



The Pirate Chain Code

V2.0

By: Draeth, FishyGuts, Flexatron, jl777, KOSIUS & ARRR/KMD Community



Abstract

A fully private cryptocurrency and shielded blockchain originating from the Komodo ecosystem. Pirate solves Zcash's "fungibility problem" through the elimination of transaction functionality to transparent addresses in its blockchain, making private usage "fool-proof". This feature results in a fully shielded user coin base in Pirate Chain. By consistently utilizing zk-SNARKs technology, Pirate leaves no usable metadata of user's transactions on its blockchain. All outgoing transactions other than mining block rewards and notary transactions are sent into shielded *Sapling* addresses maximizing the efficiency and speed of its chain. Pirate utilizes the consensus algorithm Equihash proof-of-work originating from Zcash, with an added security layer of delayed proof-of-work from Komodo which provides a higher than BTC-grade level of security to the Pirate blockchain. The future of private decentralized payments is here.

Table of contents

The Pirate Chain Code.....	5
Mission Statement.....	5
Value propositions.....	5
Why focus on privacy?.....	5
The Team.....	6
Introduction.....	7
Cryptocurrencies	7
Privacy.....	7
Main drawbacks illustrated of current decentralized payment protocols	7
Monero Ring CT Signatures scheme	7
Zcash’s shielded addresses implementation and spend types	9
Our solution	10
Pirate Chain: Privacy, fungibility and security	11
29 th of August 2018 - The call for full anonymity	11
Komodo – Zcash fork – zk-SNARKs	11
Komodo Asset chains.....	11
Forced z-transactions.....	11
Delayed Proof-of-Work: Maximum security and flexibility	12
What is delayed Proof-of-Work?.....	12
What are the mechanics behind delayed Proof-of-Work?	13
Examples of attacks on blockchains	14
Sapling integration and activation.....	15
Sapling integration	15
The migration to Sapling.....	15
Emission scheme and technical characteristics	16
TOR support	17
Centralized exchanges support	17
Roadmap	18
The Pirate Chain Guide	19
Official Website	19
Buy and Trade Pirate Chain.....	19
Social media	19
Coin Statistics Websites	20

Source code	20
Wallets	20
References.....	21

The Pirate Chain Code


Mission Statement

The mission of Pirate Chain is to preserve people's financial privacy in a system dominated by transparent transactions, to ensure their financial freedom.


Value propositions

 *All Pirate Chain transactions are private by default.*


This alleviates the fungibility problems that many cryptocurrencies with optional privacy introduce into their protocol. This complete privacy protocol provides users with more assurance that no authorities are able to claim that user's funds are "tainted" due to previous transactions, now and in the future.

 *Pirate Chain is fully decentralized.*

There is no third party in charge of your funds at any time. Private transactions are confirmed in a trustless manner on the blockchain meaning you do not need a third party to verify that your transactions are valid, the pirate code takes care of that.

 *Pirate Chain allows for secure and quick transfer of value.*

Pirate Chain is secured by a mechanism harder to crack than bitcoin, called delayed Proof-of-Work (dPoW). Usage fees are very inexpensive for both the customer and the vendor. Furthermore, there is no chance for fraudulent chargebacks, no erroneous fund verification periods, and transactions are confirmed and secured within minutes. These features alone can save merchants and vendors across the globe billions of dollars by cutting out facilitation fees.

 *Pirate Chain uses the strongest privacy protocol.*

The highly advanced and respected privacy protocol zk-SNARKs doesn't require the data from your transaction to be viewable on the public ledgers. This is considered by many prominent developers to be one of the strongest methods of hiding your financial data on the blockchain

Why focus on privacy?

Crypto offers advantages to users and business, but this shouldn't come at the cost of financial privacy.

Today's FIAT currencies are already making a mass exodus towards digital systems (Japparova en Rupeika-Apoga 2017). Crypto has shown to offer numerous advantages for business such as cost-savings in fees and transaction speed. In our opinion, users deserve privacy in those transactions.

Why show the owner of the shop the size of your wealth or spending habits?

Financial privacy may therefore be needed by all parties that want to accept cryptocurrency such as vendors, distributors, merchants, purchasers, suppliers, service providers and customers. Businesses can assure their clients and themselves that both parties to the transaction will receive the best combination of privacy, speed and cost-savings through using Pirate.

The Team

Being a truly decentralized cryptocurrency, Pirate welcomes developers and contributors of all skillsets.

