

The Reality Behind the Myth of Transparent Blockchains

October 25, 2023


The cryptocurrency industry often claims that cryptocurrencies are not effective money laundering tools because the blockchains that the transactions are recorded on are public and transparent. This transparency, they argue, enables law enforcement to track the movement of funds on a blockchain to a digital wallet. However, these arguments are baseless and they ignore the reality that bad actors have tools to launder illicit funds through blockchains. The undeniable truth is that cryptocurrencies have quickly become an effective and favored tool for money laundering, terrorist financing, ransomware attacks, and sanctions evasion. The blockchain transparency claimed by crypto promoters is a myth.

While blockchains are often public ledgers that openly display recorded transactions from one digital wallet to another, it is a myth that blockchains by themselves are not an effective means of moving illicit funds. That is because: (1) blockchains include no beneficial ownership information; (2) blockchains can be corrupted by the use of mixers; and (3) centralized or decentralized entities accessing blockchains, and performing off-chain transactions, often are not required to comply with know-your-customer or anti-money laundering and bank secrecy act laws and regulations.

Blockchain Wallet Addresses Are Reflected as a Series of Numbers and Letters That Do Not Identify Beneficial Owners

While blockchains can be public ledgers that record transactions, the reality is that these “transparent” transactions only record transactions from one digital wallet to another. Digital wallets themselves are reflected on the blockchain as a random series of letters and numbers without any other identifiable information. While law enforcement may be able to track illicit funds on a blockchain, it is much more difficult to identify the beneficial owner of a digital wallet in a blockchain transaction. For example, a recent [CNBC article](#) details the story of a Georgia man who hacked and stole more than 50,000 bitcoin in 2012 from the Silk Road, a dark web marketplace used in the early days of cryptocurrency primarily to purchase and sell drugs. His cache of stolen bitcoin was valued at roughly \$3 billion when seized by law enforcement. While federal investigators could track the location of the stolen bitcoin on the blockchain for years, they were unable to determine who the beneficial owner was of the hacked bitcoin.

The article details that investigators “watched and waited for years as the hacker transferred funds from account to account, peeled some away, and pushed some of it through crypto ‘mixers’ designed to obscure the source of the money.” The hacker was only caught after making a small mistake when he had transferred \$800 to a cryptocurrency exchange that did hold beneficial ownership information of its users’ digital wallets. While the blockchain helped investigators track the stolen money, it took a decade for the identity of the hacker to become known to law



enforcement, because the wallet addresses that held the funds were not tied to any personal identifiable information.

Mixers Can Make it Difficult to Track Funds Flowing Through Blockchains

Virtual currency mixers enable bad actors to functionally obfuscate the source, destination, or amount involved in a crypto transaction. A [U.S. Department of the Treasury report](#) explains that mixers can work in a variety of ways, including (1) pooling crypto assets from multiple different digital wallet addresses into one transaction; (2) splitting the same assets into several smaller, independent transactions, or (3) using code to alter the structure of the transaction. All of these methods—and there are many more—make it difficult to track funds on otherwise public blockchains.

Last year, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) sanctioned [Blender.io](#) and [Tornado Cash](#), two virtual currency mixers. These sanction orders detail how these entities enabled North Korea’s Lazarus Group, a state-sponsored cyber hacking group, to launder millions of stolen cryptocurrency to help [fund its nuclear program](#). The U.S. Department of the Treasury sanction order against of Tornado Cash alleges that the virtual currency mixer has been used to launder more than \$7 billion worth of cryptocurrencies since its creation in 2019.

Importantly, the U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) [recently proposed a rule](#) to identify convertible virtual currency mixing as a class of transactions that are a primary money laundering concern. In the release, FinCEN notes an increase in the use of virtual currency mixers by terrorist groups, such as Hamas and the Islamic State of Iraq and Syria (ISIS). It also cites the use of mixers by “criminals and state actors to facilitate a range of illicit activity, including, but not limited to, money laundering, sanctions evasion and WMD proliferation by the Democratic People’s Republic of Korea (DPRK or North Korea), Russian-associated ransomware attacks, and illicit darknet markets.”

