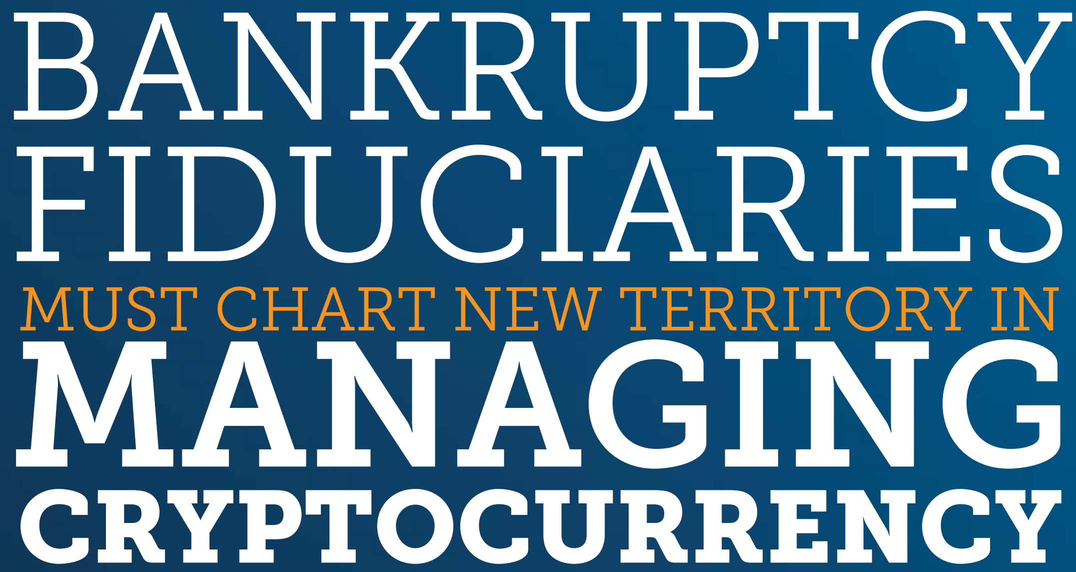


BANKRUPTCY FIDUCIARIES MUST CHART NEW TERRITORY IN MANAGING CRYPTOCURRENCY

BY ERIC KURTZMAN, CO-CEO & JUSTIN DOLES, CHIEF INFORMATION SECURITY OFFICER, STRETTO

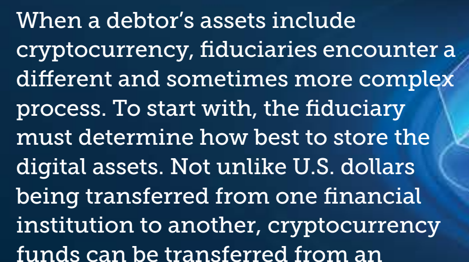
As cryptocurrency has entered the U.S. economy as a widely held and circulated asset, its presence within the bankruptcy process is quickly evolving. For bankruptcy fiduciaries, cryptocurrency poses unprecedented legal and case administration challenges. One of the most pressing issues for fiduciaries is how to manage cryptocurrency as an asset compared to how they have traditionally handled U.S. dollars.

In following the journey of an asset through the bankruptcy process, this article examines the considerations fiduciaries should apply to cryptocurrency accounts that don't apply in the same way to traditional U.S. dollar accounts. Also, while termed "currency," digital assets differ considerably from currency as traditionally understood in the context of bankruptcy; fiduciaries should avoid conflating their treatment with the treatment of fiat currencies.

Bank Accounts vs. Digital Wallets

In a typical case, bankruptcy fiduciaries deposit debtors' U.S. dollar-based assets into a bank. This process and the regulations that guide this transaction are generally well-established and predictable for the fiduciary and other involved parties. Fiduciaries must ensure that the institution meets FDIC insurance requirements and/or the Executive Office of the United States Trustee's requirements, such as the form and frequency of reporting, and must consider the type of account that is best suited for each debtor's assets. In addition, fiduciaries must be aware of United States Trustee guidelines and tax regulations associated with any fees paid or interest earned.