Already over 100 contributors have provided services to the growth and development of Pirate Chain since its infancy, whether it be coding, marketing, development of partnerships or various other aspects. Developers are working in a coherent team fashion to bring in knowledge and experience from all parts of the crypto-sphere. With our diverse group, there is always a person with the knowledge of how to complete a needed task, or someone with a connection to someone who can.

Pirate has completed many first time accomplishments in the cryptocurrency industry when it comes to privacy protection (see Roadmap) and Pirate will continue to work with third parties on innovative techniques to facilitate stronger privacy for all.

Introduction

Cryptocurrencies

Since the release of the famous whitepaper written by Satoshi Nakamoto in 2008 (Nakamoto 2008), Bitcoin has grown into a multi-billion dollar market cap digital asset. A number of alternative cryptocurrencies have spawned since then attempting to fill the void of a plethora of use-cases, with their own respective communities. Using cryptocurrencies as a means of payment is one of the most popular use-cases and also the main purpose for which Satoshi wrote the whitepaper. The goal of Bitcoin is to enable every person to transfer value anywhere in the world at any time instantly using an internet connection in a peer-to-peer, trustless fashion. Bitcoin utilizes a distributed ledger to facilitate and record transactions of which the truthfulness is determined through the consensus algorithm Proof-of-Work (PoW).

Privacy

One large concern about the usage of this technology is the ability of observers to analyze your spending behavior and wealth status (Moser 2013). This greatly compromises the financial privacy of the user. A number of cryptocurrency protocols have been developed that seek to improve on the privacy aspects of Bitcoin. The most notable protocols that have been developed thus far are CryptoNote (Van Saberhagen 2013) and Zerocash (Sasson et al. 2014). The first protocol utilizes Ring Confidential Signatures while the latter uses zero-knowledge proofs to obfuscate transactions and account balances, more in detail on that later. Both protocols have their advantages and disadvantages. This whitepaper addresses how Pirate (ARRR) attempts to improve on the privacy aspects of current decentralized payment protocols.

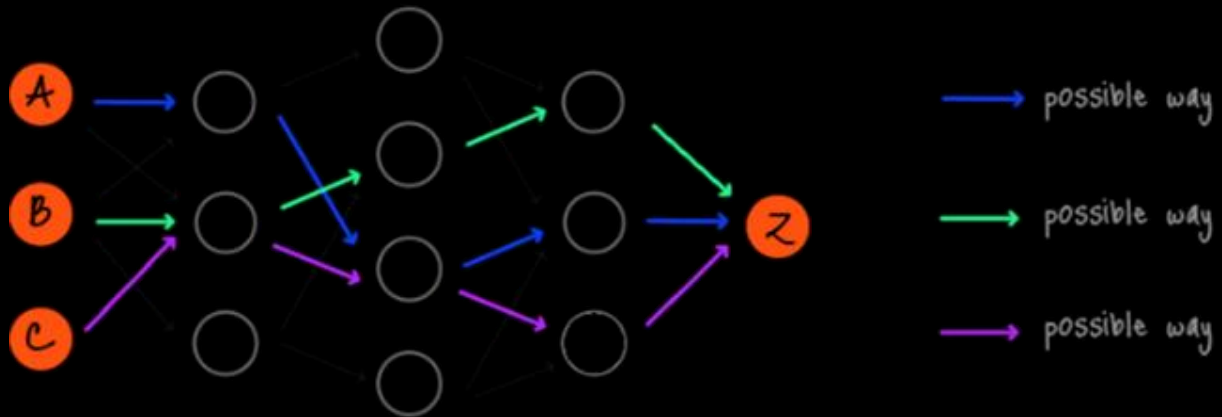
Main drawbacks illustrated of current decentralized payment protocols

Monero Ring CT Signatures scheme

Monero, a fork of Bytecoin based on the CryptoNote protocol, utilizes a Ring Signature scheme in their transactions combined with stealth addresses, random one-time addresses for every transaction on behalf of the recipient. Ring signatures make it increasingly difficult to trace back the sender depending on the ring size. However, this leaves the ability of parties to analyze the available data with sophisticated analytic tools right now and in the future.

Due to its use of ring signatures, analysis of Monero's blockchain is difficult, as seen in Figure 1.

Figure 1 Ring signature blockchain analysis. Source: <https://cryptonote.org/inside#untraceable-payments>



The difficulty of finding the correct sender is increasingly difficult with bigger ring sizes. The ring size is the total number of possible signers including yours, which in turn determines the complexity and difficulty of finding the “real output”. A higher ring size number thus provides a higher level of privacy than a lower number. However, it's not advised to reuse an odd recognizable ring size number to prevent standing out from other transactions [3].

