



The  
CRYPTO VIGILANTE



## TCV Featured Crypto Asset: Pirate Chain (ARRR)



Rafael LaVerde & Mr. X

August 18, 2020



# Pirate

**Pirate Chain (ARRR) is everything we wanted Zcash (ZEC) to be!**

*Pirate Chain started off as a challenge among Zcash (ZEC) and Komodo (KMD) developers to fork ZEC's code into a private-by-default **delayed Proof of Work (dPoW)** blockchain with 51% attack resistance. Their endeavor worked so well that this "test project" ended up becoming the real deal.*

### Why is ARRR important?

“Pirate Chain (ARRR) has entered the scene, claiming to have the best of both worlds - mandatory privacy combined with cutting-edge zk-SNARKs, enforced for all transactions by default.” -page 27 of this report

### Where do I buy it?

We like TradeOgre the best - there is no KYC required or withdrawal limits, and it currently has the most liquidity/volume:

<https://tradeogre.com/exchange/BTC-ARRR>

Other exchanges:

<https://exchange.bitcoin.com/ARRR-to-BTC>

<https://www.coinex.com/exchange?currency=BTC&dest=ARRR>

### How do I store it?

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



# Zcash

## Zcash (ZEC)

During a talk in 2018, privacy advocate and NSA whistleblower Edward Snowden **said this**:

*“When we talk about which cryptocurrencies are interesting to me, I’ve said it before and I’ll say it again, Zcash for me is the most interesting right now, because the privacy properties of it are truly unique, but we see more and more projects that are trying to emulate this and I think this is a positive thing.”*

Zcash (ZEC) is well-known for its innovative usage of cutting-edge zk-SNARKs cryptography. According to the Zcash [website](#):

*“The acronym zk-SNARK stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,” and refers to a proof construction where one can prove possession of certain information, e.g. a secret key, without revealing that information, and without any interaction between the prover and verifier.”*

## **Major Privacy Flaws in Zcash (ZEC)**

Even in spite of Zcash’s innovative usage of this cryptographic privacy technology, its implementation has always been severely lacking because this privacy feature is not enabled by default, much less enforced for all transactions at the protocol level.

ZEC could have been Monero (XMR)’s greatest competitor, but unfortunately its community insisted on developing ZEC as a coin with optional privacy, which is a fatal flaw in its quest to become private digital cash. Zcash also has other flaws which we will discuss later throughout this report.

***At TCV we consider optional privacy to be no privacy at all; therefore, Zcash is not truly fungible.***

ZEC utilizes two types of addresses: z-addresses (shielded addresses) and t-addresses (transparent addresses).

- Z-Addresses are private/shielded addresses that use zero knowledge proofs as part of the transactions.
- T-Addresses are transparent addresses, which are essentially identical to Bitcoin addresses, and are completely transparent. T-Addresses are fully traceable and visible.

There have been several studies showing us throughout the years that in practice, ZEC does not live up to its privacy claims and is not really private at all. After looking at the [Zcash block explorer’s public statistics](#), one can clearly see that very few transactions are shielded in comparison to those that are transparent.

A recent academic study entitled “[Alt-coin Traceability](#)” published on May 18, 2020 by Carnegie Mellon University showed that only 0.1% of ZEC users are using z-addresses properly. 99.9% of ZEC transactions are traceable since they are using transparent t-addresses. In that report, Dash was also shown to utterly fail in regards to its false claims of privacy as well.

***We might as well call it “Tcash” instead of Zcash since no one actually uses z-addresses!***



Chainalysis' June 8, 2020 report verified the findings of the study by Carnegie Mellon:

*“But of the transactions that interact with a shielded pool, only 6% are completely shielded, i.e. sender, receiver, and transaction amount are all encrypted. That’s only 0.9% of all Zcash transactions.*

*So even though the obfuscation on Zcash is stronger due to the zk-SNARK encryption, Chainalysis can still provide the transaction value and at least one address for over 99% of ZEC activity.”*

**In addition to exposing the privacy flaws in Zcash, this Chainalysis report further proves that we were correct in our decision to remove **Dash (DASH)** and **Private Instant Verified Transaction (PIVX)** - an **insecure Proof-of-Stake (PoS)** fork of Dash - from the TDV crypto portfolio for misleading people by claiming to be private when in fact, they were not.**

**For further details, please read our two in-depth articles: “*DASH: Digital Cash or Digital Trash?*” from the **TDV August 2019 Issue** (starting on page 29), and our follow-up article, “*Doubling Down: DASH Is Digital Trash*” from the **TDV September 2019 Dispatch** (starting on page 28).**

In addition to the problems exposed by the research paper above, other academic papers have also examined the serious problems with Zcash’s optional privacy and the negative consequences for its privacy as a whole.

For example, in the 2018 paper *An Empirical Analysis of Anonymity in Zcash* (George Kappos, Haaron Yousaf, Mary Maller, and Sarah Meiklejohn, University College London) presented at the **27th USENIX Security Symposium in 2018**, the researchers shared some **fascinating discoveries** after analyzing the 2,242,847 transactions on the Zcash blockchain at the time.

In order to understand Zcash, it is necessary to understand the kinds of transactions on its network. As explained earlier, there are two types of addresses in Zcash: t-addresses & z-addresses. Listed below are the four main types of Zcash transactions, and they are further described in the following diagram underneath.

- *Transparent* transactions move funds from t-addresses to t-addresses
- *Shielded* transactions move funds from t-addresses to z-addresses
- *Des shielded* transactions move funds from z-addresses to t-addresses
- *Private* transactions move funds between z-addresses

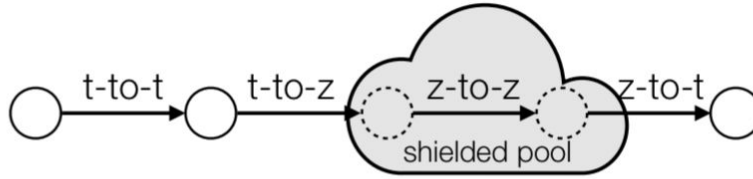


Figure 1: A simple diagram illustrating the different types of Zcash transactions. All transaction types are depicted and described with respect to a single input and output, but can be generalized to handle multiple inputs and outputs. In a t-to-t transaction, visible quantities of ZEC move between visible t-addresses ( $zIn, zOut \neq \emptyset$ ). In a t-to-z transaction, a visible amount of ZEC moves from a visible t-address into the shielded pool, at which point it belongs to a hidden z-address ( $zOut = \emptyset$ ). In a z-to-z transaction, a hidden quantity of ZEC moves between hidden z-addresses ( $zIn, zOut = \emptyset$ ). Finally, in a z-to-t transaction, a hidden quantity of ZEC moves from a hidden z-address out of the shielded pool, at which point a visible quantity of it belongs to a visible t-address ( $zIn = \emptyset$ ).

*The four main types of Zcash transactions*

In their report, the researchers categorized the 2,242,847 transactions according to their transaction type (which includes the four types above, with some additional combinations for mined coins, etc.) as seen in the table below.

Type	Number	Percentage
Transparent	1,648,745	73.5
Coingen	258,472	11.5
Deshielded	177,009	7.9
Shielded	140,796	6.3
Mixed	10,891	0.5
Private	6934	0.3

Table 1: The total number of each transaction type.

*Totals for each transaction type category*

The researchers graphed the total number of transactions within each transaction type category over time, as seen in the figure below.

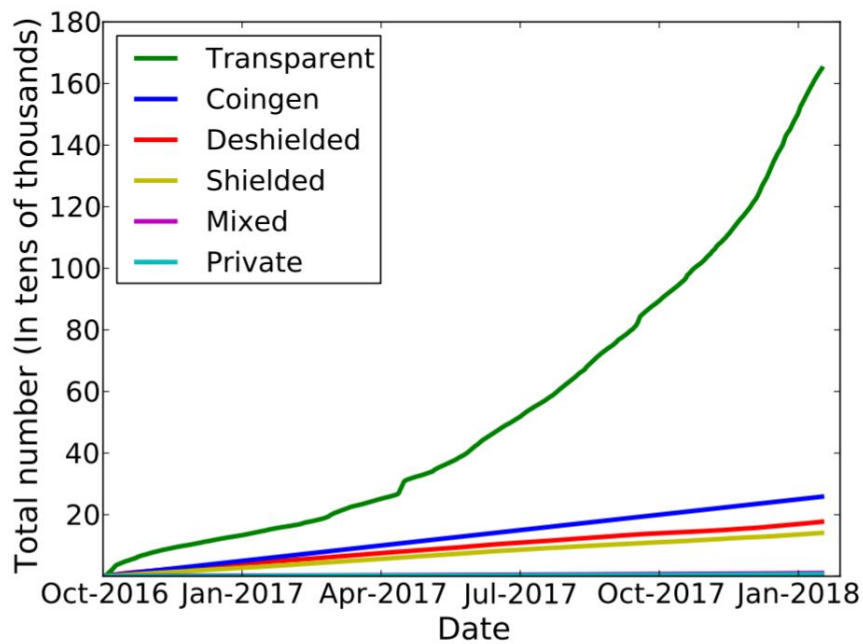


Figure 2: The total number of each of the different types of transactions over time.

*Totals of transaction types over time*

It is evident from the graph above that the number of transparent transactions has significantly grown, and much more so than the other types of transactions. Notice also that the total number of fully private (z-to-z) transactions is so tiny in comparison that they are barely noticeable at the bottom of the graph (light blue line).

It is clear from the above graph that Zcash's actual privacy is very poor, and that in practice, the vast majority of transactions are fully public and transparent, very much like we see in Bitcoin. As we have written about in many of our reports, transparent coins like Bitcoin are, in effect, "surveillance coins" which are studied by governments and their big data blockchain analytics corporate contractors.

In the paper's abstract, the researchers said this:

*"We conclude that while it is possible to use Zcash in a private way, it is also possible to shrink its anonymity set considerably by developing simple heuristics based on identifiable patterns of usage."*

The researchers later concluded:

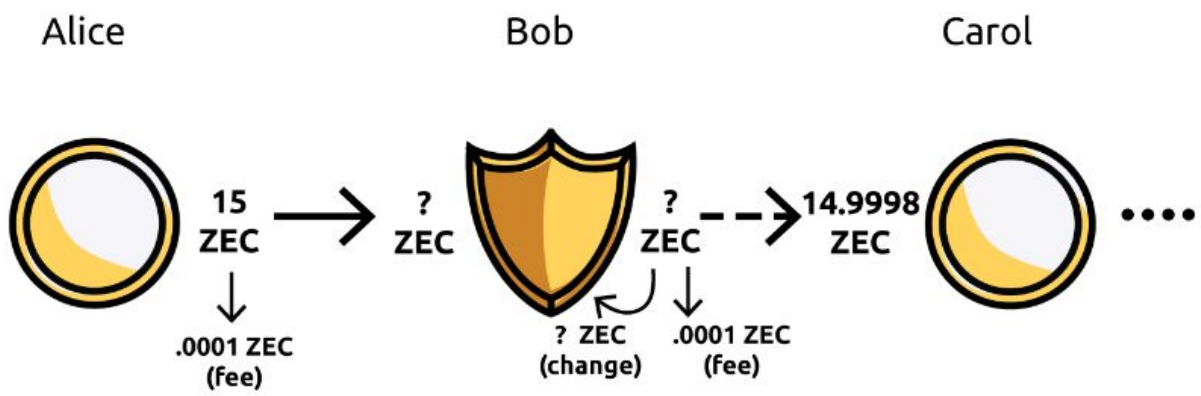
*"...our study has shown that most users are not taking advantage of the main privacy features of Zcash at all. Furthermore, the participants who do engage with the shielded pool do so in a way that is identifiable, which has the effect of significantly eroding the anonymity of other users by shrinking the overall anonymity set."*

This research paper was referenced in a Motherboard Vice article, "[Cryptocurrency Transactions May Uncover Sales of Shadow Broker Hacking Tools](#)" and included a case study analyzing possible Zcash payments sent to The Shadow Brokers hacking group who were selling stolen code from the NSA.

From this university research study, it is evident that Zcash's claims of privacy have been significantly exaggerated. In contrast, the Monero (XMR) community takes its privacy claims much more seriously. Several experts in the Monero community have also addressed Zcash's major flaws in [this Reddit thread](#), some of which were shown in that same academic paper as well.

Another research paper, [On the linkability of Zcash transactions](#) (Jeffrey Quesnelle, University of Michigan-Dearborn, 2017) examined some fascinating metrics concerning the utilization of Zcash's shielded addresses. In the study, the author observed that the majority of ZEC sent to shielded (z) addresses are sent back to transparent (t) addresses in the future, as seen in the diagram below.





*“Improper use of z-addrs can lead to transaction linkability.”*

This pattern of transaction activity revealed an existence of a large number of round-trip transactions (RTTs), where “the same, or nearly the same number of coins are sent from a transparent address, to a shielded address, and back again to a transparent address.” After performing a search for these RTTs, the researcher performed a heuristic analysis which enabled them to link “31.5% of all coins sent to shielded addresses.” The author argued that the habitual usage of these so-called round-trip transactions “exhibits high linkability, especially when they occur nearby temporally.”

$\Delta$ block time	# RTT	$\Sigma$ coins	Top $n$ JoinSplits	# RTT	$\Sigma$ coins
[0, 5)	1373	156,237	10	10	34,153
[5, 15)	5022	421,021	50	49	143,924
[15, 30)	1479	147,546	250	236	500,163
[30, 60)	1015	95,034	500	460	765,212
[60, 120)	500	35,741	1000	585	834,301
[120, 1440)	284	60,518			
[1440, $\infty$ )	402	3,120			

*“(Left) Stats on RTTs found (Right) Top 250  $t \rightarrow z$  transactions”*

The Monero community has also made some interesting **observations** regarding this research paper, and apparently, the paper’s author collaborated with the Monero Research Lab on it as well.

BTC Manager published a helpful **article** about this research, and Bitcoin developer Peter Todd commented on it in some tweets as well, as seen below.

 **Peter Todd** @peterktodd

While great that [@realjeffq](#) quantified this risk in detail, lots of people have been warning that Zcash's failure to mandate private txs, as in Monero, was obviously dangerous.

Zcash seems focused on shiny new math instead of competent engineering - why the trusted setup failed.

 **Jeffrey Quesnelle** @realjeffq · Dec 4, 2017  
Today I'm publishing a paper on the linkability of certain types of #Zcash transactions: [jeffq.com/blog/on-the-li...](#) Found that 31.5% of all coins sent to z-addr may be linkable by matching to an identical outgoing transaction. Raw data: [jeffq.com/zcash-rtts.htm](#)

1:09 AM · Dec 5, 2017 · [Twitter Web Client](#)

39 Retweets and comments 93 Likes

 **Peter Todd** @peterktodd · Dec 5, 2017  
Replying to [@peterktodd](#) and [@realjeffq](#)  
Failing to mandate private txs was also dishonest: it's significantly helps Zcash adoption, directly benefiting the founders who receive 20% of coins generated, while failing to provide users the privacy they expected (esp those mistakenly using wallets w/o shielded tx support).

