This would raise the price substantially and it would become impossible to acquire the needed GoByte.

With the addition of the Masternode network and the collateral requirements, we can use this secondary network to do highly sensitive tasks in a trustless way, where no single entity can control the outcome. By selecting N pseudo random Masternodes from the total pool to perform the same task, these nodes can act as an oracle, without having the whole network do the task.

For an example, implementation of a trustless quorum (see InstantSend), which uses quorums to approve transactions and lock the inputs or the proof-of-service implementation.

Another example use for trustless quorums can include utilizing the Masternode network as a decentralized oracle for financial markets, making secure decentralized contracts a possibility. As an example, contract, if Apple Stock (AAPL) is over \$300 on Dec 31, 2016 pay public key A, otherwise pay public key B.

Roles and Proof-Of-Service

Masternodes can provide any number of extra services to the network. As a proof-of-concept, our first implementation included PrivateSend and InstantSend. By utilizing what we call proof-of-service, we can require that these nodes are online, responding and even at the correct block height.

Bad actors could also run Masternodes, but not provide any of the quality service that is required of the rest of the network. To reduce the possibility of people using the system to their advantage nodes must ping the rest of the network to ensure they remain active. This work is done by the Masternode network by selecting 2 quorums per block. Quorum A checks the service of Quorum B, each block. Quorum A are the closest nodes to the current block hash, while Quorum B are the furthest nodes from said hash

Masternode A (1) checks Masternode B (rank 2300) Masternode A (2) checks Masternode B (rank 2299) Masternode A (3) checks Masternode B (rank 2298)

All work done to check the network to prove that nodes are active is done by the Masternode network itself. Approximately 1% of the network will be checked each block. This results in the entire network being checked about six times per day. In order to keep this system trustless, we select nodes randomly via the Quorum system, then we also require a minimum of six violations in order to deactivate a node.

In order to trick this system, an attacker will need to be selected six times in a row. Otherwise, violations will be cancelled out by the system as other nodes are selected by the quorum system.

Attacker Controlled Masternodes / Total Masternodes	Required Picked Times In A Row	Probability of success $(n/t)^r$	GoByte Required
1/2300	6	6.75e-21	1,000GBX
10/2300	6	6.75e-15	10,000GBX
100/2300	6	6.75e-09	100,000GBX
500/2300	6	0.01055%	500,000GBX
1000/2300	6	0.6755%	1,000,000GBX

Table 1. The probability of tricking the system representing one individual Masternode as failing proof-

The selection of Masternodes is pseudo random based on the Quorum system.

Masternode protocol

The Masternodes are propagated around the network using a series of protocol extensions including a Masternode announce message and Masternode ping message. These two messages are all that is needed to make a node active on the network, beyond these there are other messages for executing a proof-of-service request, PrivateSend and InstantSend.

Masternodes are originally formed by sending 1,000GBX to a specific address in a wallet that will “activate” the node making it capable of being propagated across the network. A secondary private key is created that is used for signing all further messages. The latter key allows the wallet to be completely locked when running in a standalone mode.

A cold mode is made possible by utilizing the secondary private key on two separate machines. The primary “hot” client signs the 1,000GBX input including the secondary signing private key in the message. Soon after the “cold” client sees a message including its secondary key and activates as a Masternode. This allows the “hot” client to be deactivated (client turned off) and leaves no possibility of an attacker gaining access to the 1,000GBX by gaining access to the Masternode after activation.

Upon starting, a Masternode sends a “Masternode Announce” message to the network, containing:

Message: (1K GBX Input, Reachable IP Address, Signature, Signature Time, 1K GBX Public Key, Secondary Public Key, Donation Public Key, Donation Percentage)

Every 15 minutes thereafter, a ping message is sent proving the node is still alive.

Message: (1K GBX Input, Signature (using secondary key), Signature Time, Stop)

After a time-to-live has expired the network will remove an inactive node from the network, causing the node to not be used by clients or paid. Nodes can also ping the network constantly, but if they do not have their ports open, they will eventually be flagged as inactive and not be paid.

Propagation of the masternode list

New clients entering the GoByte network must be made aware of the currently active Masternodes on the network to be able to utilize their services. As soon as they join the mesh network, a command is sent to their peers asking for the known list of Masternodes. A cache object is used for clients to record Masternodes and their current status, so when clients restart they will simply load this file rather than asking for the full list of Masternodes.

Payments via mining and enforcement

To ensure that each Masternode is paid its fair share of the block reward, the network must enforce that blocks pay the correct Masternode. If a miner is non-compliant their blocks must be rejected by the network, otherwise cheating will be incentivized.

Masternodes form quorums, select a winning Masternode and broadcast their message. After N messages have been broadcast to select the same target payee, a consensus will be formed and the chosen block will be required to pay that Masternode.

When mining on the network, pool software (websites that merge the efforts of individual miners) use the RPC API interface to get information about how to make a block. To pay the Masternodes, this interface must be extended by adding a secondary payee to GetBlockTemplate. Pools then propagate their successfully mined blocks, with a split payment between themselves and a Masternode.

To ensure that each Masternode is paid its fair share of the block reward, the network must enforce that blocks pay the correct Masternode. If a miner is non-compliant their blocks must be rejected by the network, otherwise cheating will be incentivized.

PrivateSend

We believe it is important to have a standard trustless implementation for improving privacy of users in the reference client. Other clients such as Electrum, Android and iPhone will also have the same anonymity layer implemented directly and utilize the protocol extensions. This allows users a common experience anonymizing funds using a well understood system.

