How to Keep Private in Crypto Today?

Original:
https://www.btcc.com/en-US/academy/crypto-basics/how-to-keep-private-in-crypto-today

Learn about the different ways crypto users can keep their activity private and the benefits privacy-oriented blockchains can bring to the broader crypto ecosystem.

Key Takeaways

- Blockchains have created a more open financial system, but they are often ineffective at helping users maintain privacy.
- Blockchain networks such as Monero, Zcash, and Secret Network focus on protecting user privacy.
- Mixing services for Bitcoin and Ethereum have also gained traction by providing users with a way to obfuscate their transaction history.

While blockchains offer an uncensored way to transfer wealth, they have never been about protecting privacy. However, in the years since Bitcoin was introduced, blockchains like Monero, Zcash, and Secret Network have developed infrastructure for private blockchain transactions. Meanwhile, coin mixing protocols like Tornado Cash and CoinJoin enable users to separate the cryptocurrency they own from their true identity.

Keeping Crypto Private On-Chain

The crypto movement has created a more open alternative to the traditional finance system. While blockchains like Bitcoin and Ethereum offer benefits such as financial inclusivity and transparency, they are not so good at preserving their users' privacy. In response to the need for helping users stay private, several blockchain-based solutions have emerged.

Monero

Arguably the most successful privacy-focused blockchain that still sees development and use today is Monero. Originally known as BitMonero, the network was deployed in 2014 and has survived due to its best-in-class anonymity, range of privacy-preserving features, and active developer community

that still includes many early contributors.

Monero makes the identity of senders, recipients, and the amounts sent in transactions anonymous by disguising the addresses used by participants. The network hides transaction details through a combination of privacy-preserving methods, including ring signatures, zero-knowledge proofs, stealth addresses, and IP address obscuring methods.

Monero has implemented several updates to improve its security and privacy features in the eight years since its launch. In December 2019, the network switched its Proof-of-Work algorithm from CryptoNight to RandomX to stop application-specific integrated circuit (ASIC) machines from mining Monero. The move improved the network's security by making it more difficult and expensive to 51% attack the network.

In May 2020, Monero implemented ZK-SNARKs into its privacy technology. This improved transactions by making them faster, more efficient, and requiring fewer confirmations.

Monero also preserves privacy by having completely fungible coins. Unlike Bitcoin, where individual coins can potentially be traced back to every wallet that held them and when they were mined, all of Monero's XMR coins are completely indistinguishable from one another.

However, as Monero is currently viewed as the gold standard for both crypto privacy and anonymity, it has become the blockchain of choice for cybercriminals. Ransomware groups, darknet marketplace users, and even North Korean hackers are all reported to have used Monero in their illicit activities. As such, the Internal Revenue Service has posted bounties of up to $625,000 for contractors that can develop Monero tracing technologies. Currently, no bounties have been claimed, which speaks to Monero's privacy technology.

Zcash

While Monero is the most popular privacy-preserving blockchain in use, it is not the only one. Another popular blockchain of choice among privacy enthusiasts is Zcash. Launched in 2016, Zcash uses zero-knowledge proofs to verify transactions without revealing the sender, receiver, or transaction amount.

Zero-knowledge proofs use advanced cryptography to let parties confirm the details of a transaction without revealing any of the specifics to one another. ZK-proofs achieve this through a special set of verifying keys that are shared among all the participants in the network. These keys let network participants cryptographically confirm changes on the Zcash ledger without revealing which addresses were involved or how many coins were transferred.

There’s one major difference between Monero and Zcash. While all Monero transactions must use the network’s privacy features, Zcash’s privacy features are optional and do not come as a default. While this system makes it easier to broadcast transactions publicly if needed, it has also had the unintended effect of compromising the privacy of those trying to hide their transactions.

Currently, less than 20% of all Zcash transactions use the network’s full privacy-preserving features. When only a small portion of total users are shielding their transactions, it makes it much easier for an attacker to isolate the few users who are using the privacy features, potentially weakening the privacy of their transactions. On the other hand, because all Monero transactions must use the network’s rigorous privacy system, no transaction stands out from others, and maximum privacy is maintained for all users.

Despite this vulnerability, the technology behind Zcash is just as secure, if not more secure, than Monero. Theoretically, the technology securing Zcash transactions is impossible to crack without the network creation event keys. However, if these keys were not destroyed and still exist somewhere, they could be used to attack the network by minting unlimited amounts of new coins or falsifying transactions.

Ethereum co-founder Vitalik Buterin has praised Zcash’s zero-knowledge cryptography, noting that the network is engaged in “cutting-edge research and deployment of privacy tech.” He also sits on the scientific advisory board for the Electric Coin Company, the firm that developed Zcash.

Tornado Cash

Those looking to stay private on Ethereum can use a dedicated coin mixing platform called Tornado Cash. It works on the same principle as CoinJoin, except users do not need to find other parties to mix their coins with. Instead, the mixing process is handled through advanced smart contracts made possible on Ethereum.

Tornado Cash is often touted as more secure than mixing Bitcoin through CoinJoin. The process connects input and output accounts through zero-knowledge proofs rather than merely obfuscating transaction data. This means it is theoretically impossible to connect the address that deposited Ethereum into Tornado Cash and the wallet that eventually receives it, as long as the user doesn’t inadvertently compromise their own privacy.