 5  11  44 

 **Monero Trader** @monerotrader · Dec 5, 2017  
Replying to [@peterktodd](#) [@petertoddbtc](#) and [@realjeffq](#)  
Newer isn't always better. I prefer #xmr over Zcash precisely because of that preference. It says a lot about the careful craftsmanship that has gone into #Monero. It deserves and has earned it's price.

  2  2 

<https://twitter.com/peterktodd/status/937926919735119872>

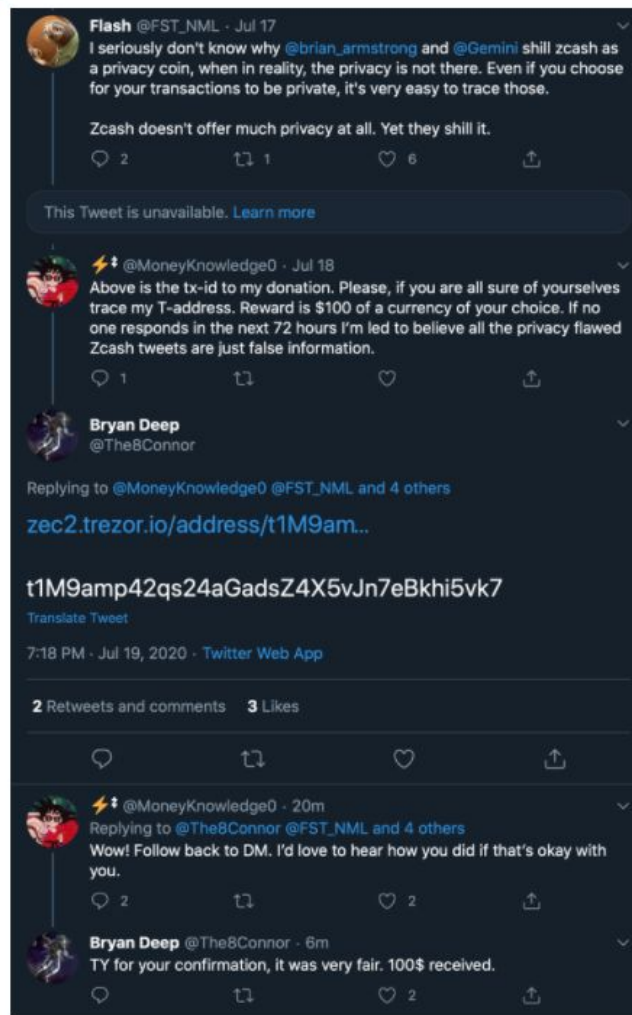
## Zcash Shielded Transaction Traced by a Smart Twitter User in July 2020

In addition to the academic papers showing the privacy weaknesses in Zcash, there was recently an incident on Twitter where a **Zcash supporter dared people to trace the T-address** of the origin of the ZEC funds sent in the transaction ID for his donation to the EFF.

A smart user **responded to the tweet by guessing the correct T-address** of the origin of his funds, essentially unmasking a shielded transaction!

↑ Posted by u/Razaberry Silver | QC: BNT 37, ETH 15 18 days ago  
1.3k  
↓ **Did we just see ZCash get cracked? Twitter user traced a ZCash Shielded Transaction back to it's T-address. In other words the Zero Knowledge Proofs have been defeated.**

MISLEADING TITLE



277 Comments Share Save Hide Report

94% Upvoted

 ⚡  
@MoneyKnowledge0

(1/2) my z2z donation block height: 905397

my T->T and T->Z block height: 905374 & 905389

It was simple for the friendly attacker especially when given the txid. He just went back a few blocks. This was my fault. It's very \*important to say this really was a lucky guess...

5:35 PM · Jul 19, 2020 · Twitter for iPhone

4 Retweets and comments 15 Likes

 ⚡ @MoneyKnowledge0 · Jul 19  
Replying to @MoneyKnowledge0

(2/2) If I were to have my Shielded ZEC in my wallet for longer than a few minutes (like I did) after the transition from T->Z (lets say a few weeks) there would have been WAY more T->T and T->Z tx's in between making it close to impossible to say it's me.

 3   10 

 **Kris Nuttycombe** @nuttycom · Jul 19  
Replying to @MoneyKnowledge0

I'm not sure I understand. You made a z->z donation, of an undisclosed amount, and they were able to associate it with the t-addr that you'd used to initially fund the z-addr? What was the actual sequence of transactions?

 1   1 

 ⚡ @MoneyKnowledge0 · Jul 19

So what he told me is that he went to the z->z donation block and from there went back a few blocks and found a transaction that was a t->z (this could have been anyone) however it was me because I made the shielded donation as soon as I turned my transparent ZEC into shielded.

 1   2 

1 more reply

 **slimb** @slimb · Jul 20  
Replying to @MoneyKnowledge0

Why downplay it as a lucky guess? It's proof that they were able to limit the anonymity set which is an attack used in many other scenarios aiming to analyse/trace "private" activities/transactions. If it was unlucky they'd just try the next one.

   1 

<https://twitter.com/MoneyKnowledge0/status/1284965051204538372>

As seen in this example, this kind of heuristic “guessing” can be surprisingly effective due to Zcash’s transparent-by-default blockchain. In order to utilize Zcash’s privacy features, its users are required to actively choose to manually shield their transactions and move funds into the shielded pool. Most Zcash wallets don’t include this feature, and it is **very** rarely enabled by default in the vast majority of ZCash wallets.

Since most users tend to be lazy in regards to their operational security, prone to bad habits, and don’t proactively take extra precautions to hide their transaction patterns, it is easy for an outside observer with additional insight (such as an exchange) to track transactions, especially if users aren’t careful to move their funds into the shielded pool and keep them in there. Also, most services (such as exchanges) only allow t-address transactions, which can erode users’ privacy. They tend to look with suspicion on users who move funds to/from the shielded pool (z-addresses).

### **Other Major Concerns About Zcash**

There are additional reasons why we distrust and dislike Zcash.

When examining the origins of Zcash, it is interesting to note that it has some globalist/deep state connections. The **original Zerocash protocol research was partially funded by DARPA and other agencies**, which raises some red flags. Inevitably, some have raised the possibility of the inclusion of a backdoor for three-letter agencies. The **original Zerocash Project** website lists the authors and sponsors for the project, as seen in the screenshot below.

# Zerocash

The Zerocash protocol is being developed into a full-fledged digital currency, [Zcash](#).

## About us

### Authors

- [Eli Ben-Sasson](#) (Technion)
- [Alessandro Chiesa](#) (UC Berkeley)
- [Christina Garman](#) (Johns Hopkins University)
- [Matthew Green](#) (Johns Hopkins University)
- [Ian Miers](#) (Johns Hopkins University)
- [Eran Tromer](#) (Tel Aviv University)
- [Madares Virza](#) (MIT)

### Sponsors

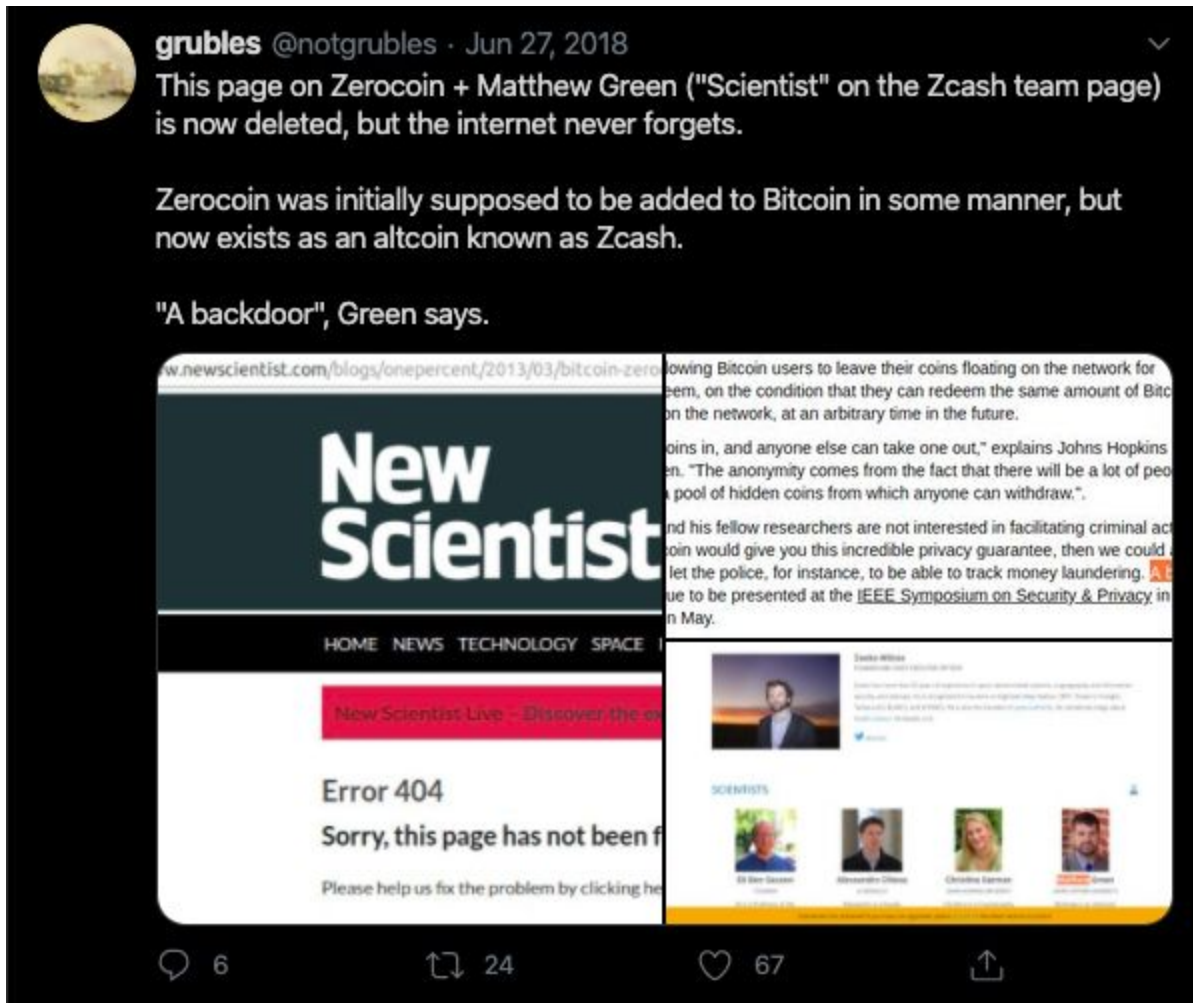
This work was supported by:

- Amazon.com through an AWS in Education research grant
- Broadcom Foundation and Tel Aviv University Authentication Initiative
- Center for Science of Information (CSol), an NSF Science and Technology Center, under grant agreement CCF-0939370
- Check Point Institute for Information Security
- U.S. Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory (AFRL) under contract FA8750-11-2-0211
- European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 240258
- Israeli Centers of Research Excellence I-CORE program (center 4/11)
- Israeli Ministry of Science and Technology
- The Leona M. and Harry B. Helmsley Charitable Trust
- Office of Naval Research under contract N00014-11-1-0470
- Simons Foundation, with a Simons Award for Graduate Students in Theoretical Computer Science
- Skolkovo Foundation under grant agreement dated 10/26/2011

The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

*Original Zerocash website*

We also distrust Zcash since one of its team members, [Dr. Matthew Green](#), **once said in a now-deleted article that he could add a police backdoor** to Zerocoin (the same technology which Zcash is built upon).



<https://twitter.com/notgrubles/status/1011830929004875777>

The fact that one of the scientists behind Zcash is a statist who is willing to publicly condone adding a **police backdoor** in its code should be very alarming! Everyone in the information security business knows that there is no such thing as a backdoor that cannot also be abused by criminals.

Additionally, Ethereum Classic developer & Cardano founder Charles Hoskinson was heard talking about Zcash being part of the conversation regarding “auditable backdoors” and “breach[ing] privacy” **during an interview** as well.

Of course, Monero core team member Riccardo “fluffypony” Spagni had something to say about this:



<https://twitter.com/fluffypony/status/1128676121309007872>

Even Zcash founder/CEO Zooko Wilcox-O’Hearn himself made a careless tweet back in 2017 where he mentioned the idea of making Zcash “too traceable for criminals” while still being “completely private & fungible” but regretted saying this the next day:





<https://twitter.com/zooko/status/863202798883577856>

These two ideas are contradictory to one another, and the fact that Zooko actually said this reveals his lack of understanding.

## Backdoor in Zcash endorsed by Green and Zooko

Security

Zooko says they want to make Zcash criminal transactions traceable:

<https://twitter.com/zooko/status/863202798883577856>

Green said already some years ago for Zcoin: "we could add on some features which let the police, for instance, to be able to track money laundering. **A back door.** Now he works on Zcash.

<https://www.newscientist.com/blogs/onepercent/2013/03/bitcoin-zerocoin.html>

Which worth has an anonymous coin, where the devs can decide which transaction they make selectively transparent?

28 Comments Share Save Hide Report

82% Upvoted

*These kinds of Reddit threads do not inspire much confidence in Zcash*

Zooko also stated during a presentation that he doesn't understand how zero-knowledge proofs actually work, but relies on other people for this (keep in mind that this kind of cryptography is very new). Understandably, this is worrisome to some potential users and investors.

Another area of concern regarding Zcash is that in our research, we found an example where the second largest Zcash mining pool was caught censoring Zcash's optionally shielded transactions! Allegedly this occurred because the pool operator didn't feel like dealing with the complexity of processing shielded transactions. Nevertheless, this analysis of the story was quite fascinating to read.

At this point, our caution regarding Zcash has elevated to the point of not even being comfortable naming it "optionally private." In the vast majority of cases, Zcash is just as transparent as Bitcoin, while offering its users a false sense of privacy.

