Cryptocurrencies & Platforms

Top 8 Privacy Coins

April 16, 2018 By Steven White

It's a common misconception that **Bitcoin and other cryptocurrencies** are fully anonymous and untraceable. In fact, many blockchains only disguise users' identities while leaving behind a public record of all transactions that have occurred on the blockchain. The data in the ledger often includes how many tokens a user has received or sent in historical transactions, as well as the balance of any cryptocurrency that they have within their wallet.

There is a concern that even with their identities disguised, users can still be identified based on their activity within a blockchain. This is why some people turn to privacy coins – cryptocurrencies that provide users with a higher level of anonymity.

Although controversial (some authorities see privacy-oriented coins as an illicit tool that can be used by criminals to engage in illegal activities, such as money laundering), privacy coins are the safest way for users to make **blockchain transactions** without their financial details being exposed to the public. These platforms typically have several privacy-centric functions, like stealth addresses or private

If you're interested in learning more about privacy coins, here are our top 8 favorites that are currently available on the market.

Monero

Monero was launched in 2014, and since then it has grown to become one of the most stable and secure privacy coins released to date. Their cryptocurrency platform is the product of a Bitcoin fork but, unlike Bitcoin, Monero was created with several anonymity features. Monero effectively allows its users to have a firm command over the privacy of their data by keeping transaction information completely anonymous within the blockchain.

Monero has a few unique features that helped it grow to become the top contender in the privacy coin market.

Ring Signatures

A ring signature is a digital signature that is created by bringing a group of signers together. Monero uses this digital signature to bring multiple signers (usually 5) into each transaction. Only the sender is able to generate and send the spend key, and only the actual recipient will be able to detect the key and spend the funds linked to it. With a ring signature in place, it is impossible to link any transaction back to any one user, offering a high grade of privacy.

Ring Confidential Transactions (RingCT)

This feature hides the amount of each transaction on Monero's network. RingCT works by creating cryptographic proof that can show that the input and output amounts are equal, without revealing any of the actual numbers.

Stealth Addresses

Monero also uses a network of stealth addresses to allow users to disconnect themselves from the blockchain. A stealth address is a one-time use address that is created for every transaction. Monero users also have a public address that is published on the blockchain, but most (if not all) of their transactions will be passed through unique stealth addresses.

With these inherently straightforward and easy to understand features, Monero has managed to remain relevant in the crypto space while offering users a completely untraceable cryptocurrency platform.

To learn more about Monero, check out "**Monero 2018 Roadmap: The Future of Private Digital Currency Looks Bright**" and "**Should You Invest in Monero? (Opinion)**".

Zcash is another Bitcoin-forked privacy coin, but it only has a handful of privacy features. The primary privacy feature that Zcash uses is zero-knowledge Succinct Non-Interactive Argument of Knowledge proofs (zk-SNARKs).

That name may be a mouthful to pronounce, but the basic functionality that this privacy method offers is simple to articulate. zk-SNARKS encrypt all transactional data that is stored on the network. This method verifies that the data being exchanged is accurate, but it does so without revealing all of the transaction details.

But it is important to note that using these privacy features is optional, as users can opt for transparent (public) or private addresses. Some critics believe that users choosing not to activate the privacy features may compromise the overall security of the entire network.

Dash

Dash is a bit different from the previously mentioned coins. Founded after a Bitcoin fork in 2014, it is an open-source peer-to-peer cryptocurrency that offers many of the same features as Bitcoin. But in addition to Bitcoin's core features, Dash also includes the option for instant and private transactions.

To ensure the integrity of their system, the developers of Dash chose to implement a Proof-of-Stake protocol as well. This part of the system is designed to provide additional support to the miners that validate transactions on the first tier of the service.

Masternodes are introduced to the network for the purpose of validating transactions on the second tier of the service, which facilitates private and instant transactions as well as governance features. In order to run a masternode, a user must have at least 1,000 tokens in their wallet.

The instant-send function sends transactions along the 2nd tier of the Dash blockchain, allowing them to be confirmed quickly.

Private transactions are sent using the CoinJoin method. This method consists of attaching transactions together to make "joint payments." But unlike a traditional joint payment, the value that was exchanged by each party and the place that the payment ended up are completely

You can **learn more about Dash here**. Get caught up on the latest from Dash and read "**Will Dash Hit its Stride in 2018 Despite Development Delays?**".

