The CRYPTO VIGILANTE

TCV Featured Crypto Asset: Dero (DERO)

Mr. X & Mr. Z

June 21, 2021

Why is DERO important?

Monero is to Bitcoin what Dero is to Ethereum.

Dero (DERO) is a proof-of-work (PoW) crypto asset which promises to solve two of the biggest problems currently facing smart contract platforms: lack of privacy and overvaluation concerns. Propelled by these advantages and a Q3 mainnet launch, we see the potential for it to capture at least 1.5% of Ethereum's market share - which translates into a massive upside target of nearly 65 times the current price.

In the near-to-intermediate term, we are targeting a more conservative level reflecting a ⅓ discount to the relative-value-basis we employ (the XMR/BTC ratio). This price target, of $110 per DERO, equates to approximately 20 times current levels.

Where do I buy it?

Before buying, we highly recommend reading Mr. X's detailed report on coin control in the TCV February 2021 Issue, focusing on pages 18-22.

We only trust TradeOgre for trading DERO right now, plus there is no KYC required or withdrawal limits, and it currently has the most liquidity/volume:
https://tradeogre.com/exchange/BTC-DERO

How do I store it?

Since it is still early in development, it only has a command line interface (CLI) wallet at the time of this writing (no graphical user interface wallet, or GUI). However, you can also use the web wallet (keep in mind that this is alpha software!). Make sure you safeguard your wallet seed!

Command line interface (CLI) Wallet:
https://github.com/deroproject/derosuite/releases

Web Wallet:
https://wallet.dero.io/
For subscribers interested in a walkthrough on using the web wallet, please see the last section of this report.

Background and Introduction

Mr. X first brought this crypto asset to our subscribers' attention in his TCV Crypto Alert – Dero (DERO) (February 21, 2021) back when the price of DERO was about $2 per coin. In this report, we will take an even deeper dive into this fascinating crypto asset.

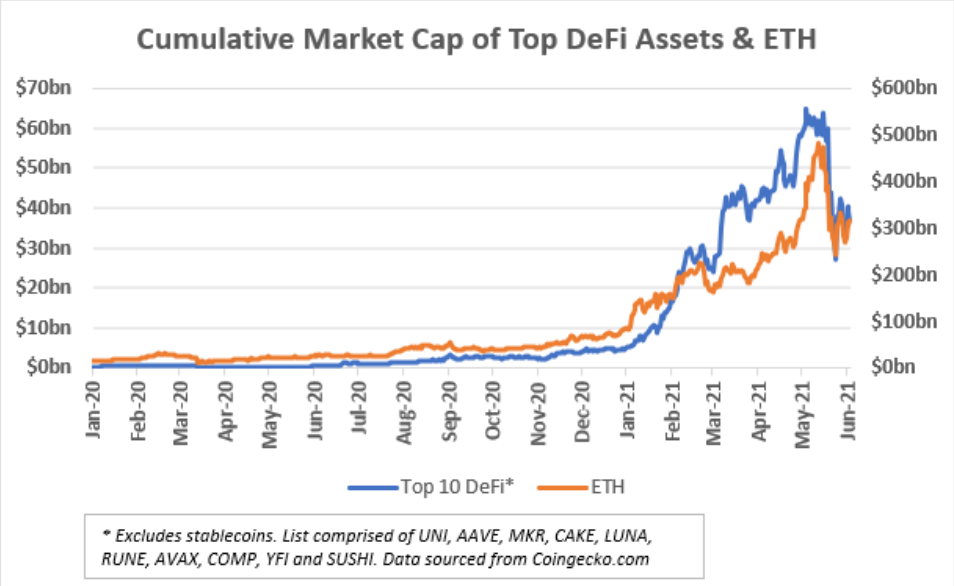
Unlike some of our other featured crypto recommendations, we largely view Dero (DERO) as a relative value play versus Ethereum (ETH) and other smart contract platforms and assets. Because of this, it's worthwhile to begin with a quick discussion of those topics.

Ethereum and Smart Contracts

As most people in the crypto-sphere are well aware, Ethereum and smart contracts have finally begun to come of age.

For a long time, they didn't have a great response to the arguments that smart contracts were a solution in need of a problem (which didn't yet exist). But that's all changed in the past couple of years.

The emergence of DeFi (decentralized finance) has addressed that argument, and in spades.



As the chart above shows, this phenomenon really took off in 2021, with the top ten DeFi assets at one point being valued in excess of $50 billion. The correspondence with ETH is notable as well, which further serves to support the idea that DeFi has played a pivotal role in Ethereum's growth. Note, however, that the top 10 DeFi list above includes RUNE, LUNA and AVAX, three assets which are not ERC-20, and hence not Ethereum-linked (though RUNE has a separate ERC-20 token as well). Nonetheless, the overall growth and correlation to Ethereum remains striking.

While there are other smart contract platforms that are competing, ETH is understood to be the market leader, and has the broadest user base, investor base, and fan base. Therefore, we think you'll agree that we can refer to it here as "the" current smart contract representative in the market today.

At a conceptually high level, smart contracts are pretty basic things. They let you run code on the blockchain (and so perform any math and logic functions you can design), while managing inputs and outputs which consist of either network tokens, or other data accessible by the blockchain.

There is, however, a school of thought that smart contracts are unnecessary. Everything that can be done via smart contracts can be done (and can arguably be done better) using Bitcoin, hashed timelock contracts, and oracles. This cool article explains that point of view. Alternatively, check out Rafael LaVerde's article in the TCV May 2021 Issue where he touches upon similar issues.

However, these arguments, while undeniably true, arguably miss two things.

Firstly, while *technically* smart contract functionality can be replicated without being embedded in a blockchain, it's questionable whether those other avenues would have supported the growth we've seen in DeFi in practice. It's not clear that any route outside the open-source and decentralized nature of blockchain would have enabled DeFi apps to be successful in achieving critical mass without big-bank sponsorship (something that would defeat the purpose of it in the first place). Has it been overkill, akin to using a sledgehammer to drive a nail? Maybe. But it kept the ne'er-do-wells out of the way.

Secondly, whether or not it's technically required anymore is potentially a moot point. It's here, it's got scale, and it's got network effects. It doesn't seem like it's going away anytime soon, so it warrants serious consideration as to whether there's a smart way to invest in it.