The fundamental problem of coin mixing methods though is that transaction data is not being hidden through encryption. RingCT is a system of disassociation where information is still visible in the blockchain. Mind that a vulnerability might be discovered at some point in the future which allows traceability since Monero's blockchain provides a record of every transaction that has taken place.

Zcash's shielded addresses implementation and spend types

Zcash, an implementation of the decentralized anonymous payment scheme Zerocash, adds a shielded payment scheme secured by zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) to the existing transparent payment scheme used by Bitcoin (Hopwood et al. 2016). The usage of shielded or non-shielded payments is free to choose by the user. The percentage of shielded transactions is assumed to rise as Zcash's recent implementation of "Sapling" makes processing shielded transactions only a fraction more computationally intensive than non-shielded transactions (Bowe 2017). Unfortunately, the relative high percentage of non-shielded transactions and balances impairs the fungibility of the coins, as it is possible to link transactions during "private" payment activity and thus possibly relate them to coin mixing. This is especially the case when conducting a "round-trip transaction", meaning sending the exact number of coins from a transparent (t-addr) to a shielded address (z-addr) and back to another transparent address (Quesnelle 2017). We refer in this paper to this phenomena as the "fungibility problem".

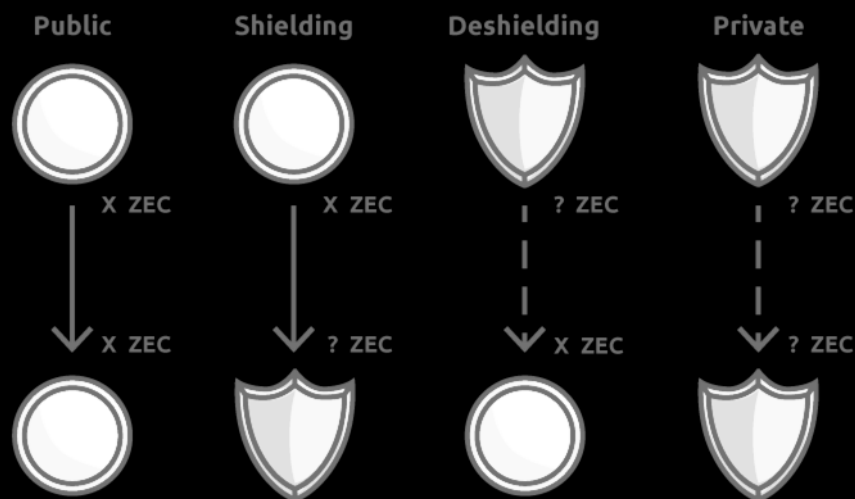


Figure 2 Users of Zcash have 4 different options of spending Zcash. Source: <https://z.cash/blog/sapling-transaction-anatomy/>

As seen in Figure 2, Zcash users are given the ability to conduct 4 different types of transactions in the current Zcash protocol. Being able to send from public to shielded address and vice versa greatly puts the fungibility of the coins at risk. It is possible to identify coin mixing patterns among the different types of transactions when users send coins back to transparent addresses, such as the case in "round-trip transactions", as this behavior has been shown to exhibit high linkability (Quesnelle 2017).

The performance upgrades of Sapling unfortunately comes at a privacy cost as Sapling transactions reveal more metadata than the "old" legacy JoinSplit operations. Sapling transactions show the number of inputs and outputs used. This functionality increases the options to differentiate between transaction types, analyze transaction data and possibly identify behavior related to mixing.

To reduce or eliminate this risk it is important to either reduce the usage of transparent addresses or simply disable it from the beginning in a new blockchain such as Pirate.

Our solution

Pirate aims to improve substantially upon the privacy and security features of Monero and fix the “fungibility problem” of Zcash. Pirate Chain does this by means of only accepting “Sapling” shielded transactions (z-tx), apart from mining rewards and notarizations, as explained in the dPoW section. Additionally, Pirate Chain is secured through the delayed Proof-of-Work mechanism making its privacy and security features currently unmatched in the blockchain industry compared to existing privacy coins.

Pirate Chain: Privacy, fungibility and security

29th of August 2018 - The call for full anonymity

Pirate started on the 29th of August in Discord as an idea of a 100% zk-SNARKs coin. The development work of *jl777c* on Komodo Asset chains enabled the ability to enforce shielded transactions usage by adjusting the asset chain parameters in a new asset chain (Grewal 2018). An asset chain is a Komodo runtime fork and is an actual independent blockchain.

