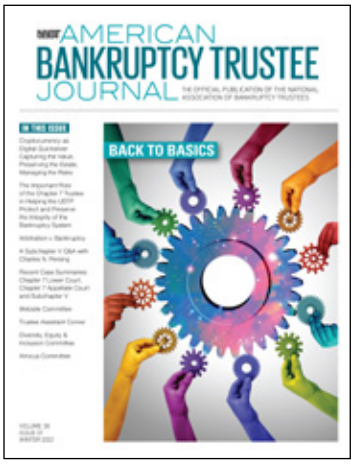
NABT AMERICAN BANKRUPTCY TRUSTEE JOURNAL

THE OFFICIAL PUBLICATION OF THE NATIONAL ASSOCIATION OF BANKRUPTCY TRUSTEES

REPRINT

Cryptocurrency as Digital Quicksilver: Capturing the Value, Preserving the Estate, Managing the Risks

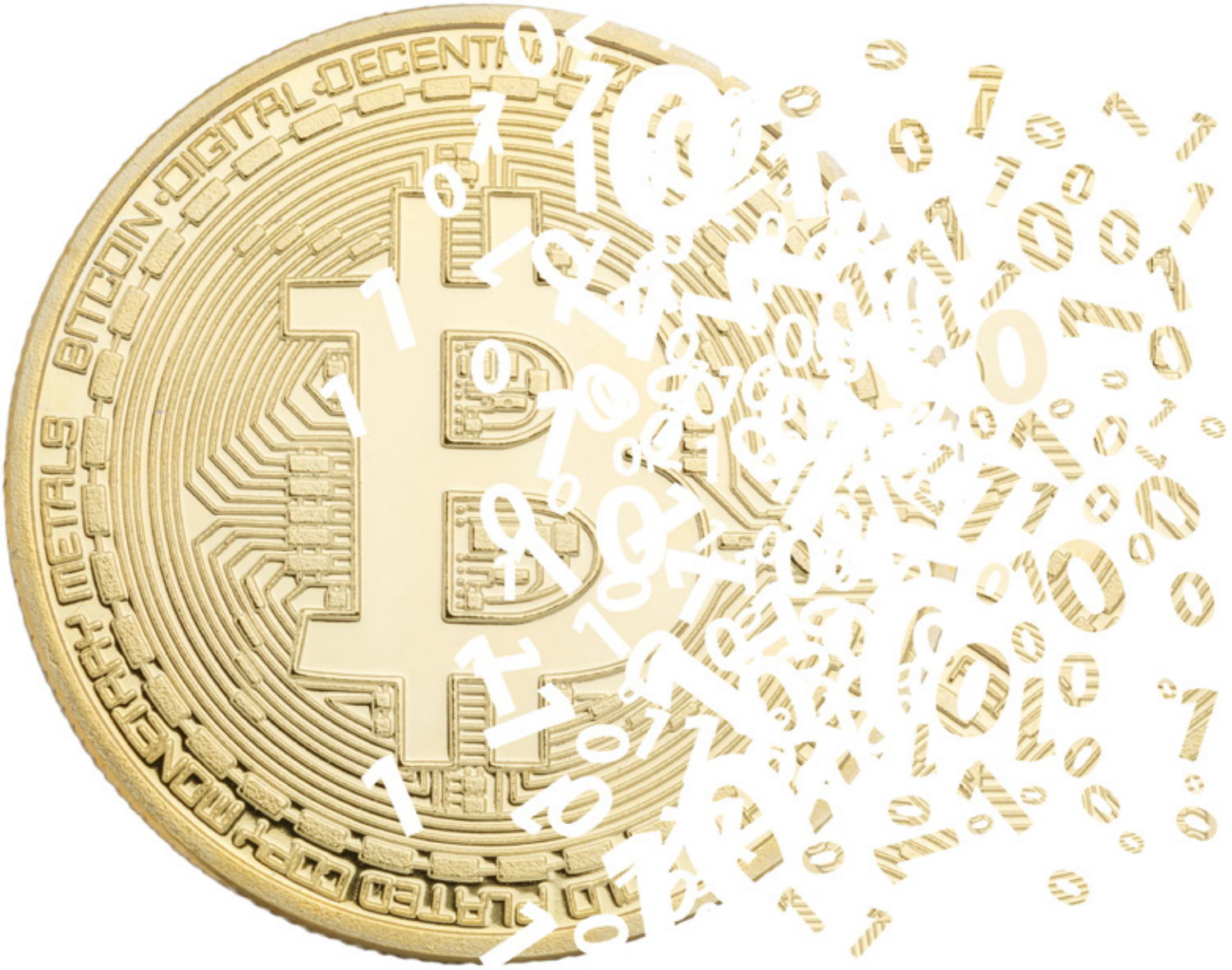
Kristofer Swanson,
Patricia Peláez and
Daniel R. William,
Charles River Associates,
Chicago, Illinois



