Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Twitter Hack Highlights Crypto Mixers' AML Issues

By **Julian Chan, Ilan Guedj and Zhong Zhang** (September 8, 2020, 4:21 PM EDT)

Julian Chan

Ilan Guedj

Zhong Zhang

On July 15, more than 100 high-profile Twitter accounts — including those of Bill Gates, Elon Musk, Barrack Obama, Jeff Bezos and Apple Inc. — were hacked to promote a scam. The scam asked individuals to send bitcoin to a specific address, with the promise that any bitcoin sent would be doubled.[1] More than $110,000 worth of bitcoin was transferred to the address before Twitter removed the scam posts.

Bitcoin and other cryptocurrencies have recently been targeted for financial scams like this one in part because of the perceived anonymity associated with the transactions. However, bitcoin transactions are not completely anonymous.

Real-life identities can be triangulated from blockchain transfer patterns along with other off-chain information like crypto exchange accounts, as happened in this case.[2] Indeed, by analyzing blockchain data alone we can discern the hackers' getaway route from the address that appeared in the scam tweets, all the way to the mixing transaction they used to try to hide their trail.

This route is shown in Figure 1. We can only track the bitcoin transactions up to the transaction right before the mixer, shown in the yellow box.

Figure 1. Twitter hacker's bitcoin "getaway" route[3]

Mixing is an effective method of making cryptocurrency payment tracing and owner identification much more difficult, if not impossible. It is such a significant challenge to law enforcement that, in February, the creator of the bitcoin mixer Helix, Larry Harmon, was arrested on money laundering charges.

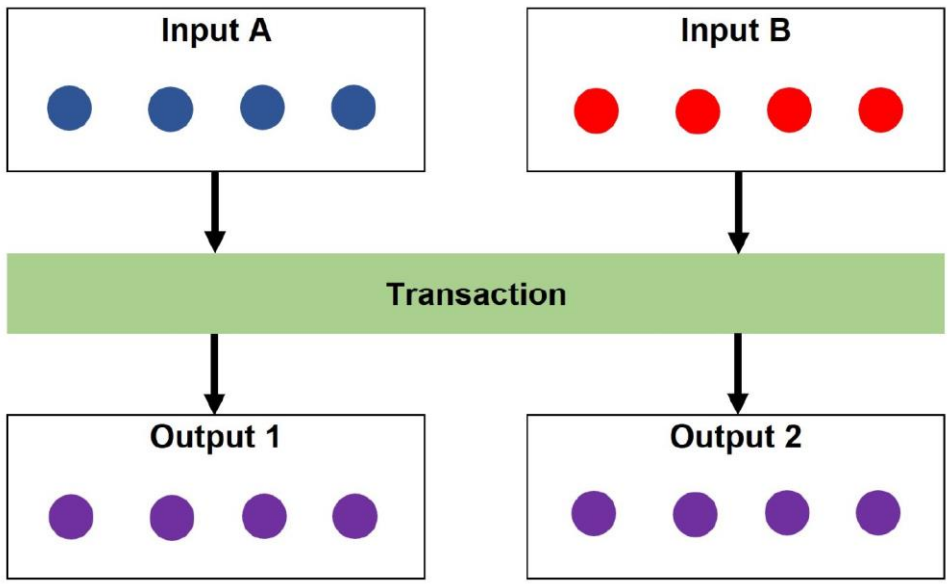
The U.S. Department of Justice stated that "seeking to obscure virtual currency transactions in this way is a crime, and that the Department can and will ensure that such crime doesn't pay."[4]

In this article we provide a primer on mixing for bitcoin and its implication on financial privacy and regulation.

Bitcoin Mixing: Technical Background

When users transfer bitcoin from one address to another, bitcoin units are packaged into structures called "input/output." In Figure 2, for example, Input A and B each contain four bitcoin units, which are transferred to Output 1 and 2 through a simple 2-to-2 transaction.

Figure 2. A simple bitcoin transaction



Due to bitcoin's privacy-focused design, bitcoin units stored in the outputs of the same transactions are indistinguishable. Hence, we cannot trace the origin of each unit in the output when there is more than one input.

For example, after the transaction in Figure 2, for each of the eight units in Outputs 1 and 2, it is impossible to know whether they came from Input A or Input B. If red units from Input B are flagged as illegitimate funds, mixing them with legitimate blue units from Input A will produce purple units that are 50% legitimate and 50% illegitimate.

Mixing illegitimate units with more legitimate ones will further reduce the illegitimate percentage in the mixed units. For example, if Input A in Figure 2 has eight instead of four units, then each of the purple units in Output 1 and 2 will be one-third illegitimate.