Pirate initially started out as an experiment to observe if forced z-transactions would work, but the community quickly realized its potential after *jl777c* successfully implemented delayed proof-of-work making Pirate essentially *feature complete*.

Komodo – Zcash fork – zk-SNARKs

Pirate is an asset chain part of the Komodo platform ecosystem. The Komodo project focuses on empowering blockchain entrepreneurs and the average cryptocurrency user with freedom and ease of use through blockchain technology (Lee 2018). Komodo began as a fork of the popular privacy coin, Zcash. The Zcash project itself is a fork of Bitcoin. Thus, all the features designed by Satoshi Nakamoto in the Bitcoin protocol are also available in Komodo.

As such, Komodo retains the same inherent privacy features as Zcash. Among these features are the Zcash parameters and zk-SNARKs technology. Zk-SNARKs is one of the most powerful forms of blockchain privacy in existence, as the provided privacy is effectively permanent.

This statement is even highlighted by the main representative of Monero, *Riccardo “fluffypony” Spagni*:

“ZCash’s zkSNARKs provide much stronger untraceability characteristics than Monero (but a much smaller privacy set and much higher systemic risks).”

Komodo Asset chains

An Asset chain (officially Parallel Chain) is an independently created blockchain that inherits all of Komodo's features like BarterDEX compatibility, Zero Knowledge Privacy and delayed Proof-of-Work etc. but also has numerous custom specifications such as custom coin supply and custom RPC-port. More custom features are currently in the pipeline to get added (PTY X 2018).

Other examples of Komodo asset chains include Bitcoin Hush (BTCH), ChainZilla (ZILLA), DEX, Equalizer (EQL), KMDice, Monaize (MNZ), PUNGO, REVS, SuperNET, Utrum and ZEX.

Forced z-transactions

The best solution to the “fungibility problem” is to disable the ability of sending to transparent addresses, in our opinion. This eliminates the existence of transactions from shielded balances to transparent balances which are often the root cause of decreased fungibility. As quoted by the main

Zcash developer himself in response to the paper called “On the linkability of Zcash transactions” by Jeffrey Quesnelle:

“But my answer is instead we're going to ban unshielded transactions. Even simpler.”

Delayed Proof-of-Work: Maximum security and flexibility

What is delayed Proof-of-Work?

Delayed Proof-of-Work stems from Komodo and provides a unique and innovative form of security which is as strong as the network it attaches to, yet does not require the cost to run that network. Delayed Proof-of-Work is a solution that utilizes multiple existing methods into a single hybrid consensus system that is as energy efficient as Proof-of-Stake (PoS), while being secured by Bitcoin’s Proof-of-Work. Users who build independent blockchains (asset chains) in the Komodo ecosystem can choose to have a block-hash, serving as a “snapshot” of their own blockchain inserted into the Komodo main chain. In this manner, the records of the asset chain are indirectly included in the block-hash of Komodo that is pushed onto the blockchain of the strongest network (now Bitcoin).

So dPoW allows even the weakest of blockchains to benefit from Bitcoin's hash-rate and this in turn makes Bitcoin's power usage more eco-friendly as it is securing the entire ecosystem of dPoW in addition to itself (JI777c 2016). Other than Pirate, dPoW has been successfully implemented in a large number of asset chains such as Game Credits, Einsteinium (EMC2), Pungo and HUSH amongst others (Komodostats 2018).