Reprinted from "Cryptocurrency as Digital Quicksilver: Capturing the Value, Preserving the Estate, Managing the Risks," by Kristofer Swanson, Patricia Peláez and Daniel R. William, Winter 2022, The American Bankruptcy Trustee Journal - The Official Publication of the National Association of Bankruptcy Trustees, Volume 38, Issue 1, pages 19-21. Copyright 2022 by The National Association of Bankruptcy Trustees. Reprinted with permission.

CRYPTOCURRENCY AS DIGITAL QUICKSILVER:

Capturing the Value, Preserving the Estate, Managing the Risks



CRYPTOCURRENCY AS DIGITAL QUICKSILVER:

Capturing the Value, Preserving the Estate, Managing the Risks

By Kristofer Swanson,Vice President and Practice Leader, Forensic Services, Charles River Associates, Chicago, Illinois, Patricia Peláez, Principal, Charles River Associates, Chicago, Illinois and Daniel R. William, Principal Charles River Associates, Chicago, Illinois

The Takeaways

As cryptocurrencies continue to grow in relevance to the global economy, bankruptcy trustees and federal equity receivers will continue to encounter these assets – currently estimated to hold approximately $2.5 trillion[1] in value – with increasing frequency.

Like cash, digital currencies are corporate assets that are considered among the most prone to theft (by either insiders or third parties), and therefore present particular risks around custody and control. Unlike cash, the corresponding tax ramifications can be complex and material, and the digital currencies themselves can be highly volatile in value and relatively illiquid when it comes time to engage in a trade.

Accordingly, when stepping into the role of bankruptcy trustee or federal equity receiver, it is important to assess quickly whether assets of the estate include cryptocurrencies (or "digital currencies"), as these present unique risks and challenges to be managed.

The purpose of this article is to identify key recommendations for locating, accessing, securing, and monetizing these assets, including tax considerations which will likely impact the monetization strategies.

1. How can cryptocurrencies be located, and their value estimated?

Forensic analysis can be an invaluable tool for quickly locating cryptocurrency assets. Key forensic steps could include:

a. reviewing the trial balance for accounts with descriptions referencing cryptocurrency assets, and reviewing the general ledger for transaction descriptions referencing cryptocurrency assets and/or cryptocurrency exchanges;

b. obtaining and reviewing bank statements for transfers to/from cryptocurrency exchanges;

c. conducting email searches and searching files on the network and on computer hard drives for digital wallets, in which public and private keys are stored;

d. reviewing internet browsing history of employees in the finance function for evidence of accessing websites, such as online exchanges or cloud mining services;

e. securing relevant mobile devices or mobile device backups to identify apps which are designed to purchase or sell cryptocurrency or to pay with cryptocurrencies for goods and services;

f. looking for purchases of mining equipment and specialized hardware wallets;

g. searching for virtual machines on the company's existing network infrastructure that may have been set up (licitly or illicitly) to mine; and

h. reviewing the office or home for mining equipment, wallet hardware, and paper wallets.

