CARLTON FIELDS

Discovering Cryptoassets: A Journey into the Unknown

May 24, 2019

Litigators need to understand how cryptoassets function to conduct successful discovery.

As cryptoassets become increasingly commonplace, litigators will need to understand how they function to effectively identify the use and/or possession of these assets through discovery. Without a clear understanding of how these assets function, how they are controlled, and how they may be transferred, counsel may miss valuable assets in collection actions, unwittingly ignore fraudulent transfers, and/or allow parties to violate bankruptcy court turnover orders.

What Are Cryptoassets?

Cryptoassets like Bitcoin are novel ephemeral assets that have no physical form and that are not an asset derived from any other asset; although a party can externalize onto physical media the information needed to control a bitcoin, Bitcoin and similar cryptoassets are purely digital. A human cannot physically hold a bitcoin. Unlike intellectual property rights and other familiar intangible assets, a bitcoin does not represent a claim of right against an existing asset. Although bitcoins rely upon the continued existence and operation of the Bitcoin network, that network is supported and operated by a globally distributed set of computer operators; the efforts or actions of a single bitcoin owner are irrelevant to the continued viability of the network. Thus, the closest analogue to a "right" to a bitcoin would be a unilaterally assignable anonymous intended beneficiary right under a contract between unrelated parties.

This ephemeral asset features its own novel system of control and transaction. Legal "ownership," "custody," and the "location" of cryptoassets like Bitcoin are not settled concepts as a matter of law. Users of Bitcoin can assert control over bitcoins by using a private key credential that, in conjunction with software known as a wallet, permits the user to "spend" or direct the transfer of its bitcoins to another. The wallet software connects to the Bitcoin network and allows users to "spend," or transact their assets to others across the network. Those transactions are identified on the network by the personally identifiable information is associated with these transactions. Although wallets are natively software, the private key needed to control the assets associated with a wallet can be

externalized onto computer hardware or written onto physical media; the private key will be saved as or appear to be a long string of numbers and letters.

Identifying Sources of Discoverable Information and Things

Evidence of transactions of cryptoassets may be found from both public and private sources. The ledgers maintained by these cryptoasset systems, known as blockchains, record their users' transaction history on every participating machine, or "node," of the blockchain network. These ledgers are generally public, viewable, and searchable via "blockchain explorer" websites that may be used as an interface to query blockchains for details of specific transactions. Blockchain explorers may be searched by public key addresses but do not identify transactions by the names of users or by users' private keys.

To attempt to correlate transaction public keys to real-world identity requires additional discovery. Parties should consider subpoenaing banks used by the discovery target to identify transfers made to cryptocurrency exchanges. These records may identify the cryptocurrency exchanges used by the discovery target. Cryptocurrency exchanges allow users to exchange cryptoassets for fiat (i.e., government- issued currency) or to trade among various cryptocurrencies, and they are a critical source of information.

Some exchanges are located in the United States and comply with various state and federal regulations. Domestic cryptocurrency exchanges are generally regarded as money transmitters and are typically required to comply with Bank Secrecy Act obligations and to retain records that associate actual user real-world identity with the public keys used to transact through those exchanges. If the cryptoassets at issue are held on an exchange (or held by a similar custodial service provider), the exchange operator in most cases will comply with valid court orders to provide information or turn over assets. Discovery should seek records from these platforms demonstrating the discovery target's use of the exchange, trading history, and correspondence with the exchange. Some exchanges, however, may be "decentralized," located offshore, unincorporated, or otherwise fail to comply with various applicable regulations; and, thus, they may not respond to traditional discovery requests or comply with court orders.

Alternatively, discovery can be taken from individuals. This discovery would include requests for production of records that evidence purchases of cryptoassets with fiat and that would evidence cryptoasset transaction or trading activity, including production of records of the discovery target's public and private keys. The effectiveness of this discovery will rest on the good-faith discovery conduct of the producing party. Although parties may are never found, targeted discovery can circumvent stonewalling tactics. First, discovery can be taken to determine whether the discovery target has visited cryptocurrency exchange websites or downloaded cryptocurrency wallets by seeking forensic examination of computing devices, including computers, tablets, and mobile

telephones. Likewise, discovery of third parties such as email providers and mobile carriers may result in production of email correspondence related to cryptocurrency exchanges; over-the-counter trading; or participation in discussion groups, chat rooms, or cryptocurrency-focused social media groups—all of which would suggest cryptocurrency use. Discovery should also seek production or examination of external storage devices or media used to store or hold private keys for cryptoassets of the discovery target.

Tips for Effective Discovery

Discovery of public key and private key addresses used by the discovery target would appear to be a clear and obvious way to associate transfers with a real-world identity. However, private keys (and therefore the cryptoassets associated with them) function like bearer instruments (assuming that cryptoassets are not left in control of a custodian like a centralized exchange or custodial service provider): whoever has a private key at any given time generally has the same ability to control assets associated with that private key as all others who have knowledge of the private key. Thus, in case of a hack or a loss of the private key, more than one party may have knowledge of the private key and more than one party may control the assets associated with that private key at that time. Of course, a party may also functionally transfer control over cryptoassets by conveying its private key to a third party; such a transfer would be difficult to identify without documentary or testimonial evidence from the parties to the transfer as it would not be documented on a blockchain explorer or on records held by a compliant exchange.

Associating a private key with a real-life identity provides clear evidence of control over assets associated with that private key, but private key disclosure creates significant risk of theft or loss of assets if the private key is disclosed to a malicious or dishonest third party. If a party seeks to produce a private key in discovery, parties should agree to confidentiality orders with strong sanctions provisions, should agree to produce the private key to a designated fiduciary who posts a bond, or should agree to use an insured escrowee to hold the private key during the pendency of litigation. If the cryptoasset owner uses the private key to transfer assets to another wallet controlled by another private key during the pendency of the litigation, the escrowed or produced private key may still be useful to evidence prior possession and control of the cryptoassets even though it may no longer actually control those cryptoassets. Parties should consider seeking the entry of injunctions to restrict transfers at appropriate times.

Conclusion

Although cryptoassets have begun to embrace intermediaries that resemble those of the conventional financial world, like exchanges and custodians, these assets still function as bearer instruments; access and control of these assets ultimately reside with the party who holds the private key for these assets. Taking discovery calculated to correlate transactions with real-world

identity is critical to prove control of cryptoassets. Litigators who need to identify, discover, or assume control over these assets must understand how they function to craft appropriate and effective discovery.

Originally published in American Bar Association, Pretrial Practice & Discovery, Vol. 2 No. 3 (Spring 2019).

Related Practices

Blockchain and Digital Currency