When a debtor's assets include cryptocurrency, fiduciaries encounter a different and sometimes more complex process. To start with, the fiduciary must determine how best to store the digital assets. Not unlike U.S. dollars being transferred from one financial institution to another, cryptocurrency funds can be transferred from an



continued on page 20

Using a cold wallet generally involves fewer fees and gives the custodian more control and greater security, but it also requires more technical knowledge to manage.

continued from page 18

exchange to another location or "wallet"—a storage device or app capable of receiving, storing, and sending digital currency. As with a traditional ACH or wire transfer to a bank account, the sender will need to provide the wallet address destination to which the digital assets should be transferred.

Fiduciaries should have a firm understanding of the differences between storing cryptocurrency on an exchange—which uses a "hot wallet"—compared to storing cryptocurrency in a "cold wallet," which is an app or physical storage device (*e.g.*, a hard drive) designed specifically to store tokens offline. Many fiduciaries may find using an exchange more convenient to manage cryptocurrency assets because exchanges provide user-friendly access to completing transactions, established consensus protocol (equivalent to a bank's call back to confirm outgoing wires), and maintenance of account information.

Certain exchanges will provide additional support to fiduciaries for their account needs, including freezing or suspending an estate's account so that assets cannot be moved from their location and providing transaction histories and account balances. They may also offer specialized services that assist fiduciaries in transferring the estate's cryptocurrency assets to a fiduciary-controlled account, convert cryptocurrency to fiat currency, and transfer crypto assets from the fiduciary account to creditors' wallets. However, the exchanges generally charge fees for such services.

In addition, some exchanges offer interest on the digital assets they store; however, this will vary depending on the type of coin. A fundamental fact that many crypto investors seem to either miss or ignore is that deposited coins don't simply grow—growth requires investment, and investment entails risk. Importantly, just as banks must use depositor dollars to create revenue that funds interest on depositors' accounts, exchanges that offer interest often use the deposited cryptocurrencies on those exchanges.

To be clear, and it's worth repeating this, an exchange that offers a high return on deposits is unlikely to be sitting on the deposits; instead, that exchange is likely leveraging and reinvesting the deposits elsewhere in the name of the exchange—*i.e.*, the depositor may have contractually made a loan to the exchange and does not own any specific tokens anymore. Conversely, unlike banks, which are insured by the FDIC and are heavily regulated, cryptocurrency exchanges have no FDIC-like insurance entity and have far less regulatory oversight; these two factors collectively create material risk to currency left on exchanges and strongly enhance the argument for cold wallets.

In addition, exchanges have been historical targets for thieves. There are many examples of failed cryptocurrency exchanges that involved either thievery by insiders or failed risk management as the exchange engaged in highly leveraged investment strategies in pursuit of a return promised to token depositors.

Using a cold wallet generally involves fewer fees and gives the custodian more control and greater security, but it also requires more technical knowledge to manage. Self-custody of digital assets requires that the fiduciary possess a strong understanding of the cryptocurrency environment and its risks.

A common fear regarding cold wallets is what happens if the password or the wallet is lost? The cautious owner of a cold wallet can create a back-up password called a seed phrase, which is a series of unrelated words that can be used to re-create the wallet. This back-up password can also require multiple seed phrases to work (*e.g.,* to re-create the wallet, an investor may require three trusted advisors to each provide their unique seed phrase) or can require some, but not all, of the existing seed phrases to work (*e.g.,* the owner can create 10 passwords, any six of which can be used to re-create the wallet, and then distribute those 10 passwords to 10 trusted professionals).

Security Considerations

Most fiduciaries can rest assured that their clients' assets in U.S. dollars held at U.S. banking institutions are secure. In addition, the United States Trustee Guidelines require collateralization for any amounts not covered by FDIC insurance. Fiduciaries face an entirely new set of considerations with cryptocurrency as an asset.

Whether the trustee uses a cold wallet or hot wallet to manage the debtor's digital assets, stringent security measures must be taken to protect them. Most cryptocurrency exchanges reduce risk with complex password requirements and multifactor authentication. In addition, fiduciaries should take advantage of all security controls available and stay vigilant against any potential phishing emails or text messages. When using a cold wallet, fiduciaries must safeguard all passwords and store the physical

device in a secure location. As a general rule, recovery/seed phrases and passwords should never be stored on a computer or smartphone.

