Digital Dissolutions: Cryptocurrency and the Marital Estate

By Andrew N. Speer

General Definitions

Cryptocurrency is a new field that family lawyers are being exposed to more frequently with each coming day. The following article was written to assist those in the legal profession better understand the complexities inherent to this new asset.

Many find the topic of cryptocurrency daunting, but to a family law attorney or judge, the definition of cryptocurrency can be reduced to the following: two lines of text, each consisting of numbers, lower-case letters, and upper-case letters. That is it, two lines of text, one called a "public key" and the other a "private key." Some "privacy coins" use three or more lines of code, but due to their complexity, that is the topic for another article.

"Public keys" (also known as "public addresses") are known to the general public. Anyone can see the key number and its contents. A public key can receive any individual cryptocurrency unit, or any subdivision thereof, can receive a private key, and is part of the public record. Multiple transactions can be sent to any public key. Anyone, opposing parties and ex-spouses, can determine the amount of cryptocurrency held by any given public key, send more funds to it, and determine where the current funds originated from. To be of value, ownership of the public key must be admitted or proven by a party, otherwise the owner of the public key is anonymous.

"Private keys" (also known as "private addresses") are unique lines of text that determine ownership of cryptocurrency units. They can be used to transmit any cryptocurrency unit from one public key to another public key. The holder of the private key is the owner of the cryptocurrency and controls its movement. Without the private key, the public key has no value. The private key is unique, and there is only one in the universe. Transferring a private key from one person to another transfers the cryptocurrency unit. Despite being the driving force and the only item that brings value to any unit of cryptocurrency, private keys have a glaring weakness, they are only text and can be copied and pasted by anyone. To prevent losses, only the first five characters of private addresses should be provided, with all other characters redacted.

Storing Cryptocurrency

Four main ways exist to store cryptocurrency (including private keys): exchanges, hot wallets, cold wallets, and paper wallets. Exchanges are online, similar to your stock brokerage, and are linked to buying, selling, or trading cryptocurrency. There are two types of exchanges: fiat-crypto exchanges, and pure crypto exchanges. Fiat-crypto exchanges take cash, while pure crypto exchanges only trade one cryptocurrency for another. These can be accessed anywhere with an internet connection, and usually provide trade history statements. They also *can* use "exchange identification numbers" instead of public keys sometimes. Hot wallets are websites, apps, or computer programs, and are linked to specific users or devices. One of the easiest ways to steal someone's private key, is to import it into a "hot wallet" on a smartphone. Cold wallets are similar

to usb keys, often with physical buttons to unlock them. An attorney should never try to guess the code to a cold wallet, as many of them automatically wipe after a certain number of wrong entries, erasing the ability to determine the public addresses and units of cryptocurrency stored on it. If wiped, the original owner can regenerate the wallet with their "seed" key which is a list of 24 words and should always be redacted. Revealing these words is the functional equivalent of revealing a private key, as seeds can be used to clone wallets, allowing a malicious character to transfer funds out of a regenerated wallet. If a party can prove that one side has a seed key, it is almost a certainty that they have or had a cold or hot wallet.

Paper wallets are printouts or engravings of public and private keys, sometimes with a QR code and can be made of metal, or carved into wood. Anything can be a paper wallet so long as the medium is capable of having text, including the private key, transcribed onto it. Most investors keep a majority of their assets in a cold wallet or paper wallet to prevent losses due to hacking. Because of this, if a family lawyer expects that the opposing party is hiding cryptocurrency, they should request to inspect the opposing party's property and safe deposit boxes, to search for and inventory any cold wallets, paper wallets, or seed keys that may be exist or be hidden. As in all other cases private keys on paper wallets should always be redacted.

Transferring Assets

Similar to deed records, public keys reveal to the current owners who the previous owner of their units of cryptocurrency were. Each public key links to a prior public key, forming a chain, creating something akin to a central appraisal district, allowing ownership to be traced over time. Just as a new deed will have a new name and recordation number, the text of the private key permanently changes upon a full or partial transfer. If it did not, the seller could copy resell the same key multiple times. To prevent this, only the new owner knows the private key's current characters. This makes all transactions irreversibly one-way. As an additional safeguard, the blockchain network verifies that the sending public key (the seller) only sent the private key to the receiving public key (the buyer), and to no other public keys, thereby preventing double spending. Trying the sell the old public key would be rejected by the network.

When drafting divorce decrees, attorneys should include public keys similar to how they include bank account numbers. In this regard, because private keys are permanently spent upon transmission, parties and lawyers must confirm that they have entered a public key correctly before transferring assets. If a typo is made entering a public key during a transfer, there is no holding period or cancellation policy to remedy the error. Assets will be transferred to the holder of the typo public key, and nobody will be able to determine who that is. To compound the typo dilemma, the sending spouse still owes the receiving spouse the amount sent to the typo public key. To prevent this, decrees should confirm specific public keys as belonging to a party, confirm the units of cryptocurrency held as of the date of divorce, and order one party to transfer the cryptocurrency units to a specific public key of the other party. A test amount should be sent first. Once the test amount is received, the remainder can be sent. In decrees, it is recommended that a party be required to confirm receipt of test amounts prior to any large transfers.

Value

Valuing cryptocurrencies is straight forward and can be done in a method similar to looking up the cash value of a stock, as both have specific dollar valuations as of specific dates. The market value can easily be narrowed down to the date and hour (or two) of any transaction using websites such as coinmarketcap.com and coindesk.com. These allow a party to determine the market value when the transaction occurred, the date of sale, or the present-day value. Exchanges typically provide their users with trade and purchase histories, showing the amount of fiat currency used to purchase specific amounts of cryptocurrency.

Tracing

In discovery a party should request the other side produce and disclose all public keys they currently or previously have or had access, control, or possession of, or that someone else on their behalf or authority has or had access, control, or possession of, along with screenshots establishing the public key, and the current units of cryptocurrency held in that public key and in the wallet. A party should also request the other side to identify the type of key held, and its physical or digital location. This will allow a party to determine whether a wallet holds multiple public keys, multiple currencies, and if any assets have been transferred. Once the public keys are identified, the assets can be traced and monitored.

Tracing is done with blockchain explorers, typically websites, which track all cryptocurrency transfers. By entering a public key, these websites provide their users with the current units held in public keys and the date, time, amount, and source of any transactions made by that public key. For example, the explorer will show that at 11:03 a.m. on December 1, 2018, 1.001 units were transferred from public key 111 to public key 222, with 222 being held by the opposing party in this example. The explorer would also establish that the 1.001 unit transfer to public key 222 was actually part of 2.000 unit transfer from public key 111 with 1.001 units being transferred from public key 111 to public key 222, and the remaining 0.999 units being transferred from public key 111 to public key 333.

The identity of public key 333 may be unknown and could be what is known as a "change address," wherein the "change" from the transaction (0.999 units) was deposited into the change address, similar to breaking a dollar and receiving coins. If public key 333 is a change address, it is actually owned by the holder of public key 111, but the blockchain requires a new public key to be created because the private key was partially divided, one part going to public key 222 (the buyer), and the remaining going to public key 333 (in two unique private keys). The owner of Public key 111 could then send the 0.999 BTC from public key 333 back to public key 111 if they wanted, or they could keep the new public key. Some hot, cold, and exchange wallets may automatically consolidate.

If the party in focus was shifted to the holder of public key 111, the seller, an attorney would have difficulty distinguishing whether public key 333 belongs to the seller or a third party. The seller

could claim that he sold 1.001 units to the buyer at public key 222, and 0.999 units to third party at public key 333, and has zeroed out his holdings, when in reality, public key 333 was a change address of the selling spouse, meaning they still own 0.999 units. This 0.999 units could be transferred to a secret hidden public key 444, and there would be no way to prove ownership of public key 444 (it wouldn't show up in the wallet). When partial transfers are made and a change address could exist, an attorney should check bank accounts and market prices at or around the transaction time. If the selling party received 2 units worth of cash on the transfer date, it is likely that the selling spouse is not the owner of public keys 333 and 444. However, if the selling spouse only received 1.001 units worth of cash on that date, the selling spouse is likely the owner of public keys 333 and 444.

Blockchain explorers allow a user to do more than simply trace. For instance, if the explorer identified that public key 111 was an exchange ID, which are very distinct, the tracing attorney would learn that an exchange account was used, and if not previously disclosed, hidden assets are a possibility (keep in mind exchanges can conduct normal public key to public key transfers too). Explorers also allow attorneys to determine whether they should subpoena exchange records, or check bank records around the time period of transactions for withdrawals or deposits. Whenever a public key is identified, attorneys should check the bank records at the time the funds were deposited into and out of the public key.

Tracing with blockchain explorers also allows a party to determine whether a spouse has transferred funds into a "node" by tracing where funds were sent to, or if the party is "mining" by tracing where funds originated from. Mining uses a computer to verify transactions, with the miner being paid in cryptocurrency for this verification. Mining often utilizes unique payment ID's in explorers, much like an exchange ID. Finding a mining ID lets a party know there may be hidden assets being generated (like a printing press), as a miner can direct funds to any public key, even secret ones. To determine if a party is mining, check electricity bills, as very high power usage is indicative of mining.

A node is a computer that stores a specific amount of cryptocurrency, and using that stored amount, verifies transactions. For these verification services, nodes are paid in cryptocurrency, similar to dividends. Some nodes require thousands of dollars' worth of a cryptocurrency to start, creating a barrier to entry. To avoid this a party may join a "node pool" which is a service that collects and pools other people's units to the amount necessary to host a node and distributes the dividends pro-rata (the pool takes a cut). Node pools are identifiable in tracing, because they typically store all contributions at a specific public key, which holds large sums of cryptocurrency, and with very high trade volumes. While the volume in and out won't match up precisely, the units transferred in and out will be very close in total amount. For instance, a Dash node pool would show that 48,000 Dash went into a public key in 2,000 transactions, and 47,900 Dash went out in 1,000 transactions. Normal crypto investors do not make 2,000 trades from the same public key. The Dash explorer may also show that except for a few outliers, the sending and receiving public keys are the same. The problem this creates is that the dividends may not be included in that node pool public key, but may come from a third unknown public key, held in escrow until opposing party orders their release. The devious spouse could withdraw the initial contribution and wait to withdraw the dividends until after the divorce is finalized, collecting dividends on those hidden dividends all the while.

Another cryptocurrency, Tron, produces results similar to Dash with its dividends, but in its own way. Instead of nodes and node pools, users cast votes with units, and receive funds for voting. In reality the voting is pledging cryptocurrency units to be used to verify transactions, but for all functional purposes, dividends are being paid, because once a vote is cast, it is automatically recast, and payments consistently repeat. In some instances, these dividends are paid in a different coin or token. This would be extremely difficult for an attorney to find without screenshots showing "voting" assets. These third-party coins could be withheld and redeemed at an unknown secret public key, and the party could once again wait until long after the divorce is finalized before cashing out.

Cryptocurrency presents many unique obstacles to the family law professional. The insights and practice tips contained herein aim to help lawyers avoid committing malpractice, and provide a better understanding of what cryptocurrency is, and how to locate, value, and transfer it. Do not substitute the advice in this article for your own professional judgment, each case and cryptocurrency are different, and will require very unique and specific approaches.

Andrew N. Speer is a family law attorney at O'Neil Wysocki, P.C. He can be reached at andrew@owlawyers.com