Specialized Mixer

Specialized bitcoin mixing services can be categorized into two groups — centralized or decentralized — based on whether users have to entrust their bitcoin to the service provider during the mixing process.

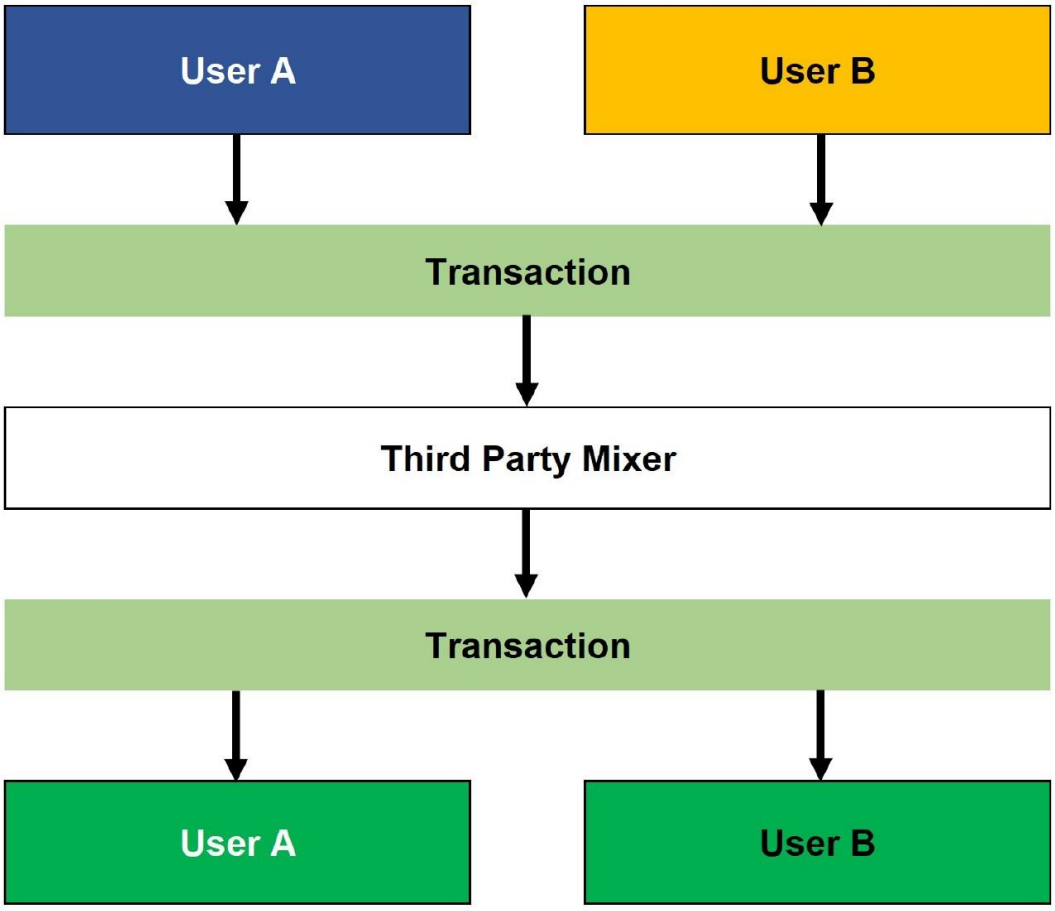
Centralized Mixer

A centralized bitcoin mixer operates like a transaction organizer. The mixer provides a deposit address for users to send bitcoin. It also asks users for a withdrawal address to return their bitcoin. Once all bitcoin deposits are received, the mixer initiates a blockchain transaction that uses all deposits as inputs and sets output addresses to each user's withdraw address.

Instead of having only two inputs and two outputs, as shown in Figure 2, an actual mixing transaction can have hundreds of inputs and outputs. If one of the inputs is comprised of illegitimate funds, then, after mixing, all the outputs will contain a small percentage of illegitimate funds.

Centralized bitcoin mixers usually charge a fee on top of bitcoin transaction costs for the mixing service. When following an optimized procedure to mix bitcoin with a large number of inputs and outputs, it is nearly impossible to trace mixed bitcoins back to their premixing owner. Figure 3 illustrates a simple centralized mixer example.

Figure 3. Centralized mixer model



Although the model of centralized mixing is straightforward and easy to implement, it has several significant disadvantages. First, users have to completely trust the mixer as custodian of their bitcoins during the mixing stage, as there is no guarantee the mixer will not simply keep the bitcoins.

Second, the mixer may collect users' digital footprints, such as IP addresses, that could later be obtained by other parties, such as law enforcement, for identifying mixing participants and thus defeat the purpose of mixing.