If a third party is involved in helping the trustee manage cryptocurrency assets, a multisignature wallet can provide another layer of security. Not unlike having multiple signers on a checking account, a multisignature wallet involves having more than one person in possession of the financial controls so that any transaction requires approval from all custodians. Also, as mentioned earlier, fiduciaries should establish a protocol for re-creating the cryptocurrency account to protect the assets in case the password is lost or the cold wallet is lost/broken.

Disbursement Challenges

Cryptocurrency assets in a bankruptcy estate complicate the disbursement process, the extent of which depends on what type of coins require disbursement and how they will be distributed. The process and its requirements will largely depend on whether disbursement of digital assets involves in-kind distribution as cryptocurrency or liquidation to U.S. dollars.

If a creditor agrees to be paid in cryptocurrency, the fiduciary may encounter challenges transferring the exact type of coin held in the estate. Unlike U.S. banking institutions that universally accept and exchange U.S. dollars, different cryptocurrency networks may not have interchangeable coins that can be sent or received. Thousands of cryptocurrencies exist, yet Coinbase, one of the leading exchanges in the world, supports transactions in less than 1% of them.

In other words, the fiduciary may not be able to pay the creditor in a compatible form of cryptocurrency and may instead, for example, have to convert the estate's currency into bitcoin if the creditor's exchange can receive bitcoin. Of course, these transactions have a transaction cost, and the value of each currency constantly fluctuates, so the value received by the creditor at the end of the transactions may differ from the value of the asset the trustee initially intended to send.

To make disbursements, the trustee may also need to liquidate cryptocurrency. This presents a myriad of questions about the valuation of the cryptocurrency. The recent fallout from the cryptocurrency industry has instilled doubts in many minds about the reliability of the value of digital assets. Today more than ever, fiduciaries must prepare for the volatility of value of cryptocurrencies being held in a bankruptcy estate and carefully consider if/when it makes sense to transfer the cryptocurrencies to a more stable asset or to leave them intact.

Government Issues

While tax regulations are well-established for U.S. dollars, fiduciaries may find less clarity when cryptocurrency is involved. Furthermore, while some coin-based exchanges may automatically generate tax reports, the cryptocurrency industry's instability has created uncertainty about the availability of tax information across different platforms.

The Internal Revenue Service issued a notice in 2014[1] deeming cryptocurrency property for federal income tax purposes and providing some guidance as to how tax principles apply to transactions involving digital assets. To the extent bankruptcy estates have potential tax liabilities, fiduciaries should consult with an accounting expert to ensure that they fulfill tax obligations.

In addition, the United States Trustee has not yet established guidelines identifying how fiduciaries are to secure and protect cryptocurrency actions. While the duties around U.S. dollars may seem cumbersome, fiduciaries can feel safe following those guidelines and doing no more. Without such guidelines, fiduciaries are left not knowing with certainty when they have done enough to secure cryptocurrency assets.

Many questions remain about the intersection of bankruptcy and cryptocurrency, and many more are likely to surface in the future. As the presence of cryptocurrency continues to grow as an asset held within estates, it's likely to add more twists and turns in the road for fiduciaries. Over time and with more case experience, fiduciaries will gain more direction to chart this new territory, but there will be traps, drops, and wild turns along the way for any who take a cavalier approach to this new asset class.

[1] irs.gov/pub/irs-drop/n-14-21.pdf

As co-CEO of Stretto, **Eric Kurtzman** directs the growth and expansion strategy for the company. He has more than 20 years of expertise and, drawing on his experience as co-founder of Kurtzman Carson Consultants, he works with Stretto's chief integration officer to conduct risk analysis, evaluate investment potential, and provide guidance to the Board of Directors on investment risk and return. Along with the chief operating officer, he outlines financial, service, and development objectives for each business division.

Justin Doles is chief information security officer with Stretto and leverages nearly 20 years of substantive systems and security-architecture experience to abide by the latest regulations and compliance requirements. Leading a team of technology experts in monitoring security vulnerabilities in network and host systems, his primary responsibilities are performing IT security-risk assessments and reporting on ways to minimize threats. Doles designs strategies to handle security incidents and trigger investigations while ensuring business continuity.