Crypto Laundering: Bitcoin + Money Laundering

Article By:
Dr. Nick Oberheiden

Bitcoin was a massive innovation to the world that allows transactions to be processed faster, makes them easier to use, lack third parties and intermediaries, and have stronger security. The technology underlying Bitcoin is the blockchain, which is the decentralized ledger where all Bitcoin transactions are stored.

At the same time, criminals are increasingly seeking to exploit the latest technology to their financial benefit. Bitcoin transactions actually have the ability to make money laundering easier for criminals because cryptocurrencies are conducted, transferred, and stored online and allow cybercriminals to move their funds instantly across borders.

This article explains the interconnection between Bitcoin and money laundering, warning signs, and how a lawyer can help you with your crypto issue.

Bitcoin as an Attractive Option for Laundering

One of the first questions many ask is why is Bitcoin such an attractive option for criminals seeking to launder money?

The most important answer is that laundering cryptocurrencies via online exchanges and then converting them to cash is much simpler than laundering bags of cash often across borders. Online transactions have no borders, and it obviates the need to physically move illegal money from place to place. Therefore, it is easy and practical.

Second, there is a certain degree of anonymity associated with Bitcoin transactions. While not 100% anonymous, these transactions are in fact pseudonymous. This means that the public Bitcoin addresses used for transactions are not registered in the names of individuals.

The transactions are stored publicly on the blockchain (the public decentralized ledger where all transactions are stored), but only the individual making the transaction has access to the account and Bitcoin wallet. Therefore, federal agencies will have a challenging time linking a particular Bitcoin transaction back to any one individual or entity. However, detection is not impossible.

To overcome this obstacle, criminals will use Bitcoin mixing services, which allow the individual to
"mix" their Bitcoins with other users and jumble the connections between individuals’ addresses.

The goal is to make it practically impossible for anyone to detect the origin and destination addresses of those illegal Bitcoin transactions. This allows criminals to cash out without fear of ever being identified. In addition, many wallet providers and online crypto exchanges have few if not no anti-money laundering (“AML”) or Know Your Customer (“KYC”) regulations, which represents a very attractive option for cybercriminals.

Third, the lack of regulation or inconsistent regulation of the crypto sphere makes detection of large Bitcoin transactions more unlikely—both the initial Bitcoin transaction and when the criminals seek to “cash-out” and convert their Bitcoins to cash.

Traditional financial and banking options are very regulated both at the state and federal levels. On the other hand, cryptocurrencies are loosely regulated. This makes the use of cryptocurrencies attractive to criminals who believe they can evade regulation and scrutiny of various law enforcement agencies within the nation and abroad.

**Warning Signs of Crypto Laundering**

Crypto laundering is a crime. Despite the lack of federal guidance on this issue, many law enforcement agencies are relying on existing laws and traditional investigative tools to uncover instances of crypto laundering. Below are some warning signs of crypto laundering:

- Transfer of crypto funds to wallets in unregulated or less regulated jurisdictions;
- Multiple high-value transactions occurring within a short period of time;
- Bitcoin or other transactions totaling amounts that are just under the amount that would trigger reporting requirements;
- Immediately withdrawing cryptocurrency deposits;
- New accounts funded with an amount that is immediately withdrawn;
- Transactions with multiple cryptocurrencies on many accounts;
- Deposits from unregulated jurisdictions or jurisdictions with poor AML and KYC regulations; and
- One wallet that is linked to multiple credit card accounts under different individuals’ names or one wallet linked to multiple bank accounts.

The above warning signs should be considered by individuals seeking to do business with a firm dealing with cryptocurrencies, by law enforcement agencies investigating certain individuals and entities, and during AML reviews within crypto service providers.

In addition, in 2020, the Financial Action Task Force (“FATF”) released a report about red flag indicators for money laundering that is intended to assist crypto wallet and exchange companies as well as financial authorities.
How An Attorney Can Help Defend You Against Crypto Laundering Allegations

Federal agencies including the Department of Justice (“DOJ”) and the Securities and Exchange Commission (“SEC”) have been especially eager to investigate alleged instances of crypto laundering fraud. On June 29, 2021, in a DOJ investigation, “Doctor Bitcoin” pleaded guilty to operating an illegal cash-to-cryptocurrency conversion business. This underscores the importance of retaining counsel experienced in defending against allegations of crypto laundering. Below are some examples of how an attorney can help you with your crypto issue:

- Conducting fraud investigations involving cryptocurrencies;
- Advising on Security Token Offerings (“STOs”) and Initial Coin Offerings (“ICOs”);
- Valuing of cryptocurrencies and assets;
- Assisting with purchasing property or other assets with cryptos;
- Advising on AML and KYC regulations;
- Checking on internal and external compliance;
- Advising on wills, trusts, and inheritances of crypto assets and cryptocurrencies;
- Drafting compliance documents or documents regarding coin issuances;
- Advising on due diligence of customers;
- Advising on identification and verification procedures involving crypto transactions; and
- Advising on monitoring crypto transactions for compliance with applicable regulations, for suspicious activity, and for certain money laundering warning signs.

“The use of cryptocurrencies such as Bitcoin to facilitate online transactions has both advantages and disadvantages. While crypto transactions offer speed, ease in use, and low transaction costs, they can also facilitate elaborate money laundering schemes, illegal purchases, and ransomware attacks. Specifically, Bitcoin laundering is becoming a cost-effective and highly appealing option for cyber criminals aiming to convert illegally obtained cryptocurrencies into legitimate cash. While there are few laws regulating cryptocurrencies, many federal agencies will go after companies and individuals alleged to have engaged in fraudulent crypto transactions under already-existing statutes. Therefore, the consequences can be just as severe—fines and penalties, disgorgement orders, injunctions, and possibly jail time.” — Dr. Nick Oberheiden, Founding Attorney of Oberheiden P.C.

Conclusion

Crypto laundering is becoming a serious problem for law enforcement agencies as cybercriminals continue to exploit new and emerging technologies for financial gain. Criminals are attracted to the cryptocurrency, Bitcoin, because it is easy and practical to move digitized money, because these transactions are very difficult to trace, and because there is a lack of consistent regulation regarding cryptocurrencies.
Identifying red flags are important safeguards for individuals, businesses, and law enforcement agencies to consider. In fact, law enforcement agencies have been especially zealous in investigating alleged instances of crypto laundering based on certain red flags.

Source URL: https://www.natlawreview.com/article/crypto-laundering-bitcoin-money-laundering