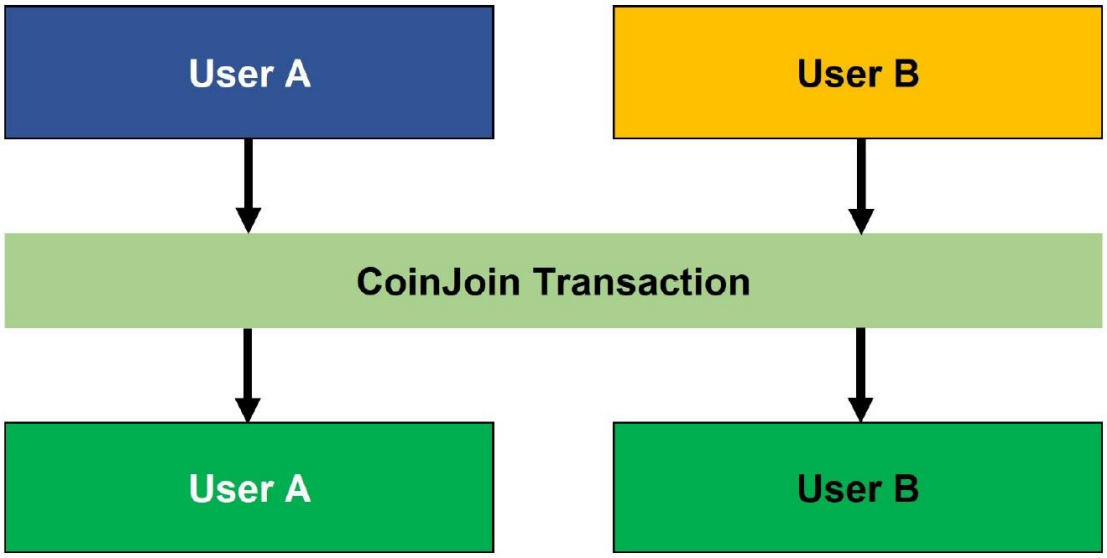
Last but not least, centralized mixers have security risks, as they usually operate their own websites, which can be attacked by a third party or shut down by authorities.

Decentralized Mixer

To overcome the drawbacks of the centralized mixing model, the bitcoin community developed CoinJoin as a decentralized mixing protocol.[5] Instead of relying on a trusted third-party mixer, CoinJoin allows users to connect with each other and initiate the mixing transaction in a trustless and decentralized manner without any intermediary, as shown in Figure 4.[6]

This method is noncustodial — users cryptographically control their bitcoins during the entire mixing process. Deploying CoinJoin does not require any dedicated website or server, as everything is processed as regular transactions on bitcoin's peer-to-peer network. This makes CoinJoin resilient against attacks and authority shutdown.

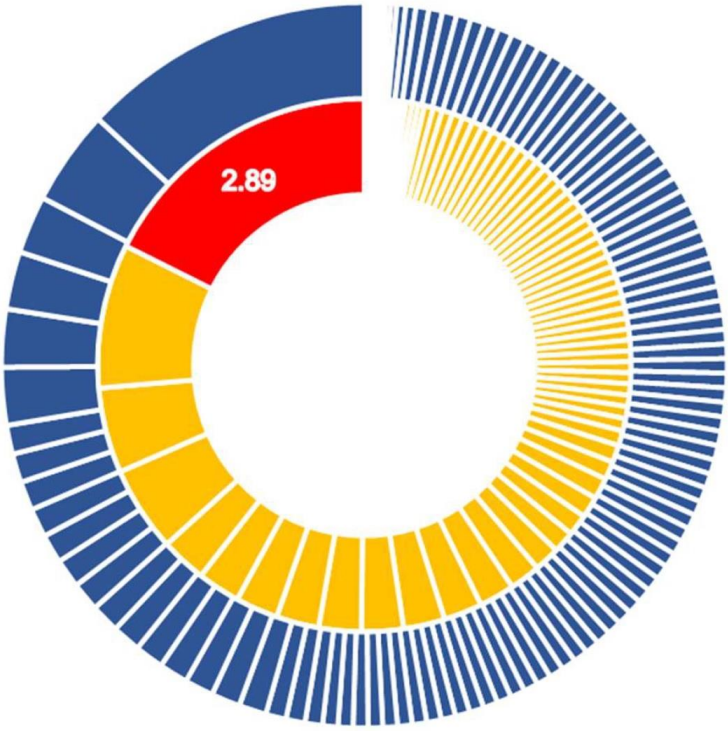
Figure 4. Decentralized mixer model



Currently the easiest way to use CoinJoin is through cryptocurrency wallet software, such as Wasabi Wallet[7] or Samourai Wallet,[8] which have built-in decentralized mixing options.