**Therefore, Zcash is not a true privacy coin.**

### Zcash Centralization Concerns

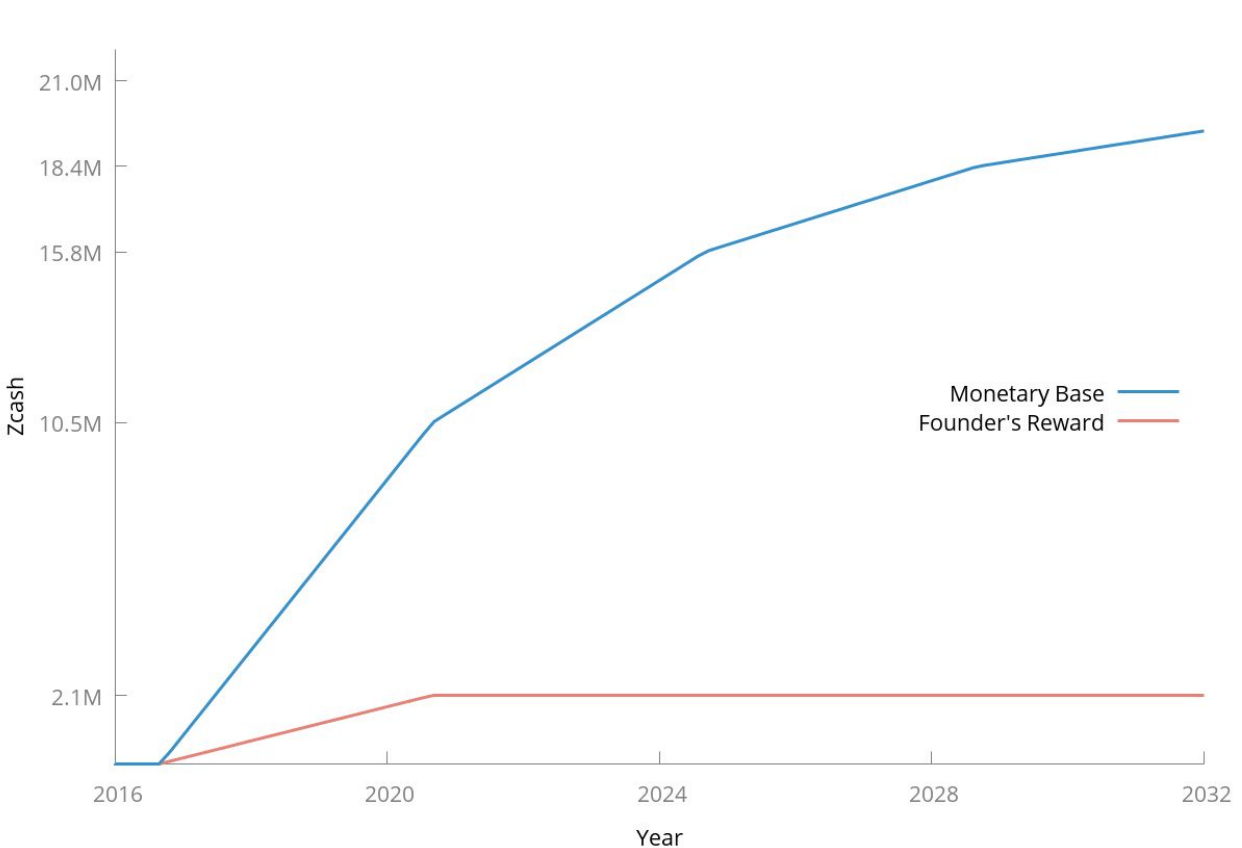
A further area of serious concern is that Zcash is essentially controlled by a US-based company with a CEO. What "decentralized" cryptocurrency has a CEO?

Zcash is backed by the **Zcash Foundation** and the Zcash **Electric Coin Company (ECC)** and is led by its founder & CEO, **Zooko Wilcox-O’Hearn**. It also has a board of directors and received \$3 million in funding from corporate investors.

Zcash’s corporate governance and structure in the USA makes it easier for the government to legally compel it to insert a backdoor, perhaps even through a top-secret **FISA court** (as we learned happened with companies like Verizon via the **Edward Snowden revelations**), which is a serious risk.

Zcash was originally launched back in 2016 with a maximum supply of 21 million coins - the same max supply as Bitcoin (BTC). In 2016, Zooko announced that the founders/insiders were going to pay themselves 10% of all Zcash mined over time (20% of all Zcash mined for the first four years, with a maximum amount of 2.1 million coins).

The Zcash team calls this controversial 20% Zcash miner “tax” the **Founders’ Reward**.



*Zcash (ZEC) “Founders’ Reward”*

This raises concerns in regards to centralization and economic fairness for a currency that is supposed to be used as money. Who wants to use money where a cabal of central bankers pay themselves 10% of all the funds in existence, just for being smart enough to help build it? That almost sounds like the current system of bankers. Many of the developers in the cryptocurrency community are appalled by this so-called “genius” miner tax.

**At this point, you may be wondering, if Zcash (ZEC) is so flawed, then why did we even include it in our crypto portfolio at all? Even with its flaws (more of which we will address further below), we admit that ZEC’s research and implementation of zk-SNARKs technology as applied to cryptocurrency has been revolutionary.**

**The research and development their team has made in this area has left a valuable impact on the cryptocurrency community and ecosystem, even though we disagree with its specific method of implementation via optional and default-disabled privacy features. Additionally, keep in mind that ZEC will be undergoing its first halving event in November 2020, which could result in a price rally as anticipation builds beforehand.**

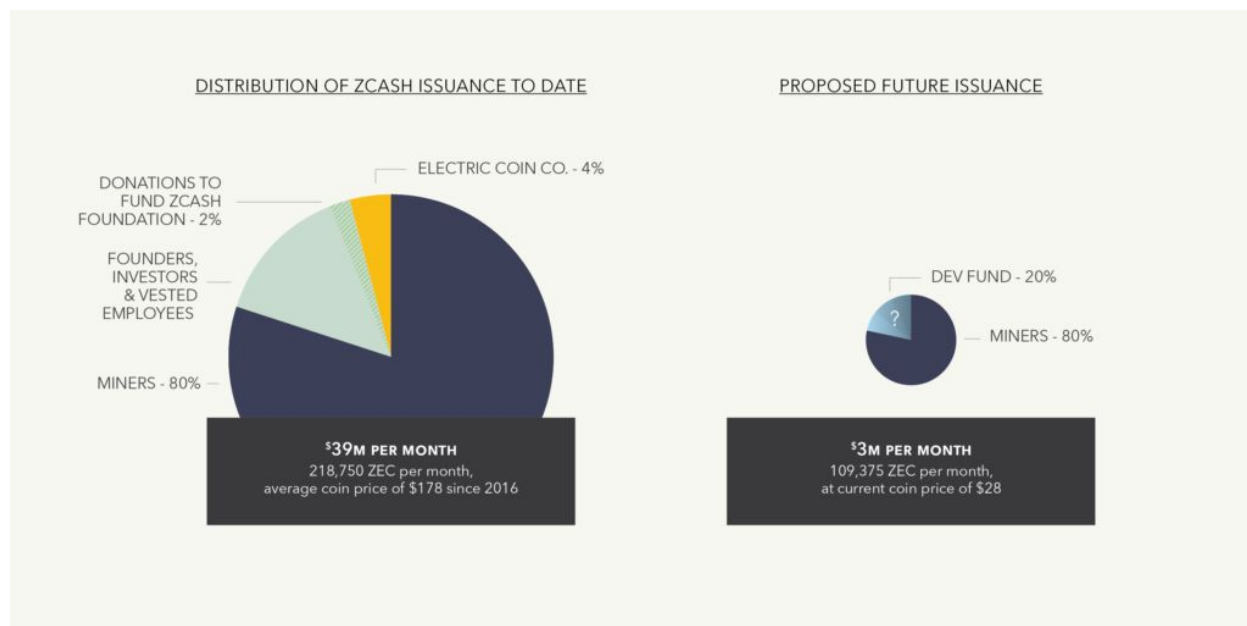
## What about ZClassic (ZCL)?

In response to the frustration over the Zcash “genius tax”, some people have praised ZClassic (ZCL) as the solution to Zcash’s flaws. ZClassic is a fork of Zcash created by crypto influencer Rhett Creighton in 2016 that simply removed the controversial 20% Zcash miner “tax” (Founders’ Reward).

In Zcash’s more recent history, we’ve begun to see some of the consequences of its centralized planning. In Zcash CEO Zooko’s [blog post](#) regarding the Founders’ Reward back in February 2016, he explained that the end result would be a total maximum ZEC supply of 21 million coins, with a total of 2.1 million going to the Founders’ Reward. Part of the Founders’ Reward would be used to [repay the original VC investors & founders](#), and would expire at the time of the Zcash block halving, set to occur around November 2020.

However, people in the Zcash community began to speculate that the central planners behind Zcash would break their promise to the community. Even after making adjustments to the Founders’ Reward, the [Zcash Electric Coin Company had been spending more money than they took in, which resulted in losses](#). A long-time Zcash supporter, Howard Loo, decided to lead the launch of a hard fork, called YCash. In a [forum post](#), Loo said, “We are also launching Ycash to uphold a promise – that the Zcash Founders Reward would be forever capped at 2.1 million coins – that we fear will come under increasing pressure between now and the expiration of the Founders Reward in October 2020.”

As a result, Zcash (ZEC) successfully forked into another coin, YCash (YEC) in 2019, in anticipation that the promise of forever capping the founders reward at 2.1 million coins would be broken. Sure enough, the Zcash central planners broke their promise. Earlier in 2020, the Zcash team essentially broke their original agreement to only take a 20% miner dev tax, and cease the tax after the first 4 years. After a **community vote**, they decided to continue taking a **20% miner tax to fund development**, as seen in the proposal below.



### *Zcash Electric Coin Company (ECC) Response to Polling Results*

Back in 2016, ZClassic **seemed like a great idea**, and miners and investors in the coin were excited about this because they didn't want to pay the miner dev tax and believed it was unfair and not the ideal plan for development (we do too!). Many of us believe that the development should be funded voluntarily through donations, rather than by a tax forced upon the miners, without any accountability for the developers. The excitement around ZCL eventually caused it to pump in price before eventually dumping.

Miner "dev taxes" are lazy in our opinion. They come forth from a socialist mentality of thinking that cryptocurrency protocol development necessitates a subsidy. However, ZClassic still suffers from the same problems facing Zcash, since its privacy is optional.

ZClassic failed to solve any of Zcash's inherent privacy problems. There is nothing significant or special about ZClassic other than the removal of the controversial dev tax. **ZClassic is really just "TClassic," therefore we dismiss it from consideration as a serious investment.**

# The Bitcoin Private (BTCP) Hidden Inflation Scam

After abandoning ZClassic, Rhett Creighton (a popular smooth-talking crypto influencer who is considered by some astute crypto analysts to be a shady character) went on to launch and promote Bitcoin Private (BTCP), a fork-merge of Bitcoin (BTC) and ZClassic (ZCL), which is known by many to be a scam.

BTCP was shilled by John McAfee and there was lots of hype regarding it, with an influx of “dumb money” investors. However, it was later revealed that John McAfee was charging \$105,000 per tweet for promoting cryptocurrency projects.



<https://twitter.com/officialmcafee/status/974111841084469250>

It was also later revealed that BTCP’s founders had secretly premined 2 million coins for themselves and hid it in the shielded pool, hoping that no one would notice. Some analysts at Coin Metrics performed some fascinating in-depth forensic research to help uncover this fraud. Mr. X previously mentioned this in his article for the TDV January 2019 Dispatch.

Rhett has been called a “serial forker and a scammer” by many respected people in the cryptocurrency community after he created Zclassic & abandoned it. He then did the same with Bitcoin Private (and got fired from the team) and then announced he was fork-merging Primecoin and Bitcoin to form Bitcoin Prime (these are all worthless coins in our opinion).

We are informing you of this cautionary tale because these are the kinds of scams and fundamentally unsound projects that we want our subscribers to avoid. Watch out for these pitfalls!



**Peter Todd**  
@peterktodd



Really interesting fraud.

to;dr: Zcash clone Bitcoin Private secretly created an extra 2 million coin premine for the founders - something like half the market cap - hiding it in the shielded pool so no-one would notice.



**nic carter** @nic\_\_carter · Dec 23, 2018

So proud of the Coinmetrics team for this forensic analysis. One of the most fascinating case studies I've come across. Praise is due to @khannib for making the discovery and pushing through the investigation.

[coinmetrics.io/bitcoin-privat...](https://coinmetrics.io/bitcoin-privat...)

[Show this thread](#)

8:30 PM · Dec 23, 2018 · [Twitter for Android](#)

**258** Retweets and comments **772** Likes

<https://twitter.com/peterktodd/status/1077013558825795586>



<https://twitter.com/whalepanda/status/990286686595829760>

As seen above, crypto investor WhalePanda and even the Aeon community were keen enough to notice these scams. Don't fall for the hype, and be sure to do your own research!

## Zcash (ZEC) vs. Monero (XMR)

Over the past few years there has been an understandable aura of rivalry and debate between the Zcash (ZEC) and Monero (XMR) communities. Now, we will briefly compare the two across several metrics.







The fact that Zcash is a corporate coin domiciled in the USA is one of the reasons why we've decided to keep Zcash at such a small percentage in our portfolio compared to Monero. Zcash is clearly much more centralized in its development than Monero. In contrast, Monero had a **fair and open launch**, no miner tax, is not controlled by any company, but rather adheres to the **FOSS ethos** and **philosophy**, as we have explained in previous writings. It is researched & developed by enthusiastic volunteers & some full time staff who receive recurring donations



from individuals and businesses in the community for their work. This atmosphere draws some of the most brilliant minds and hackers to beef up the network’s security.

In the quest for digital cash, Monero firmly beats Zcash. In the 2016 article “[On Fungibility, Bitcoin, Monero and why ZCash is a bad idea](#)” by dnaelor, the owner of the website, [WeUse.Cash](#) has shared some helpful information comparing XMR to ZEC. This article explains the rise of blockchain analytics and Bitcoin tracing, and the growing need for a fungible digital cash where all transactions and balances are private by default. The author shares some information regarding the weaknesses and risks of Bitcoin mixers, CoinJoin, DASH, and how Monero avoids these risks. He also outlines the risks of Zcash, including its “trusted setup” (or cryptographic “toxic waste”) problem where an attacker could create invisible coins out of thin air without anyone else knowing - a topic which we will address in more detail in a section further below.

The folks behind the website [LocalMonero](#) have done a great job in creating a very informative article, “[Why Monero is Better than Dash, Zcash, Zcoin \(Even with Lelantus\), Grin and Bitcoin Mixers Like Wasabi \(Updated May 2020\)](#)” with a comparison chart and analysis of Monero (XMR) vs. other popular so-called privacy cryptocurrencies, including Dash, Zcash, Zcoin, Grin (Mimblewimble), and Bitcoin (BTC) mixers, as seen below.

						
Private	✓	✗	✗	✓	?	✗
Untraceable	✓	✗	?	✓	✗	✗
Secure	✓	✓	✓	✓	✓	✓
Fungible	✓	✗	✗	✓	?	✗
Decentralized	✓	✗	✗	✗	✓	?

*Comparison chart of Monero vs. other so-called privacy cryptocurrencies*

This article also mentions Zcash’s “trusted setup” problem, and the fact that Zcash’s transactions are public and transparent by default, and several of the other issues that we’ve already covered in this report. Since privacy isn’t mandated on Zcash’s network, this means that miners could censor certain transactions or blacklist certain coins/addresses, or even blacklist private

transactions in general (as we explained earlier). This results in some ZEC being less valuable than others, and undermines its fungibility.

In contrast, Monero (XMR) is indeed fungible. The article explains how Monero is both private and therefore fungible, since all balances, transaction amounts, sources, destinations, and wallet addresses, etc. are not publicly shown on the blockchain. Unlike the vast majority of **other** cryptocurrencies, Monero does not have a **rich list**, which is very important.

## Why Privacy Matters

It's important for **everyone**

- ✘ Targeted advertisements
- ✘ Who shall I rob today?
- ✘ Gossip on how you spend your money
- ✘ Look, boss, I'm part of a trade union!
- ✘ Unwittingly tainted money (fungibility)
- ✘ Contracts, salaries, margins, suppliers...
- ✘ Miners can become censors



*Monero is fundamentally private by default. Privacy Matters!*

Monero's privacy, **fungibility**, unlinkability, and untraceability are enforced by Monero's usage of **stealth addresses**, **ring signatures**, and **Ring CT**. Combined together, these technologies make it practically impossible for an observer to determine which funds have been spent, to link a transaction to a particular individual, or to determine the balance of one's funds. The fact that Monero enforces all transactions on its network to use its privacy features vastly increases its anonymity set (especially as its network of users grows).