So with that backdrop, we turn to the problems with Ethereum, which have led us to our DERO recommendation.

Problems with Ethereum

We have reservations about Ethereum - and for some time now. These don't directly relate to *this* investment thesis, but are worth mentioning quickly.

In short, for anyone who likes to think it could be used as money, we would say that it's *not* "sound" money. Far from it.

Unlike Ethereum Classic (ETC), Ethereum (ETH) has proven itself to *not* be immutable (see some of our team's past writings on this subject in the TCV February 2020 Issue on pages 23-25, the TCV May 2020 Issue on pages 18-19, and the TCV August 2020 Issue on pages 29-30).

ETH also lacks privacy and therefore fungibility. It's also increasingly centralized.

If ETH only claimed to be a competitor to Bitcoin or Monero/Pirate Chain as money, we think it would've been put to rest a long time ago. But of course, it's more than that - it's the smart contract network backbone which we've just spoken about.

So what are our issues with it from a smart contract perspective?

Privacy

Ethereum is not private. Not at all.

Just like Bitcoin, all transactions in it are public and free to see for anyone who has the interest and means to do so. Additionally, there are actually features of Ethereum that make it even *less* private than Bitcoin (see here and here).

As you probably know if you've read other articles from us here at TCV, we're big proponents of privacy - not just from a moral or philosophical point of view, but from a technical one.

When it comes to what you're using as "money", you need privacy because without it, the money is not fungible, and is prone to all sorts of problems and eventual failure.
Now we'll grant you - especially for someone new to the concept - that the topic of fungibility and why it's important can be tricky to wrap your head around.

But there's good news here - the importance of privacy for smart contracts is much easier to understand. All it takes is some common sense to see how not having privacy in smart contracts can cause some real problems, and may ultimately be a big stumbling block for greater levels of adoption.

Unfortunately for Ethereum, it uses a non-private token (ETH) as its core currency/means of value transfer. While there have been some attempts to work around this lack of privacy, they've all fallen short in offering seamless execution of private smart contract transactions that can be applied to most, if not all use cases.

If you are going to conduct business via a smart contract - whether that's lending, borrowing, buying or selling financial instruments (tokens, stocks, bonds), *do you really want the world to be able to see everything you're doing?*

This is especially true if you're doing the transactions for enormous dollar amounts, or on behalf of a private company. Why on earth would you want your full transaction history to be public?

What institutional investor, who buys tokenized stocks and bonds (the wrapped securities of the future), wants every one of their trades to be on public display? What *private* investor for that matter?

If you are relying on the seemingly more complicated (and therefore obscured) nature of smart contract transactions for privacy, you have likely not kept up on just how advanced chain analysis has become - and it's only going to get more effective. This means that you should expect zero privacy for every Ethereum based transaction you do - whether it's a simple token transfer or more complicated yield farming strategies on decentralized platforms.

We believe that the fact that all smart contract transactions on the Ethereum network are public will become an increasingly acknowledged barrier to broader public adoption. Whether this happens gradually over time, or all at once with a shock (like for instance people getting notified by tax agencies that they have failed to report their yield farming gains) we can't say. But given the increased ease with which transparency on the Ethereum network is achieved, we are confident that it's coming. It's actually remarkable that this hasn't been flagged in a big way until now, considering how obvious it seems once someone explains it like this.

As such, a network or token which solves this problem will be one that warrants capturing a significant portion of Ethereum's market share and valuation.

Value

We also have major concerns with ETH from a valuation perspective (and so, something to be taken into account as an investment). By our measures, it appears to be significantly overvalued with respect to the pending increase in supply.

"What supply increase?" you may ask.

For a detailed answer to this, please check out Mr. Z's article, "The Secret ETH Supply Problem (aka A Strange Farm Visit)" in the TCV May 2021 Issue on pages 15-25.

In short, the network upgrades to the Ethereum network (and Layer 2 solutions) will have the effect of *massively* increasing supply through its higher transaction processing capability. As a consequence, once the market catches on to this, ETH is at risk of suffering a correction that may be quite significant.

The argument is not that smart contracts aren't valuable (and the ability for a blockchain network to offer their use), but rather that *demand for ETH tokens would need to grow by literally millions of times in the near future to justify its current price.*

In summary, between the privacy and valuation issue, it's got some real headwinds as an investment.

So - without further ado, let's talk about Dero.

Dero (DERO) - What Is It?

Dero is a crypto asset which enables private smart contracts.

If you like, you can think of it like this: *Monero is to Bitcoin what Dero is to Ethereum.*

That analogy is a pretty good (albeit imperfect) place to start. So let's give a bit more context.

The DERO Token & Smart Contracts

The Dero token is actually, by itself, a private token - arguably on par with Monero or Wownero. It's fast, mandatorily private (and therefore fungible), and uses different technology than either Monero or Pirate Chain (although it's closer to Monero overall, as it forked from the same underlying code base).

If you wanted to forget for a moment everything about smart contracts, you could actually just think of it as another option in the privacy coin world. Since its fundamental architecture differs from the leaders (XMR and ARRR) you might even view it as something of a hedge to any potential technological roadblocks others might face.

However, DERO is more than that.

Much like Ethereum has its EVM (Ethereum Virtual Machine) which enables it to run programs embedded in the blockchain, **Dero has its DVM (Dero Virtual Machine)** - a Turing complete, 256-bit environment for DERO Smart Contracts.

The real point of DERO is to be able to run *private* smart contracts (although they can be made public).

What is needed is for the network's underlying token to be truly private, but also for the network itself to hide transaction sizes when processing smart contracts.

December 2020 Testnet Release Announcement of the DERO Homomorphic Encryption Blockchain Protocol (DHEBP)

The former is achieved by the innately private nature of the DERO token. The latter is achieved by something called Homomorphic encryption - which allows calculations to be performed on encrypted data *without first decrypting it*. Some very cool tech indeed.

We view this is a significant opportunity from an investment and adoption perspective. As institutions and individuals realize that all their Ethereum (and other public smart contract) transactions are being done with no privacy and for all to see, we believe that there will be a natural and growing shift to the platform that solves this problem with native privacy.

Note: by private smart contracts we mean the transfers of tokens in and out of smart contracts are kept entirely hidden. The code of the smart contract itself remains public which allows for audit and scrutiny - something necessary to ensure its integrity.