PrivateSend is an improved and extended version of CoinJoin. In addition to the core concept of CoinJoin, we employ a series of improvements such as decentralization, strong anonymity by using a chaining approach, denominations and passive ahead-of-time mixing. The greatest challenge when improving privacy and fungibility of a cryptocurrency is doing it in a way that does not obscure the entire blockchain. In Bitcoin based cryptocurrencies, one can tell which outputs are unspent and which are not. These are commonly called UTXO, which stands for unspent transaction output. This results in a public ledger that allows any user to act as guarantor of the integrity of transactions. The Bitcoin protocol is designed to function without the participation of trusted counterparties. In their absence, it is critical that auditing capabilities remain readily accessible to the users through the public blockchain. Our goal is to improve privacy and fungibility without losing these key elements that we believe make a successful currency. By having a decentralized mixing service within the currency, we gain the ability to keep the currency itself perfectly fungible. Fungibility is an attribute of money, that dictates that all units of a currency should remain equal. When you receive money within a currency, it should not come with any history from the previous users of the currency or the users should have an easy way to disassociate themselves from that history, thus keeping all coins equal. At the same time, any user should be able to act as an auditor to guarantee the financial integrity of the public ledger without compromising others privacy.

To improve the fungibility and keep the integrity of the public blockchain, GoByte uses an ahead-of-time decentralized trustless mixing strategy. To be effective at keeping the currency fungible, this service is directly built into the currency, is easy to use and safe for the average user.

Tracing CoinJoin by amounts

A common strategy in existing Bitcoin implementations of CoinJoin is simply merging transactions together. This exposes the users to various methods of following the users' coins through these joined transactions.

43	0000000001033c8f9d3c97a642199cd81f6d7453570eab6895210d3ed5abf67	22nd Dec 2017 12:27:01	
Input Addresses		Recipients	
Address	Amount (GBX)	Address	Amount (GBX)
GfH7YUxnepZ88tbkY7Z9gxu87c3yLgT2j5	0.97000000	Gyp5MZ44x65dFMtNL0ewE5kArXmpCq8JyL	0.01000913
GTQVgjBhG9g8vSjBtYyYejGu8a9En6uDq	0.01405927	GazpFNnLzNh5RDTznp3wXQRhXpESu4rp6L	1.22000000
GSEHccBzXwaEFd1EHYVuPw3ZVh8BZSDAh	0.11318657		
GTK3mSchznsLxfaPeYSgohFNBqX6ksLKsd	0.00102766		
GcBsbHDAa2PIYmhqxL1a3KNmeYxdqs4qkp	0.13198743		

Figure 1: An example CoinJoin transaction with 2 users

To identify the source of the money, one simply has to add up the values on the right until they match one of the values on the left. This gets exponentially more difficult as more users are added to the mixer. However, these sessions can be retroactively de-anonymized at any point in the future.

In other proposed implementations of CoinJoin, it is possible that a user anonymizes money then eventually sends change from that transaction to an exchange or other entity that knows the user's identity. This breaks the anonymity and allows the entity to walk backwards through that user's transactions. We call this type of attack "Forward Linking":

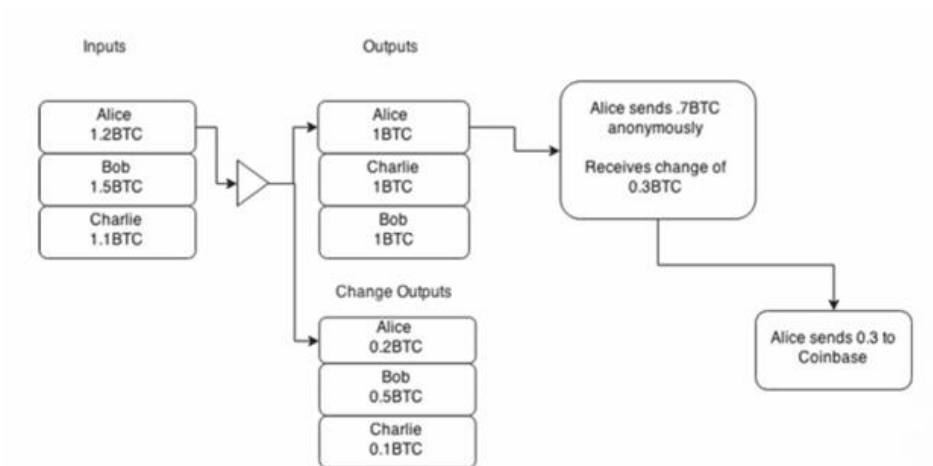


Figure 2: Forward Change Linking

In this example, Alice anonymizes 1.2BTC, which goes to two outputs, 1BTC and 0.2BTC. She then spends 0.7BTC from the 1BTC output, receiving change of 0.3BTC. That 0.3BTC then goes to an identifiable source, confirming Alice also spent the 0.7BTC in the prior transaction.

To identify the sender of the anonymous transaction, start at the "exchange" transaction and go backwards in the blockchain till you get to the "Alice sends 0.7BTC anonymously". As the exchange, you know it was your user who just recently bought something anonymously, thus breaking the anonymity completely. We call this type of attack "Through Change Linking".