# Regulatory Compliance

View keys allow transparency *optionally and on-demand*



*Monero is voluntarily/optionally transparent by address & transaction*

Monero is also optionally transparent. As explained in the diagram above, Monero users can voluntarily reveal transaction information via a **view key**. This can be useful for optionally revealing transaction information to selected parties, and can come in useful for auditing purposes, oversight of charities, or parents who are monitoring their children’s spending, just to name a few examples.

The FBI has expressed some **worry about criminals using Monero in the past**. More recently, a **leaked document from the FBI earlier this year** shows that they are **frustrated** with the fact that darknet market (DNM) users have converted “illicitly obtained Bitcoin into anonymity-enhanced cryptocurrency (AEC) Monero using the MorphToken cryptocurrency exchange, impeding law enforcement’s ability to trace the destination of the proceeds.”

In contrast to Monero, Zcash is not private in practice, as we have explained earlier. Remember that Zcash does not enforce privacy - it is transparent by default, and the vast majority of users do not use its privacy features.

As we explained earlier, it is well-known that zk-SNARKs are a strong privacy technology. Even Monero core contributor Riccardo “fluffypony” Spagni admitted this back in 2018. When comparing with Monero, he said that Zcash’s zk-SNARKs provided “much stronger untraceability characteristics than Monero (but a much smaller privacy set and much higher systemic risks)” at the time.



<https://twitter.com/fluffypony/status/1052095452651376640>

Keep in mind that since fluffypony’s tweet in 2018, Monero has continued to upgrade its privacy features. As of the time of this writing, Monero has stronger **ring signatures** at a currently enforced ring size of 11, **stealth addresses**, **Ring CT**, and Dandelion++.

Within the past few years, Monero upgraded to **bulletproofs** to make the range proofs required for its Ring CT technology more compact and efficient. Monero’s Ring CT (ring confidential transactions) utilizes a cryptographic primitive for encoding called a **Pedersen commitment** to hide the amounts in its transactions. Bulletproofs themselves are a form of NIZKP, or *non-interactive zero-knowledge proof* which does not require a “trusted setup” (explained further below).

Zero-knowledge proofs in the form of zk-SNARKs (as seen in ZEC) are a newer form of cryptographic technology than ring signatures. Ring signatures have been around for a while, and we know that they work well. The **idea behind ring signatures began in a 1991 research paper co-authored by cryptographer David Chaum**. However, zk-SNARKs are a newer

cryptographic technology, are more experimental, and are less peer-reviewed than the time-tested cryptographic technology of ring signatures.

Nevertheless, the technology behind zk-SNARKs is incredible, and it always bothered us that Zcash only provides them as an optional setting, as we explained earlier. Since Zcash does not require the usage of z-addresses and since the vast majority of users do not use them, ZEC ends up being almost as transparent as Bitcoin in practice.

For the past several years, Monero (XMR) has distinguished itself as the king of privacy coins by enforcing mandatory privacy for all transactions by default. But more recently, Pirate Chain (ARRR) has entered the scene, claiming to have the best of both worlds - mandatory privacy combined with cutting-edge zk-SNARKs, enforced for all transactions by default.

## The Flaw of the “Trusted Setup” Inherited From Zcash

On the [home page of its website](#), Pirate Chain (ARRR) claims to be the most private and secure cryptocurrency in existence to date, due to its mandatory usage of zk-SNARKs and integration with [Komodo \(KMD\)](#) for 51% attack protection via [Delayed Proof of Work \(dPoW\)](#). Its technology is quite revolutionary, and we will go into further detail later on in this report.



However, even if we were to assume the enforcement of mandatory zk-SNARKs in a hypothetical code fork of ZEC, there are still some [other points of debate in regards to design decisions about privacy and security](#) between the [Monero and Zcash communities](#), with some overlapping concerns that also apply to Pirate Chain as well. One of these overlapping concerns is Zcash’s “**trusted setup**” problem, which also shares some applications to Pirate Chain.

When Zcash was first launched back in 2016, it was heavily criticized for its so-called “trusted setup” which involved the [generation of secret master keys for its SNARK parameters](#) which are

required to generate its zero-knowledge proofs. This was accomplished by what their team referred to as a [multi-party protocol for generating the Zcash parameters](#).

In this helpful article, "[The Untrusted Setup – Why you shouldn't trust ZCash](#)" the author explains several risks and concerns regarding Zcash. One of the biggest concerns he mentions is a worrisome problem introduced by the "trusted setup" process, namely, the possibility of unlimited secret inflation by whoever possesses the secret master key.

*You could think of this secret master key as the Ring of Power which must be destroyed. He who possesses this secret master key could secretly create unlimited inflation, thereby giving a theoretically infinite number of coins to himself, whilst going completely undetected!*

In Zcash's so-called "trusted setup," this "cryptographic toxic waste" was allegedly created and then destroyed by six participants in Zcash's parameter generation ceremony. However, you absolutely **must** trust that at least one of six participants was honest, did not collude, was extremely thorough, exercised his/her duties perfectly, and did not in any way compromise the ceremony and allow anyone to secretly keep this key for him/herself or anyone else. In other words, there had to be at least one fully honest participant who did everything perfectly, thereby making it impossible for anyone to recover the secret master key.

In fact, Bitcoin developer Peter Todd was one of the six participants in the ceremony, and he [warned about some of the ceremony's risks in a blog post](#), and some tweets. This [article](#) contains some of this research, along with more helpful information on some of the risks of Zcash and Dash.



Peter Todd @petertoddbtc · Nov 1

The @zcashco trusted setup is not reproducible: there is NO way I can prove to you that I did not subvert it. END OF STORY. FULL STOP.

**Rudd-O @RuddO**  
 In re @zcashco @petertoddbtc / the trustworthiness of Zcash, which apparently is too hard to accept for people who ran anon software earlier

Julian Tech Article makes absolute sense. Crypto currencies are meant to be...  
 We gotta remember...  
 Rudd-O Stop with the trusted setup documented and it's reproducible, if...  
 "But you're not supposed to trust an untrusted trust" from the ACM paper...  
 SOMEBODY enhances are, however software yourself. Reason lacking to understand that trusting that at least...  
 ability their own hardware is a nice...  
 paranoia

21 42



Peter Todd @petertoddbtc · Nov 1

Only redeeming feature of the @zcashco backdoor is (as far as we know) it can't be used to violate privacy; can be used to shutdown Zcash.

**Peter Todd @petertoddbtc**  
 Let's be 100% clear: the @zcashco trusted setup is a backdoor, with no way of proving it has been disabled.

100% unlike other svstems. twitter.com/RuddO/status/7...

12 23

 **Peter Todd** @peterktodd

Let's be 100% clear: the @zcashco trusted setup is a backdoor, with \_no\_ way of \_proving\_ it has been disabled.

100% unlike other systems.  
[twitter.com/RuddO/status/7...](https://twitter.com/RuddO/status/793584540891643906)

This Tweet is unavailable.

6:44 PM · Nov 1, 2016 · [Twitter for Android](#)

58 Retweets and comments 76 Likes

 **Chaparro** @Alex\_Chaparro · Nov 1, 2016  
Replying to @peterktodd @petertoddbtc and @zcashco  
Does that mean what i think it means?

 1   

 **Peter Todd** @peterktodd · Nov 1, 2016  
Maybe? In don't read minds. :)

 2   3 

 **Chaparro** @Alex\_Chaparro · Nov 1, 2016  
Who knows effectively if it was disabled? Just you? You and @zooko?

 1   

 **Peter Todd** @peterktodd · Nov 1, 2016  
None of us do for sure - you try your best and hope it's good enough.

  1  2 

<https://twitter.com/peterktodd/status/793584540891643906>



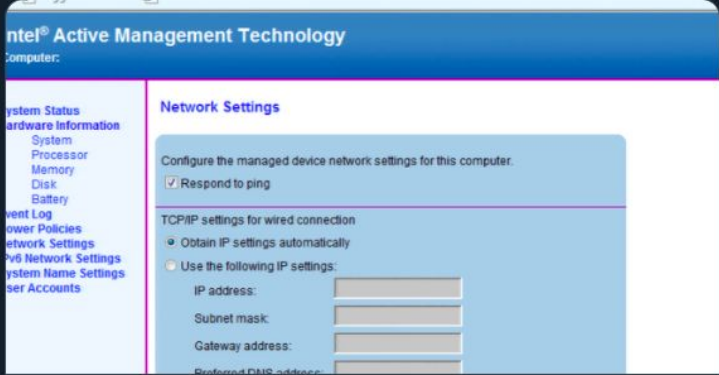


<https://twitter.com/peterktodd/status/793687647273230336>

**Peter Todd** @peterktodd

Thinkpad T520 I used for the @zcashco trusted setup was 100% vulnerable to this:  
[arstechnica.com/security/2017/...](http://arstechnica.com/security/2017/...)

See: [support.lenovo.com/it/en/product\\_...](http://support.lenovo.com/it/en/product_...)



The hijacking flaw that lurked in Intel chips is worse than anyone thought  
 Patch for severe authentication bypass bug won't be available until next week.  
[arstechnica.com](http://arstechnica.com)

7:19 PM · May 8, 2017 · Twitter Web Client

38 Retweets and comments 70 Likes

**Peter Todd** @peterktodd · May 8, 2017  
 Replying to @peterktodd and @zcashco  
 Just the networking computer, \*not\* compute node, so the airgap should have protected the setup. But shows the paranoia was 100% justified.

**Peter Todd** @peterktodd · May 8, 2017  
 Without the airgap the Intel AMT backdoor could have 100% compromised the @zcash trusted setup.

**Ethan Buchman** @buchmanster · May 12, 2017  
 Replying to @peterktodd @petertoddbtc and 2 others  
 List of entities that likely compromised ZCash setup is growing:

- 1) Canada Border Services Agency
- 2) Intel

Cool beans

<https://twitter.com/peterktodd/status/861722253788160000>

**Peter Todd** @peterktodd · May 8, 2017  
 Without the airgap the Intel AMT backdoor could have 100% compromised the @zcash trusted setup.

1 7 25

**Bathrobe Billionaire** @BRBillionaire · May 8, 2017  
 does this change anything in your mind regarding the sanctity of the zcash ceremony?

1 1

**Peter Todd** @peterktodd · May 8, 2017  
 Yes: an attacker may have compromised the DVD's, which were burnt and verified on vulnerable laptops.

1 4 6

**Peter Todd** @peterktodd · May 8, 2017  
 I'm going to have to recheck them on a clean computer, and even then it's a bit dubious: DVD's are \*not\* read-only - can be further burned.

1 1 5

**Emanuel Bronshtein** @e3amn2l · May 8, 2017  
 how are you going to recheck the DVDs? I guess it's possible to backdoor DVD via twin sector method [en.wikipedia.org/wiki/Compact\\_D...](https://en.wikipedia.org/wiki/Compact_Disc_1/2)

2 1 3

**Peter Todd** @peterktodd  
 Replying to @e3amn2l @BRBillionaire and 2 others

**At minimum finding a few DVD drives \*without\* burn capability, and rechecking w/ diverse controlling computes seems like a good idea.**

7:56 PM · May 8, 2017 · [Twitter Web Client](#)

5 Likes

**Riccardo Spagni** @fluffypony · May 9, 2017  
 Replying to @peterktodd @petertoddbtc and 4 others  
 Even then, the ISO could've been compromised in subtle ways (specific known-bad libraries for e.g.), or the MPC implementation could be bad.

1 2 3

**Peter Todd** @peterktodd · May 9, 2017  
 Yeah, there hasn't been enough attention paid to that IMO. Although at least that's stuff that can be determined after the fact.

1 4

<https://twitter.com/peterktodd/status/861731468921491456>

Some of these concerns were also addressed in the Crypto Briefing article, “[zk-SNARK Glitch Could Result In Crypto Double Take](#)” which explains some of the zk-SNARKs algorithm’s assumptions, including the first Knowledge of Exponent Assumption (KEA1), which “states that transactions must be correct if they have a certain output.” If this was ever broken, then an attacker would be able to falsify the cryptographic proofs and create coins out of thin air.

Peter also had additional concerns about the ZEC trusted setup, thinking that it could be theoretically backdoored as explained [here](#). Whether or not these concerns are valid has been the subject of debate.

Therefore, it makes sense when we hear discussion of distrust for Zcash’s leadership and their “trusted setup.” Several members of the Monero community have voiced their [comments and concerns regarding the disaster of Zcash’s trusted setup](#).

*“Zcash is not unconditionally sound, can’t be with current tech...requires a trusted setup... will need to redo the procedure [Trusted Setup] to upgrade the crypto over time so it’s a vulnerability.”*

- Gregory Maxwell, Bitcoin Core developer and cryptographer, [in a presentation to Coinbase](#)

In the [article “Battle Of The Privacycoins: Zcash Is Groundbreaking \(If You Trust It\)”](#) from [Bitcoin Magazine](#), the author argues that Zcash fails the “don't trust, verify” test which Bitcoiners often swear by. The author claims that Zcash’s trusted setup not only allows for unlimited hidden inflation, but that it could undermine its privacy as well.

Another helpful article, “[The Zcash Catch](#)” explains the risks of Zcash’s trusted setup. A followup article, “[How To Compromise Zcash And Take Over The World](#)” explains even more implications of these risks.

Additionally, Peter Todd has raised concerns claiming that not only does a trusted setup introduce the risk of unlimited secret inflation, it also could introduce risks of breaking users’ privacy as well, as seen in the tweets below.

**Peter Todd** @peterktodd

There's been some claims made recently that a compromise of the Zcash trusted setup can't compromise privacy.

I checked with one of the cryptographers working on zk-SNARKs, and these claims are false.

A compromised MPC absolutely can wreck privacy; Zooko needs to correct this.

the SNARK parameters securely? >>

If the Zcash Ceremony was compromised, could the attacker compromise user privacy? — @feministPLT

Replying to @AnonOnAMoose and @peterktodd

The powers of tau ceremony will also have this property. It won't "fix" it because Peter's statement about the previous ceremony is wrong - as he or his anonymous cryptographer would have seen if they had read even

3:18 AM · Sep 27, 2018 · Twitter for Android

44 Retweets and comments 110 Likes

---

**Peter Todd** @peterktodd · Sep 27, 2018

Replying to @peterktodd

The problem is that the final public parameters can be constructed in such a way that they do not protect privacy. Doing this correctly is the responsibility of the MPC coordinator; the Zcash daemon is unable to verify that the parameters are correctly constructed.

4 7 14

---

**Peter Todd** @peterktodd · Sep 27, 2018

I raised this issue months ago and nothing was done. In fact, as of writing it's not possible to verify the MPC correctly generated public parameters as the necessary files are missing; a GitHub issue for this problem has been open for six months:

Amazon S3 links in README are broken · Issue #10 · zcash/mpc  
github.com

2 6 20

**Peter Todd** @peterktodd · Sep 27, 2018  
 Not the only trusted setup related issue that's been ignored by the Zcash team: the build process broke a month after the ceremony, and Zcash has been ignoring patches to fix even these basic issues.