History and Roadmap

DERO launched in December 2017 based on the CryptoNote protocol - something it has in common with Monero.

Unfortunately, at least from our perspective, it launched with a significant premine of 2 million DERO. The premine is understood to not be part of the current circulating supply and was done with the stated intent of using it to finance development and marketing.

However, we're generally not fans of premines. We'll talk more about this a bit more later on, but in short, while we view this as an overall negative, we understand the rationale behind it, and in the grand scheme of the value proposition, we are able to look past it. Plus, from a valuation perspective it may actually *help* in the near-term.

DERO started with a team of three full-time developers. Their first big post-launch landmark event was successfully migrating in April 2018 to a CryptoNote codebase fully rewritten in Golang - a language touted as having a high degree of immunity to certain security threats.

Since then, there have been a number of technological developments upgrading the network. The main ones include the incorporation of Bulletproofs in mid-late 2018 and a DAG protocol (directed acyclic graph).

If you're a Monero follower, then bulletproofs should be familiar to you. In October 2018 Monero introduced bulletproofs (which substantially reduced the size of transactions, resulting in faster verification times and lower fees).

The DAG though, is something different and calls for a slightly deeper explanation, which we provide in the next section.

Development over the next couple of years continued, but definitely slowed since the original breakneck pace following launch. To some extent, this can be forgiven as a function of the crypto bear market. The deep bear market impacted smaller projects more adversely, as they generally had far more limited assets available to support development.

Even against that backdrop though, progress continued. In early 2020 a new mining algorithm, AstroBWT, was released and implemented on the DERO network which made it significantly more ASIC resistant - something we definitely appreciate.

So where does that leave them now? Well, the next "big one" appears to be just around the corner.

Stargate: Release Candidate 2

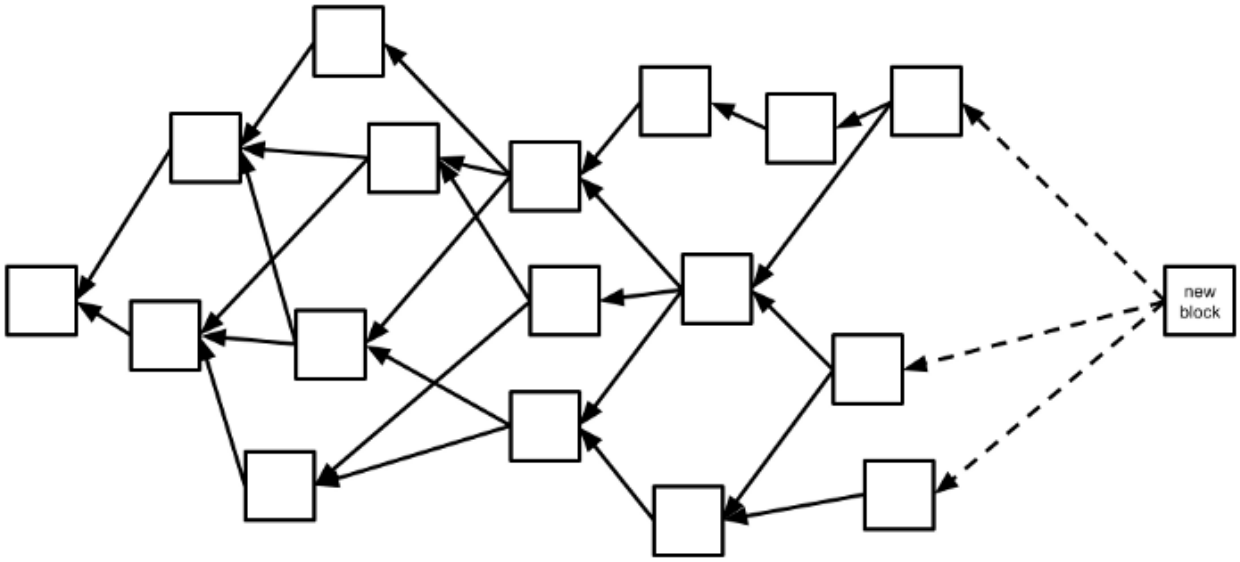
This is the mainnet launch of Private Smart Contracts - something which until now has been part of the big picture roadmap, but was still off in the distance.

Right now, the implementation and testing of their Smart Contract protocols are underway on their testnet under the name Stargate RC2. Mainnet launch is planned for Q3 2021.

A Note on DAG

As we alluded to earlier, DERO uses different protocols than both Monero and Pirate Chain (and ETH for that matter).

DERO is a Proof of Work (PoW) coin; however, unlike all those others, it also makes use of a DAG protocol. DAG stands for Directed Acyclic Graph, and is technically not even a blockchain.



"In a blockDAG ledger, new blocks reference all tips of the graph (blocks that have not yet been referenced) that their miners see locally. As in a blockchain, blocks are published immediately."
-from "An Introduction to the BlockDAG Paradigm"

DAG by itself actually doesn't need blocks (but rather transactions) to work, and there are potentially serious centralization issues with it. For instance, IOTA is a large and well-publicized project that utilizes a *pure* DAG, and we do not recommend it. All else aside about IOTA (and there's plenty to criticize) - their pure DAG structure is ultimately highly centralized with respect to authority, and we see that as anathema to the whole purpose of blockchain.

We won't go into further detail on DAG here, but we have included some links for additional reading below which we recommend for those who are interested.

However, the important thing to note though is that DERO is *not* a pure DAG protocol system, but is rather a *hybrid* blockchain/DAG structure. The inclusion of the DAG architecture (something they call Block DAG) enables the DERO network to process transactions more quickly, avoid orphan blocks, and make it more defensible against 51% attacks.

Valuation

Considerations

As mentioned earlier, we view the investment case for DERO as largely a value proposition relative to ETH. Over time, as it grows bigger and if it acquires a more "leading" space in the

market, that may change - but for now, given its small size, its relation to ETH is the easiest way to value it.

We've already discussed how DERO solves the first ETH smart contract problem identified above - privacy.

We haven't spoken about how it addresses the second ETH problem - that of a massive pending supply increase due to incredibly expanded processing ability.

DERO solves this problem (or rather, sidesteps it) in two ways.