To use Tornado Cash, users generate a random key and deposit Ethereum or ERC-20 tokens, then submit a hash of their key to the Tornado Cash smart contract. After depositing, it’s advised to wait some amount of time before withdrawing funds to a new wallet. The longer the period between the deposit and withdrawal is, the more secure the transfer will be. To withdraw funds, users must

submit a zero-knowledge proof of their key to Tornado Cash, and the smart contract will withdraw the deposited funds to a specified recipient.

CoinJoin

CoinJoin uses a transaction privacy method where several users collaborate to obscure the sources and destinations of Bitcoin sent between them. Users sign a digital smart contract to mix their coins in a new Bitcoin transaction, where the output leaves participants with the same number of coins but mixes the addresses to make external tracking difficult. The process anonymizes Bitcoin transactions without the need for a centralized operator.

Greg Maxwell first proposed the process of using CoinJoin in 2013, and it has since become one of the most popular ways to preserve privacy among Bitcoin holders. Initially, the biggest obstacle to using CoinJoin was finding enough holders who also wished to mix their coins. Now, Bitcoin wallets like Wasabi and Samourai have directly implemented CoinJoin, offering users an easy way to connect, mix coins, and preserve privacy.

While coin mixing effectively preserves the privacy of Bitcoin holdings, there is increasing evidence that mixing through CoinJoin may not be as secure as previously thought. In February, Forbes journalist Laura Shin claimed that blockchain data platform Chainalysis was able to “demix” Bitcoins sent through CoinJoin to identify the 2016 Ethereum DAO hacker. While demixing CoinJoin is theoretically possible, it’s unclear whether Chainalysis found a way to trace mixed Bitcoins or whether the hacker made mistakes that led to his identity being revealed.

Coin Mixers

While dedicated privacy-preserving blockchains offer effective ways to stay private, those holding funds on other public blockchains such as Bitcoin and Ethereum may also want to take measures to maintain privacy. Network activity cannot be hidden by the nature of how most networks operate; however, coin mixing services can be used to break the trail of transactions between addresses, letting users keep their crypto wallets separate from their real-life identities.

There are several reasons why someone would want to use coin mixing services. People often use mixers for operational security purposes. People who have a large amount of crypto wealth tied to their real-life identity have increasingly been targeted by hackers, social engineering scams, and even kidnapping. Wallets with vast amounts of coins are fully visible on-chain and can be traced back to the holder’s real-life identity with relatively little effort. Coin mixing services such as CoinJoins and Tornado Cash can help users break the connection between high-value crypto wallets and their real-life identities, helping to protect them from being targeted.

Secret Network

Secret Network is an emerging privacy-focused blockchain that's starting to gain traction. Unlike Monero and Zcash, Secret Network is Turing complete. That means it can handle smart contracts like those found on blockchains like Ethereum and Solana. The network is pioneering what it calls "Secret Finance," comprised of DeFi applications enabled by privately encrypted smart contracts.

Secret Contracts preserve privacy by encrypting the input, state, and output of all transactions. However, compared to Monero and Zcash, other transaction details, such as block height, time, chain ID, sender, address, sent funds, and contract hash, are not encrypted. Secret Network, therefore, is less interested in maintaining anonymity than other privacy-oriented networks, but it still ensures that the interactions between users and smart contracts remain completely private.

Private smart contracts offer several advantages over public ones. Unlike Ethereum and other Layer 1 networks, transactions on Secret Network are resistant to frontrunning since they are never visible in the mempool. This means that opportunists cannot extract value through MEV, a popular practice in which users pay to rearrange transactions in blocks.

Additionally, because Secret Network's smart contracts operate as encrypted "black boxes," they can handle sensitive data without the risk of broadcasting it publicly. This guarantee allows private blockchain networks to run their operations on Secret Network, opening up interoperability with other applications built on the network.

Secret Network's privacy features extend beyond its own applications and token. Through the network's "Secret Bridges," users can bridge tokens from other networks such as Ethereum or BNB Chain and take advantage of all of Secret Network's privacy-preserving features. When assets are bridged, they become encrypted and are only visible to their owners or to those holding a viewing key. Bridged tokens can then be used across the Secret Network ecosystem.

Despite all of its promises, compared to the more time-tested Monero and Zcash, the technology behind Secret Network is relatively unproven. The network minted its genesis block in February 2020 and has only started onboarding a large number of users over the past few months. According to data from Defi Llama, Secret Network currently hosts only $40 million of total value locked across its DeFi protocols, highlighting how underdeveloped its ecosystem is compared to other competing Layer 1 blockchains. Despite its current low usage, the network's native SCRT token has reached a market cap of over $766.7 million.

Conclusion

For many people who hold crypto, staying private is incredibly important. Privacy-preserving blockchains and protocols like Zcash and Tornado Cash help users stay private, improve security for

high net worth individuals, and allow those living under totalitarian regimes to preserve their assets.

However, it’s also important to acknowledge the costs of privacy. Blockchains like Monero have helped cybercriminals execute ransomware attacks and hide millions of dollars. Tornado Cash also allows hackers launder illegally obtained tokens from DeFi protocol exploits and phishing attacks.

As crypto continue to enter the mainstream, governments may crack down on privacy-preserving technologies in the name of reducing cryptocurrency-related crime. While this is an admirable goal, striking a balance between privacy and crime reduction will be key to allowing crypto to reach its true potential.