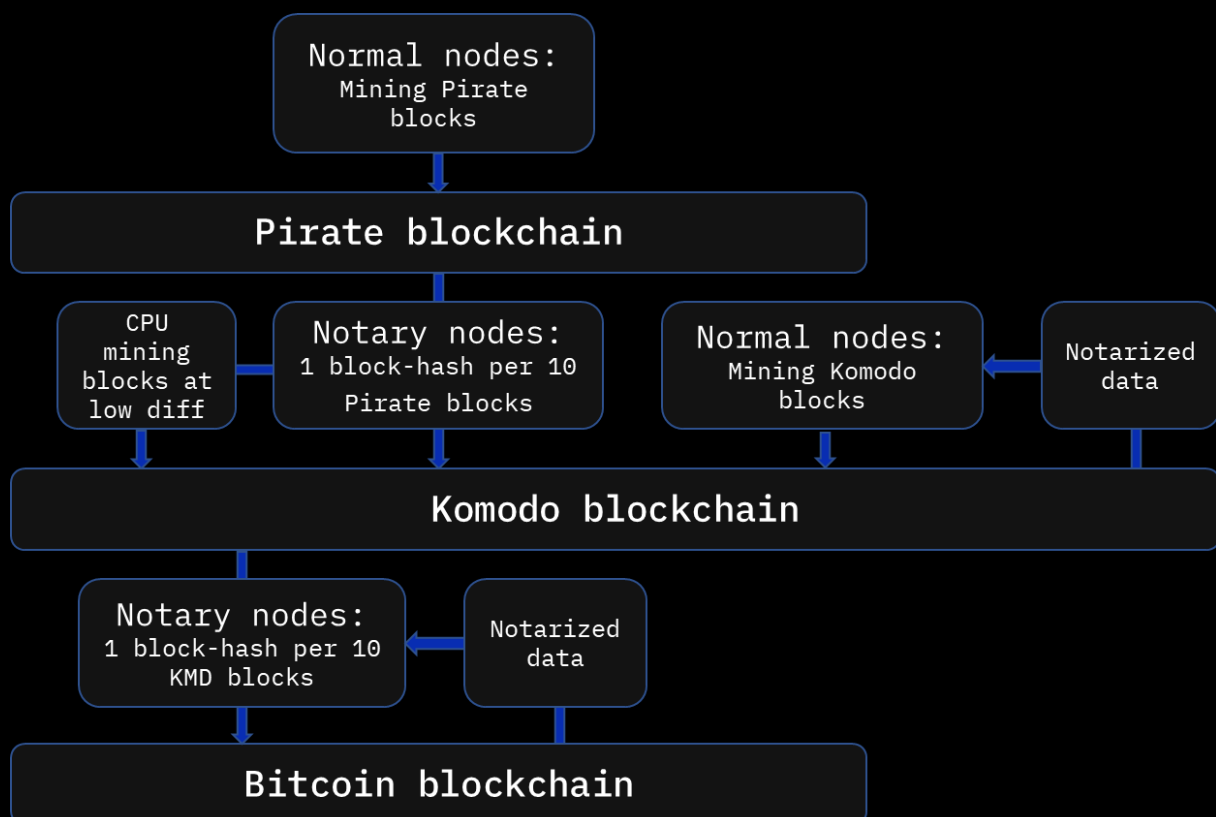
What are the mechanics behind delayed Proof-of-Work?

The Komodo security service is performed by notary nodes which are needed to record block-hashes onto the Bitcoin blockchain, referred to as *notarization* (Figure 3). Notarization entails the creation of a group signed bitcoin transaction containing the most recent block-hash of Komodo, signed by an unknown combination of 33 of 64 notary nodes (Jl777c 2016). Block-hashes of Pirate Chain (amongst other asset chains) are inserted in the Komodo blockchain in a timely fashion as well using the same method. In this manner, even a single surviving copy of the Komodo main chain will allow the entire ecosystem of asset chains to overwrite and overrule any of an attacker's attempted changes. The notary nodes pay the Bitcoin transaction fee for notarizing the Komodo blockchain. The bitcoin transaction fee costs for notary nodes is compensated for by block rewards and transaction fees of the Komodo blockchain going towards notary nodes. It is therefore expected that the financial interests of the stakeholders is to be voting for notary nodes that the stakeholders are comfortable with. 64 largely distributed notary nodes are up for election and are expected to be an optimal representation of a decentralized ecosystem making any type of 51% attack highly improbable.

Figure 3 A schematic representation of delayed Proof-of-Work.

So in order to reorganize and attack Pirate the attacker would need to destroy:

- 🔗 all existing copies of the Pirate Chain;
- 🔗 all copies of the Komodo main chain;
- 🔗 the PoW security network (Bitcoin) into which the Komodo blockchain notarized data is inserted.



Furthermore, notary nodes have the freedom to switch the notarization process to another PoW network if a shift in hash rates between the large blockchains occurs in the future.

Delayed Proof-of-Work provides Pirate with a higher than Bitcoin-level security, while avoiding the excessive financial and eco-unfriendly costs. Through dPoW's flexibility it offers a more flexible and adaptive nature than Bitcoin itself.

Examples of attacks on blockchains

There are a number of examples which highlight the need for a mechanism like delayed Proof-of-Work:

In April 2018, a bug in the retargeting mechanism of the algorithms of Vergecurrency (XVG) was exploited by means of a 51% attack. Using spoofed timestamps, the need for a different algorithm each block was circumvented. The hackers were able to submit blocks to the chain at a mining speed of 1 block per second, effectively denying 99% of the legitimate pools' blocks and causing them to lose money (Ocminer 2018a). During May 2018 the same attack happened but with a different approach: hackers sent one block with Scrypt algorithm containing a spoofed timestamp followed by a block with Lyra2re algorithm containing a spoofed timestamp and by repeating that process and thus lowering the difficulty, the hackers were able to mine several blocks per minute (Ocminer 2018b).