The first is that simply by virtue of its microcap size, its valuation is nowhere *near* levels where we would start to worry that it's gotten ahead of itself with respect to TPS-related supply issues. Even though its TPS capabilities are quite high, the kinds of numbers (and supply) associated with ETH 2.0 and Layer 2's would be far off in the future, which leads to the second point.

The fact that it's a private token makes Layer 2 scaling more complicated to begin with. Layer 2's have already had many issues developing on public chains. Never say never (especially in crypto space) but successfully building a suitable Layer 2 solution on a private base layer (which includes homomorphic encryption) makes it that much more difficult, and so we can rest more easily and have confidence that any "supply shock" associated with Layer 2 scaling solutions would not impact DERO for quite some time yet - and only at valuations enormously higher than current levels.

Numbers

Our starting point is to value DERO analogously with other privacy projects.

As we said earlier, DERO is to ETH as XMR is to BTC. Let's look at what that means in value.

Asset	Market Cap ($)
Bitcoin (BTC)	669,322,220,816
Monero (XMR)	4,744,360,739
XMR/BTC	***0.71%***

Asset	Market Cap ($)
Ethereum (ETH)	262,349,305,195
Dero (DERO)	60,292,626
DERO/ETH	***0.02%***

Note: prices as of June 20, 2021.

As of June 20, 2021, Dero was trading at less than 1/30th of the ratio which XMR was trading at relative to Bitcoin.

What should be the "right" number as the project, and awareness of it, progresses? Well, there are some puts and takes to consider.

XMR is well advanced in terms of its user base and technology, whereas DERO is still at an early stage and won't launch mainnet smart contracts until Q3. However, if we view this from the perspective of where Dero could *go* if their launch is successful, and if the "if you build it, they will come" aspect of crypto holds true, then longer term, Monero's percentage of Bitcoin's market cap may be a reasonable starting point.

But there are also other considerations which are more bullish for Dero.

As we discussed, the value proposition for Monero relative to Bitcoin is largely based on fungibility - a topic that can be difficult for many to understand. Plus, there's the added negative taint associating Monero with illicit activity (though we think of it more as an unfair smear campaign).

Dero's privacy argument doesn't require an appreciation for fungibility - but rather just business sense. Big (and institutional) adopters of smart contracts will want privacy. There's nothing to really point at that's unseemly there, even for those who may want to smear.

As such, it's possible that using the XMR/BTC ratio as a target could be significantly too conservative.

Never mind that we at TCV believe that XMR/BTC ratio will be going quite a lot higher in the not too distant future, it's reasonable to believe that the appropriate DERO/ETH ratio could be significantly higher - so let's assume a still modest sounding 1.5% of ETH market cap. If that were the case, the numbers speak for themselves.

Asset	Current Market Cap ($)	Theoretical Market Cap ($)
Ethereum (ETH)	262,349,305,195	262,349,305,195
Dero (DERO)	60,292,626	3,935,239,578
DERO/ETH	***0.02%***	***1.50%***
DERO price per coin	5.65	363.12

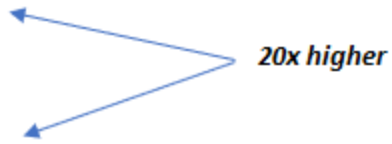
nearly 65x higher

Note: prices as of June 20, 2021.

As enticing as that looks, we'd recommend a more cautious valuation approach - at least for the near-term.

With respect to project life-stage, timing, and execution of the mainnet launch, we feel comfortable with a much more modest target - ⅓ *lower* than the current XMR/BTC ratio, or 0.47%. As you can see below, this would represent a 20x return and result in a target of over $110 per DERO.

Asset	Current Market Cap ($)	Theoretical Market Cap ($)
Ethereum (ETH)	262,349,305,195	262,349,305,195
Dero (DERO)	60,292,626	1,239,741,443
DERO/ETH	***0.02%***	***0.47%***
DERO price per coin	5.65	110.53



Note: prices as of June 20, 2021.

We recognize that having a short-to-intermediate term price target of 20x current levels may seem extraordinary. It certainly gives us pause - as there's a big difference between a valuation analysis and an actual price target.

But there are real reasons to think this is a fair expectation.

- The fundamental valuation, with our first estimation of approximately $360 per DERO, seems reasonable. The more conservative value of $110 is far more achievable.
- Price increases for assets with such a small market cap regularly rally by orders of this magnitude as they cross thresholds in their development roadmap and public awareness - two things which DERO has going for it right now.
- The market cap at $110 per DERO is just over $1.2 billion - which wouldn't even place it in the top 60 projects by market capitalization for something that offers real value.
- There would still be ample room for upside (toward the fundamental valuation) even at $110. Leaving "meat on the bone" is a critical element of achieving price targets, as it provides big upside for latecomers to still get involved in a significant way.

There's one additional point we'd like to make on the valuation, and that relates to the premine.

The Dero plan is to launch a more targeted marketing campaign upon the successful mainnet launch in Q3 2021.

In this regard, the premine (the 2 million tokens where half of them were intended for the "community") may actually be a boost to the token.

If DERO rises in value, that effectively means that more funds will be available to market it further. More marketing means more awareness, which may mean higher prices. There's the potential for something of a virtuous loop here.

We still remain negative on premines in general, but we need to acknowledge the reality that to the extent these resources are spent on marketing and increasing awareness, any price uptrend could be significantly reinforced.

Risks and Limitations

There are many risks to be aware of. Some of these are:

There could be issues with mainnet launch

As with all things launch related, there could be problems, errors or delays. However, barring something catastrophic, we largely view the possibility of these things as items that would postpone, rather than derail, the upside case.

There are some competitors and more may spring up

We don't see this as a major risk. Another similar project we have come across is called Secret (SCRT), and works on very different technology. We will be exploring this more in times to come, but from a high level, we dislike that it relies on PoS and we have many questions about its mechanics from an underlying governance and privacy perspective.

That's not to say we may not ultimately be constructive on it, but it's a bit too early for us and from what we know about DERO, it is our preferential choice on a number of fronts (PoW, speed, homomorphic encryption, and a truly private and fungible base token).

Either way, this space is young and we see the "size of the pie" sufficiently large such that our price targets could be supported even with competition. In fact, more competition may actually be *good*. Anything that raises awareness of the limitations of non-private smart contracts should boost this space, and as they say, "a rising tide lifts all ships."