PIVX

PIVX is another new privacy coin that works similar to Dash, but operates on Proof-of-Stake rather than Proof-of-Work. PIVX users are allowed to run master nodes which help keep the network running smoothly. Commanding one of these nodes requires a stake of at least 10,000 tokens (in comparison, Dash only requires 1,000 DASH). With this much higher threshold, PIVX has more of its available token supply tied up in various master nodes.

PIVX has fast transaction verification, and supports both private and instant transactions. Transactions can be made completely anonymous, preventing discovery of a person's real-world identity by analyzing the blockchain.

At the time of writing, the block time is about 60 seconds. Transaction fees are also quite small. These qualities make PIVX a worthy mention in the privacy coin conversation.

Visit the **PIVX website** to learn more about this project.

NavCoin

NavCoin is a decentralized cryptocurrency that was forked from Bitcoin. It aims to solve 2 problems that are typically found in blockchain platforms:

- Data is made public on the blockchain, leaving it vulnerable to malicious attacks by illicit users.
- Most blockchains use "roll backs" as the solution to data vulnerability. They reset the blockchain to a backed-up point after a data breach, meaning transactions made leading up to the roll back are erased.

The NavTech system is a combination of the traditional Bitcoin blockchain and a NAV subchain. Using two chains allows users to send transactions with complete anonymity.

Over the course of 2017, NAV managed to achieve significant growth and now manages a community of more than 50,000 users. Through 2018, they are aiming to implement a platform for building blockchain applications within the network. In addition to that goal, they also hope to add support for instant exchanges across different currencies.

Find out more about NavCoin on their **website**.

Cloak is a veteran privacy coin that is growing slowly, although it has been active in the privacy niche for approximately 4 years. The blockchain is operated using a Proof-of-Stake consensus protocol. It has relatively short blocktimes and quickly processes transactions.

The platform also offers 2 different methods of making your transactions untraceable.First is their onion-routing privacy protocol. Onion routing involves encrypting messages with many layers (similar to an onion).

It also offers the Enigma process to provide additional privacy cloaking on transactions. Enigma cloaking is applied when a user requests a cloaked enigma transaction. These transactions are carried across dedicated Enigma nodes, which are designed to cloak transaction data by shuffling it with other random data. Only these Enigma nodes are able to identify if the input and output data is accurate.

To learn more about CloakCoin, check out **their whitepaper**.

Enigma

The Enigma project is entirely separate from the Enigma cloaking process used in CloakCoin transactions. Enigma is not a cryptocurrency nor a blockchain; instead, it is a privacy protocol that can be deployed on blockchains and decentralized applications. Therefore its token, ENG, is a distinct addition to the list of top privacy coins.

The Enigma network provides privacy by making nodes unable to see the data that they compute. Although they are unable to clearly see exactly what they are working on, these nodes are still capable of verifying that their computations have been run correctly. With the data masked like this, Enigma hopes to open the door for what they call a new type of smart contracts – "secret contracts" – wherein the underlying data processed in a smart contract remains encrypted at all times.

Enigma's token must be purchased in order to run a node on their network. After buying the Enigma token, you can receive rewards for processing data. But in order to process data, each node must make a security deposit. If the data is tampered during the verification process, the deposit will be split between any nodes that processed the data without error.

To learn more about Enigma, **click here**.

DeepOnion

DeepOnion is a new privacy coin project that is generating some interest in the community. Like a few of the other coins in this list, DeepOnion uses TOR to send untraceable transactions. It also uses a mix of Proof-of-Stake and Proof-of-Work protocols to offer fast confirmation times.

DeepOnion also employs stealth addresses to keep transactions private. As mentioned before, a stealth address allows the sender to use a one-time user address for their transactions. The recipient only needs a single address, but before they receive the value that is sent, that block is sent to unique addresses on the chain where they cannot be connected to the sender or recipient's personal address. This ensures that only the sender and receiver can consistently know where payments originated and where they were sent.

The DeepOnion team is currently working on DeepSend and DeepVault. DeepSend will use a multi-signature method to prevent payments from being traced. DeepVault is an information storage service that allows users to store data in the blockchain forever. To be more precise, DeepVault allows users to store hashes of files within the blockchain. In order to verify the integrity of a file, a user only needs to compare their current version of the file with the backup. This can be beneficial for the purpose of verifying the integrity of important documents.

As the community develops, DeepOnion will also launch their VoteCentral function. It will allow users of the platform to vote on new developments and present their ideas for future projects. This project is small now, but in some regards it does show promise.