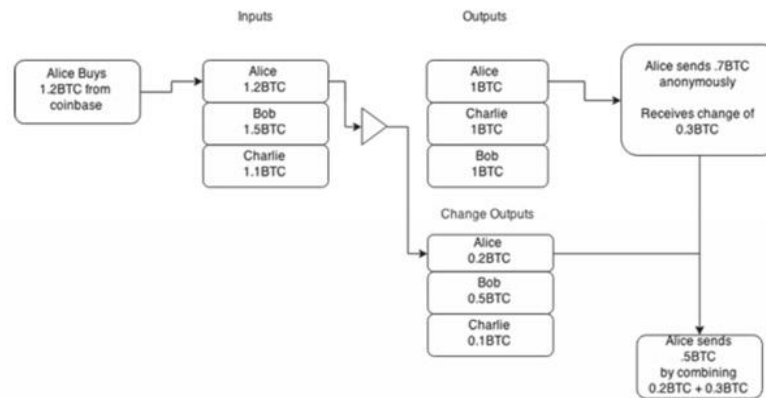


Figure 3: Forward Change Linking

In the second example, Alice buys 1.2 BTC from coinbase , then anonymizes this amount into a 1BTC output. She then spends the 1BTC, receives change in the amount of 0.3BTC and then combines that with her 0.2BTC earlier change.

By combining the change from the anonymous transaction (0.3BTC) and the change she received from the CoinJoin transaction, you can link the entire history before and after, completely breaking the anonymity.

Improved privacy and denial-of-service (DOS) resistance

PrivateSend uses the fact that a transaction can be formed by multiple parties and made out to multiple parties to merge funds together in a way where they cannot be uncoupled thereafter. Given that all PrivateSend transactions are setup for users to pay themselves, the system is highly secure against theft and users coins always remain safe. Currently to mix using PrivateSend requires at least three participants.

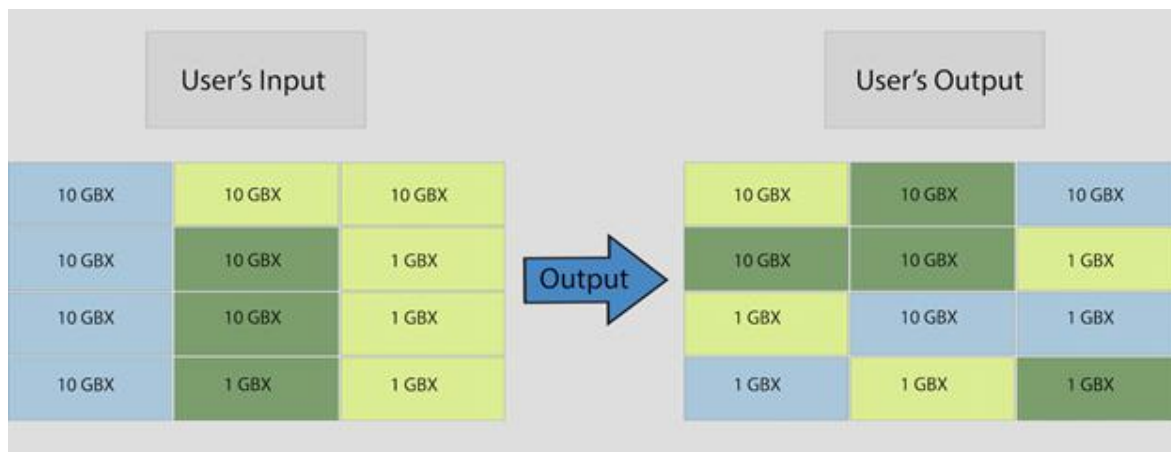


Figure 4: Forward Change Linking

To improve the privacy of the system as a whole we use common denominations of 0.1GBX, 1GBX, 10GBX AND 100GBX. In each mixing session, all users should submit the same denominations as inputs and outputs. In addition to denominations, fees should be removed from the transactions and charged in bulk in separate, sporadic unlink able transactions.

To address possible DOS attacks, all users submit a transaction as collateral to the pool when joining. This transaction will be made out to themselves and will pay a high fee to miners. In the case when a user submits a request to the mixing pool, they must provide collateral at the beginning of this exchange. If at any point any user fails to cooperate, by refusing to sign for example, the collateral transaction will automatically be broadcasted. This will make it expensive to do a sustained attack on the privacy network.

Passive anonymization of funds and chaining

PrivateSend is limited to 1,000GBX per session and requires multiple sessions to thoroughly anonymize significant amounts of money. To make the user experience easy and make timing attacks very difficult, PrivateSend runs in a passive mode. At set intervals, a user's client will request to join with other clients via a Masternode. Upon entry into the Masternode, a queue object is propagated throughout the network detailing the denominations the user is looking to anonymize, but no information that can be used to identify the user.

Each PrivateSend session can be thought of as an independent event increasing the anonymity of user's funds. However, each session is limited to three clients, so an observer has a one in three chances of being able to follow a transaction. To increase the quality of anonymity provided, a chaining approach is employed, which funds are

Depth Of The Chain	Possible Users (n) ^r
2	9
4	81
8	6561

Table 2. How many users could possibly be involved in N mixing sessions.