The wallet tech is early

There is currently no GUI wallet for Dero - only a command line interface (CLI). There is, however, a web wallet which we have tested - and so far, it appears to be fairly robust (allowing you to own the seed-phrase/private key) but there are still risks with web wallets and we advise caution in relying too heavily on it.

When it comes to investing in earlier stage projects, sometimes thoughtful compromises have to be made. Waiting until the tech (and wallets) are fully developed could mean missing the biggest price appreciation opportunities. That said, you should always give yourself the best chance to avoid any pitfalls or negative surprises.

For those not willing or able to go through the effort to set up a CLI wallet, we are in a delicate position recommendation-wise, as your choices are between relying on the web wallet or leaving DERO in your exchange account (TradeOgre). While TradeOgre has thus far been remarkably resilient and fair, there's the old adage "not your keys, not your coins" of which to be mindful. Between the two, our personal preference is to use the web wallet - based on our preliminary assessment of it, as well as a general aversion to keeping coins on exchanges.

That said, we recommend you pursue setting up the CLI wallet on your machine, especially if DERO's value winds up rising as we think it will. While we are only giving our TCV portfolio a 2% weighting to DERO, it's important to be mindful of the impact big price rises have on overall exposure, and therefore wallet reliance. Like many experienced with ARRR, portfolio weightings can change quickly, and while this will hopefully be a "high quality problem" to deal with (i.e., protecting gains) you want to make sure you're being smart and proactive.

Previous launches have been criticized for not being careful enough

When DERO launched their bulletproofs, they were criticized for not waiting until the cryptography was fully audited. You can read more of one redditor's criticisms of it here.

In hindsight, there weren't any issues, so their internal checks were sufficient. But it's hard to argue that it was in accordance with best practices.

To this, all we can say is that we hope that they've learned from the lesson of the criticism and will move more carefully in the future. Anything but a completely thorough and careful launch is in no one's best interests, and we're hard pressed to think that such behavior (from a couple of years ago) will be repeated. It remains, however, a blemish on the record.

Finally, as always, please read our "very important disclaimer" below, and respect that investing in anything at an early stage (especially in crypto) will have risks - many of which we may not even be aware of, but only in hindsight.

Very important disclaimer:

If you are going to invest, make sure you only invest what you can afford to lose. We have added DERO to the TCV portfolio, but it is an extremely small cap coin, so it's very likely that its price movements will be extremely volatile. We have

allocated DERO at only 2% of the entire crypto portfolio due to its very tiny market cap. As of June 20, 2021, the price was $5.65.

While we believe the upside/downside is skewed in favor of a long position, if DERO rises exponentially too quickly, it could easily drop back down just as quickly. However, we could also potentially raise our target if the buying volume appears to remain strong and if there is major fundamentally positive news to support that move. Please be mindful of risk management, and 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 bull market. Please use caution!

Dero (DERO) Exchange

If you are interested in trading DERO, we recommend using TradeOgre since it appears to be the most liquid, trusted, secure, and stable exchange for this coin at this time.

https://tradeogre.com/exchange/BTC-DERO

DERO Wallet Software and Additional Resources

The official Dero project site can be found at https://dero.io/. There you can find a plethora of information around and supporting the project.

For the Dero wallet, we only recommend using the official software for any significant amounts at this point in time since it is so early in development. You can use either the CLI (command-line, for advanced users only) or the web wallet, both of which are available at the website. Although the web wallet allows you to own your private keys, we don't recommend storing a significant amount of funds there as web wallets in general introduce risks.

For those interested in learning more about DAG, Block DAG, and Dero's implementation, you may find the below articles useful.

https://academy.binance.com/en/articles/what-is-a-directed-acyclic-graph-dag-in-cryptocurrency

https://ancapalex.medium.com/an-introduction-to-the-blockdag-paradigm-50027f44facb

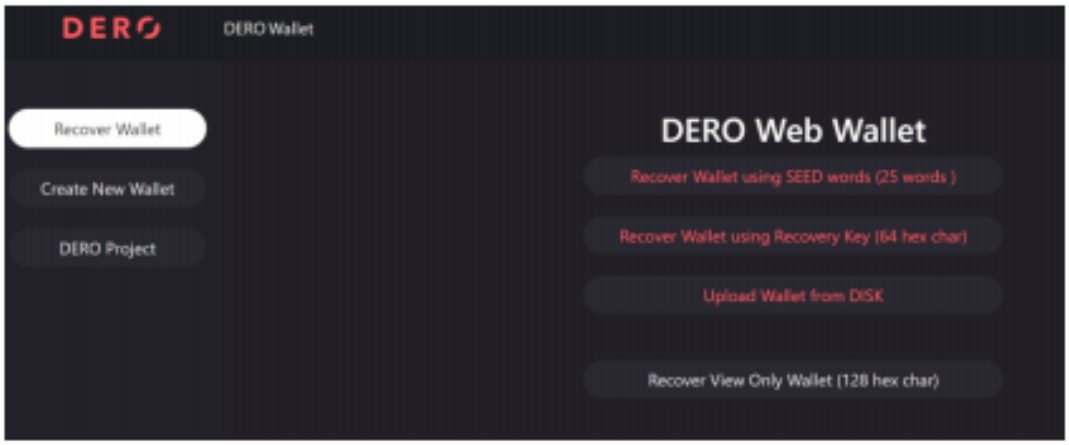
https://www.thebirbnest.com/uncategorized/dero-the-formula-1-privacy-coin-is-just-starting-its-engines/