The Twitter hacker in July apparently used a CoinJoin mixer on 2.89 illegally acquired bitcoin. Figure 5 illustrates the structure of this specific mixing transaction.[9] The inside doughnut represents 86 inputs of various sizes, including the red-colored illegitimate fund from the Twitter hacker. The outside doughnut represents 131 outputs after the mixing transaction, which hides the illegitimate fund among all the outputs.

Figure 5. Decentralized CoinJoin mixer used by Twitter hacker



The CoinJoin protocol is so effective that the European Union Agency for Law Enforcement Cooperation produced a comprehensive internal report about the Wasabi Wallet in April.[10]

Mixing Through Cryptocurrency Exchanges

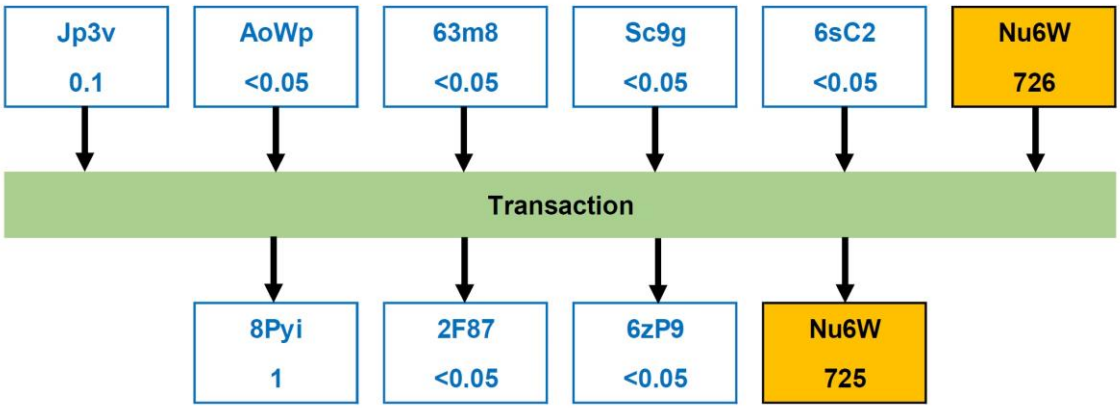
In addition to specialized mixers, cryptocurrency exchanges may serve as unintended bitcoin mixers, although they are far from perfect.

Users can send bitcoin to a crypto exchange's deposit address, wait for the exchange's confirmation of receipt of the funds, and then withdraw bitcoin from the exchange back to the users' own addresses. In most cases, users will receive bitcoin transferred from the exchange's inventory — that is, not the same bitcoin they deposited earlier.

Figure 6 provides an example of a cryptocurrency exchange mixing customers' bitcoin deposit with its inventory. Five small customer deposits, shown in blue, are mixed with exchange inventory, Nu6W, as inputs for this transaction.

The four outputs include three small payments to customer withdrawal addresses, in blue, and one large change payment back to the exchange inventory. Without account-level data about each customer's deposit and withdrawal record, we cannot determine the origin of the three small outputs.

Figure 6. Example of mixing through crypto exchange



In the rare case where users' original deposits are used as input for the withdrawal transaction, most exchanges will unintentionally mix many users' funds due to payment batching, which was designed to save blockchain space and reduce transaction cost.[11]

Mixing bitcoin through a crypto exchange is not a guaranteed method to hide one's identity, as most trustworthy exchanges keep a complete record of deposits and withdrawals, along with other customer information. Therefore, it is possible to trace the bitcoin fund flow through these exchanges. Shaky exchanges that either are subject to insufficient regulatory oversight, or that seek to evade such oversight, may not obtain or retain much customer information, but when users rely on less reputable exchanges, they may risk losing their deposited funds altogether

Implications of Bitcoin Mixing

Decentralized cryptocurrencies and mixing are double-edged swords, like many innovative technologies. Many users see these technologies as providing powerful tools for protecting financial privacy and individual liberty on a global scale against financial surveillance and government control, including by authoritarian regimes. However, these technologies also introduce significant challenges to law enforcement.

On Financial Privacy and Individual Liberty

Protection of customers' financial privacy at traditional financial institutions was established by the 1978 Right to Financial Privacy Act. However, bitcoin and other decentralized cryptocurrencies are, by design, global digital payment networks that operate independent of the fiat banking system.

Bitcoin's development is rooted in a movement that advocates the use of strong cryptography to guard privacy and individual liberty. Libertarianism also has had a profound influence in the broader crypto community.