Once a wallet is located, a block explorer tool can be used to accumulate the transactions and estimate the value of the cryptocurrency associated with it. Having an estimate of the materiality of these assets, and their approximate holding period, will be important for developing appropriate risk-based strategies to secure and monetize them, as discussed further below.

2. How can cryptocurrencies be accessed?

To access the funds, the trustee will need either a) the exchange platform associated with the wallet, the account username, and the account passcode, or b) the wallet address and the private key or keys needed to access the wallet.

With either set of information, the trustee can transfer the associated wallet balance to a new wallet address controlled by the trustee. Without a full set of either type of information, the value of the cryptocurrency could be deemed irretrievable and constructively lost forever. Accordingly, if a trustee has only the wallet address but not the private key, for example, a digital forensic effort will often be recommended to search for files on computers and networks where the private key information may have been recorded by a user.

Sometimes, passcodes and private keys are recorded in password-protected files. Fortunately, digital forensic tools can be employed to endeavor to crack such files, although the process can take from milliseconds to years, depending on the length and complexity of the password.

Why can't the same digital forensic technology be used to crack private keys? The answer is that private keys are usually expressed as an alphanumeric string, with hundreds of digits. Because they are typically so much longer than the typical user-generated password or phrase, it could easily take many decades to reverse engineer a private key, using current technologies.

However, if the private key has been stored with a third party, the trustee may be able to petition the court to obtain a subpoena or search warrant to compel sufficient cooperation to gain control of the cryptocurrency.

3. How can wallets be secured?

Once the trustee has located cryptocurrencies, wallets, and their associated private keys, the next decision to be made is how best to quickly secure these assets. The most common options

About the Authors



Kristofer Swanson, CPA/CFF, CAMS, CFE is a vice president and Global Practice Leader of the Forensics Services Practice at Charles River Associates. He can be contacted via email at **kswanson@crai.com** or by phone at +1-312-619-3313. Patricia Peláez, CPA/CFF, CFE, CPC, CAMS is a principal in the Forensics Services Practice at Charles River Associates. She can be contacted via email at **ppelaez@crai.com** or by phone at +1-312-577-4180. Daniel William, CPA, is a principal in the Forensics Practice at Charles River Associates. He can be contacted via email at **drwilliam@crai.com** or by phone at +1-312-377-5201.

CRA's Forensic Services Practice has been recognized by *The National Law Journal* as being one of the top three Forensic Accounting Providers in the country, and by Global Investigations Review as one of the leading investigative consultancies from around the world for handling sophisticated cross-border, government-driven, and internal investigations. In addition, the Practice earned rankings from Chambers in its "Litigation Support" and "Crisis & Risk Management" guides. The Practice – including our state-of-the art digital forensics, eDiscovery, and cyber incident response lab – has been certified under International Organization for Standardization (ISO) 27001:2013 requirements as part of our industry-leading commitment to our clients and their information security. If you have questions or wish to further discuss this article or related matters to CRA's Forensic Services Practice, please contact one of the authors listed above.

are hot storage, cold storage, and custodial services. Each method comes with its own advantages and risks, and it is unlikely that each will be equally appropriate in any given situation.

a. Hot storage

This type of storage relies on devices or systems that connect to the internet, such as desktop wallets, mobile wallets, and web-based wallets. While this can make it easier and more convenient to manage, monitor, and access cryptocurrencies, it can also make it easier for former employees, hackers, and other bad actors to gain access and pilfer these assets.

b. Cold storage

This type of method reduces hacking risk by relying on tools that are not connected to the internet – such as smartcards, USB devices, paper wallets with QR codes, etc. – to record private keys.

However, these tools can come with comparatively greater risk of physical theft and/or damage from fires, floods, and other disasters. These risks can be mitigated somewhat by using a safe or safe deposit box, and by making backups and storing them in multiple secure locations.

