

Forum: [Hack Forums](#)

Thread: [Privacy Coins Discussion](#)

Ninja™ - August 4, 2021, 2:41 am

Hi,

I dont see much threads here regarding privacy coins discussion.
I saw FocusBroken's thread regarding wallet bug recently.

And few other I searched were very old and no recent posts on them.

I am making this as privacy coins deserve the attention they usually dont get.
I mean one of the main reason of crypto rise is privacy.

Monero is has all-time love.?

<https://coinmarketcap.com/currencies/monero/>

If you wanna setup a paper wallet just to see incoming tx(to know you sent funds to correct addy & also balance) , here is the guide:

https://www.getmonero.org/resources/user-guides/view_only.html

also here you can generate paper wallet:

<https://moneroaddress.org/>

<https://wallet.mymonero.com/>

PirateChain (ARR) too is promising.

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

I am part of the discord there and it quite active .

If anyone wanna take a look at the whitepaper.

https://pirate.black/files/whitepaper/The_Pirate_Code_V2.0.pdf

Havent used the Zcash till now, so would like to hear feedback.

Feel free to share if you found any other interesting ones.

x_x - August 4, 2021, 2:56 am

Monero has a brother "Wownero" it is alledged even more private than Monero but I haven't researched it enough to confirm that. Doesn't ARR already have almost the entire supply mined?

trashy - August 4, 2021, 2:58 am

There is XHV which it seems to be better than monero, but I think it got hacked months ago.
anyways they are with the project

<https://havenprotocol.org/whitepaper/>

<https://coinmarketcap.com/currencies/haven-protocol/>

Ninja™ - August 4, 2021, 3:26 am

Updated the bio with setting paper xmr wallet and setting view only wallet.

T0Bi - August 4, 2021, 11:14 am

(Aug 4, 2021 06:04 AM)Focus Broken Wrote: [\[CITE\]](#) I had a short discussion with [BalleJatta](#) on [another thread](#) about Mimblewimble development for Litecoin. Definitely something to look into, here's the second version of the whitepaper:

<https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf>

There are two other mimblewimble implementations, Beam and Grin.

I looked into them last year or the year before, but the tokenomics just sucked...

But afaik Beam and Grin are the only mimblewimble implementations that are currently live, so one might want to take a look at them.

Also Litecoins mimblewimble will probably take a few months until it can be released.

T0Bi - August 4, 2021, 11:28 am

(Aug 4, 2021 11:21 AM)Focus Broken Wrote: [\[CITE\]](#) I'm more interested now about whether or not Litecoin can integrate it via an extension block, as that would set the precedence for having MW on Bitcoin.

Oh yes, same here.

It's just sad to see that the two projects that actually implemented such ground breaking technology completely fucked up their tokenomics and both in different ways.. And since the market is hype and price driven and technology doesn't seem to matter for the average investor, they never took off and probably never will.

Afaik Litecoins MW is already code complete and we're 'just' waiting for code reviews & fixes.

And if everything works fine, we'll probably have MW on Bitcoin in a few years, depending on how the core devs feel lol

Frost Crypt - August 5, 2021, 1:32 pm

i heard something about monero not being private if you send coins in less than 1 hour after you receive them.

i think monero biggest let down is it's hard implementation in autobuy systems due to their privacy .

Ninja™ - August 5, 2021, 1:41 pm

(Aug 5, 2021 01:32 PM)Nano Shield Wrote: [\[CITE\]](#) i heard something about monero not being private if you send coins in less than 1 hour after you receive them.

i think monero biggest let down is it's hard implementation in autobuy systems due to their privacy .

The bug will be fixed soon as devs are working on it.

I am not sure about that, I have seen plenty of places that support XMR autobuy.

SUI-3183372 - August 5, 2021, 5:24 pm

https://twitter.com/railgun_project

Interesting project for on-chain privacy on Ethereum.

Ninja™ - August 6, 2021, 9:49 am

(Aug 5, 2021 05:24 PM)BV1 Wrote: [\[CITE\]](#) https://twitter.com/railgun_project

Interesting project for on-chain privacy on Ethereum.

<https://tornado.cash/>

another one with someone mentioned this one in some other threads.
looks promising.

Its open source too.

UnoOne - August 6, 2021, 10:01 am

(Aug 6, 2021 09:49 AM)Ninja™ Wrote: [\[CITE\]](#) <https://tornado.cash/>
another one with someone mentioned this one in some other threads.
looks promising.

Its open source too.

there is also <http://sherpa.cash> fork of TORN ,on avalanche

It's brand new project..IDO was last week for 15 cents

Ninja™ - September 16, 2021, 1:26 am

I have watched monero ring CT video, my question may sound dumb but if monero is open source and everyone can see how it works, can same encryption and decryption be done if procedure is followed? like isnt open source something that can be replicated exactly or like can be done same thing from the source? How open source code integrates with monero's privacy system?

Interested in hearing your thoughts.

Voxcon - September 16, 2021, 2:31 am

(Sep 16, 2021 01:26 AM)Ninja™ Wrote: [\[CITE\]](#) I have watched monero ring CT video, my question may sound dumb but if monero is open source and everyone can see how it works, can same encryption and decryption be done if procedure is followed? like isnt open source something that can be replicated exactly or like can be done same thing from the source? How open source code integrates with monero's privacy system?

Interested in hearing your thoughts.

Bitcoin is open source as well and still can't be "hacked" unless you have control over at least 51% of the network hash rate. The thing which makes BTC as well as Monero "unhackable" is the fact, that they use one-way hash functions (SHA-256, ECDSA, Keccak-256) to encrypt their data. Meaning it's computationally easy to encrypt data, but almost impossible to decrypt it. That's the case because the only viable way to find a decryption match is via brute-forcing random bits of data (aka mining).

Best regards,
Vox

Ninja™ - October 11, 2021, 5:25 pm

[Video: <https://www.youtube.com/watch?v=SwX0zfw0irA>]