On May 16 2018, Bitcoin Gold was attacked by an unknown actor who managed to steal over 388,000 BTG from cryptocurrency exchanges, the coins were worth 17.5 million dollars during the attack (Roberts 2018).

NiceHash currently offers more than enough hash power for rent to attack a number of small to mid-cap cryptocurrencies. The term "Nicehashable" has been coined for the ability to rent hash to attack a coin and sites have already popped up to showcase the hacking opportunities (EXAKING 2018).

Sapling integration and activation

Sapling integration

Sapling integration into Pirate Chain has been a success due to the cooperation between members of the Komodo ecosystem, with a special thanks to Mike Toutonghi from the Veruscoin project.

Pirate stands for fast, cheap and 100% private transactions and Sapling is the best version of the zk-SNARKs technology which offers that. For that reason, Sapling usage is forced from the 15th of February 2019 and onwards to make sure the chain works efficiently and privately. Users that own Pirate need to migrate their coins from their Sprout addresses to Sapling addresses before that date.

The timing of the hard-fork for Sapling activation was based on a block timestamp around the 15th of December, 1 AM UTC. The deadline for the migration from Sprout to Sapling was set to the 15th of February 2019 in order to create a sense of urgency and get everyone owning Pirate involved. The sooner the migration is done the better the situation for centralized exchanges and other third party apps.

A decentralized app (dApp) called “zMigrate” that automatically converts the user’s funds in Sprout addresses into a Sapling address was developed by *j1777c* to streamline the migration process to Sapling. All nodes were needed to complete this process by the 15th of February 2019 and pools likewise made the jump to Sapling addresses after the hard-fork.

The migration to Sapling

The dApp zMigrate is a standalone program which interacts with the daemon “Komodod”. The dApp will send the Pirate in the user’s Sprout address(es) to a one-time used, randomized transparent address in a maximum of 10K Pirate per transaction. As many onetime t-addresses are created as needed to move all funds, with the last transaction probably containing less than 10K (unless funds are divisible by 10K). Consequently, the funds from each t-addr are sent to the designated Sapling shielded address. In this manner the user is in control of the funds the entire time and the movement of transparent funds will look as homogenous as possible to reduce the damage to fungibility of the chain. The result of the process is that all the funds of the user are transferred from the old Sprout address to their Sapling address of choice.

The technical improvements of Sapling enables the development of the following features:

- 🔗 Point-of-Sale integration
- 🔗 Hardware wallets
- 🔗 Web Shop Plugins (Fast)
- 🔗 Mobile wallets through enabling Simple Payment Verification (zSPV) (in development)

Emission scheme and technical characteristics

Pirate chain contains the following technical characteristics and features after the 15th of December:

- 🔗 Mining algorithm: Equihash Proof-of-Work
- 🔗 Delayed Proof-of-Work
- 🔗 Block-time: 60 seconds
- 🔗 Transaction fee: 0.0001 ARRR
- 🔗 Transaction signing under seconds
- 🔗 Transactions per second: 50–80 TPS
- 🔗 Send to up to 100 addresses in a single transaction
- 🔗 Tx sizes of +- 2000 bytes with a max. of 200 kB
- 🔗 Memory usage of only 40 MB (Raspberry Pi)
- 🔗 Block size of 4 MB maximum
- 🔗 Viewing keys which offer the ability to see all sent transactions of an assigned address
- 🔗 Ability to generate “endless” number of “Lite” wallets