From an operational perspective, one potential disadvantage to using cold storage is that it can take longer to engage in a transaction. The trustee would typically have to physically retrieve the cold storage device, and then import the wallet's private key into a hot wallet (one that connects to the internet), to enter a sell order (either for fiat currency, or in exchange for another type of cryptocurrency which can then be converted into fiat).

c. Custodial services

Over the past decade, various companies have started offering digital currency custodial services, typically focused on institutional investors that are holding large quantities of cryptocurrency. Many custodians tout their use of military-grade cold wallets, geographically dispersed private keys, frequent audits by third parties, micro-segmentation of data, and even the use of deactivated nuclear bunkers for storage. At least one custodian represents that it insures all the assets that it holds, to provide further protection for its clients.

These services tend to be more cost-effective if a client has large investments in cryptocurrencies and intends to invest in digital currencies for the long term, and accordingly may or may not be an ideal option for a bankruptcy trustee.

4. What tax considerations should be considered before implementing a monetization strategy?

Unlike transactions with fiat currency, any sale of cryptocurrencies, or any use of these assets to pay for goods or services, is considered a separate taxable event under the US Federal Tax Code, with either short-term or long-term capital gains implications for the estate.[2]

However, these are not the only times in which tax liabilities can be triggered. The Internal Revenue Service (IRS) considers "mining cryptocurrency, … and hard forks and split chains"[3] to also be taxable events. The IRS even considers the exchange of cryptocurrency for another type of cryptocurrency to be a taxable event, and not a like-kind exchange.[4]

Accordingly, it is essential for the trustee to ensure that he or she has a robust process in place to track and calculate the gains and losses each time he or she causes the estate to engage in a cryptocurrency transaction. This includes situations in which digital currencies are used to purchase goods or services in which the fair value of such is higher or lower than the book value of the cryptocurrency used to make the purchase.

Additional tax liabilities can arise if currency transactions and their associated tax liabilities are not timely and correctly reported.[5]

5. So how can these oft volatile and relatively illiquid assets be monetized?

It is important to remember that not all cryptocurrency holdings are of equal risk. Historically, some have been more volatile in value than others, some have had greater "staying power" in the market than others, some are more widely accepted as forms of payment for goods and services than others, and some are more liquid and easier to monetize than others.

Similarly, not all monetization strategies are of equal risk. Some might be faster, but could result in higher transaction fees, for example.

Accordingly, and while bearing the appropriate tax considerations in mind, taking a risk-based, cost-benefit approach to monetizing the various cryptocurrencies is recommended.

From a tactical perspective, common monetization methods include the following:

a. Cryptocurrency exchanges. Exchanges often make markets in multiple digital currencies, and sometimes more than one exchange will make a market in the same digital currency. Once the trustee selects an appropriate exchange, a sell order can be executed, and fiat currency can typically be withdrawn.

i. Some exchanges do not support fiat currency withdrawals or allow only limited amounts to be withdrawn at a time

ii. Depending on what kind of cryptocurrency is being bought or sold, and in what amount, transactions may take some time to be confirmed; transactions are typically not instantaneous.

b. Cryptocurrency swapping platforms. These can be used to convert lesser-known or lesser-used cryptocurrencies into more commonly used cryptocurrencies, generally at lower fees and more favorable exchange rates than exchanges.

c. Purchase transactions. The estate's digital currencies can be used to directly acquire needed goods or services. A peer-to-peer wallet exchange allows the buyer and seller of goods and services to exchange private keys, which reduces transaction time and applicable fees. 🏛

ENDNOTES:

1 https://www.investopedia.com/tech/how-much-worlds-money-bitcoin/

2 https://www.cpajournal.com/2019/01/24/the-taxation-of-cryptocurrency/

3 *Id.*

4 *Id.*

5 *Id.*