Security considerations

As transactions are merged, Masternodes can possibly "snoop" on users' funds as they pass through. This is not considered a serious limitation due to the requirement for Masternode's to hold 1,000GBX and the fact that users utilize random Masternodes that they select to host their joins. The probability of following a transaction throughout a chaining event can be calculated as follows:

Attacker Controlled Masternodes / Total Masternodes	Depth Of The Chain	Probability of success $(n/t)^r$	GoByte Required
10/1010	2	9.80e-05	10,000GBX
10/1010	4	9.60e-09	10,000GBX
10/1010	8	9.51e-11	10,000GBX
100/1100	2	8.26e-03	100,000GBX
100/1100	4	6.83e-05	100,000GBX
100/1100	8	4.66e-09	100,000GBX
1000/2000	2	25%	1,000,000GBX
1000/2000	4	6.25%	1,000,000GBX
1000/2000	8	0.39%	1,000,000GBX
2000/3000	2	44.4%	2,000,000GBX
2000/3000	4	19.75%	2,000,000GBX
2000/3000	8	3.90%	2,000,000GBX

Table 3. The probability of follow a PrivateSend transaction on the network given the attacker controls N Nodes.

Where:

n is the total number of nodes controlled by the attacker t is the total number of Masternodes in the network

r is the depth of the chain

The selection of Masternodes is random.

Considering the limited supply of GBX (943 thousands at the time of writing, March 2018) and the low liquidity available on the market, it becomes an impossibility to attain a large enough number of Masternodes to succeed at such an attack.

Extending the system by blinding Masternodes to the transactions taking place on their node will also greatly enhance the security of the system.

Masternode blinding via relay system

We previously described the probabilities of following a single transaction through multiple sessions of PrivateSend mixing. This can further be addressed by blinding Masternodes, so they cannot see which inputs/outputs belong to which users. To do this we a simple relay system has been implemented that users can use to protect their identity.

Instead of a user submitting the inputs and outputs directly into the pool, they will pick a random Masternode from the network and request that it relays the inputs/outputs/signatures to the target Masternode. This means that the Masternode will receive N sets of inputs/outputs and N sets of signatures. Each set belongs to one of the users, but the Masternode can't know which belongs to which.

Instant transactions via InstantSend

By utilizing Masternode quorums, users are able to send and receive instant irreversible transactions. Once a quorum has been formed, the inputs of the transaction are locked to only be spendable in a specific transaction, a transaction lock takes about four seconds to be set currently on the network. If consensus is reached on a lock by the Masternode network, all conflicting transactions or conflicting blocks would be rejected thereafter, unless they matched the exact transaction ID of the lock in place.

This will allow vendors to use mobile devices in place of traditional POS systems for real world commerce and users to quickly settle face-to-face non-commercial transactions as with traditional cash. This is done without a central authority. An extensive overview of this feature can be found in the InstantSend white paper.

GoByte Point of Sale(POS) terminals specification

The POS Terminal has a magnetic card reader that supports 1/2/3 magnetic track bi-directional reading, high coercivity magnetic card reading, supports ISO 7810 ISO7811-1,2,3,4,5,6 ISO7813 standard magnetic card reading and supports 0.1m/s 1m/s swiping card speed.

For the IC Card Reader, the terminal supports 3V or 5V card and ISO7816CPU card, conform to PBOC and EMV standards.

The Contactless Card Reader, which is optional for the merchants, has the following specifications: 13.56MHZ support type A/B, mifare one card.

The SAM Card Reader: One piece, conform to ISO7816 standard.

We rely on the QR codes in order to ease the copy-pasting of the address and amount needed to be sent, so the terminal will have a built-in 1D/2D barcode reader.

As from communication point of view, the terminal will use GPRS connectivity.

As for the battery and size, the terminal will have a built-in rechargeable lithium battery: 7.4V 2600mAH and should be around 186.5 mm X 80.6 mm X 52.3mm in size.

Certifications that the terminal own are:

- CCC cert, Telecom access cert.
- EMV/PBOC 3.0 level1 & level2 cert.
- PBOC 3.0 non-contact level1 & level2 cert.
- PIN input device security certification
- UnionPay direct connect POS application test
- UnionPay network cert.

For CPU and Memory, a high performance 32-bit security processor and 8MB large capacity memory will be used.

So, by creating a Crypto card for the Crypto world that is able to operate inside the Crypto world only should be a huge step ahead for GoByte and Crypto world.

The expected price of the POS Terminal is around 150 USD, without the shipping fees, and the expected supply should be of around 150000 Pieces per Month.

The supported languages should be English, Spanish, Portuguese, French, German, Polish, Japanese, Russian or according to your request.

The merchants will not pay any installation/customization fee, except the POS Terminal price & shipment fee, the installation of the "Pay" module and any update or customization will be supported by the GoByte Network team.

The won't be any minimum or maximum amount to order.

The Terminal can be bought with GoByte Tokens only.

So, we hope that this way we will provide an easy way for physical merchants to accept payments on the go, from restaurants to cloth stores also to allow us the creation of our own Crypto cards for the GoByte Network.

