How Crypto Cos. Can Help Curb Pandemic Relief Fraud

By **Brian Miller and Chris Cooke** (September 22, 2021)

Brian Miller

Chris Cooke

Breakthrough technology can power progress just as easily as it can buoy bad actors. Cryptocurrency is no exception.

As the October 2020 report from the attorney general's Cyber-Digital Task Force put it, "distributed ledger technology, upon which all cryptocurrencies build, raises breathtaking possibilities for human flourishing."[1]

These possibilities should be celebrated. The difficulty from a law enforcement perspective, however, is anonymity.

In short, cryptocurrency offers a variety of tools for shielding the identity of its users. This can prevent law enforcement from determining who holds stolen funds.

That problem is exacerbated, in part, by entities within the current crypto ecosystem that have yet to establish Bank Secrecy Act protocols, or that may not yet be required to do so.

This potentially impedes oversight of pandemic relief funds and raises serious questions about whether taxpayer dollars are making their way to bad actors overseas.

We therefore write to highlight that the conversion of pandemic relief funds to cryptocurrency raises a red flag, and to encourage partnership between law enforcement and crypto-involved companies.

The Basics

Somewhat paradoxically, cryptocurrency can be both more transparent and yet more anonymous than fiat currency. This turns the traditional law enforcement fact pattern on its head.

For example, if an individual deposits a large sum of cash into a bank account, it is easy to identify who gave and received the money — but it can be difficult to trace where the funds have traveled.

With cryptocurrency, however, it is easy to trace transactions on the blockchain, but it is more difficult to determine who the parties are behind those transactions.

Why is that?

Individuals and entities generally store their cryptocurrency in crypto wallets, which are digital files that store crypto addresses.

Each crypto address contains a specific balance of a cryptocurrency, and typically consists of both a private key and a public key.

The public key allows anyone on the relevant network to view and verify a transaction involving that address, but it doesn't reveal the address holder's identity. And usually, only the address holder knows the private key.

Moreover, the private key is necessary to access the funds stored at the address, meaning anyone not in possession of the private key is unable to freeze the funds at the address.

One particularly common way to move cryptocurrency is through a crypto exchange.

Most exchanges allow users to exchange value between various fiat and cryptocurrencies. That is, a user could deposit U.S. dollars from their bank account, exchange it for bitcoin, trade that for ether and so forth.

The user could then store the cryptocurrency on the exchange, transfer it to their wallet, or cash out and transfer their money back into the traditional banking system.

Another crypto player worth highlighting here are so-called mixers, or tumblers. These entities receive orders from multiple users, mix the users' units of cryptocurrency and then make payments out to various addresses.

By commingling the cryptocurrency of multiple customers before sending payments to designated addresses, mixers make it difficult for anyone to trace a specific payment back to the true sender of the payment.

A number of issues within this basic process flow can create hurdles for law enforcement.

Crypto Challenges and Pandemic Relief

In June, the Financial Crimes Enforcement Network hired Michele Korver as its first chief digital currency adviser.[2]

As Korver put it, the law enforcement challenges posed by cryptocurrency, at bottom, don't reflect a new kind of crime.[3] Instead, they represent the availability of new tools to financial criminals. And the primary issue law enforcement seems to be having is the ease with which criminals can move and store their ill-gotten gains anonymously.

We have already seen the anonymity issue rear its head in the pandemic relief fraud context.

For example, one common fraud scheme deployed during the pandemic has been the so-called romance scam.[4] In the pandemic relief context, a romance scam often involves a scammer convincing a duped romantic partner via the internet to apply for pandemic relief funds, such as a Paycheck Protection Program loan.

The funds are then usually moved several times through money mules. Ultimately, a money mule or an associate converts the funds to cryptocurrency. At that point, the funds are moved — perhaps first through a series of mixers — to a final address held by unknown individuals.

According to the Federal Trade Commission, a record $304 million in losses to romance scams were reported last year, representing about a 50% increase over 2019.[5]

If law enforcement is unable to identify the ultimate beneficiaries behind these kinds of

schemes, those tasked with deterring and redressing pandemic fraud are unable to do their job.

And the inability to identify the recipients of pandemic relief funds raises even more chilling concerns.

For example, cryptocurrency could facilitate the transfer of stolen pandemic funds to criminal and terrorist groups overseas. Some investigations already involve the suspected movement of stolen pandemic funds in crypto form to individuals believed to be overseas.

As outlined above, law enforcement may struggle to identify who has received such funds. What if these taxpayer dollars are being funneled to terrorist organizations or other entities with interests adverse to the U.S.?

What's more, investigating agents are often unable to freeze the cryptocurrency held at a given address — even though they may be able to track the funds directly to criminal wrongdoing.