As a result, bitcoin was designed around three critical properties: being fungible, permissionless and censorship-free. These properties attracted many users around the world who sought a way out from financial surveillance and restrictions imposed by authoritarian regimes.

HKmap.live, a geolocation data provider supporting Hong Kong protests, started accepting donations in bitcoin and other cryptocurrencies in late 2019 to protect its anonymous developers from being exposed by their fiat banking transactions.[12] The independent newspaper, Hong Kong Free Press, accepts bitcoin donations.[13] In Russia, activists have embraced bitcoin and other cryptocurrencies to

avoid the fiat banking system that is closely monitored by the government.[14]

Bitcoin mixing makes it exceedingly difficult to trace the flow of funds and to blacklist specific bitcoin addresses, thus improving bitcoin's function as a global platform for financial privacy and liberty.

On Anti-Money Laundering

The Bank Secrecy Act requires financial institutions in the U.S. to assist government agencies in detecting and preventing money laundering.[15] However, a bitcoin transfer from one address to another, without conversion into a fiat currency, remains completely on the peer-to-peer blockchain network and out of the traditional banking system.

Nevertheless, in a recent ruling regarding the mixer Helix, referring to the Money Transmitters Act, U.S. District Judge Beryl Howell concluded that "[t]he term 'money' ... commonly means a medium of exchange, method of payment, or store of value. Bitcoin is these things," and "Bitcoin is money under the MTA."[16]

Currently, cryptocurrency anti-money-laundering, or AML, actions can be taken both at the blockchain level and at the regulated on- and off-ramp for fiat/crypto conversion.

In March, the U.S. Department of the Treasury blacklisted 20 bitcoin addresses linked to the Lazarus Group, a cyber crime group possibly affiliated with the North Korean government.[17] Bitcoin mixing effectively removes useful information for blockchain forensic analysis. But traceability will reappear when mixed bitcoin are collected for conversion into fiat currency.

AML rules can also be imposed at regulated on- and off-ramps for bitcoin, such as crypto exchanges that have fiat banking relationships. Know-your-customer practices such as establishing customer identities by crypto exchanges can connect users' cryptocurrency activities with fiat banking information, thus providing a valuable lead for backing out a more complete picture of crypto ownership and transfer.

Conclusion

The recent Twitter hack revealed that, although bitcoin and other cryptocurrencies can provide more transactional privacy than fiat currencies, they are not completely anonymous. Mixers allow users to try to hide their transactions from being identified in the blockchain, but real-life identities can still be triangulated from blockchain transfer patterns along with other off-chain information, like crypto exchange account information, as happened in the July Twitter hack.

Given that mixers can be used to facilitate money laundering, we expect regulators to pay increased attention to their use in financial transactions.

Julian Chan, Ph.D, is a lead data scientist, Ilan Guedj, Ph.D, is a prinicipal, and Zhong Zhang, Ph.D, is a senior economist at Bates White.

[1] The address in Bech32 format is bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh. For blockchain transfer records,
see https://www.blockchain.com/btc/address/bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh.

[2] On July 31, federal authorities arrested three individuals connected to the hack.
See https://www.wsj.com/articles/federal-authorities-arrest-suspect-in-twitter-hack-11596223550.

[3] Figure 1 only shows one of the bitcoin blockchain "getaway" routes.

[4] See: ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million" target="_blank">https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million.

[5] See https://en.bitcoin.it/wiki/CoinJoin.

[6] A cryptocurrency electronic payment system, such as Bitcoin, is based on cryptographic proof instead of trust in a third-party intermediary. This "trustless" system allows any two willing parties to transact directly with each other without the need for a trusted third party.

[7] See https://docs.wasabiwallet.io/using-wasabi/CoinJoin.html#doing-coinjoin-step-by-step.

[8] See: https://samouraiwallet.com/whirlpool.

[9] For blockchain record,
see https://www.blockchain.com/btc/tx/da2de4a38eec8175e494b62efa6e17e1cef2dc23d51462081692e823159f9aca.

[10] See: https://www.tbstat.com/wp/uploads/2020/06/Europol-Wasabi-Wallet-Report.pdf.

[11] See https://en.bitcoin.it/wiki/Techniques_to_reduce_transaction_fees#Payment_batching.

[12] See https://eng.ambcrypto.com/hk-protests-geolocation-data-provider-accepts-btc-xrp-among-others/.

[13] See https://support.hongkongfp.com/.

[14] See https://www.coindesk.com/russian-activists-use-crypto-kremlin-doesnt-like-it.

[15] See https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.

[16] See https://www.law360.com/articles/1295311.

[17] See https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20200302.aspx.