CLIFFORD
CHANCE

BUSTING BITCOIN'S ANONYMITY – THE IMPLICATIONS FOR FINANCIAL INSTITUTIONS

– THOUGHT LEADERSHIP

SEPTEMBER 2019

BUSTING BITCOIN'S ANONYMITY – THE IMPLICATIONS FOR FINANCIAL INSTITUTIONS

A deliberate design feature of Bitcoin is that it enables users to buy or sell anything without revealing their identity. Yet, paradoxically, all Bitcoin transactions are stored publicly and permanently on blockchain. Now, as seen in recent cases, enterprising US prosecutors and private plaintiffs' lawyers are using software called blockchain explorer to crack Bitcoin's anonymity. The US Treasury Financial Crimes Enforcement Network (FinCEN) also appears to suggest that financial institutions and crypto businesses should consider how explorer software could help them meet their own anti-money laundering (AML) and sanctions obligations.

How do explorers work?

Blockchain explorer software can search the public Bitcoin blockchain (or other public blockchain platforms) and identify all transactions associated with a given public key. Finding interactions between that public key and a financial institution or other entity with AML/KYC or books and records retention requirements – e.g. a regulated virtual currency exchange – that can be subpoenaed (or made the subject of a search warrant), means that personal information can be unlocked that could help identify the owners of the public key.

Explorers as a compliance tool

Industry awareness of blockchain explorer technology is growing: an article in the February 2019 edition of the U.S. Department of Justice's Journal of Federal Law and Practice, "Attribution in Cryptocurrency Cases", written by the Digital Currency Counsel in the Criminal Division's Money Laundering and Asset Recovery Section, recognizes that "third-party blockchain analysis software is used as anti-money laundering software by financial institutions worldwide." Accordingly, we expect to see increasing use for customer due diligence including for compliance with AML/KYC obligations. Existing compliance tools are unlikely to take advantage of all the data points offered by blockchain technology.

In the US at least, there appears to be a regulatory push for widespread adoption of explorer software as a compliance tool. On October 1, 2018, FinCEN released Advisory 2018-A006, which focuses on Iran's attempts to gain access to the global financial system through its use of virtual currency for evasive purposes. FinCEN suggests that financial institutions should take blockchain-specific countermeasures to counteract Iran's efforts, emphasizing that:

- Institutions should consider reviewing blockchain ledgers for activity that may originate or terminate in Iran.
- Institutions can utilize technology created to monitor open blockchains and investigate transactions to or from peer to peer (P2P) exchange platforms.

In November 2018, the Office of Foreign Assets Control (OFAC) added the Bitcoin wallet addresses of two Iranian ransomware operators to the Specially Designated Nationals (SDN) list. In August 2019, OFAC added a dozen virtual currency wallet addresses of Chinese narcotics traffickers to the SDN list. Blockchain explorer software could potentially be employed to screen the upstream chain of provenance of virtual currency involved in any given transaction for transfers involving these addresses.

Additionally, on May 9, 2019, FinCEN released Advisory 2019-A003 to assist financial institutions in identifying suspicious activity involving the use of virtual currencies for money laundering, sanctions evasion, and other illicit purposes, including "red flags" that are particularly likely indicators of illicit activity. Red flag number 4 instructs financial institutions to be alert for situations where "blockchain analytics" indicate that a wallet transferring virtual currency has a suspicious source of funds, e.g., a darknet marketplace. To date, however, FinCEN has not, however, provided background on, or explained, these references to "blockchain analytics," "reviewing blockchain ledgers" and utilizing "technology created to monitor open blockchains." We are hopeful that additional guidance for financial institutions will follow.

Explorers as a regulatory investigation tool

Other US authorities have also recognized the potential of blockchain explorer technology for cracking the anonymity otherwise afforded by many cryptocurrencies. An article titled "A Shot in the Dark: Using Asset Forfeiture Tools to Identify and Restrain Criminals' Cryptocurrency" in the October 2018 edition of the U.S. Department of Justice's Journal of Federal Law and Practice explains that:

- "There are various online tools, called blockchain or block "explorers," that are publicly available on the internet that enable one to search the data contained in the blockchain. Thus, for example, if an investigator learns of a Bitcoin address associated with a particular scheme, the investigator can search the address through a blockchain explorer in order to locate possible Bitcoin transactions involving that particular address. The block explorer search can reveal the following transactional information: the Bitcoin transaction ID and Date/Time Stamp (in Universal Coordinated Time/UTC), the amount of Bitcoin (BTC) transacted, the sender's public key or Bitcoin address, and the receiver's public key or Bitcoin address. IP address information may also be revealed but the IP addresses may not be the true locations of the Bitcoin senders and receivers, because many exchangers and wallet providers may use proxy IPs or IPs that do not constitute the true location of the computer or device used to access the Bitcoin network to carry out the transaction. That being said, if an investigator is aware of a particular IP address utilized by a subject, the investigator can use that IP address to execute a search using the block explorer online tool to identify any cryptocurrency transactions executed using that IP address. Once a suspicious cryptocurrency transaction has been identified, and if it is determined that the transaction was effected through a cryptocurrency payment processor, a subpoena can be issued to the payment processor requesting, among other things, any wallet address(es) associated with the transaction, any bank account number(s) registered to the user, and any personal information linked to the account user (for example, name, email, address, phone number, IP logs, and credit card information)."