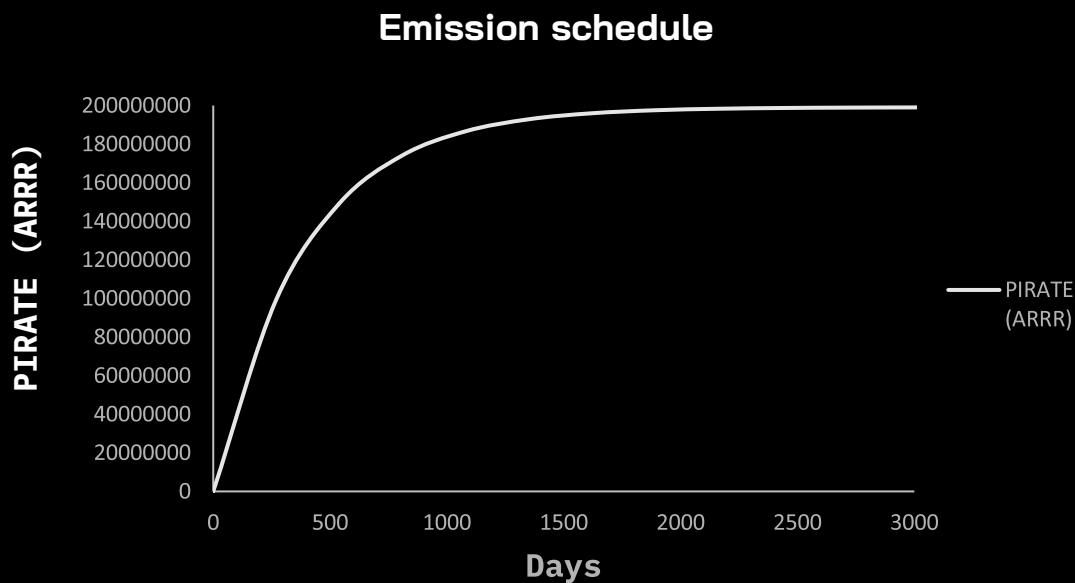


Figure 4 The emission schedule of Pirate (ARRR)

There is a halving event in block rewards every 388885 blocks which equates to roughly 270 days per reward period. The supply is maxed at roughly 200 million Pirate (ARRR).

TOR support

It is possible to run Pirate chain over the TOR Network and obfuscate your IP address, a number which is linked to your geographical location. As a user you need a TOR browser and the Komodo binaries to be able to run Pirate Chain. A step-by-step guide is available at pirate.black. TOR support request has been shared with Agama Wallet developers. Once done, setting up Tor for a coin or asset chain is very easy.

Centralized exchanges support

The community was unsure if centralized exchanges would be able to accept Pirate at first because of the lack of transparent addresses. Not long after the inception of Pirate Chain, it has worked with exchange developers and coders to facilitate the use of Z-address deposits and withdrawals as a world's first. This particular exchange is DigitalPrice (now Altsbit) and successfully launched trading at the end of October 2018.

Roadmap

2018 Completed

- Z address mining pools -
- Z address Discord tool -
- Pirate non-security Compliance / Howey letter -
- Z address Only Exchange Capabilities Initiated -
- Z address exchange DigitalPrice -
- Website Rebrand -
- Onboarding Referral Program -
- Z address lottery bot -
- Sapling integration - December 15, 2018

2019 Completed

- Sapling only - February 15, 2019 -
- Solo Mining pool -
- ZCommerce with VerusPay and Shopify Script -
- Pirate Physical Commemorative Coins -
- Pirate Full Node (KMD + Asset Chains) -
- Pirate Notary Services -
- Developer Ticketing System -
- Paper Wallet -
- ARRRmada | ecommerce vendors who accept ARRR -
- ARRRmada Web Service -
- SevenSeas Fullnode & Wallet -
- Treasure Chest Node Case -
- CryptoCurrency Checkout Integration -
- SevenSeas Companion Android App -
- Pirates Week Festival Campaign -
- Lite Wallet -
- GhostShipOS -
- Exchange Listing: Bilaxy -
- Exchange Listing: Coinex -
- Exchange Listing: SafeTrade -

2020

- Q1 -

- CryptoCurrency Checkout CoMarketing -
- Kovri Integration -
- Mobile Lite Wallet -
- Website Rebrand -
- TurtleNetwork Partnership -
- VPN Partnership -
- TurtleNetwork Wallet Integration in PirateOS -
- Translate Website in over 20 Languages -

- Q2 -

- QT Wallet Upgrades -
- Privatebay (working title) -
- GalleonOS -
- Pirate .onion (TOR) + .EPP -
- Exchange Integration into PirateOS -

- Q3 -

- Point of Sale System Register -
- Pirate Foundation -
- Snarkz: private chat -

- Q4 -

- Point of Sale System Global Rollout -
- Fiat Integration into Point of Sale System -
- ARRRtomic | Ztx DEX Integration -
- ZSPV -
- Snarkz: private chat -

The Pirate Chain Guide

Official Website

<https://pirate.black/>

How to mine

Calculate your estimated earnings:

<https://dexstats.info/piratecalc.php>

Mine Pirate with ASIC/GPU:

<https://medium.com/piratechain/how-to-mine-pirate-step-by-step-with-gpu-s-4c98f3dbcf5e>