A DERO Web Wallet Walkthrough

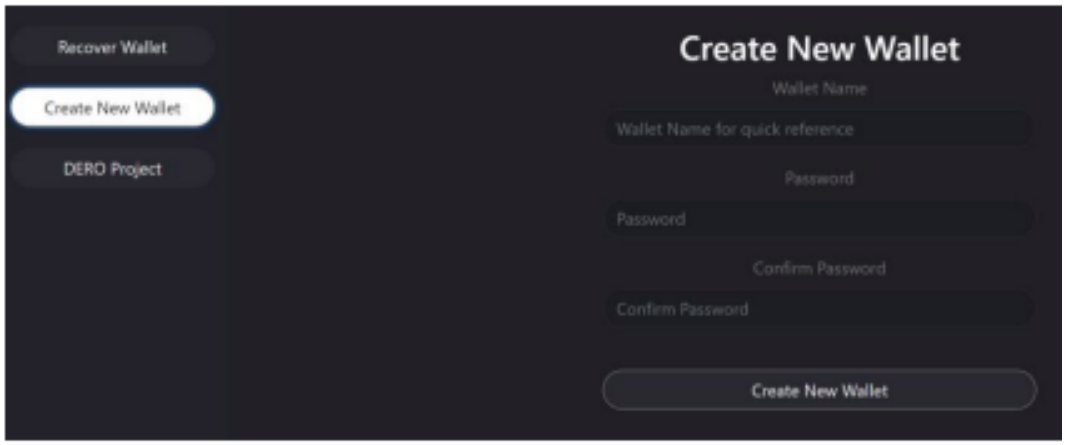
While many of our subscribers are seasoned crypto veterans, we recognize that many others are relatively new to the space. In general, as wallets go, the Dero web wallet is fairly painless to navigate. However, we understand that it can still be a bit overwhelming for some, and wanted to offer this simple walkthrough for those who need a little extra help.

*Please note - **we are not tech support** and as mentioned earlier, are not vouching for the wallet. We simply are including this little walkthrough in response to feedback we received in previous instances where we introduced a new asset and wallet.*

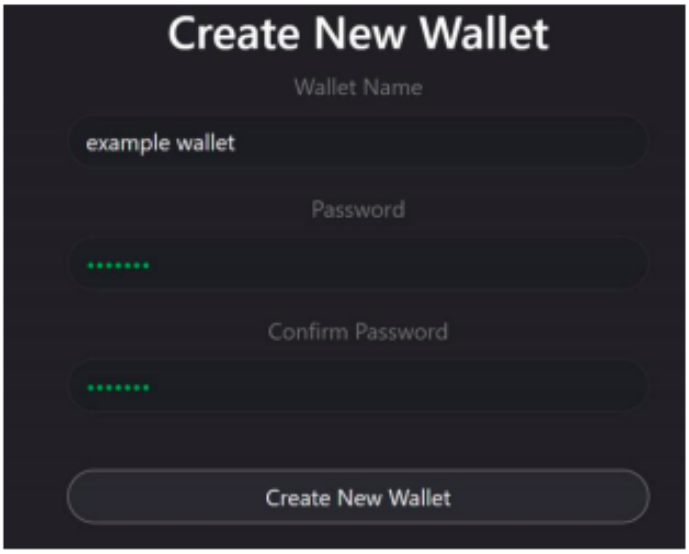
Below is what you should see when you arrive at the site https://wallet.dero.io - presumably whilst using a VPN - such as the free ProtonVPN.



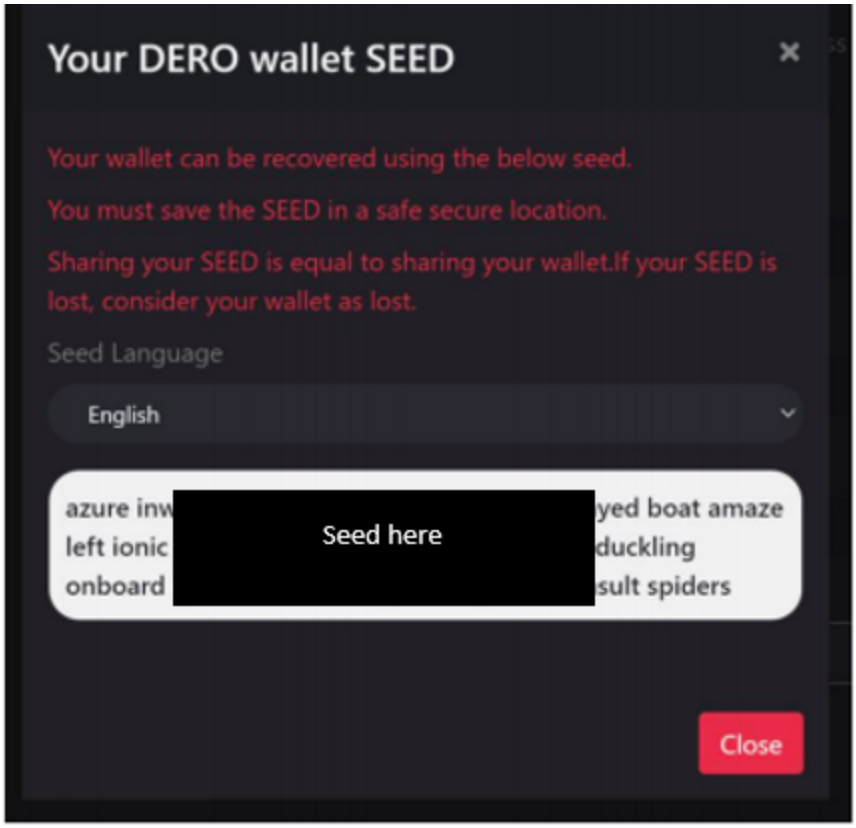
Click 'Create New Wallet', and you'll be taken to the below screen.



We'll create a new wallet together here. We're going to name this one 'example wallet', but of course you pick whatever you like. Enter the name of the wallet (whatever you want to call it), and put a strong password in for yourself. If the password symbols are red, not green, it means that your passwords don't match. Make sure they do or you won't be able to progress further.