A second article in the February 2019 edition of the same publication, titled "Attribution in Cryptocurrency Cases" (see "Explorers as a compliance tool" above), underscores the point that using blockchain explorer technology to track a transaction to an exchange or payment processor may enable the transacting party's anonymity to be cracked due to records maintained by such entities on their customers:

- "On its own, viewing cryptocurrency transactions on the blockchain shows only the transfer of some quantity of funds from one string of letters and numbers to another at a point in time. Correlating that activity to real world events – for example, the payment of funds by a victim or an undercover agent – provides additional context. The greatest value, however, may come from the ability to associate certain addresses with known entities, particularly virtual currency exchanges. The known entities may collect records regarding the user's true identity and by tracing a target's funds to the entity, law enforcement can glean valuable insight into a target's true identity."

Explorers as a litigation tool

It's not just regulators that can glean useful information and improve their position using blockchain explorer software. A recent civil case related to failed cryptocurrency purchases in the U.S. District Court of the Southern District of New York illustrates how blockchain explorers can be used to track down and freeze a party's Bitcoin ahead of a pending trial. In this case, the plaintiffs monitored all of the defendant's online activity, in the course of which they located a web forum post in which the defendant disclosed one of his Bitcoin public keys. They then hired a London-based firm that provides blockchain explorer-type services to trace the transaction history of the defendant's public key, discovering that roughly U.S.$30 million worth of bitcoins were transferred from the defendant's public key to several U.S.-based wallet and cryptocurrency exchange firms – Xapo, Coinbase, Bittrex, and Poloniex (Circle) – that conduct activities in New York. The NY court granted the plaintiffs' application for prejudgment attachment, i.e. a provisional remedy providing for security to be taken over the defendant's assets ahead of pending litigation. As a result of using the explorer software, the plaintiffs were able to obtain additional personal information about the defendant and the defendant's assets, including bank account information, from the defendant's US wallet providers and crypto exchanges, shattering the defendant's anonymity and taking control of U.S.$30 million worth of his assets pending the outcome of the litigation.

What does this mean for crypto businesses?

To the extent they aren't already, financial institutions dealing in cryptoassets should be considering incorporating blockchain explorer technology into their AML and sanctions compliance processes, as for US-based firms at least, the FinCEN Advisory 2018-A006 appears to say they "can" and "should".

Crypto exchanges and wallet providers should also expect to be on the receiving end of an increasing number of requests to freeze customer assets, or to turn over personal identifying information associated with a particular public key address, as part of court proceedings or government investigations. Exchanges and wallet providers must adopt policies and procedures that will allow them to store and retrieve such information, as the volume of such requests is only likely to increase in the future. Consideration of interaction with relevant data privacy regimes will also be crucial here.

The FinCEN Advisories indicate the likely direction of travel that US (and other jurisdictions') authorities may increasingly move toward in the future, as they attempt to trace transaction history through immutable (and not quite anonymous) public blockchains.

CONTACTS

Jesse Overall
Associate
New York
T: +1 212 878 8289
E: jesse.overall@cliffordchance.com

Steven Gatti
Partner
Washington, D.C.
T: +1 202 912 5095
E: steven.gatti@cliffordchance.com

Benjamin Peacock
Associate
New York
T: +1 212 878 8051
E: benjamin.peacock@cliffordchance.com

Jamal El-Hindi
Counsel
Washington, D.C.
T: +1 202 912 5167
E: jamal.elhindi@cliffordchance.com

Megan Gordon
Partner
Washington, D.C.
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Weisiyu Jiang
Associate
Washington, D.C.
T: +1 202 912 5303
E: weisiyu.jiang@cliffordchance.com

Diego Ballon Ossio
Senior Associate
London
T: +44 207006 3425
E: diego.ballonossio@cliffordchance.com

Ellen Lake
Senior Associate
London
T: +44 207006 8345
E: ellen.lake@cliffordchance.com

Laura Nixon
Knowledge Director - Fintech
London
T: +44 207006 8385
E: laura.nixon@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2302-004670