Mine Pirate without ASIC/GPU (Rent)

<https://medium.com/@flexatron/how-to-mine-pirate-arr-rr-without-owning-an-expensive-rig-b8c26e409ae5>

Keep an eye on Pirate hash-rate:

<https://dexstats.info/piratehash.php>

Buy and Trade Pirate Chain

Sign-up and trade ARRR for BTC, BCH, ETH, EUR, KMD, USD or USDT:

<https://pirate.black/exchanges/> (REF links included)

Social media

Bitcointalk: <https://bitcointalk.org/index.php?topic=4979549.0>

Discord: <https://pirate.black/discord>

Facebook: <https://www.facebook.com/PirateChain/>

Instagram: <https://www.instagram.com/PirateChain/>

LinkedIn: <https://www.linkedin.com/company/PirateChain>

Medium: <https://medium.com/@PirateChain>

Reddit: <https://www.reddit.com/user/PirateChain>

Steemit: <https://steemit.com/@PirateChain>

Telegram: <https://t.me/PirateChain>

Trello: <https://trello.com/b/BqhdZbiS/Pirate-Chain-Progress-Board>

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

YouTube: <https://www.youtube.com/c/PirateChain>

Coin Statistics Websites

CoinGecko: <https://www.coingecko.com/en/coins/pirate-chain>

CoinMarketCap: <https://coinmarketcap.com/currencies/pirate-chain/>

CoinPaprika: <https://coinpaprika.com/coin/arrr-pirate/>

And many more!

Source code

GitHub: <https://github.com/PirateNetwork>

Wallets

Wallets: <https://pirate.black/wallets/>

References

- Bowe, S. 2017. "Cultivating Sapling: Faster zk-SNARKs--Zcash Blog". Zcash Blog.
- EXAKING. 2018. "PoW 51% Attack Cost". 2018. <https://www.exaking.com/51>.
- Grewal, Satinder. 2018. "Satinder's notes on the PIRATE chain". 2018. <https://blog.komodoplatform.com/pirates-of-komodo-platform-cdc991b424df>.
- Hopwood, Daira, Sean Bowe, Taylor Hornby, en Nathan Wilcox. 2016. "Zcash protocol specification".
- Japparova, Irina, en Ramona Rupeika-Apoga. 2017. "Banking Business Models of the Digital Future: The Case of Latvia". European Research Studies 20 (3A). Professor El Thalassinos: 846.
- Jl777c. 2016. "Delayed Proof of Work (dPoW) Whitepaper". Github. 2016. [https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-\(dPoW\)-Whitepaper](https://github.com/KomodoPlatform/komodo/wiki/Delayed-Proof-of-Work-(dPoW)-Whitepaper).
- Kappos, George, Haaron Yousaf, Mary Maller, en Sarah Meiklejohn. 2018. "An Empirical Analysis of Anonymity in Zcash". arXiv preprint arXiv:1805.03180.
- Komodostats. 2018. "Asset Chains Notarizations Summary". 2018. <https://komodostats.com/acs.php>.
- Lee, James. 2018. "Komodo: An Advanced Blockchain Technology, Focused on Freedom." Komodo. 2018.
- Moser, Malte. 2013. "Anonymity of bitcoin transactions".
- Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system". Working Paper.
- Ocminer. 2018a. "Network Attack on XVG / VERGE". Bitcointalk. 2018. <https://bitcointalk.org/index.php?topic=3256693.0>.
- . 2018b. "Network Attack on XVG / VERGE (Page 57)". Bitcointalk. 2018. <https://bitcointalk.org/index.php?topic=3256693.msg38135174#msg38135174>.
- PTY X. 2018. "What is a Parallel Chain (Asset Chain)?" Komodo Platform. 2018. <https://komodoplatform.atlassian.net/wiki/spaces/KPSD/pages/71729160/What+is+a+Parallel+Chain+Asset+Chain>.
- Quesnelle, Jeffrey. 2017. "On the linkability of Zcash transactions". arXiv preprint arXiv:1712.01210.
- Roberts, Jeff John. 2018. "Bitcoin Spinoff Hacked in Rare '51% Attack'". FORTUNE. 2018. <http://fortune.com/2018/05/29/bitcoin-gold-hack/>.
- Saberhagen, Nicolas Van. 2013. "CryptoNote v 2.0".
- Sasson, Eli Ben, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, en Madars Virza. 2014. "Zerocash: Decentralized anonymous payments from bitcoin". In 2014 IEEE Symposium on Security and Privacy (SP), 459–74.