Highly suspicious they have zero interest in people auditing the trusted setup.

2 8 34

**Peter Todd** @peterktodd · Sep 27, 2018  
 Zooko and others need to correct these false statements, fix the trusted setup auditing issues, and apologize.

With Zooko is paid about \$250k/month directly from the ZEC block rewards, standards for ethical conduct around accurate disclosures are high.

4 10 58

**Daira Hopwood (abolish ICE)** @feministPLT · Sep 27, 2018  
 Replying to @peterktodd  
 The claim is correct. We will fix the availability of files needed to verify the MPC; I apologize for having overlooked that.

1 1 8

**Peter Todd** @peterktodd · Sep 27, 2018  
 So to be clear, you're saying that regardless of what the trusted setup process did, privacy is preserved?

2 1

**Daira Hopwood (abolish ICE)** @feministPLT · Sep 28, 2018  
 I'm saying that if you verify the setup (when the necessary files are restored), and check that the hashes of the verified parameters match those in fetch-params, then privacy is preserved modulo any bugs or design flaws (which is a question that needs to be addressed separately)

2 1 6

**Peter Todd** @peterktodd · Sep 28, 2018  
 Which is what I'm claiming: a compromised setup can wreck privacy.

The Zcash FAQ makes a stronger claim: that even a completely compromised setup couldn't harm privacy. Failures of the MPC are included in that.

How many impls of it exist? One afaik.

2 3

**Peter Todd** @peterktodd · Sep 28, 2018  
 Notice how this was hardly know until I started publicising it, strong evidence that people are being mislead.

1

<https://twitter.com/peterktodd/status/1045210959407706112>

So, how does Monero compare to Zcash in regards to the “trusted setup”? In contrast to Zcash’s trusted setup, Monero is unique from a design perspective because it is trustless, and does not require trusting any party to destroy the cryptographic “toxic waste” of an all-powerful secret master key, because no such key exists due to its design. Instead, Monero is based on time-tested cryptographic assumptions that are universally accepted, and have undergone more thorough peer-review.

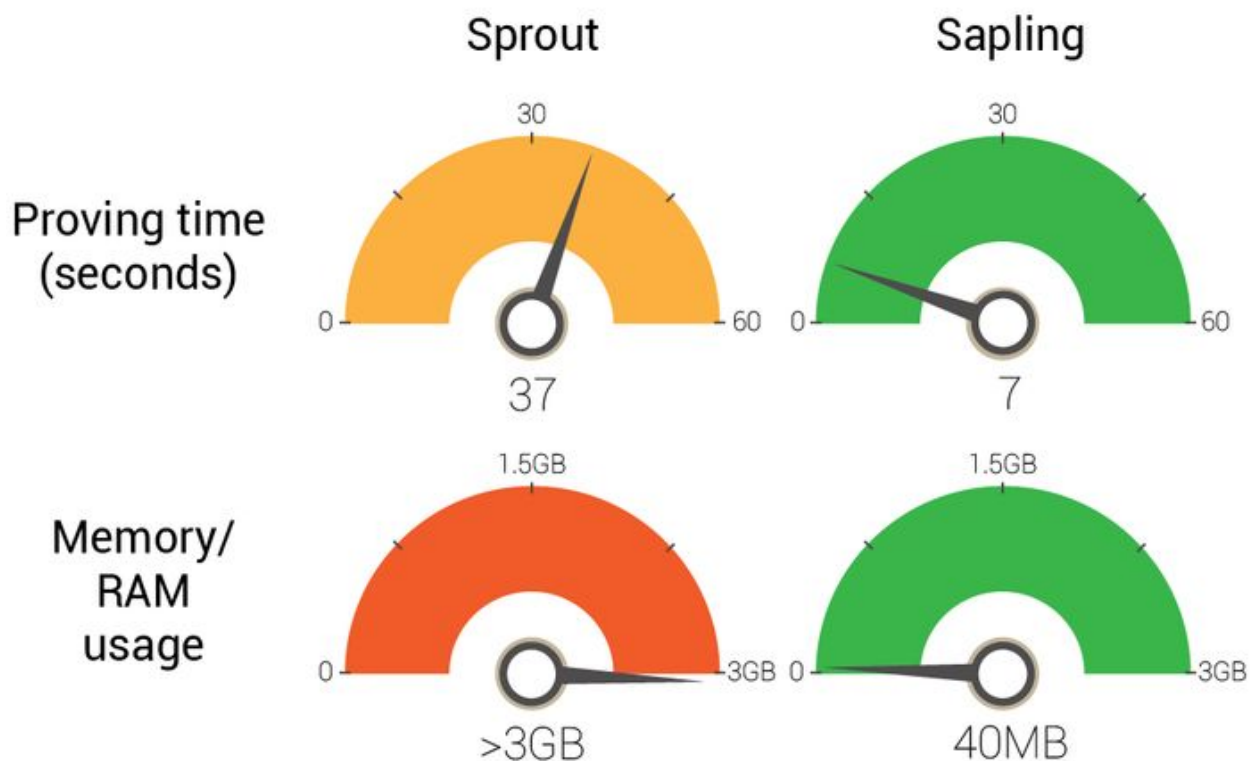
We recommend reading the Monero StackExchange question and comments on the page “[What is the difference between “trustless” and “trusted” system?](#)” since it explains more details regarding this important fundamental difference between Monero and Zcash’s design. Monero’s design choice to use a trustless system is also the reason why we have such a large portfolio allocation to Monero, because it is more trustless (its security relies more on math and cryptography itself rather than humans).

Basically we consider Zcash to be more of a centrally planned “privacy” since it requires that you trust the founders. That is a poor design choice in our opinion. In contrast, Monero is much more trustless, and only requires trusting math & cryptography. Remember that Zcash’s cryptography is less peer-reviewed than Monero’s cryptography.

Based on this information, all of these red flags have given reason for us to be cautious regarding allocating a large percentage of the TCV Portfolio to ZEC.

## **Zcash Upgrades**

Zcash proponents have argued that since the time of the original “[trusted setup](#)” ceremony in 2016, the Zcash team has upgraded its zk-SNARKs system, (including the parameter generation). Also, another criticism of ZEC was that it was resource intensive and took a long period of time to generate the zero-knowledge proofs to utilize z-addresses (especially in the original Zcash “Sprout” network). However, after upgrading to “Sapling”, ZEC has made some [significant improvements in efficiency and speed](#).



*Faster & more efficient zk-SNARKs as seen in Zcash's Sapling upgrade*

In order to mitigate the risk of cryptographic “toxic waste” the Zcash team constructed multi-party computation (MPC) protocols so that various different people could work together to generate the parameters securely. As we explained above, Zcash’s **original parameter generation in the 2016 Sprout MPC ceremony** was heavily criticized by Bitcoin developer Peter Todd and others.

For Zcash’s second set of public parameters, there were two phases - the *Powers of Tau*, and the *Sapling MPC*. The Zcash Foundation announced the **Powers of Tau MPC ceremony** in November 2017, and **completed it** in early 2018. Instead of what was seen in the Sprout MPC, which required six participants to all be available and maintain custody of their hardware for the entirety of the process, the **Powers of Tau ceremony** had a total of 87 participants, each of whom performed computations to be used for generating new zk-SNARK parameters. The Zcash Company organized the **Sapling MPC** for constructing Sapling’s final zk-SNARK parameters and accepted over 90 contributions, and after completing the process, the parameters were included in the 2.0.0 Zcash software release.

In this second set of public parameters, Zcash Electric Coin Company engineer Sean Bowe **said**, “each of these phases [Powers of Tau & Sapling MPC] has the property that only one of its participants must be honest for the final parameters to be secure.” According to Sean, both the



Powers of Tau and Sapling MPC were open to anyone who wanted to contribute, meaning that there was much a greater chance of at least one honest person participating in each ceremony.

## **Comparing & Contrasting Pirate Chain (ARRR) vs. Monero (XMR)**

Remember that Pirate Chain (ARRR) is based on much of ZEC's code. As we mentioned earlier, in ARRR there is a theoretical risk of unlimited inflation if the ZEC trusted setup was compromised, but much of this risk has since been mitigated. This is due to the fact that ARRR implemented the zk-SNARKs parameters that were generated during ZEC's Sapling upgrade (the ARRR developers copied the relevant code from ZEC). When the ARRR developers upgraded Pirate to Sapling, they used the same Sapling master key as ZEC, which utilized the new parameters generated from the Powers of Tau & Sapling MPC which was more secure than the Sprout parameter generation.

Even though much of the original risk of ZEC's original Sprout trusted setup has been arguably mitigated, the fact is that ZEC & ARRR still both suffer from a trusted setup (the Powers of Tau/Sapling one) which is still a design flaw in our opinion. At a fundamental level, the fact that a trusted setup is needed *at all* is a problem by itself.

Therefore, we consider both ZEC & ARRR to be both inferior to Monero (XMR) & Wownero (WOW) in regards to **trustless** privacy & fungibility. In other words, we consider ARRR to be more risky in its cryptographic assumptions than Monero or Wownero because it requires trust that the ZEC Sapling trusted setup's participants initialized the zk-SNARK parameters in a secure way. Nevertheless, it remains clear that ARRR's privacy is much, much stronger than ZEC's privacy, since ARRR enforces the usage of z-addresses and ZEC does not (as we explained earlier).

Assuming that its trusted setup wasn't compromised, ARRR would theoretically have a larger anonymity set for its private transactions when comparing with XMR. However, keep in mind that ARRR is not *pure* Proof-of-Work (PoW) like BTC or XMR since it also uses Komodo's delayed Proof-of-Work (dPoW) technology (as we will explain further below), and it is not ASIC-resistant like XMR, since ARRR uses Equihash instead of RandomX. For example, there are ASICs available for the Equihash algorithm, as seen below.

# 蚂蚁矿机 Z15

突破重围 打造非凡

420 KSol/s | 1510 W

14:00 开售



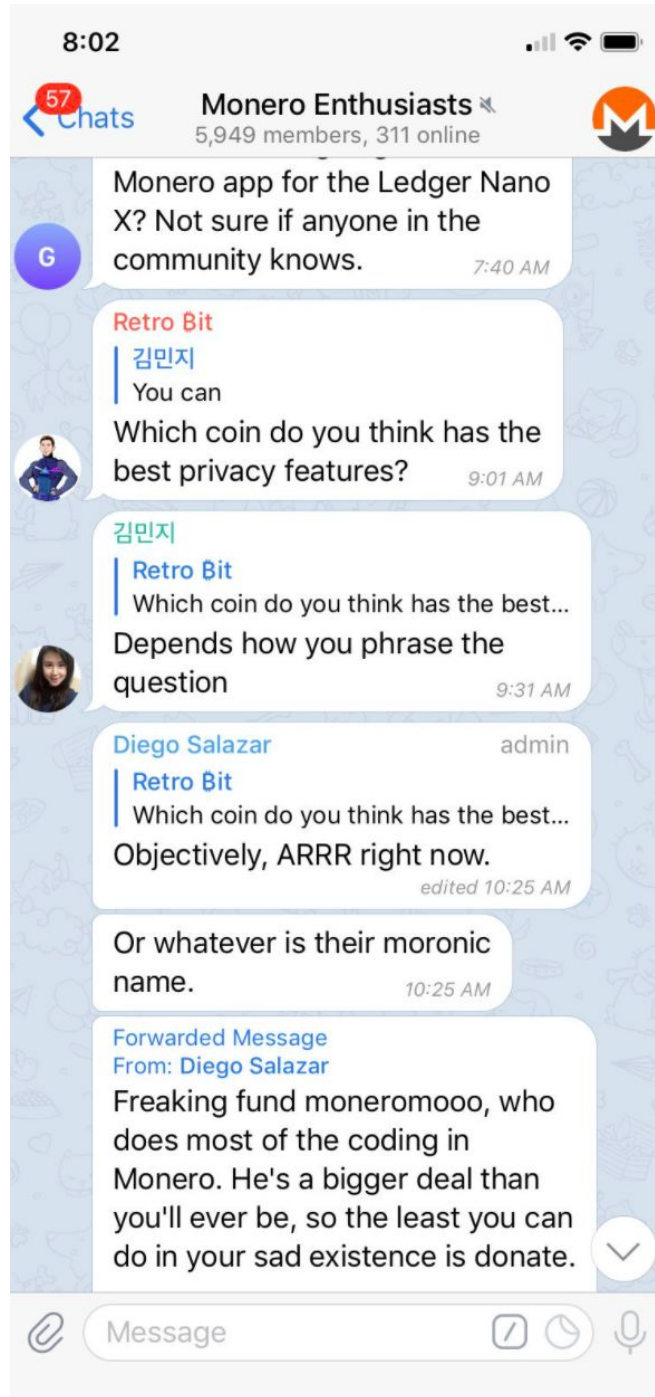
**BITMAIN | ANTMINER**  
<https://shop.bitmain.com>

*Bitmain's new Antminer Z15 Equihash (ZEC) ASIC miner*

From a technical standpoint, one could also argue that ARRR has stronger privacy than XMR and WOW due to its usage of mandatory zk-SNARKs. As we mentioned earlier, ARRR claims to be the most private cryptocurrency in the world to date. This may actually be true, especially as more people begin to adopt it, as we explain further below.

However, this leads into a counter-argument from XMR's standpoint, since ARRR currently has a much smaller user base than XMR as of the time of this writing. Therefore, Monero's much larger community and number of active users increases its anonymity set beyond that of ARRR, since XMR's ring signature decoys are selected randomly from historical transactions on its blockchain. This implies that any benefit provided by a theoretically greater anonymity set of ARRR per transaction could potentially be comparable, or even smaller than XMR's anonymity set, in practice. **As of the time of this writing, we would consider this point to be debatable, and more research is needed in this area.**

Several people have commended Pirate Chain (ARRR) for its large anonymity set and high level of privacy. For example, the Zcash Foundation has allegedly recognized ARRR for this, and even [Diego Salazar](#), a respected member of the Monero community, has praised Pirate Chain for their privacy innovations as seen in the Telegram screenshots & tweets below.



<https://twitter.com/xKOSIUSx/status/1191777213391233024/photo/1>

## Conclusions

- (i) Privacy-respecting currencies can provide only plausible deniability (alternative explanations for the ledger are readily available). No such thing as perfectly anonymous currency.
- (ii) As anonymity set size increases, claims of plausible deniability get stronger, (best performance with the full anonymity set i.e. ARRR).
- (iii) I think there is a critical ring size above which claims of plausible deniability are "good enough" vs. threat model like a curious-but-honest Eve.
- (iv) For sufficiently large anonymity set size, default-on small anonymity sets outperform opt-in large sets (preliminary results indicate this is correct).