GoByte premine

Distribution

- Total premine: 850 000 GBX
- We allocated for masternode auctions and paid advertising, an amount of 150 000 GBX
- We allocated for bounties and events, an amount of 30 000 GBX
- We allocated for further development and growth of GoByte's Network, an amount of 570 000 GBX
- We allocated for developer's personal use, an amount of 100 000 GBX

Important premine movements

- 18th Nov 2017 – First GoByte masternodes auction
- 19th Nov 2017 – Second GoByte masternodes auction
- 19th Nov 2017 – CoinsMarkets Listing
- 19th Nov 2017 – Mnrank.com Listing
- 21st Nov 2017 – Masternode.online Listing
- 21st Nov 2017 – Masternodes.pro Listing
- 25th Nov 2017 – Cryptopia Listing
- 04th Dec 2017 – CoinExchange Listing
- 11st Jan 2018 – HitBTC Listing

Additional improvements

NeoScript hashing algorithm

In the life cycle of Bitcoin, mining began with hobbyists which used Central Processing Units (CPUs) to mine the currency, then shortly after Graphical Processing Units (GPUs) software was created, which quickly replaced the CPUs. Years after the GPUs cycle, ASICs or Application Specific Integrated Circuits were created, which quickly replaced the GPUs.

Due to the complexity and die size required to create an ASIC for mining NeoScript, we expect that it will take considerably longer than it did in Bitcoin, allowing for hobbyists to take part in the mining for a longer period of time. We believe this is highly important for good distribution and growth of a cryptocurrency.

Another benefit of the chaining hashing approach is high end CPUs give an average return similar to that of GPUs. Also, GPUs have been reported to run 30-50% cooler, with less wattage than the Scrypt algorithm used by most current cryptocurrencies.

Mining supply

A different approach to restricting the in ation of mining is taken in GoByte, using a 15% reduction of the supply per year. This is done instead of the halving implemented by other currencies. In addition, supply of each block is directly tied to the number of miners on the network; more miners results in lower mining rewards.

Production of GoByte is scheduled to carry on throughout several years, slowly grinding down until finally near the year 2243, when production will cease.

Proof of Work

The GoByte network will rely on a Proof of Work consensus algorithm. As mentioned previously, Proof of Work is the process by which miners, individuals who dedicate their computational resources to solve difficult mathematical challenges, prove that they have done the necessary work required by the network to validate blocks, which are data containers for a large list of new transactions. It is referred to as a consensus algorithm because a majority of overall mining processing power is needed in order to enforce any new protocol update proposal.

To motivate miners to participate in the mining process and cover their costs, the first miner to find a new block is compensated for their efforts. This introduces an element of economic competition between miners and prevents the network from being attacked as attacks become too costly and thus, economically unviable. As GoByte uses the ASIC-resistant NeoScript Algorithm previously mentioned, any party can participate in the mining process regardless of their device type and hardware capabilities, which prevents the concentration and centralization of decision-making power in the hands of the few and enables a true democratic process.

GoByte's block time is set at 150 seconds, meaning the network aims for blocks to be created every 150 seconds. This aim is facilitated by what is known as a difficulty retargeting algorithm, which increases or decreases the difficulty of finding a block in proportion to the total hashing rate (processing power) being contributed to the network. If, for example, the hashing rate suddenly doubles, the difficulty will increase to ensure that blocks are not recovered every 30 seconds and vice versa. This is of extreme importance as we have witnessed the danger of a frozen blockchain with Bitcoin, whose retargeting algorithm adjusts every 2016 blocks, or every 14 days at 10 minutes per blocks. This means that if mining power suddenly drops (due to lowered mining profitability for instance), it will take the network two weeks to lower the difficulty accordingly, during which time the blockchain could grind to a halt. To prevent this from happening, GoByte's algorithm adjusts the difficulty level every block, or every 150 seconds.

As we have seen, the risks of high inflation and its devaluing implications on national currencies, GoByte attempts to reverse this trend by offering an ever-decreasing emission rate, which ensures it remains a disinflationary currency in nature. This was designed to preserve and protect GoByte's innate coin value. Please refer to the table below to see GoByte's coin emission schedule per stage (or Epoch); the distribution of miners' rewards vs. masternode operator rewards are listed next to each stag.

Reward Allocation or PoW Block Rewards (starting on November 16th, 2017 | for 7 years):

Block 2 – 207360	15	Masternodes 50% / Miners 50%
Block 207360 – 414720	12.75	Masternodes 55% / Miners 45%
Block 414720 – 622080	10.8375	Masternodes 60% / Miners 40%
Block 622080 – 829440	9.211875	Masternodes 65% / Miners 35%
Block 829440 – 1036800	7.83009375	Masternodes 70% / Miners 30%
Block 1036800 – 1244160	6.6555796875	Masternodes 75% / Miners 25%

On Block 1 (Genesis Block), 850,000 GoByte were created (premine) in order to set up 3 masternodes and support and stabilize the GoByte network (at 1,000 GoByte per node collateral). These are scheduled to be used later in 2018 and will not be used in any other way than helping the further development of the GoByte Network.

Lastly, block maturity is defined as the minimum age of a block, in terms of blocks rather than standard time units, before it is safely considered to be part of the chain. The logic behind this is that since each block validates all of its predecessors, the more blocks are added on top of a block, the more valid and safe for consideration it becomes. The standard block maturity for Bitcoin is 101 blocks. While GoByte's block maturity is set at 111 blocks, given GoByte's far quicker block time at 2.5 minutes, a block can be considered mature in under 5 hours, giving the network a very solid foundation for security references.

Dark Gravity Wave

DGW or Dark Gravity Wave is an open source difficulty-adjusting algorithm for Bitcoin-based cryptocurrencies that was first used in Darkcoin/Dash and has been adopted by other digital currencies.

DGW was authored by Evan Duffield, the developer and creator of X11/Darkcoin/Dash, as a response to a time-warp exploit found in Kimoto's Gravity Well.

