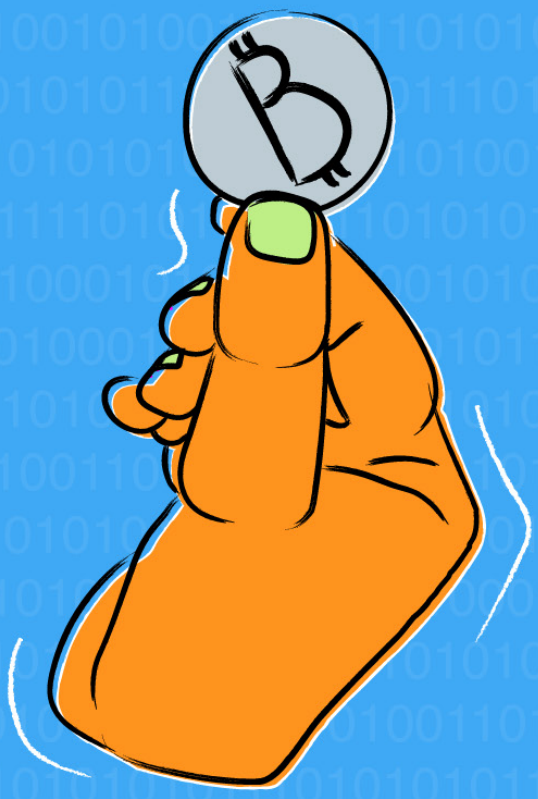

An Issue Brief on

Cryptocurrency Surveillance

RESTORE the FOURTH

Cryptocurrency[1] has grown from a niche interest in 2008 to a household topic in 2021. From the original Bitcoin, an enormous variety of cryptocurrencies have blossomed, including the NFT-backing Ethereum, the meme-based Dogecoin, and the privacy-oriented Monero and Zcash. As this new kind of asset expands, so do its use cases for people and marginalized groups concerned about protecting their privacy from prying government and corporate eyes.

How does cryptocurrency work?

Blockchain implementations, such as cryptocurrencies, tend to share two features:

1. A set of shared data:

For cryptocurrencies, this shared data is digital ledger entries that form an immutable audit trail of all unspent balances and past transactions. The shared data forms a large, append-only database, where each entry is time-stamped and cryptographically linked to all previous entries. Full network participants in a blockchain protocol, sometimes referred to as 'nodes,' keep a copy of the entire set of shared data and help broadcast new information to the rest of the network.

2. An incentive system (consensus rules):

These are designed to ensure that shared data can be updated and maintained so as to keep a record that is consistent between participants in the network. Trust is generated by decentralized additions to the unchangeable blockchain, and resolved by a network protocol. Consequently, blockchain-based technologies, similarly to gold, cash, or community currencies like BerkShares, do not need third-party intermediaries in order to be a trusted store of value. Indeed, this decentralized attribute is often what attracts privacy-minded people to store value in the form of cryptocurrency.

Cryptocurrency is held in digital wallets, which are simply locations on a computer accessible via password. Often users' wallets are hosted externally, on services like Coinbase, just as regular money is often held in bank accounts. When wallets are externally hosted, it is easier for governments to regulate them.

Whether for hosted or unhosted wallets, open source cryptography enables transacting on the blockchain while minimizing what information is revealed to the network. Innovations in this area provide an increasing tool chain for users to limit the information disclosed only to counterparties, while remaining compatible with Anti-Money Laundering (AML) and Know Your Customer (KYC) obligations, because the counterparties themselves retain the information needed for compliance.

How are cryptocurrencies regulated?

The cryptocurrency industry is actively exploring an open source alternative to the existing banking and exchange infrastructure that goes by the term Decentralized Finance or DeFi. This area has seen enormous growth over the last 2 years but operates in a regulatory gray area.

In the United States, cryptocurrency regulation has been handled at the state level, which poses problems for state legislators who are often unfamiliar with the technology they are regulating. For example, the State of New York implemented the overzealous "BitLicense Law" in 2017, only to see cryptocurrency businesses flee the state.