Visit the **DeepOnion website** to learn more.

Conclusion

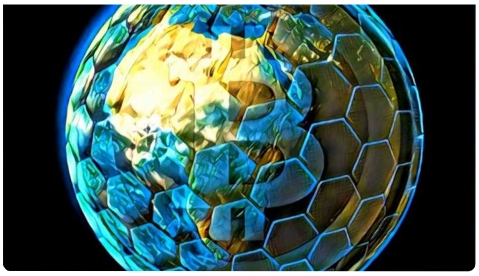
Privacy coins are a niche group of cryptocurrencies. Some people may have no concerns about whether their transaction history is discoverable by third parties. But others might adamantly refuse to participate in any cryptocurrency platform that cannot guarantee them complete privacy.

If you are interested in investing in blockchain but have concerns about personal privacy, consider getting started with some of the privacy coins mentioned here.

Related: Top 5 Undervalued Platform Coins

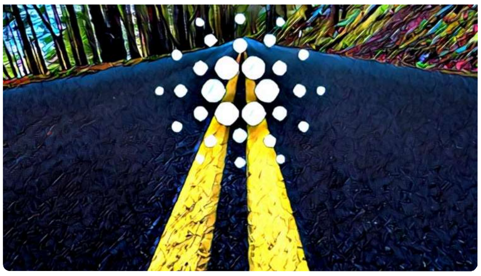
If Steemit And Medium Had A Baby: Publish0x Rewards Both Authors And Readers In Crypto

JUNE 20, 2019



Bitcoin As A Hedge Against Upcoming Global Market Crash

JUNE 19, 2019



Cardano Updates Its Roadmap – What's In For Investors?

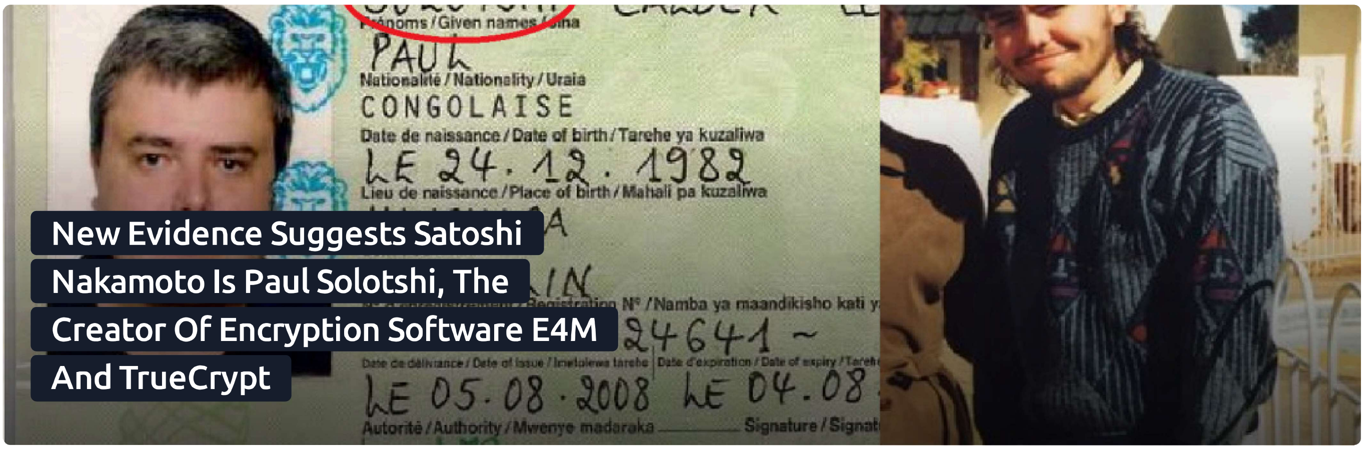
JUNE 13, 2019

Tags: CloakCoin, Cryptocurrencies, Dash, DeepOnion, enigma, Monero, NavCoin, PIVX, privacy coins, ZCash

About Steven White

Steven is a cryptocurrency writer, blogger, and traveler. Having gotten plenty of entrepreneurial experience at an early age, Steven has refocused his talents into writing content targeted at inspiring other people to pursue a better future for themselves

Read More →



New Evidence Suggests Satoshi Nakamoto Is Paul Solotshi, The Creator Of Encryption Software E4M And TrueCrypt

Trending Now →