18 / 18

8:48:40 / 9:29:30

<https://twitter.com/xKOSIUSx/status/1191777213391233024/photo/2>



**Zcash Foundation**  
@ZcashFoundation

Replying to @PirateChain and @dukeleto

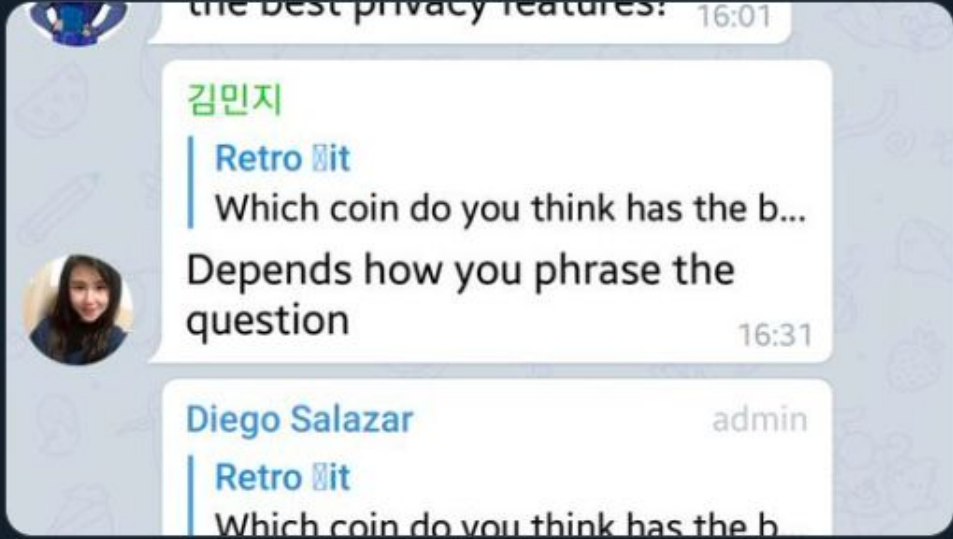
**We commend your work in this area, and the size of the PirateChain anonymity set is awesome!**

12:04 PM · Jun 23, 2019 · [Twitter Web Client](#)

<https://twitter.com/xKOSIUSx/status/1191777213391233024/photo/3>

**Stephen "Crrrrrrrrrrrrumb" York** @StephenYork111 · Jun 17, 2019

Even the @monero Telegram community admin admits, that @PirateChain offers the best privacy right now!  
 #FinancialPrivacy  
 @BBCTech @cnntech @crypto @ForbesCrypto @WIRED @CaitlinLong\_ @emilychangtv @mikejcasey @ResearchCircle @GrayscaleInvest



2    16    23

**Diego "rehrar" Salazar** @ofthesalazar · Jun 17, 2019

I should have known that anything I'd say would get posted. I'll watch it from now on. While I'd still stand by my statement, I'd put a huuuuuuuge asterisk next to it. Particularly in not knowing what attack vectors being built on Komodo introduces (since I don't know Komodo) 1/2

1    2    3

**Replies**

**Diego "rehrar" Salazar** @ofthesalazar · Jun 17, 2019

Replying to @ofthesalazar @StephenYork111 and 12 others

and, secondly all of this being predicated on the trusted setup being done properly, as people like Peter @peterktodd have claimed that a compromised trusted setup may indeed compromise privacy and not just infinite inflation. I assume no competency. So all this is in theory. :)

1    2

<https://twitter.com/ofthesalazar/status/1140657299293233152?s=19>

After Diego's message was publicized, he clarified that there could be potential risks associated with it being built on Komodo and the assumption of a successfully executed trusted setup, as seen in the above screenshot.

On the other hand, if ARRR's user base and adoption grows significantly in the future, and if it is able to somehow improve its cryptography to no longer require a trusted setup, then we believe it could potentially rise in adoption and therefore in price to compete with Monero for first place in the realm of private, fungible, digital cash that actually works in practice (rather than in theory, like ZEC).

Keep in mind that XMR has remained competitive throughout this time, and has been constantly innovating and improving its privacy as well. Monero has a far more established user base and larger team of Ph.D. mathematicians, cryptographers, and researchers which gives it more of a competitive advantage over ARRR. For example, there is **exciting new research and work already being done by the Monero Research Lab into post-quantum cryptography** to make Monero more future-proof. The Monero Research Lab has also been innovating and researching more advanced privacy technologies with **Triptych & Arcturus** which would massively increase Monero's privacy & efficiency if implemented.

*“A post-quantum world would destroy Amazon, Wells Fargo, Visa, and most world governments. But there's no reason it has to also destroy Monero.” -Surae Noether (Dr. Brandon Goodell), Monero Research Lab*

**For all the people who would be quick to call ARRR a guaranteed “Monero killer”, we would say, “hold your horses.” As we've explained, although ARRR is probably Monero's closest competitor in terms of privacy, it is nevertheless important to understand that each coin is built on different premises and cryptographic assumptions. Now of course, that doesn't mean that it's guaranteed to be impossible for ARRR to eventually overtake XMR in the future and take its place on the throne as the new king of privacy in the crypto sphere.**

As we've explained, it's important to note that ARRR's design choice suffers from the same trusted setup flaw as ZEC, which could theoretically allow unlimited secret inflation of coins (and possibly even a risk of privacy being broken, according to Peter Todd) in the unlikely event that it was compromised somehow. ARRR's design also involves assumptions regarding zk-SNARKs, which are less peer-reviewed and time-tested than Monero's ring signatures.

**When evaluating the risks of Pirate Chain (ARRR) vs. Monero (XMR), a potential risk with XMR is that in the future, there is the possibility that a powerful attacker with a quantum computer could theoretically deanonymize today's transactions**

since the coins are essentially obfuscated via ring signature “decoy” transactions with a smaller anonymity set for each particular transaction (currently at a ring size of 11). Some of **Monero’s early transactions (pre-2017)** which were thought to be private, and ended up being vulnerable to some tracing attacks (**these vulnerabilities have since been patched**). In contrast, zk-SNARKs are more private than ring signatures since they have a higher anonymity set for each transaction (all other transactions in the system).

Assuming that ARRR’s trusted setup was executed properly and that zk-SNARKs are never broken in the future, ARRR could potentially end up being more secure and private than XMR in the longer term, and time will tell. Keep in mind that Monero is continually improving its privacy, so a lot of this also depends on the caliber of the team who is developing each coin, and their skills at staying ahead in the privacy cat and mouse game.

Time will tell whether or not ARRR can rise up to compete with XMR, but from our analysis, we consider it to be a strong possibility, and hence we believe that ARRR is massively undervalued, as we will explain further below.



# Why **Pirate Chain (ARRR)**?

## Zcash (ZEC) vs. Pirate Chain (ARRR) Comparison

Category	ZEC	ARRR
Launch date	2016-10-28	2018-08-29
Block time	75 seconds	60 seconds
Mining algorithm	Equihash Proof of Work (PoW)	Equihash with delayed Proof of Work (dPoW)
Outstanding supply	9,838,756 (source: <a href="https://api.zcha.in/v2/mainnet/network">https://api.zcha.in/v2/mainnet/network</a> )	164,936,255 (source: <a href="https://explorer.pirate.block/api/supply">https://explorer.pirate.block/api/supply</a> )
Market price	\$88.48	\$0.06076
Market capitalization	\$869,756,628	\$10,021,526
Privacy	Fully private z-to-z transactions are optional, but extremely rare in practice. <b>Only 0.1% of transactions on the network use its zk-SNARKs privacy features correctly.</b>	Transactions to t-addresses are not allowed - users can only send to z-addresses, resulting in enforced zk-SNARKs privacy.



**The Beginnings of Pirate Chain (ARRR)**

The Pirate Chain whitepaper’s abstract says this:

*“[Pirate Chain is] 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.” -The Pirate Chain Code V2.0*

Pirate Chain (ARRR) was launched on August 29, 2018, and initially started out as an experiment to see if mandatory usage of z-addresses would work on a **Komodo (KMD)** asset chain, in an effort to solve Zcash (ZEC)’s fungibility problems. It began **as an experimental challenge when contributors to the Komodo project decided to create an asset chain with enforced usage of zk-SNARKS**, according to **Komodo** developer and community member Satinder Grewal. Essentially, the team’s goal was to make a dPoW-protected Komodo asset chain with code forked from ZEC that would remove the optional usage of transparent t-addresses seen in ZEC, and enforce the usage of z-addresses only.

According to the **Pirate Chain Beginner’s Guide**:

*“The goal was simple: to create a completely anonymous cryptocurrency that is secure, untraceable and keep the identity of those who transact with it anonymous. Developers of various cryptocurrencies came together to create Pirate Chain to show the world that it’s not only possible, but also necessary. It has been proven by government agencies and chain analysts that Bitcoin, as well as all of the other “privacy” cryptocurrencies, can be traced and data can be taken from them in order to find out who uses these currencies, how much they spend and who they transact with. Pirate Chain, on the other hand, has none of these issues, as it uses military grade encryption and delayed proof of work to make it the most secure and anonymous cryptocurrency in the world!”*

Another exciting fact about Pirate Chain is that it was created in what we consider to be an organic and honest way. Similarly to Monero, ARRR was launched fairly, and has had no ICO, IEO, premine, or miner/dev tax/fee. This is icing on the cake in our opinion, since an abundance of crypto projects are created without any real innovation, and are mostly intended to make the founder(s) rich.

Some of the most innovative coins (like Bitcoin and Monero for example) were created voluntarily and fairly in a decentralized way, and not by a company, but rather by passionate

volunteers who were excited about creating what they believe to be the best kind of cryptocurrency that could fulfill the qualities of sound money. Since ARRR was essentially created in a Discord chatroom and announced on the BitcoinTalk forums without much advance notice, some of the early miners decided to give out airdrops and rewards for promoting the coin in order to help bring it some publicity, and others began engaging in OTC (over the counter) trading of their Komodo (KMD) (or other coins) for PIRATE (the old name before rebranding to ARRR), as seen in these screenshots archived by Satinder Grewal from the early BitcoinTalk forum and Discord discussions.





**grewalsatinder** 08/31/2018

I found better name for it 😊

if want it can buy it

pirate.black

domain

If we are really going the way of trading then I guess I can go ahead and put an ASK for PIRATE coin.



will buy 1000 PIRATE for 1 KMD



**SHossain** 08/31/2018

@grewalsatinder for you 1000 PIRATE for 10 KMD 💀



**grewalsatinder** 08/31/2018



nope

1 KMD for 1000 PIRATE

let me know if anyone selling.



**scubapanda** 08/31/2018

Pirate.business is also available 😊



**grewalsatinder** 08/31/2018

Leaving the domain buying and decisions to community.

I don't want to be part of this management and stuff 😊

happy just being dev


if need to setup a simple github.io webpage, there I can help for sure 😊

**jl777B**  
Full Member  


 **Re: [ANN][PIRATE] A zk-SNARKS transactions only blockchain**  
September 04, 2018, 09:08:02 PM

[quote](#) **+Merit**  
#35

Activity: 448  
Merit: 133

  
Trust:  
**0**: -0 / +0  
Ignore

I suggested that a reasonable amount of PIRATE be made available to the community at mining costs. Something like 5000 PIRATE lots, with some limit like 50 people.

that is 250,000 PIRATE and over 10% the current supply. The community is now knowing about this unexpectedly popular PIRATE and the early birds are willing to set aside a big percentage of their PIRATE for the community.

Mining cost is being calculated now, distribution will have to wait until the weekend. I believe most of the initial sales were at 0.001 KMD per PIRATE, so that is 5KMD per 5000 PIRATE.

first 50 to reserve their spot will get their 5000 PIRATE, no newbie accounts

[Report to moderator](#)

*ARRR developer jl777 suggests selling coins to community at mining costs*

grewalsatinder

Full Member



Online

Activity: 185

Merit: 100

Posts: 185



Blockchain  
Technology  
Enthusiast, IT Pro



Trust: 0: -0 / +0

Re: [ANN][PIRATE] A zk-SNARKS transactions only  
blockchain

September 04, 2018, 10:33:33 PM

quote

edit

delete

+Merit #39

Quote from: Big Naturals on September 04, 2018, 10:13:09 PM

Quote from: grewalsatinder on September 04, 2018, 09:27:56 PM

I have edited the OP post and removed Test.

Please figure out as a community what you guys want.

**I do not and can not control this assetchain, as I'm neither a miner nor a developer for this assetchain.**

Wants to fresh start, do it. wants to make a new assetchain do it.

Don't blame me of what I did not do.

I know you worked hard on komodo for many years, you have a reputation as a hard working contributor who has done a lot to make komodo successful. Getting negative feedback can hurt, but it's honestly given, everyone here dreams of stacking a bag of a future top coin @ fractions of a penny, and then cashing in 50% and making 250k USD, there's nothing wrong with that BUT, in this case with pirate you should not have been telling others not to buy while you were obviously buying big yourself. You probably didn't want to be held responsible in case pirate failed, but in crypto where there are so many scammers everywhere it was a bad look, and can easily be misinterpreted forever, like Dash launch.

Thanks for some nice words.

You do realise the proposal James mentioned, all those PIRATES will solely coming from my pocket which I bought for KMD price of range from 0.001 KMD to 0.00180.

I still agree with u all that discard this chain and start fresh if u want. But that's not my decision. I can not do anything else to help u guys other than expressing my thoughts on the situation and giving the amount what James is proposing.

I don't care if my KMD bought PIRATE goes poof!

Just don't blame me of what it did not do.

Since I was traveling and spending some family time I could not edit the posts on time. Done that today.

**Pirate\_Arr**  
Newbie

Re: [ANN][PIRATE] A zk-SNARKS transactions only blockchain  
September 05, 2018, 08:35:07 AM

quote +Merit #54

Arr PIRATE maties,

More than 10% of current PIRATE supply will be airdropped to those who missed out on early days mining.

There is now a public pool with working payouts to Z-addresses, if you want to mine it easily (thanks to Webworker01): <https://pirate.komodostats.com>  
To qualify for the airdrop all you need to do is supply a Z-address in a PM.

**RULES:**

- > The airdrop amount is 250,000 PIRATE
- > Send your z-address in a PM to this user
- > The airdrop will happen on: 19th of September 2018
- > Cut off for supplying Z address is the day before: 18th September at 0 UTC
- > Any Z-address submitted after this time will not be included in the airdrop
- > The PIRATE will be divided evenly over the addresses supplied. If 250,000 people apply you will each get 1.
- > Any BTT accounts made after 1st September 2018 or newbie accounts, will not be included in the airdrop!

(This account will be the official PIRATE account from now on)

Report to moderator

**grewalsatinder**  
Full Member

Re: [ANN][PIRATE] A zk-SNARKS only blockchain, Tor, secured by dPoW and BTC hash  
September 25, 2018, 09:45:13 AM

quote edit delete +Merit #132


Online

Sent PIRATE to all Z address in giveaway list.