The ability of law enforcement to figuratively stare stolen funds in the face while lacking the power to seize them is a fact of the current crypto reality.

There are other potential pandemic relief implications, too.

If pandemic relief money is converted to cryptocurrency, gauging a recipient's compliance with the conditions of that money is complicated.

Recipients of Main Street Lending Program loans, for example, are prohibited from paying dividends or increasing executive compensation, among other things. And recipients of Payroll Support Program funds may only use those funds for certain purposes.

But if a recipient converts relief funds to cryptocurrency and then makes payments from the funds in crypto form, it may be difficult to determine who received the funds. Perhaps the business sent a portion of the funds to an executive's crypto wallet, flouting the rules on increased executive compensation. Or maybe the money was used to purchase a private jet, skirting restrictions on the use of Payroll Support Program funds.

The problem is we may not know. And if law enforcement can't determine who is receiving relief funds, we can't know how they have been used, or for whose benefit.

For all these reasons, the conversion of pandemic relief funds into cryptocurrency raises a red flag.

The Bank Secrecy Act

According to the U.S. Department of Justice, mixers and tumblers "are engaged in money transmission," and therefore subject to the requirements of the BSA.[6]

The DOJ warns:

> In addition to facing BSA liability for failing to register, conduct anti-money laundering (AML) procedures, or collect customer identification, operators of these services can be criminally liable for money laundering because these mixers and

> tumblers are designed specifically to "conceal or disguise the nature, the location, the source, the ownership, or the control" of a financial transaction.

The DOJ also expects crypto exchanges, including foreign exchanges doing business in the U.S., "to follow FinCEN record keeping and reporting requirements."

But as then-FinCEN Director Kenneth Blanco noted in 2020, some foreign businesses "continue to try to do business with U.S. persons without complying with [FinCEN's] rules."[7]

This issue is not limited to foreign entities. As a result, and consistent with their warnings, the DOJ and FinCEN are taking action.

Last month, Larry Dean Harmon, the operator of a mixer named Helix, pled guilty to a money laundering conspiracy.[8]

Also last month, FinCEN announced a $100 million civil penalty against BitMEX in connection with a global settlement involving the U.S. Commodity Futures Trading Commission.[9] According to FinCEN's press release, BitMEX is "one of the oldest and largest convertible virtual currency derivatives exchanges."

In its announcement, FinCEN noted the penalty resulted from BitMEX's failure to comply with applicable BSA requirements.

These recent actions show that the DOJ, FinCEN and other agencies are committed to ensuring entities operating within the crypto ecosystem comply with the BSA, and any entity currently failing to do so should take note.

Conclusion

Ongoing enforcement efforts related to the BSA will doubtless aid law enforcement and the oversight community in identifying and deterring fraud.

In the meantime, the conversion of pandemic relief funds to cryptocurrency raises a red flag due to the known challenges the technology raises to the ability of law enforcement and oversight entities to determine who is receiving U.S. taxpayer dollars.

It is our hope, however, that companies in the crypto space will step forward and partner with law enforcement to deter and detect the use of cryptocurrency and other blockchain technologies for financial crime.

For decades, financial institutions have played a similar partnership role. Crypto-involved companies now have an opportunity to do the same.

Some companies are already leading on this front. Some, for example, have established formal procedures for receiving and processing subpoenas and other law enforcement inquiries.

This should be standard. Companies should consider implementing know-your-customer and anti-money laundering protocols, as well.

The more entities prepare themselves to cooperate with law enforcement, the less law enforcement will be left in the dark when investigating crime and tracing pandemic relief

funds. And by proactively partnering with law enforcement, crypto-involved companies may garner trust and credibility while protecting the reputation of the crypto community.

Perhaps future legislation will prohibit the conversion of government-backed relief funds to cryptocurrency.

But we leave policy decisions to the policymakers. Our perspective is that of law enforcement.

From our perspective, entities within the crypto ecosystem would do well to posture themselves as law enforcement partners, knowing that the movement of relief funds into crypto is viewed as a red flag.

Brian D. Miller is the Special Inspector General for Pandemic Recovery.

Chris Cooke is an attorney at Norton Rose Fulbright. Previously he was special counsel to the SIGPR.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of Portfolio Media Inc. or any of its respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.justice.gov/archives/ag/page/file/1326061/download.

[2] https://www.fincen.gov/news/news-releases/fincen-welcomes-first-ever-chief-digital-currency-advisor-and-first-director.

[3] https://www.law360.com/articles/1407996/fincen-s-new-adviser-aims-to-crack-down-on-crypto-crime.

[4] https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams.

[5] https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020.

[6] https://www.justice.gov/archives/ag/page/file/1326061/download.

[7] https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-consensus-blockchain.

[8] https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

[9] https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures.