Cryptocurrency Basics for Litigators

BY RONALD KOCH

Crypto assets and the crypto-asset ecosystem have introduced novel legal challenges, many of which have reached the US judicial system.[1] Cryptocurrency is an unregulated system with potential to fund illegal activities. Entire investments of personal wealth are increasingly stored virtually. Once a novelty, we now read about cryptocurrency not only in the business sections of daily websites or financial publications, but also on their front pages. Entire sections of news publications are becoming devoted to cryptocurrencies like Bitcoin.

Cybersecurity risk and chances of online fraud in cryptocurrency is becoming a global crisis involving billions of dollars. Hacking is a major threat today for individuals, banks, and institutions. Even the most secured US Federal Reserve, the US central banking system, has seen hundreds of cyberattacks in the last decade. A cyberattack could result in losses for investors who have put their life savings in crypto assets. Governments globally are worried that terrorism could be financed through cryptocurrency.

It is important for legal practitioners to embrace and expand their knowledge of cryptocurrency to assist their clients in fraud matters and asset protection. In domestic relations cases, being able to track down hidden crypto assets is an ever-increasing problem. This article seeks to assist the legal community in both understanding cryptocurrency as well as in finding and tracing crypto assets and transactions. The appendix on page 22 contains a glossary of cryptocurrency-related terminology and definitions that practitioners new to this subject area may find helpful.

What Is Cryptocurrency?

Cryptocurrency is a type of virtual currency that relies on an encrypted network to execute, verify, and record transactions without a centralized authority such as a government or bank.2 It was first introduced to the world in 2009 after the global economic crisis. Bitcoin was the first cryptocurrency, and its developers wanted to empower individuals to initiate online transactions that were fast, irreversible, secure, anonymous, and performed without the involvement of banks or other third parties.

From a technical standpoint, cryptocurrency is often open source, publicly available computer code. Therefore, anybody can create a cryptocurrency. Over 20,800 cryptocurrencies currently exist. Bitcoin, Ethereum, Litecoin, Dash, Solana, and many more are virtual currencies that use encryption techniques to control the transfer of value and publicly verify the transfer of funds via a blockchain.

What Is a Blockchain?

A blockchain is a transparent, permanent ledger that registers every transaction by cryptographically linking each transaction together in a series of blocks, forming a giant publicly accessible journal where every entry (transaction) is recorded chronologically. Think of your DNA string, where each code determines a specific human feature, such as eye color, height, hair color, and each physical trait. A blockchain is a series of individual blocks representing each individual transaction. Each transaction (block) is linked to the previous block (transaction) using cryptography, creating a series of blocks into a chain representing every transaction that has occurred since the currency's formation. A blockchain can, therefore, represent years of prior data (transactions) of the coin's trading history.

The blockchain makes it virtually impossible to tamper with the transactional data contained within the chain. A network of computers verifies each transaction and agrees on the state of the digital ledger by tracing back to the previous time the currency was traded and confirming that it hasn't been spent twice. This process is called consensus and ensures the accuracy of the data.

Blockchain software has broad applications beyond cryptocurrencies, including in supply chain management, voting systems, healthcare, and intellectual property around copyrights, patents, and trademarks. Using blockchain in these areas helps ensure transparency and efficiency when tracking and moving files, goods, and materials. A blockchain network can verify these transactions to ensure they're valid.

Buying and Selling Cryptocurrencies

Cryptocurrency is a unique asset in that it can be bought and sold like an investment as well as used like a currency and traded for goods and services. Additionally, there are cryptocurrency debit cards, such as the Coinbase Visa Debit Card, that allow customers to spend their cryptocurrency from their Coinbase exchange wallet account anywhere Visa is accepted. Visa and Coinbase handle the cryptocurrency exchange, and the merchant receives payment in its native currency. This type of transaction, from the merchant's perspective, is the same as any other Visa transaction.

Cryptocurrencies are decentralized networks, unlike traditional currencies controlled by the US Treasury and banks.[3] Because they operate on a distributed network that holds copies of the blockchain, no single entity con-

trols them, which makes them more transparent and secure. Cryptocurrencies have units (coins/tokens), such as Bitcoin (BTC) and Ether (ETH). Individuals can access their coins/tokens via a digital wallet (password-controlled account), which is comparable to an online bank account.

Exchanges are third-party websites that facilitate the buying and selling of cryptocurrency. Buying and selling cryptocurrencies online through exchanges is similar to buying stocks. Exchanges generally control the private keys and initiate all transactions; a user merely has an account with the third-party exchange, like a brokerage account. This concept is significant in the virtual currency ecosystem. The cryptocurrency private keys (passwords) grant full control over one's wallet. Because of this, cryptocurrency circles have an often-repeated mantra: "Not your keys, not your coins."

How a Blockchain Is Built Through Transactions

When you send cryptocurrency to someone, the transaction gets broadcast to the network at large. Computers on the network (nodes) verify the transaction and add it to the blockchain. This process can take minutes to hours, depending on the currency. The transaction will appear on several nodes to ensure there's a distributed record of all transactions, preventing tampering or manipulation.

The first node operator to access the transaction will verify and secure the existing blockchain and create the new block. Nodes use specialized software to create a "hash" that meets the blockchain's criteria, and "miners" act like auditors, verifying and adding transactions to the blockchain. This ensures that everyone agrees on the chronological order and the validity of the transaction, preventing double-spending and fraud.

A hash is a unique "fingerprint" of data; it's a fixed-length string generated by applying a mathematical function to a piece of information to be added to the blockchain. A block contains a header with essential information like timestamp, previous block hash, and transaction data. A unique hash is generated from this header, acting as a tamper-proof identifier for the block. Transactions within a block are grouped and hashed to create a "Merkle tree" (like DNA). The root hash of this tree is included in the block header, allowing efficient verification of individual transaction inclusion without needing to access the entire transaction data. The chained structure with linked hashes creates a tamper-proof record, as altering any block would require recalculating all subsequent hashes (blocks), an almost impossible task.

What's in Your (Digital) Wallet?

When an individual wants to participate in the cryptocurrency market, the first step is to set up an account (wallet). During this process, the wallet software automatically generates a pair of cryptographic keys: a private key (secretive and never shared) and a public key (derived from the private key and freely shareable). This happens behind the scenes, without one needing to create or remember the keys manually. The software uses secure algorithms to ensure the randomness and strength of the keys. A private key is a password to one's digital wallet.

As such, cryptocurrency is a bearer instrument that is essentially in the possession of anyone with the correct private key. If a private key is lost or destroyed, the individual will permanently lose access to the funds the private key protects. If a private key is stolen or copied by hackers, the hackers can steal that cryptocurrency, and the original owner will have little to no recourse. Individuals can also generate their own keys; some advanced users prefer to generate their own keys for more control and flexibility, which is done using specialized software. However, this approach requires greater technical knowledge and responsibility, as securely storing and managing the keys becomes the individual's sole responsibility.

There are different types of wallets to suit different needs. A paper wallet is a physical piece of paper containing cryptographic keys in the form of an alphanumeric string or QR code used to facilitate your cryptocurrency transactions. Paper wallets are secure if kept in a secure location like a safety deposit box or a fireproof safe. However, they can be easily lost or destroyed if not stored securely, and they are inconvenient for frequent use.

A hardware wallet is a physical device, like a USB drive, where users can store their private keys. Hardware wallets are not connected to the internet, which makes them immune to hacks and malware attacks. They are designed to provide a high level of security and are often recommended for users with large amounts of cryptocurrency.

A software wallet is a digital wallet that is stored on a device, such as a computer or mobile phone. It's an app or a program that the user can download. Software wallets are easy to use and can be accessed from anywhere with an internet connection. However, this accessibility makes them more susceptible to hacks and malware attacks.

Tracing a Cryptocurrency Transaction

As explained above, every transaction ever made on the crypto network is publicly recorded and linked to the block before and after it, creating a transparent chain of evidence from inception of the coin or token. Tracing is following the trail on this digital ledger/blockchain. As with traditional currencies, tracing cryptocurren-

cy transactions may be necessary in cases involving divorce, money laundering, fraud, or embezzlement. Its complex nature makes cryptocurrency harder to locate, track, and seize than tangible currency.

The following is a general overview of how to trace a cryptocurrency transaction:

1. Identify the transaction you want to trace. You'll need either the transaction ID (TxID) (a unique identifier for each transaction), or the address of the cryptocurrency involved in the transaction. You can find these details on a wallet provided by the exchange platform with a valid private key or from the recipient's wallet (if known). In a litigation environment, you will have to request printouts or copies of these transactions and/or digital access to such data, which may require documents to be subpoenaed.
2. Search and view transactions using a Blockchain Explorer website like Blockchain.com, Blockchair, and Mempool.space. From the website, simply enter the TxID or cryptocurrency address in the search bar and hit enter.
3. Review the transaction details, including:
   - amount sent and received (how much cryptocurrency was transferred in the transaction)
   - sending and receiving addresses (the parties involved in the transaction)
   - confirmation status (how many confirmations the transaction has received; transactions with more confirmations are considered more secure)
   - timestamp (when the transaction took place)
   - fees (the transaction fee paid to miners for processing the transaction).
4. Click on the "input/output" addresses to explore past and future transactions associated with the transaction, potentially revealing further details about the origin and destination of the cryptocurrency.

Cryptocurrency addresses are pseudonymous (i.e., written under false name), not anonymous (i.e., where the individual wishes to remain unidentified or unknown). While you can track the movement of cryptocurrency, you may not be able to identify the individuals behind the addresses. In that case, a subpoena may be necessary to move forward.

Tracing is a time-consuming process that may require the filing of numerous subpoenas and the court's willingness to allow such tracing. Most purchases and sales of cryptocurrency occur on exchanges, and US-based exchanges will generally respond to subpoenas. The exchanges can provide information on all the user's transactions on that exchange, as well as any addresses the cryptocurrency was forwarded to or received from.

If the party owning and controlling a particular cryptocurrency address is the client or is willing (or compelled by the court) to work with the investigator, much can be determined from the transaction records pertaining to that address. However, it's critical that private keys or addresses not be shared or made public through court records, as that would allow access to the client's cryptocurrency.

Blockchain Analysis

Blockchain analysis is the process of analyzing and interpreting data stored on a blockchain. Because every cryptocurrency transaction ever made is recorded on the blockchain and publicly available for anyone to see (including details like the amount sent, the addresses involved, and the timestamp), there is a rich dataset for analysis. It's like peering through a digital microscope to uncover insights and patterns hidden within the vast network of transactions.

In general, the main questions to consider when evaluating a blockchain ledger are:

- Who owns the address?
- How many transactions have occurred?
- When did they occur?
- Where did the money go?
- Where did it come from?
- Which address is the "change address"?

While interpreting a cryptocurrency transaction ledger can be daunting at first glance, with the right tools and understanding, it can be quite fascinating. Below are some of the most popular tools used in blockchain analysis:

- **TxStreet:** Transforms transaction data into interactive graphs and charts, visualizing the flow of funds between addresses over time.
- **CoinFlow:** Similar to TxStreet, but with additional features like filtering by cur-

rency and identifying potential money laundering patterns.

- **Walli:** Creates network visualizations of Bitcoin transactions, highlighting clusters and connections between addresses.
- **Bitcoin Decoder:** Provides detailed analysis of individual Bitcoin transactions, including potential spending habits based on transaction patterns and exchange identification.
- **Blockcypher:** Offers similar functionalities to Bitcoin Decoder, with additional support for multiple cryptocurrencies.
- **Whale Alert:** Tracks large cryptocurrency transactions ("whale movements") in real time, potentially indicating market trends or significant events.
- **Elliptic:** Provides blockchain intelligence and risk management solutions for financial institutions and law enforcement agencies.
- **Chainalysis:** A blockchain analysis company offering advanced tools and expertise for investigators and financial institutions.
- **Crystal Blockchain:** An investigative platform specializing in identifying illicit activity on the blockchain.

In addition, online forums, Reddit communities, the American Institute of CPAs, and Discord servers provide a platform to ask questions and learn from experienced users. You can also find helpful tutorials and guides specifically designed for interpreting cryptocurrency transaction ledgers.

Understanding UTXOs

When investigating cryptocurrency transactions, it is important to understand that each token (or coin) represents a specific value of a particular cryptocurrency, so when it is used to purchase an item, it is broken down into a fraction. That fraction represents a specific value corresponding to the amount of the cryptocurrency. In further transactions, it may be sub-fractioned again. Every transaction made with cryptocurrency is like taking a certain number of tokens from the bucket (spending them). You can break the tokens, so if you use a .10-token piece to pay for a .05-token item, you don't get .05 individual token back. Instead, you get a new .05-token piece as your change. This is called the unspent transaction output (UTXO). This leftover piece can be used in another transaction later. "UTXOs" simply means multiple unspent transaction outputs.

UTXOs make the blockchain more efficient by avoiding the need to track every individual unit of cryptocurrency—that is, they eliminate "tracking change" from being returned to the purchaser. This provides a clear, linear audit trail of how tokens have been moved around the network. They enable complex transactions involving multiple inputs and outputs.

Understanding UTXOs can be helpful for anyone who wants a deeper understanding of how cryptocurrencies work, especially when dealing with more complex transactions or exploring blockchain platforms.

In addition, there can be multi-signature (multi-sig) wallets that require multiple private keys to authorize transactions. Unlike traditional wallets where just one key unlocks the door (opens the wallet), multi-sig wallets add an extra layer of security by requiring collaboration, but they also make tracing more complex and time consuming.

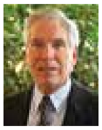
The Importance of Seed Phrases

The holy grail of cryptocurrency investigation is finding the seed phrase of the target of the investigation. The investigator who uncovers the target's seed phrase will be able to not only view the transactions in the related wallet but also initiate transactions in the wallet (disregarding the legality of doing so). Though this could be a huge triumph for the investigation, the target may have control of more than one set of seed phrases. The same is potentially true for finding their hardware wallet. Hardware wallets can have a seed phrase programmed into them, but they are generally password-protected. A hardware wallet will be useless without the associated password.

Most hardware and software wallets are hierarchical deterministic (HD) wallets, which are generally considered the best tradeoff for security, key management, and ease of use. HD wallets start with a single randomly generated seed phrase that is generally 12, 15, 18, 21, or 24 words. Those seed words are then mathematically modified through multiple "hash functions" to create private keys, public keys, and addresses. Although the process is more complicated than explained above, access to these keys can be an important step to developing a full fact picture in an investigation.

Conclusion

Blockchain analysis requires a basic understanding of blockchain technology and cryptocurrency concepts. It is a complex and ever-evolving field with new techniques and tools emerging constantly. While powerful, it is not foolproof and should be used alongside other investigative techniques. Be cautious when using online tools, especially those requiring private keys, and only use reputable and trusted platforms. CL



Ronald Koch, CPA, ABV, is an expert in litigation support, business valuation, economic damages, tax litigation, and embezzlement cases. He has given numerous lectures and published several articles regarding the valuation of closely held companies, tax/trust issues, and forensic investigations—rkoch@vlacpa.com.

Coordinating Editor: James R. Paravecchio, jvecc13@yahoo.com

NOTES

[1] *See* Ghodoosit, "Crypto Litigation: An Empirical View," *Yale J. of Regul.* (Nov. 28, 2022), https://www.yalejreg.com/bulletin/crypto-litigation-an-empirical-view (listing all crypto cases as of November 2022).

[2] Montevirgen, "What Are Cryptocurrencies and Why Is the World Paying Attention?" Encyclopedia Britannica (Sept. 18 2022), https://www.britannica.com/money/what-is-cryptocurrency.

[3] Koechner and Wolverton, "Crypto Sleuthing 101 for Forensic Accountants," AICPA Forensic and Litigation Services Digital Assets Task Force (2023), https://www.aicpa-cima.com/resources/landing/crypto-sleuthing-for-forensic-accountants.

APPENDIX

Glossary of Cryptocurrency-Related Terms*

Address	A "bank account number" for holding crypto assets. It is an alphanumeric string of letters and numbers that is part of an individual's wallet. Different crypto assets have unique address formats.
Block	A package of digitally recorded data; a group of transactions
Blockchain	A transparent, permanent ledger that registers every transaction and cryptographically links them together a series of blocks in a way that prevents modifying previous blocks. It is the underlying technology that powers Bitcoin and other cryptocurrencies.
Change address	The cryptocurrency wallet address that is used to receive the change generated during a cryptocurrency transaction. When a user sends cryptocurrency to another user, they may not use the entire balance of their wallet to fund the transaction. Instead, the wallet may use a portion of the balance to fund the transaction and then generate a new address, known as the change address, to receive the remaining balance.
Consensus	The process by which a group of nodes on a network determine which blockchain transactions are valid and which are not
Miners	Individuals or companies around the world that help validate blockchain transactions to prevent double-spending and fraud. Miners will only allow the transfer of funds by individuals who can produce the correct private key. Miners receive the native tokens/coins as compensation for their services.
Mining	The act of processing and confirming transactions on the blockchain using a series of advanced computations. The process of mining generally consumes a lot of electricity and can be a profitable endeavor for the miners if their electricity costs are low enough.
Node	A computer or device that holds a copy of a blockchain. Each node communicates with other nodes to share transaction information. Depending on the cryptocurrency, some nodes may also process or validate cryptocurrency transactions.
Nonfungible token (NFT)	A unique digital identifier that is generally used on platforms that offer collectible items, access keys, lottery tickets, numbered seats for concerts and sports matches, and so on. Each token is unique or part of a limited set (i.e., 1 of 100 copies).
Privacy coin	A type of crypto asset that strongly focuses on anonymity and lack of traceability. A few examples of privacy coins are Monero (XMR); ZCash (ZEC); and Dash (DASH) (Dash has a "private send" option, but most transactions are public).
Private key	A string of random letters and numbers that allows access to and management of crypto fund; similar to a private password
Seed or seed phrases	A series of 12 to 25 words that is used to generate private keys for cryptocurrency funds. The holder of seed phrases will be able to not only view the transactions of the related wallet but also initiate new transactions.
Types of virtual currency	• Protocol tokens: exist solely as an asset for system participants • Utility tokens: provide the holder with a right or privilege within a specific computer program or distributed ledger • NFTs: each unit is unique or is part of a limited collection • Tokenized assets or asset-backed tokens: confers a right to an asset (i.e., stock certificate or property deed)
Wallet	A method of storage (either virtual or in hardware form such as a USB stick) that allows users to store private keys for cryptocurrencies, enabling users to send and receive coins. Types of wallets include: software wallet—phone or computer application that can generate private keys; hardware wallet—password-protected electronic device; and paper wallet—storing private keys on physical paper.

*Many of these definitions derive from Koechner and Wolverton, "Crypto Sleuthing 101 for Forensic Accountants," Definitions, AICPA Forensic and Litigation Services Digital Assets Task Force (2023), https://www.aicpa-cima.com/resources/landing/crypto-sleuthing-for-forensic-accountants.