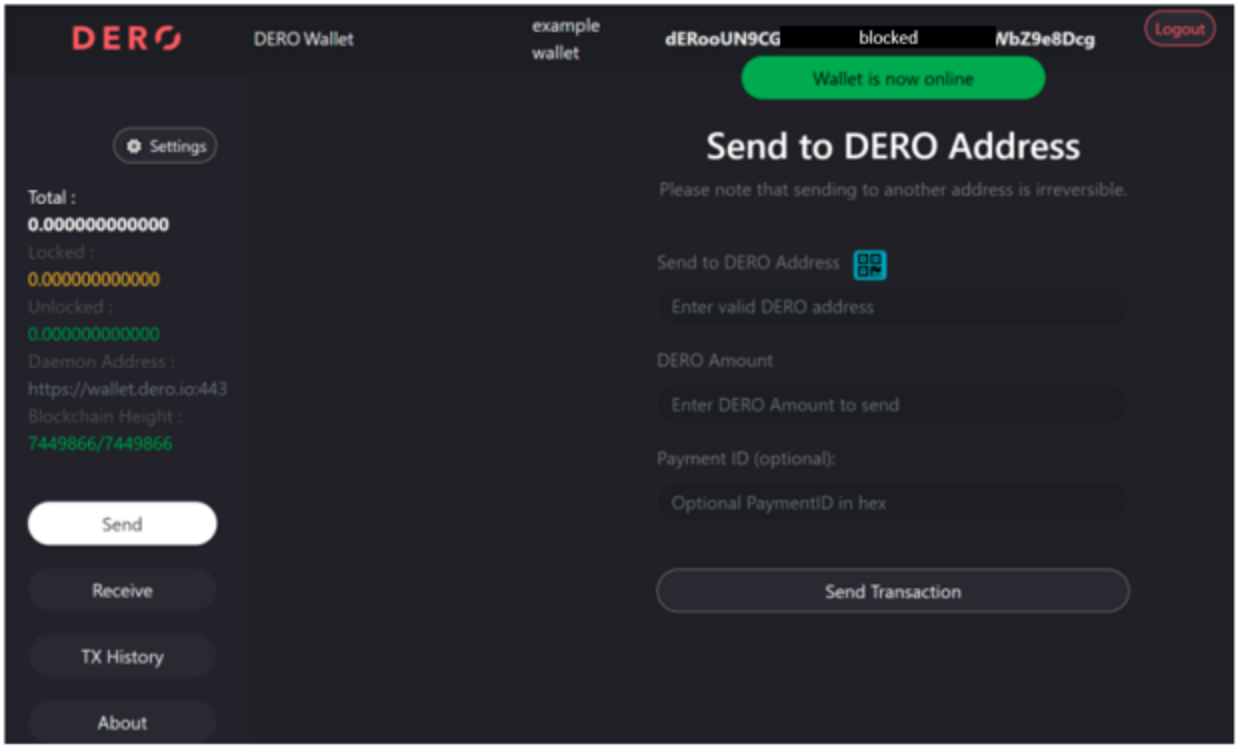
Let's go ahead and create the wallet now by clicking 'Create New Wallet'.



These 25 words are your seed key. Do not copy these to your clipboard (i.e., copy/paste). Instead, write them down. Save them in a secure location.

(Note: this sample wallet will never hold any tokens, but for operational security and privacy purposes some parts of the screenshots have been blacked out)

Once that's done, hit close, and you should see something like the picture below.



That's about it. You're set up now!

However, for your peace of mind in case you ever are forced to rely on your seed phrase to restore the wallet, we recommend you close the wallet and try to restore it with the seed.

Before you do though, note two values:

1. The blockchain height on the left-hand side of the screen.

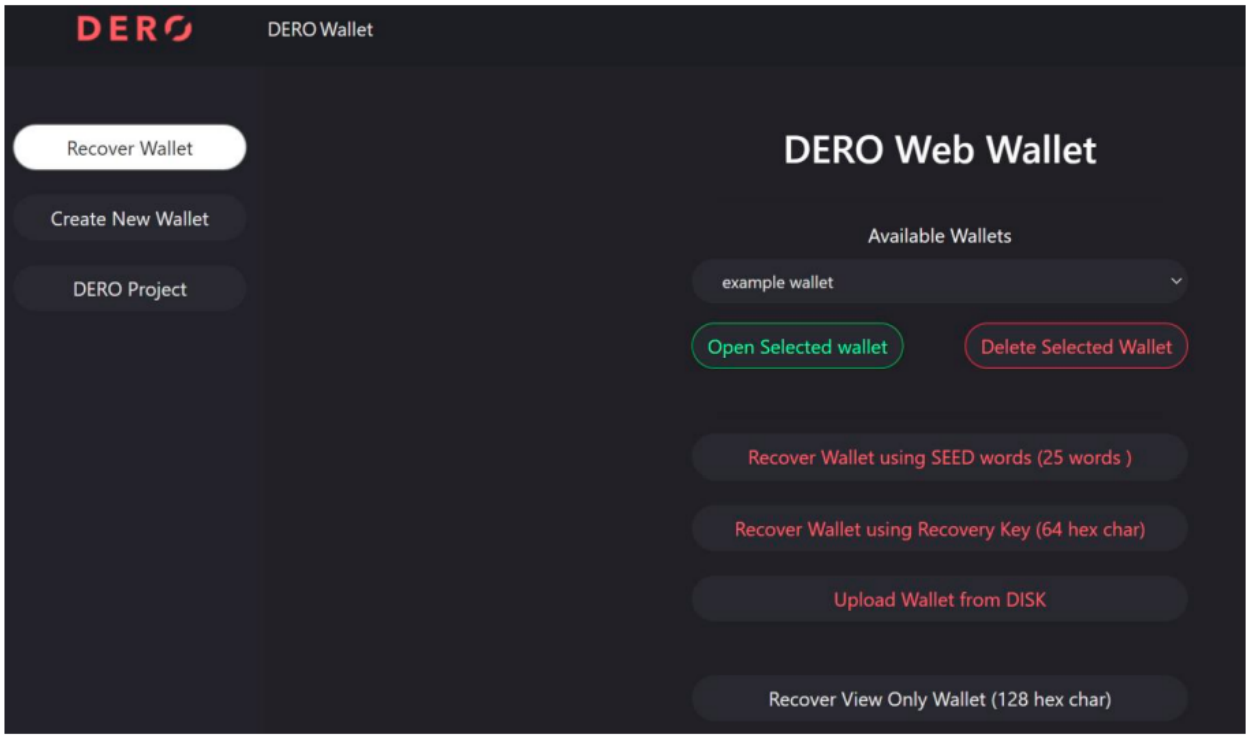
   In this example it is 7449886. Subtract 1000-2000 from this number and make it a nice easy round number. We'll use 7448000.