In concept, DGW is similar to Kimoto Gravity Well, adjusting the difficulty levels every block (instead of every 2016 blocks like Bitcoin) by using statistical data of the last blocks found. In this way block issuing times can remain consistent, despite high fluctuations in hash power. However, it doesn't suffer from the time-warp exploit.

Version 2.0 of DGW was implemented in Darkcoin/Dash from block 45,000 onwards in order to completely alleviate the time-warp exploit.

Version 3.0 was implemented on GoByte from block 700 on November 17 of 2017 to further improve difficulty re-targeting with smoother transitions. It also fixes issues with various architectures that had different levels of floating-point accuracy through the use of integers.

NeoScript algorithm

Password based key derivation function (KDF) is a deterministic algorithm used to derive a cryptographic key from an input datum known as a password. An additional input datum known as a salt may be employed in order to increase strength of the algorithm against attacks using pre-computed hashes also known as rainbow tables. The derived key length may be specified usually, and one of the most popular uses of KDFs is key stretching. It increases effective length of a user password by constructing an enhanced key to provide with a better resistance against brute force attacks. Another popular use is password storage. Keeping user passwords in unencrypted form is very undesired as it may be possible for an attacker to gain access to the password file and retrieve the passwords stored immediately. Brute force attacks may be the only possible approach against strong KDFs. This kind of attack can be parallelized usually to a great extent. High requirements on computational resources such as processor time and memory space allow to reduce parallelization efficiency and keep these attacks expensive far beyond reasonable limits.

As the name suggests, NeoScript is a further development of Script as described in Percival. It is aimed at increased security and better performance on general purpose computer hardware while maintaining comparable costs and requirements. This document focuses on functional differences between NeoScript and Script.

Script specification

The most popular implementation of Script employed by many cryptocurrencies since 2011 is $N = 1024, r = 1, p = 1$ abbreviated usually to (1024, 1, 1). N is the primary parameter defining number of memory segments used and must be a power of 2. May be also described through N_{factor} .

$$N = (1 \ll (N_{factor} + 1)) \quad N_{factor} = \text{lb}(N) - 1$$

The default memory segment size for the 32-bit implementation is 128 bytes. r is the segment size multiplier. p is the computational multiplier. They may be also described through r_{factor} and p_{factor} respectively.

$$r = (1 \ll r_{factor}) \quad p = (1 \ll p_{factor})$$

A single instance of Script utilises $(N + 2) * r * 128$ bytes of memory space, i.e. 128.25Kb for the (1024, 1, 1) configuration. Actual data mixing in memory is performed by Salsa20, a stream cipher introduced by Bernstein. A reduced strength 8-round implementation has been chosen (Salsa20/8). Every run of the Script core engine executes it $4 * r * N$ times, i.e. 4096 times for the (1024, 1, 1) configuration. Every execution of Salsa20 mixes one half of a memory segment with itself.

The Script core engine has no provisions for key stretching or compressing as well as salting, therefore additional cryptographic functions need to be deployed. In case of cryptocurrencies, a typical configuration operates with 80 bytes of input data (block header) which is also a salt. It is passed to PBKDF2, a password based KDF capable of deriving variable length keys with salting. It works with SHA-256, a cryptographic hash function delivering digests up to 32 bytes in size through 64 internal rounds. It doesn't support keyed hashing, therefore a pseudorandom function (PRF) such as HMAC is required, and the whole big-endian construction may be called PBKDF2-HMAC-SHA256. It feeds $r * 128$ bytes of derived data to the Script core and receives it back after mixing to be used as a salt for another PBKDF2-HMAC-SHA256 run which compresses 80 bytes of input data into 32 bytes of hash.

NeoScript specification

Although a very innovative design when launched, Scrypt has developed certain vulnerabilities. The first announced differential cryptanalysis of Salsa20/8 by Tsunoo in 2007 did not deliver any advantage over 256-bit brute force attack, but the following research by Aumasson reduced time complexity to break it from 2255 to 2251 with 50% success probability. It was improved by Shi in 2012 to 2250. Although this is not critical yet, better attacks on Salsa20/8 may be developed in the future.

PBKDF2 is a very popular KDF and may be configured to require considerably large amounts of processor time, but it does not require complex logic or significant amounts of memory to operate. Therefore, brute force attacks can be carried out on general purpose hardware such as GPUs or custom designs (ASICs) with reasonably low costs. SHA-256 also allows numerous performance optimisations in this context. It is also worth to mention that Scrypt relies very little on PBKDF2- HMAC-SHA256 strength as it is configured to run in the fastest 1-iteration mode even though 1000-iteration minimum advised in general.

NeoScript addresses these issues. The core engine is configured to employ non-reduced Salsa20 of 20 rounds (Salsa20/20) as well as non-reduced ChaCha20 of 20 rounds (ChaCha20/20). Both of them are used to produce the final salt as their outputs are XOR'ed into it. They may be configured to run either in series or parallel depending on application objectives. The default NeoScript configuration is (128, 2, 1). A single instance of NeoScript utilises $(N + 3) * r * 128$ bytes of memory space, i.e. 32.75Kb, in series mode or $(2 * N + 3) * r * 128$ bytes, i.e. 64.75Kb, in parallel mode. Every run of the NeoScript core engine executes Salsa20/20 and ChaCha20/20 1024 times each which might seem inferior to 4096 times of Salsa20/8 of the Scrypt core engine. However, NeoScript operates with double the memory segment size requiring larger temporal buffers, also with higher round count of each stream cipher iteration as explained above. If approximated to abstract load/ store units, NeoScript is 1.25 times more memory intensive than Scrypt. There are no known successful attacks on non-reduced Salsa20 and ChaCha20 other than exhaustive brute force search.

NeoScript replaces SHA-256 with BLAKE2s which is a further development of BLAKE-256 [10], one of 5 NIST SHA-3 contest finalists. Based upon ChaCha20, operates with a lower round count of 10, supports keyed hashing, is native little endian and faster significantly than SHA-256 and even BLAKE-256. It could be interfaced directly to PBKDF2 with no need of HMAC. However, PBKDF2 constructs derived keys using blocks. It means a minor change in an input datum, such as nonce increment, may not result in an entirely different derived key. A replacement KDF has been developed to address this issue.

FastKDF is a buffered password based KDF which also supports salting. It operates with 2 primary buffers for password and salt each. They must be a power of 2 in size and not less than any input (password, salt) or output (derived key) data. The default configuration works with 256-byte buffers. Password and salt are loaded initially into these buffers in a repetitive manner until the end of buffer is reached. The salt buffer is modified through operations while the password buffer remains constant. The buffer pointers are set to zero (start) on the first run. When a PRF chosen delivers a digest, a sum of all its bytes modulo buffer size defines the next buffer pointer. The digest is XOR'ed into the salt buffer at the new buffer pointer and the next iteration starts. If a read or write operation goes past a buffer end, it is continued from the buffer start. BLAKE2s is configured to operate with 64-byte input (password), 32-byte key (salt) and 32-byte output (digest). When the final FastKDF iteration is completed, the password buffer using zero buffer pointer is XOR'ed into the salt buffer using the last buffer pointer to produce the derived key of length required which is copied into the output buffer. FastKDF-BLAKE2s is configured to run through 32 iterations by default. It is little endian for easier deployment and additional minor performance advantage on popular general-purpose computer hardware.

Atomic swaps

We regard the explosive growth of the cryptocurrency space to be indicative of a growing market-wide demand for decentralized and economical solutions across a multitude of industries. As a result, over the past few years, cryptocurrency projects have emerged tending to specific niches, industries and utility sets. These range from agriculture, construction, health, banking, law, manufacturing, energy, communication industries and others. Rather than hold the belief that there will be one single coin to rule them all, we view the current landscape as rapidly and divergently evolving.

With this in mind, instead of restricting a users choice of currency, we have decided to accommodate their broad desire by introducing the Atomic Swaps mechanism. An Atomic Swap is the process by which user A who owns coin X can exchange their coin with user B owning coin Y both having separate blockchains, in a fast, secure and trustless way. Once an exchange rate is agreed upon by both parties, a cross- chain swap takes place. It's the decentralized world's equivalent of over-the-counter («OTC») trades as they don't require a 3rd party. Furthermore, atomic swaps have the added benefit of utilizing a very specific type of smart contract, being hash and time lock. This means that user A sends their funds to a certain address which then locks up the funds. If user B then fails to come through by a certain agreed upon time, the funds are unlocked, the transaction is reversed by the blockchain and user A gets their funds back.

In our implementation of Atomic Swaps, we wish to take the concept further and make it a component of a payment transaction. Rather than limiting users paying for something using GoByte Pay to just GBX, our goal is to create a seamless method for a shopper that has ETH to be able to purchase from a GoByte merchant by connecting their wallets and creating a swap with other users or a GoByte bank in real time.

Atomic Swaps will be implemented in the near future.

In order to perform an on-chain atomic swap between two cryptocurrencies, there are several prerequisites to factor in. Both chains must support:

- Branched transaction scripts
- The same hashing algorithm
- Signature checks for transaction scripts

On-Chain atomic swaps are mostly useful in cases where users want to perform an exchange that is characterized by a larger trade that is not subject to a particular time constraint. Since the process involves on-chain transactions, the speed of the process is bound by the mining or staking of blocks on both chains, and the slower of the two at that. This can take roughly an hour when transacting with the Bitcoin blockchain. Additionally, users must pay transaction fees for both the swap and the redemption transaction on each chain, which can have a non-trivial cost with Bitcoin.

Furthermore, since these swaps are on-chain, there are some privacy implications that users should be aware of. The swap transaction on each chain include the same hashed value, meaning that anyone who surveils on the corresponding blockchains can link the coins on one side of the swap to the coins on the other side. Further down the road, GoByte will implement solutions for off-chain transactions that will eliminate the concerns outlined above.

Security analysis

A vital assumption in proof-of-stake models is assuming honest nodes hold at least 51% stake and are online and participating in staking. This is also required in the security analysis.

Follow the correct chain
Building on next block

Honest nodes should always build upon the latest valid block containing the lowest weighted value from hash-chain A. Usually this will result in a chain composed of blocks containing consecutive winning hash-chain A weighted reveal values. In practice the node implementation currently uses a matrix of received blocks (a buffer) which sits in memory and is x blocks in length, sat atop the chain.

Buffer rules

1. Always build upon block sequence with consecutive lowest adjusted hashchain A value whilst in the buffer (x blocks deep) - this may result in nodes discarding later blocks in the buffer and building upon a 'stronger' but shorter chain on occasion when a block arrives late
2. New blocks arriving deeper than x are ignored.

Fork rules

True chain forks may only occur which are more than x blocks deep and less than y blocks from the current blockheight (assuming signatures are correct on both sides of the fork), where x is the length of the buffer and y is the number of blocks of replay attack protection offered by B set of hash-chains.

1. For a fork (deeper than x , above y blocks) choose the side of the fork with the most cumulative stake in the reveals in the blockheader of each block. Nodes should not consider forks: deeper than y , which cross an epoch transition, or which grow the chain forward into the future fraudulently (assessed by NTP-corrected blockheader timestamps).
2. New stakers should always build on top of the chain with highest stake score as per 1.

Double spend

Conventional double spending attempts may occur by displacing one transaction with another different transaction which is confirmed earlier into a block. To give certainty that the transaction history of the chain may not change by a fork up to depth y blocks, it is necessary then to wait for y confirmations.

Nothing at stake

When a fork happens, honest nodes should build on top of the strongest chain by sequence of stake-weighted hash-chain A reveal. However, there is no theoretical reason for nodes to not also try to build on top of weaker permutations. As new blocks require signatures from winners, it is possible for the whole network to see a node trying to build on top of a wrong chain. It is possible to put a penalty on this, for example all coins of that attacker can be transferred to all honest nodes, creating an incentive to behave honest but also another incentive to participate in staking. The authors feel this attack is theoretical as honest node behaviour in the event of two reveal votes arriving from a particular stake validator is to discard the second vote automatically.

Long range attacks / Hash replay attack

In this case, an attacker tries to make a completely different fabricated chain in his favour from an earlier blockheight.

This will be non-trivial to achieve for the following reasons:

1. The attacker must create a chain to the current blockheight with valid winning blocks (each containing a valid XMSS signature of the blockheader from the victorious stake validator).
2. As the epoch progresses the hash indexes of earlier hash-chain A reveals are known by the network. To prevent earlier stake validator votes being replayed to falsely demonstrate stake validator support for the attacker fork, a second reveal hash for each validator (hash-chain B reveal hash) must also be supplied. Given we set a reorg limit of y blocks we can be sure that this strategy is unlikely to succeed. The only mitigation the attacker can achieve is to remove stake validator reveal votes he is unable to replay into the forged block - but this will result in less total amount of committed stake per block, which in turn means honest nodes will continue to follow the correct/ original chain during a fork recovery process.

As the honest nodes will accept a fork less than x blocks deep, the attacker wants to construct a fork of at least x blocks deep. Furthermore, he needs to win each block honestly for two reasons: to get more cumulative stake weight and to be able to construct a valid signature, as he does not get that from other winners. Assuming the attacker has about 50% stake (this means we assume the strongest attacker possible), his probability of winning all x block equals $(1/2)^x$. Having the correct hash reveal of chain B, which we take 50 chains, of k stakers, equals at most $x50k$. So the total success probability of attacking the chain and «stealing» the hash-reveals of an honest staker equals

By taking $x = 10$ blocks deep buffer and only $k = 10$ stakers, we get a success probability of 2^{-33} . In other words, the attacker has to compute 233 hashvalues (similar to mining) to get a correct malicious blockchain. This will take significant amount of time on current computers. On top of that, the honest chain will also move forwards, which means he needs to do this attack faster than one new block creation. We do not see this possible. In the future, both value x and number of chains in set B can be increased easily for improved security.

Block withholding attacks

A block withholding attack is an attack in which the block winner does not reveal that he won the block, but withholds it to his advantage instead. A block withholding attack in our protocol cannot occur by keeping the block more than x blocks, as after that no reorg changes are allowed to the main chain which then becomes immutable. Withholding a winning reveal hash costs the attacker the block reward of the block. Furthermore, our protocol instructs nodes which believe they are close to the winning vote to also produce blocks which may be selected if the true winner fails to construct a block in a timely manner.

Pre-mining (of hash-chain A)

You might think that someone can pre-mine his hash-chain to get highest probability of winning a block. However, there are two main reasons why this fails. Since the initial seed S_0 is constructed by using randomness of all participants, no attacker can account for what this seed will be. This means an attacker cannot know how to optimize his hash-chain to win the most blocks. Furthermore, as the seed S_j is updated for each block j , an attacker cannot look further than one block, which is the same behaviour as in proof-of-work.

References

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Available at: <https://bitcoin.org/en/developer-reference#block-headers>

Crosby, M., Nachiappan, Pattanayak, P., Verma, S., et al., 2015. BlockChain technology. Available at: <http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>

Kiraly, B., 2017a. InstantSend. Available at: <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146928/InstantSend>

Kiraly, B., 2017b. PrivateSend. Available at: <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/1146924/PrivateSend>

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Available at: <https://bitcoin.org/bitcoin.pdf>

Okupski, K., 2016. Bitcoin developer reference., pp.3–4. Available at: https://lopp.net/pdf/Bitcoin_Developer_Reference.pdf

Strophy, 2017. Understanding sporks. Available at: <https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks>

Wiecko, R., 2017. Dash instamine issue clarification.

Available at: <https://dashpay.atlassian.net/wiki/spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification>

Jakiman, 2017. PIVX purple paper. Available at: <https://pivx.org/wp-content/uploads/2017/03/PIVX-purple-paper-Technincal-Notes.pdf>

John Doering, 2014. NeoScript,a Strong Memory Intensive Key Derivation Function Available at http://phoenixcoin.org/archive/neoscript_v1.pdf