Quote

```
$ pirate-cli z_sendmany "zcZ97kb3zUrMnrkgSmFaaRRqti7nsM2NN8zgtc8D38jXjuPz5vHD8yQcgrcss8mSpbKnqWWRZXSfFaaQs8xXbkNwSgyDtfSs" [{"address": "zc8dk2U4XFA33YyPj1cwcYX7WEVY5df65ytxK645vt4SDuVeryXBjd54gEHEH2mKlRv5rAzrqbmLrqS2fDPWdLTd7ia3Q9w", "amount": 8333.33333333}, {"address": "zc8hxawZwMBJsDFunJdCBH5YtmxKJeYg9Q7YGY41QdktTCCqVbPEAagnxwzxcwccyBIMB54UY2TYZff9HHJz5EJk33UxQPh", "amount": 8333.33333333}, {"address": "zc8jkn4toCtS8qyQEAH9nixwxFJs9pRtrKgmQXdLWvyYUH2MECetwrRrxHNGb1NwMSYYPvwLxEDZfiPaHyDmdE8SkMe6n6", "amount": 8333.33333333}, {"address": "zc8w3sBtD2psDvrT4QisZmudhvZDVixnK2DYtn95vM69NvrZRMHdAbCIBjm55hyp8P7NmQLfHTAwdWIzqd436eN14ajBv", "amount": 8333.33333333}, {"address": "zc9LhAgdFcXp4HBQ2gmWSuDMF2uRzZYdGCZ5M5GKve8QoYsfqoZoB86TKIC4q5ZPyJ4S49XuZA3WybbR5L4w13pzMCsUpWi", "amount": 8333.33333333}, {"address": "zca7mpEFZi2V1Spqhxt13MSRu7Cw858YVDDZocVanmzmGafshXhzSnnkbumdLm7ghTGme68sqYXWkaN"}]
```

Activity: 185  
Merit: 100  
Posts: 185



Blockchain Technology Enthusiast, IT Pro

Trust: 0: -0 / +0

*Satinder and early community members/miners decide to do a giveaway of 250,000 coins instead of relaunching the chain from scratch in order to avoid complaints of an unfair launch like what was seen in DASH*

There is a beautiful scrollable timeline of the history of Pirate Chain available [here](#). It's worth a look!

## Pirate Chain (ARRR)'s Privacy and Security Innovations

Pirate Chain (ARRR) is the first fully private-by-default zk-SNARKS cryptocurrency in the world, and has already been listed on several exchanges. Since its blockchain does not allow users to make any transactions to t-addresses, ARRR is completely private, and doesn't leak metadata (three letter agencies crave this). The only times that t-addresses are used is when new coins are mined (block rewards) and for delayed Proof-of-Work (dPoW) notarizations. This is in order to ensure the integrity of the chain, and to help provide accountability of the block rewards such that the current supply of outstanding coins in circulation is public knowledge. However,



privacy is still preserved, since all of those coins are forced to move to z-addresses and are essentially invisible going forward. With ARRR, the blockchain observers cannot see users' balances, amounts transacted, or determine which addresses transacted with whom.

Pirate Chain is also recognized for its highly secure blockchain due to its integration with Komodo. ARRR claims to have advanced immunity against 51% attacks, and is protected by Komodo's **delayed proof of work (dPoW)** algorithm, as **explained** below.



**delayed Proof of Work (dPoW)**  
protects Pirate's blockchain from damage against double spends and 51% attacks by attaching a backup of the ARRR chain to the Bitcoin Blockchain.

find us on [www.pirate.black](http://www.pirate.black)

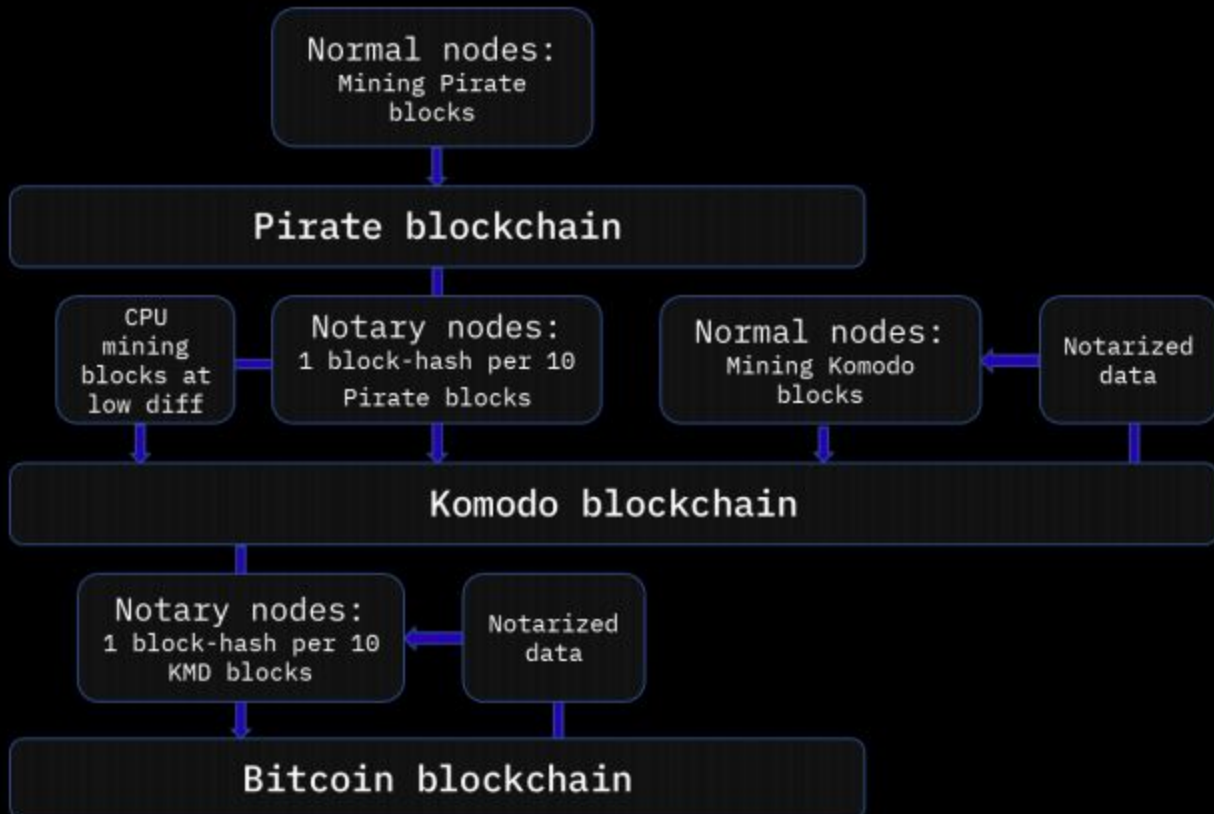
*Pirate Chain (ARRR) uses Delayed Proof of Work (dPoW)*

In order to successfully 51% attack Pirate Chain, the attacker must also 51% attack the BTC chain and the Komodo asset chain itself simultaneously in order to change anything, as seen in the diagram below.

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.



*Pirate Chain's delayed Proof-of-Work, ARRR whitepaper, page 13*

However, this **does not mean that ARRR is dependent on Komodo**. If Komodo were to disappear tomorrow, ARRR would still exist; it would only lose its delayed proof of work (dPoW). If Komodo were to disappear tomorrow, ARRR would essentially become a normal PoW cryptocurrency that uses the Equihash PoW algorithm.

Delayed proof of work acts like a checkpoint. Komodo transactions are notarized on the BTC blockchain every 2 minutes, and are protected by the strength of BTC's massive hash power.

The same thing happens with Pirate Chain transactions. ARRR transactions are notarized on the Komodo blockchain, which are then notarized on the BTC blockchain. An attacker would have to successfully 51% attack all three chains in order to change the history of Pirate Chain, which makes it highly secure (while still maintaining decentralization) in comparison to Proof-Of-Stake (PoS) or more centralized masternode-based cryptocurrencies which have **suffered attacks the past.**



<https://twitter.com/AgoristN/status/1276963331836792832>

ARRR's Captain Draeth said in a **June 27, 2020** interview on the Agorist Nexus podcast that **Pirate Chain is “the best of both Monero and Zcash combined, meaning that, [ARRR is] private by default like Monero, but [ARRR uses] the best...privacy protocol which is zk-SNARKs...”**

ARRR's emission schedule results in a maximum coin supply approaching roughly 200 million coins over a period about 3,000 days (to be more exact, a total of 199,109,119.99420500 coins by the year 2043+), as seen on page 16 of the Pirate Chain whitepaper below.

### Emission scheme and technical characteristics

Pirate chain contains the following technical characteristics and features after the 15<sup>th</sup> 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

### Emission schedule

Days	PIRATE (ARRR)
0	0
500	~1,200,000,000
1000	~1,800,000,000
1500	~1,950,000,000
2000	~1,980,000,000
2500	~1,990,000,000
3000	~1,994,205,000

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).

*ARRR coin emission schedule, ARRR whitepaper, page 16*

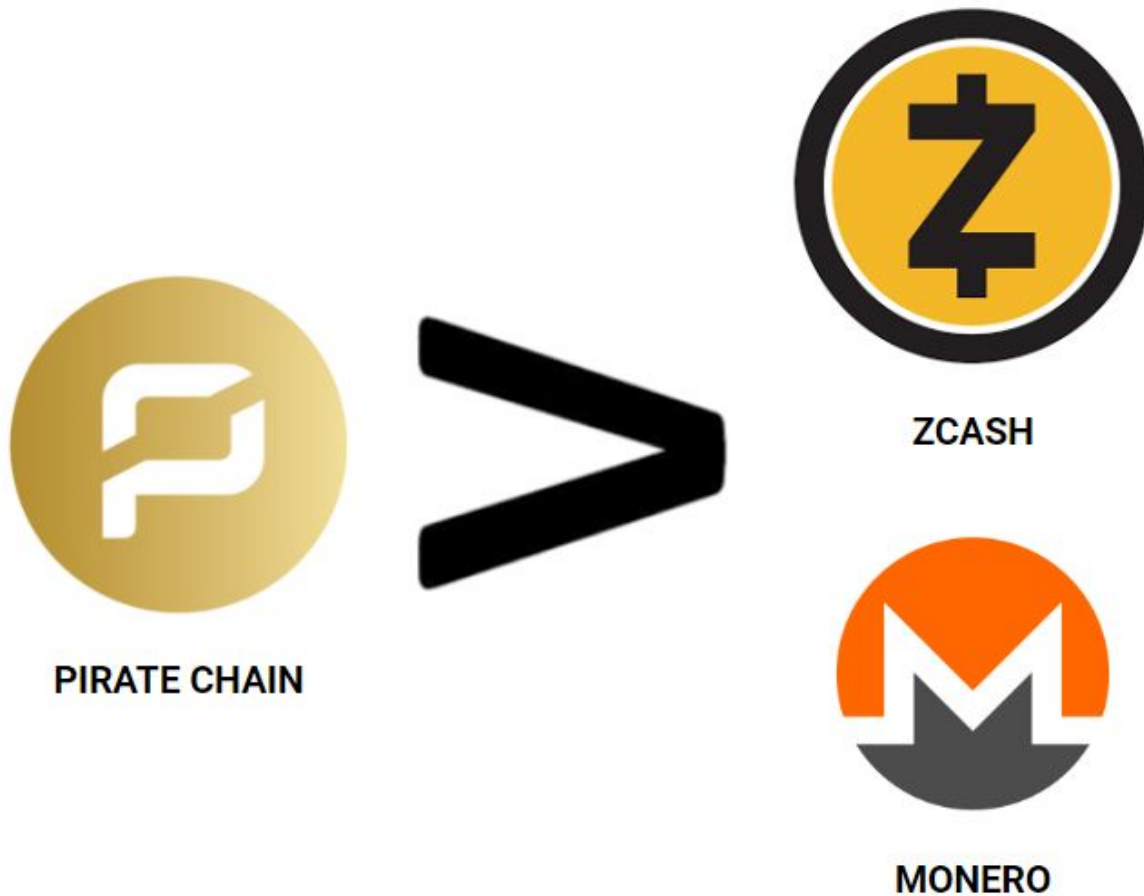
Other investors are beginning to notice the value in Pirate Chain. In the article, "[Pirate Chain|New Contender for Top Privacy Coin](#)" the author explains that its entire blockchain is entirely encrypted and essentially future-proofed against blockchain analytics, thanks to its mandatory usage of zk-SNARKs. As we explained earlier, zk-SNARKs is cutting edge cryptography which allows for an extremely high degree of anonymity since transactions which use this technology are fully encrypted and private. The author also observes that although Monero is good, "*instead of completely breaking the digital footprint of transactions by encrypting it, like Pirate does, XMR attempts to obscure them through creating computationally difficult to trace transactions with a large set of possible senders and receivers for any one transaction.*" The author then argues that a potential risk of Monero is that in the future, a transaction could later be tied to your name if its obfuscated transactions are ever broken at some point.

The author also discusses the innovative integration of Komodo's dPoW which claims to make it as secure as 51% attacks against Bitcoin itself. According to the author, "*dPow is like a cheat-code that calls upon the King's guard for protection, and has been an effective way to ensure world-class security and decentralized funds from the onset of a project.*"

Finally, the author also sees the value of ARRR's organic and honest community-driven development:

*"[ARRR] is non-ICO, no premine, no founder fee, and community supported. This means there isn't a big 'ol stash of OG coins waiting to dump on your head at any moment like 90% of new projects these days."*

We agree with this author's observations, and we are very bullish on ARRR too.



*“Pirate Chain > Zcash & Monero?”*

In a May 2, 2020 [interview](#) with GAINS Associates, Draeth (Captain of Pirate Chain) and DreamTim (First Mate of Pirate Chain) explained some of the benefits of ARRR over XMR and ZEC. In the interview they made a compelling argument that Pirate Chain is essentially the best of Zcash and Monero combined.

*“Pirate Chain is the most anonymous cryptocurrency in the market, as well as the most secure...We ARRR truly the digital equivalent of cash.”*

*-Draeth, Captain of Pirate Chain*

They explained that while ZEC was recently found to have [99.9% of its transactions shown to be traceable](#), ARRR successfully shields all user-generated transactions on its chain. They also mentioned that ARRR’s zk-SNARKs privacy technology is superior to XMR’s privacy technology, and that ARRR enforces it, resulting in 100% z-z p2p transactions. They made the case that ARRR is the most secure and private cryptocurrency to date, thanks to its delayed

Proof-of-Work (dPoW) algorithm. Furthermore, they mentioned that the ARRR team has developed an operating system (**PirateOS**), is working on an anonymous messaging app, as well as a point of sale system.



*“The Pirate Chain Equation”*

*“Pirate Chain is a project about financial freedom. It provides 100% shielded z-z P2P transactions to preserve the privacy and anonymity of the user. It is run by a passionate community of volunteers of which I am one... ...when you are investing in Pirate Chain the bet you are placing is that privacy and anonymity will become so important to everyone that this will increase value, adoption, and subsequently the price, following a similar path as Monero has.”*

*-DreamTim, First Mate at Pirate Chain*

Since that interview, the Pirate Chain team has accomplished more milestones, including releasing the **beta version of their Android Mobile Lite Wallet**.



More of Pirate Chain’s roadmap can be seen below.