2. Copy and paste the wallet's public key to someplace you can check shortly.

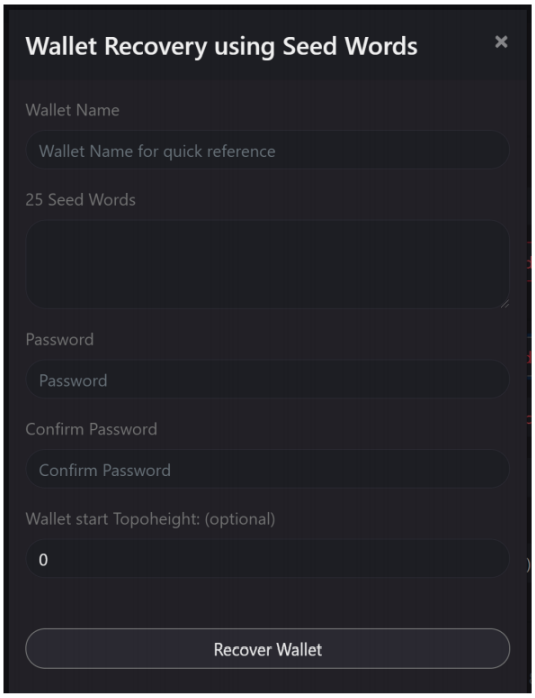
   This is the value just above the 'Wallet is now online' green button, beginning with "dERo".

   Clicking it once should select it. Then copy and paste it somewhere. No need to worry about using the copy/paste function here. It's fine to use. We'll reference this in a minute.

Now logout (top right corner button), and refresh the web page. It should look like the picture below.



Instead of opening the selected wallet (which would prompt you for your password), click ‘Recover Wallet using SEED words’ (25 words). You’ll see the below screenshot.

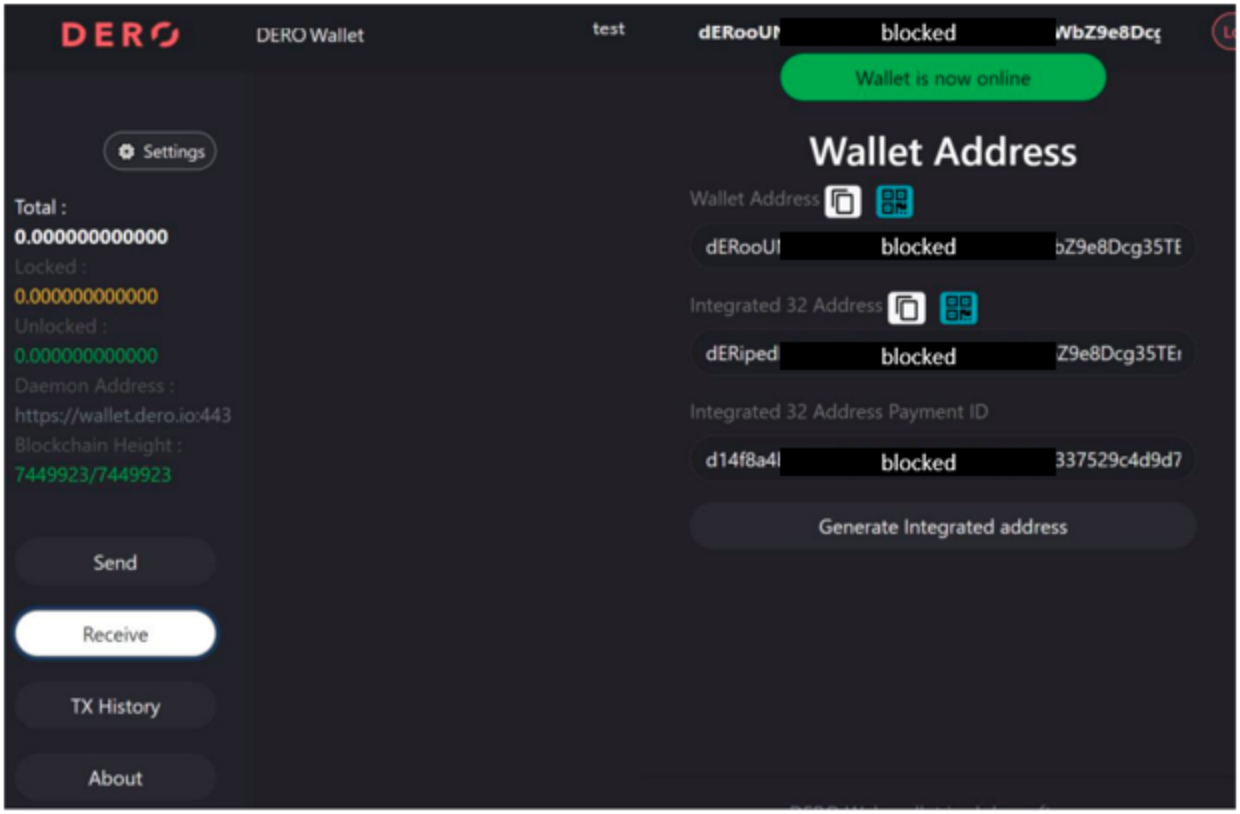


Put a new name for the wallet here, a new password, and the 25 word seed phrase you wrote down. For the optional wallet start value, put in the value we derived previously - here it's 7448000 (this will save you from having to wait for the whole blockchain to sync).

Once that's done, click 'Recover Wallet'. It shouldn't take more than a few minutes for you to be back online. You can confirm it's the same wallet by comparing the public address (value above the 'Wallet is now online' button to the same value you copy/pasted before).

So, with proving to yourself that you can recreate the wallet with the seed, you can move on to receiving and sending.

To get the receive address, just click on 'Receive' on the left.



Clicking that first white button under 'Wallet Address' copies the address to your clipboard. Note it's the same as the wallet address on top. Once done, paste it as plain text into TradeOgre as the address to which you want to withdraw DERO. Visually scan to at least make sure the beginning and ending characters match.

Sending it is even more straightforward. Assuming you're sending to TradeOgre, you simply copy and paste the TradeOgre address into the 'Send to DERO Address' line along with the amount. Click send, re-enter your wallet password, and you're done.

The Dero network is fast. You should see your balance show up as a locked balance in less than a minute, and unlocked shortly afterwards. Easy!

ONE more thing to do though before we finish, and this is important.

Logout again, and go through the same process of recovering your wallet with the 25 word seed phrase. See anything interesting? Yeah. It stored your seed phrase and left it on the screen. You don't want this there.

Highlight and delete the seed phrase so if someone else gets your computer they can't see it. Then close the window. You should be able to re-open it now and see that it's blank. You're now good to go.

Mr. X & Mr. Z

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) 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.