Lackluster KYC and BSA/AML Compliance Is Common in Crypto and It Thwarts Law Enforcement

Illicit funds, like water, flow down the path of least resistance. The global trading nature of cryptocurrencies makes it difficult to regulate because the regulatory regimes with the weakest know-your-customer and bank secrecy/anti-money laundering laws and regulations have become havens for cryptocurrency companies and protocols. Unless cryptocurrency exchanges and intermediaries have robust know-your-customer and BSA/AML policies and procedures, the random series of numbers and letters that appear on a blockchain are largely useless to law enforcement.

We have already seen several examples of crypto companies reportedly acknowledging that terrorist organizations, countries under sanctions, and criminals are using their platforms to launder money. For example, the largest cryptocurrency exchange in the world, Binance, has reportedly knowingly hosted bad actors on their platform with little regard for U.S. law. Here are some examples:

- A [CFTC complaint](#) against the company cited internal employee messages that suggested they knew that Hamas and certain Russian individuals were trading on their platform, acknowledging in an internal chat message: “Like come on. They are here for crime” and the other employee responding, “we see the bad, but we close 2 eyes.”
- That same CFTC complaint details internal messages where one employee flags an account for over \$5 million in transactions sourced from questionable accounts and recommending it be offloaded to which the other employee responds, “we would want to advise the user that they can make a new account...let him know to be careful with his flow of funds...he can come back with a new account But this current one has to go, its tainted.”
- In May, [Israel seized roughly 190 crypto accounts](#) maintained at Binance since 2021, “including two it said were linked to Islamic State and dozens of others it said were owned by Palestinian firms connected to the Islamist Hamas group.”
- Last week, [Israel froze several more crypto accounts](#) on the Binance platform that have been used to solicit donations for Hamas.
- An [SEC complaint](#) alleges that Binance did not require **any** KYC information for any individual seeking to withdraw up to two bitcoin per day (valued at more than \$90,000 per day at the time conduct was alleged)
- Binance was the largest counterparty to Bizlato, a crypto exchange since indicted by the Department of Justice that allegedly laundered more than \$700 million in illicit funds. Binance’s own AML vendor [estimated](#) that 48 percent of Bizlato’s receipts were “illicit or risky.”

In spite of these allegations and reports of absent or weak KYC and BSA/AML policies and procedures and in spite of the fact that Binance has been barred or severely restricted from operating in several countries around the world, they remain the largest cryptocurrency exchange in the world.

Recent actions taken by the U.S. Department of the Treasury, namely adding a Gaza-based crypto exchange to the sanctions list and a recent proposal by FinCEN to crack down on cryptocurrency mixing should help to crack down on the use of cryptocurrency for money laundering. However, until the U.S. Department of Justice starts to bring criminal cases against crypto executives and companies, civil fines will just remain the cost of enabling money laundering, terrorist financing, and sanctions evasion.

Conclusion

Cryptocurrencies have inflicted huge losses on investors without demonstrating any credible use case. The notion that the blockchain technology underlying cryptocurrencies represents a transparent medium that can assist law enforcement and thwart criminals is, like so many claims surrounding crypto, a false claim, offered as part of the desperate attempt to legitimize this dangerous craze in finance.



Better Banks | Better Businesses
Better Jobs | Better Economic Growth
Better Lives | Better Communities

Better Markets is a public interest 501(c)(3) non-profit based in Washington, D.C. that advocates for greater transparency, accountability, and oversight in the domestic and global capital and commodity markets, to protect the American Dream of homes, jobs, savings, education, a secure retirement, and a rising standard of living.

Better Markets fights for the economic security, opportunity, and prosperity of the American people by working to enact financial reform to prevent another financial crash and the diversion of trillions of taxpayer dollars to bailing out the financial system.

By being a counterweight to Wall Street’s biggest financial firms through the policymaking and rulemaking process, Better Markets is supporting pragmatic rules and a strong banking and financial system that enables stability, growth, and broad-based prosperity. Better Markets also fights to refocus finance on the real economy, empower the buy-side, and protect investors and consumers.

For press inquiries, please contact us at press@bettermarkets.org or (202) 618-6430.



SUBSCRIBE to our Monthly Newsletter

FOLLOW US ON SOCIAL



2000 Pennsylvania Avenue, NW | Suite 4008 | Washington, DC 20006 | (202) 618-6464 | www.BetterMarkets.org

© 2023 Better Markets, Inc. All rights reserved.