## 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 Completed

- CryptoCurrencyCheckout Co-Marketing -
  - TurtleNetwork Partnership -
  - Integration with the BPSAA -
    - Listing on TNDex -
  - 20+ Website Translations -
  - Pirate Notary Services -
  - Pirate .onion (TOR) + .EPP -

## 2020

### - Q2 -

- Election of More Pirate Notary Node Operators -
  - Mobile Lite Wallet -
  - Pirate Branded VPN -
  - I2P Integration -
  - QT Wallet Upgrades -
  - SubAtomic Swaps -
- GalleonOS development begins -

### - Q3 -

- Privatebay (working title) -
- Website Upgrade w/ Managers -
- Point of Sale System Register -
  - BPSAA Legal Foundation -
  - RumRunner private chat -
- Exchange Integration into Galleon OS-

### - Q4 -

- Sponsor Pirates Week in the Cayman Islands -
  - Point of Sale System Global Rollout -
- Fiat Integration into Point of Sale System -
  - ARRRtomic | Ztx DEX Integration -
  - ZSPV -

*ARRR Roadmap*



## Pirate Chain (ARRR) Community & Adoption



The screenshot shows the ARRRmada website. At the top, there is a logo for 'ARRRmada accepted here' featuring a pirate ship icon. Below the logo, a navigation bar contains links: HOME, WORDPRESS PLUGIN, SHOPIFY PLUGIN, MULTI GATEWAY, DONATION BUTTON, and WEBSERVICE. The main content area features a video player with a play button, titled 'MACO TOONS PRESENT'. A small icon in the top right corner says 'Copy link'. Below the video player, there are two columns of text. The left column is titled 'What is ARRR' and includes a yellow circular icon with a white 'P' and a paragraph of text. The right column is titled 'Our ARRRmada' and includes a pirate ship icon and a paragraph of text.

**ARRRmada**  
accepted here

How would you like to pay? PirateChain ARRR

Copy link

**MACO**

**TOONS**

*PRESENT*

**HOME** WORDPRESS PLUGIN SHOPIFY PLUGIN MULTI GATEWAY DONATION BUTTON WEBSERVICE



































































### What is ARRR

 Pirate (ARRR) is an anonymous and secure crypto currency. Piratechain uses **zk-SNARKS** to encrypt and anonymize transactions. This means that no conclusions can be drawn about user behaviour. The piratechain does not allow any metadata to be transmitted outside, so ARRR is invisible. And secure against 51% attacks, as the pirate chain additionally protects itself via the Hashrate from Komodo and Bitcoin. It's possible with Komodo's Security Mechanism: **Delayed Proof of Work (dPoW)**. Visit the [official website](#) of Pirate ARRR for more information.

### Our ARRRmada

 The ARRRmada are stores, service providers and companies that accept ARRR as a means of payment. If you would like to pay with the crypto currency ARRR, you will find all acceptance points here. The ARRRmada use our WordPress- or Shopify-Plugin for their shops or receive donations with our Donation-Script. If you also have a service, a store or a company and want to accept ARRR, then you can find out more about the menu items. Detailed descriptions of the points of acceptance can also be found in our blog. [ARRR accepted here](#).

## Stores which accept ARRR as payment method

GROWING	MEDICAL	OTHER
 Ancient Path Naturals  3	 Magic Morpheus  1	 streamARRR  11
 Social Media Marketing  10	 Calliston Design  11	 McTricky s Liquidations  4
 Rockin Prices  6	 Lynx Art Collection  11	 IdealVape  6
 Pirate Pool  12	 CryptoCloaks  6	 LOT POT  2
 Piratepool.us  6	 Crypto Posters  6	 Drippin Junkies  1
 Kryptika  2	 FIG  5	 TheHUB  13
 Official Website Pirate  16	 Mobile Pay Coin Marketplace  10	 TMT-Hosting  4
 Pirate Explorer  9	 Software Sales  5	 VPS Coins  2
 Physical Crypto Coins  23	 Crypcy  4	 Psychedelic Press  12
 Hidden Treasures  8	 Human Action  19	
	 Blockchain Stuff  19	
	 Black ARRRmy  15	
	 SatFam  8	
	 The BOB Shop  7	

Some of Pirate Chain's community members have built an online store called [ARRRmada](#) which provides resources for customers & merchants accepting ARRR as payment. Their team has made it easy for online businesses to accept ARRR as payment, with a [WordPress plugin](#), [Shopify plugin](#), [cryptocurrency checkout \(multiple payment gateway\)](#), an anonymous website [donation button](#), and a Pirate Chain community-provided [web service](#), based on WordPress and WooCommerce.



Businesses that are interested in accepting ARRR can fill out a web form to join the ARRRmada and be listed on the website.

Another exciting aspect of ARRR is their membership in the [BPSAA](#), or Blockchain Privacy, Security, & Adoption Alliance.

For the Pirate Chain halvening event which occurred on February 27, 2020, some of their community members created a [web page](#) providing helpful information regarding stock-to-flow models. On this page, they calculated the stock-to-flow ratios for ARRR over time, and compared ARRR's S2F ratios with S2F ratios for other assets as well.

## **Pirate Chain (ARRR) Crypto Asset Valuation & Outlook**

As we've explained, we are very bullish on [Pirate Chain \(ARRR\)](#) because of its successful innovations in the areas of strong privacy, security, fungibility, and strong commitment to fulfill these basic requirements for sound crypto money. We are also pleased with ARRR's organic launch and development, and by its resilient and growing community.

In the arena of privacy coins, [Monero \(XMR\)](#) is the clear market leader (and currently our favorite coin and largest holding in the TCV portfolio), with a market capitalization of \$1.648

billion USD as of today. At its peak, XMR reached a market capitalization of \$8.45 billion on January 8, 2018 during the last major crypto bubble.

**Zcash (ZEC)** is currently sitting at a market capitalization of \$874 million. If Pirate Chain can manage to compete with Monero and Zcash, then we believe it is possible for it to potentially rival Zcash in market capitalization, and perhaps rise halfway to XMR's market cap (implying a market cap of \$824 million for ARRR). However, keep in mind that we still believe that XMR is massively undervalued, and should really be in the top 3 coins (which would imply a fair value market capitalization of at least \$14 billion for XMR right now). Based on that assumption, if ARRR achieves mass adoption then we could see its market cap go to a conservative estimate of \$7+ billion in the very long run, implying a *potential future market price of about \$35.00 per ARRR (or about 576x the current price of \$0.06076, based on the maximum future supply of 200 million ARRR)*.

More realistically, we would expect to see ARRR at least rival known "shitcoins" such as **Verge (XVG)** which currently has a market cap slightly over \$116 million. Verge is known among crypto OGs for being a massively overhyped coin that falsely claimed to be private when it is not. ARRR should easily match and beat XVG since its fundamentals are far, far better. If ARRR were to simply match XVG's current market cap today, then its target price would be over \$0.70 per coin. This is still over 10x the current price of ARRR (based on an outstanding supply of 164,936,255 coins as of today). However, it is very clear ARRR is far, far better than XVG.

Ideally Pirate Chain should really be competing with Monero, but we will stay somewhat conservative and keep ARRR's target market cap as only half of XMR's market cap. Remember that XMR's market cap is about \$1.648 billion, so that would make ARRR's future market cap a minimum of \$824 million as we mentioned earlier, without even accounting for XMR's future massive growth. With an outstanding coin supply of 164,936,255 coins, that would imply a near-term *target price of about \$4.996 per ARRR (or about 82x the current price)*.

We invite you to climb aboard this pirate ship with us! ARRR!!!



***Very important disclaimer:***

***Remember - if you are going to invest, make sure you only invest what you can afford to lose. We have added ARRR to our new TCV portfolio, but it is a very small cap coin, so it almost certainly will be extremely volatile. We have allocated ARRR at only 1% of the entire crypto portfolio due to its small market cap. At the time of writing, the price is \$0.06076. We recommend being cautious and buying on dips. Therefore, we only recommend buying ARRR up to \$0.95 especially in the short term (we believe that \$1.00 would act as strong psychological resistance). If ARRR rises many times its value too quickly, it could easily drop back down just as quickly. However, we could raise our target if the buying appears strong. Keep in mind your investment time horizon, because if the price drops, it could remain low for a long period of time before the next bubble. Once again, please be careful and only invest what you can afford to completely lose!***

**Pirate Chain (ARRR) exchanges**

We like TradeOgre the best - there is no KYC required or withdrawal limits, and it currently has the most liquidity/volume:

<https://tradeogre.com/exchange/BTC-ARRR>

<https://exchange.bitcoin.com/ARRR-to-BTC>

<https://www.coinex.com/exchange?currency=BTC&dest=ARRR>

**Pirate Chain (ARRR) wallet software downloads**

*Note: For ARRR wallets, we recommend the latest **official wallet releases** as of the time of this writing.*

You can download your preferred wallet option from the ARRR official website:

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

### **Pirate Chain (ARRR) resources & links**

ARRR official website: <https://pirate.black/>

ARRR website #2: <https://www.pirate.si/>

ARRR News: <http://piratechainnews.com/>

ARRR subreddit: <https://www.reddit.com/r/PirateChain/>

Github (official ARRR software downloads for advanced users):

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

General ARRR info page (CoinGecko):

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

General ARRR info page (CoinMarketCap):

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

ARRR block explorers:

<https://explorer.pirate.black/>

<https://pirate.kmdexplorer.io/>

<https://pirate.explorer.dexstats.info/>

ARRR Pirate Community:

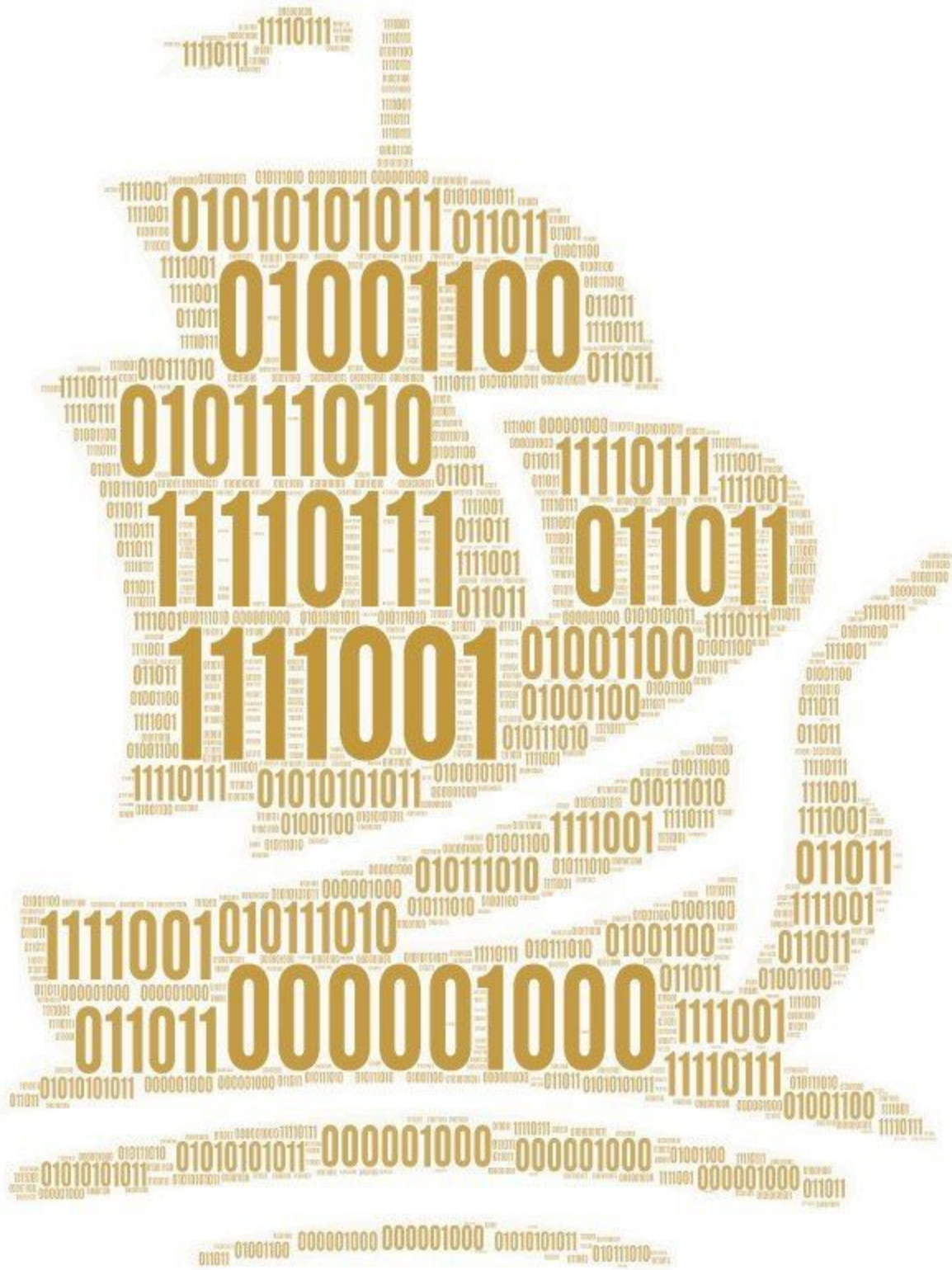
<https://medium.com/piratechain>

<https://discord.com/invite/CNZXMmZ>

<https://www.youtube.com/c/piratechain>

ARRR BitcoinTalk Announcement Thread:

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



---

Disclaimer: The Crypto Vigilante needs no disclaimer. Everything we say here is what we believe. Furthermore we need no disclaimer because we believe that all nation states, governments, securities agencies or other legislative bodies are illegitimate and we do not recognize them nor believe we need their permission to say what we feel about any topic and frankly think it is hilarious that people think a government body should be there to protect them.

However, because we know that all manner of Government agencies will come after us just for showing such disdain for them we are going to include a standard, cookie-cutter disclaimer below just to keep them off our backs.

Enjoy reading it, bureaucrats at the SEC. Information contained in The Crypto Vigilante Emails or on The Crypto Vigilante website ([www.cryptovigilante.io](http://www.cryptovigilante.io)) is obtained from sources believed to be reliable, but its accuracy cannot be guaranteed. The information contained in such publications is not intended to constitute individual investment advice and is not designed to meet your personal financial situation. The opinions expressed in such publications are those of the publisher and are subject to change without notice. The information in such publications may become outdated and there is no obligation to update any such information, such as cryptographic advice. Jeff Berwick, Ed Bugos, Rafael LaVerde, Mr. X, and other analysts or employees of The Crypto Vigilante may from time to time have positions in the crypto assets, securities or commodities covered in these publications or web site. Any Crypto Vigilante publication or web site and its content and images, as well as all copyright, trademark and other rights therein, are owned by The Crypto Vigilante (TCV). No portion of any TCV publication or web site may be extracted or reproduced without permission of The Crypto Vigilante. Unauthorized use, reproduction or rebroadcast of any content of any TCV publication or web site, including communicating investment recommendations in such publication or web site to non-subscribers in any manner, is prohibited and shall be considered an infringement and/or misappropriation of the proprietary rights of TCV. TCV reserves the right to cancel any subscription at any time, and if it does so it will promptly refund to the subscriber the amount of the subscription payment previously received relating to the remaining subscription period. Cancellation of a subscription may result from any unauthorized use or reproduction or rebroadcast of any TCV publication or website, any infringement or misappropriation of TCV proprietary rights, or any other reason determined in the sole discretion of TCV.