Louisiana (wholly) and Rhode Island (partially) have implemented the "Virtual Currencies Businesses Act," which focuses on licensing larger cryptocurrency operators. FINCEN is currently considering a set of regulations to strike "a reasonable balance between financial inclusion and consumer privacy and the importance of preventing terrorism financing, money laundering, and other illicit financial activity"; its proposed changes would require banks, exchanges, and other custodians to record and report the name and physical address of personal wallet owners who transact with their

[1] Our use of the common term "cryptocurrency" rather than the term "cryptoasset" does not indicate that we believe that trading in cryptocurrencies should be subject to the same kind of regulation as trading in "fiat" currencies.

customers in amounts exceeding, or aggregating to, $10,000. Not only, that, but they would have to identify and verify, with name and physical address, hosted wallet customers who engage in transactions of over $3,000 with unhosted wallet counterparts. The changes ban structuring, and define cryptocurrency as a "monetary instrument" for the purposes of bank reporting.

Some countries regulate cryptocurrencies and a few have outright banned citizens from using them. In China, the government has encouraged the disappearance of cash and has tried to ban cryptocurrency so that they can track every electronic transaction; dissidents have been prohibited from buying train tickets and participating in many aspects of everyday life. In Venezuela, cryptocurrency has allowed Venezuelans to shelter their assets against seizure by the government.

Why should you be worried about cryptocurrency regulations?

Unfortunately, FINCEN's international counterpart, the Financial Assets Task Force or FATF, has proposed even more expansive guidance than FINCEN's. Notably, at several points it suggests that member states should consider banning exchanges from allowing peer-to-peer transactions or transactions involving "privacy coins." Regulating this won't stop such the kind of illegal transactions they profess to be concerned about—transactions involving money laundering, terrorism or drugs; but they will stop, for example, dissidents being able to send bitcoin donations to organizations like BYSOL in Belarus or the Feminist Coalition in Nigeria. The guidance also sets up contradictory and broad definitions of "virtual asset service providers" that, for the first time, would treat many people conducting peer-to-peer financial transactions as if they are in fact financial intermediaries instead.

There may come a day when legislators are familiar enough with blockchain to be able to regulate with a light and intelligent hand. But most regulators have not experienced a state that is hostile to them or their families; have not been dissidents, exiles, undocumented immigrants or refugees. Undocumented immigrants often cannot meet the criteria for opening a bank account, and need to send remittances to their families. In 2012, Ripple and MoneyGram became one of the first remittance/blockchain partnerships (although this partnership has since ended); Western Union, similarly uses cryptocurrency transactions for a large portion of its business. Small remittance services are common, and heavy regulation would hit hardest in the US on undocumented people.

> **"But, even if we did trust our government, FINCEN rules would render cryptocurrency transactions transparent to foreign governments who make data request of the US government."**

Perhaps the re-establishment of a congressional Office of Technology Assessment would help expand Congressmembers' understanding of the topic. But as of today, any effort by Congress, FINCEN, or FATF, is likely to do more harm to this sector than good. Large firms may be able to shoulder the burden of complex licensing, regulation and reporting, but cryptocurrency businesses that do not perform any third party custodial services should be exempted from money transmission regulations as much as possible.

Beyond the economic there is a deeper privacy-oriented argument here. It's important to preserve some methods of financial transactions that are hard for the government to trace and choke off—like cash and cryptocurrency. People use peer-to-peer cryptocurrency transactions precisely to hedge against the risk of government seizures. We can already see that the US government and corporations are willing to abuse payment systems to disfavor payments to groups of which it disapproves; such as WikiLeaks, antifascists, and sex workers. In other words, payments systems are political. Dissidents and historically targeted groups reasonably want a store of value that is proof against seizure by an oppressive government, and we

cannot trust that the US government should have the power to choose which groups do and do not deserve to be able to transact in cryptocurrency.

But, even if we did trust our government, FINCEN rules would render cryptocurrency transactions transparent to foreign governments who make data requests of the US government. For example, this could mean cryptocurrency transactions could be made visible to the Turkish government if they data requested the US government in an attempt to trace the financing of Kurdish groups.

What has Restore the Fourth done on this issue?

Between 2015 and 2017, Restore The Fourth – NYC helped small cryptocurrency traders who were adversely affected by the "BitLicense" law. Nationally, in 2021 we helped to publicize Fight For The Future's "Stop Financial Surveillance" campaign.

Restore the Fourth has also been involved in efforts to amend the infrastructure bill to preserve cryptocurrency user privacy. This amendment was called the Wyden-Lummis-Toomey amendment. You can learn more and read our letter to congress here.

What can you do?

To get involved with efforts to block cryptocurrency surveillance, please email here.