From: stevesletters@leimbergservices.com <stevesletters@leimbergservices.com>
Sent: Tuesday, October 27, 2026 8:53 AM
To: Martin Shenkman <Shenkman@shenkmanlaw.com>
Subject: Karolis Matulis, Martin Shenkman, Thomas Tietz, Christine Pronek & Jonathan Blattmachr: Cryptocurrency and Digital Assets - Estate Planning, Income Tax, and Fiduciary Issues Steve Leimberg's Estate Planning Newsletter

EXTERNAL: This email originated from outside of the organization.

Steve Leimberg's Estate Planning Email Newsletter - Archive Message #3345

Date: **27-Oct-26**

From: **Steve Leimberg's Estate Planning Newsletter**

Subject: **Karolis Matulis, Martin Shenkman, Thomas Tietz, Christine Pronek & Jonathan Blattmachr: Cryptocurrency and Digital Assets - Estate Planning, Income Tax, and Fiduciary Issues**

"The central lesson is that cryptocurrency planning must respect the reality of control. Whoever can move the asset has practical power over it. Estate planning documents should not ignore that reality. They should be drafted and implemented so that the legal plan and the blockchain mechanics point in the same direction."

Karolis Matulis, Martin Shenkman, Thomas Tietz, Christine Pronek and Jonathan Blattmachr provide commentary on the estate planning, income tax, and fiduciary issues raised by cryptocurrency and other digital assets, and on why practical control of the private key, not legal title alone, often determines whether a gift, trust, or estate plan actually works.

Karolis Matulis, CPA, CITP, CVA, is a Principal at WilkinGuttenplan, an accounting firm in East Brunswick, New Jersey, where he has worked since 2013. He focuses on tax efficiency, deal structuring, and valuations for clients in complex transactions, and he advises on digital assets. Karolis leads the firm's Innovation Council and chairs the NJCPA Emerging Technology Group. He holds a B.S. in Accountancy from The College of New Jersey.

Martin M. Shenkman, CPA, MBA, JD, PFS, AEP (Distinguished) is author of more than 40 books and more than 1,400 articles on estate planning and related topics. He is a frequent lecturer for numerous trade, professional and other organizations. He is active in numerous charitable endeavors. He has practiced estate planning for 35+ years.

Thomas A. Tietz, JD, is an attorney in private practice in New Jersey and New York who helps clients with estate planning. He has written more than 30 articles, published in Trusts & Estates, the ABA E-Report, the NAEPC Journal of Estate and Tax Planning, and LISI. He has lectured for the Notre Dame Tax & Estate Planning Institute, the New Jersey State Bar Association, CPA Academy, and the National Academy of Continuing Legal Education.

Christine G. Pronek, CPA, is a Partner at WilkinGuttenplan with more than two decades of accounting experience in trust, estate, gift, and income tax matters. Before joining the firm, she was partner-in-charge of the trust and estate department at PKF O'Connor Davies. Early in her career, she spent three years as a revenue agent with the IRS.

Jonathan G. Blattmachr is a retired member of Milbank, Tweed, Hadley & McCloy LLP in New York and a Principal in ILS Management, LLC. He is co-founder and Editor-in-Chief of Wealth Transfer Planning. Jonathan is a Fellow and former Regent of the American College of Trust and Estate Counsel and a former chair of the New York State Bar Association's Trusts and Estates Law Section. He has written or co-written eight books and more than 500 articles. He holds a JD from Columbia University School of Law and a mathematics degree from Bucknell University.

Here is their commentary:

EXECUTIVE SUMMARY:

Cryptocurrency and other digital assets require advisers to think simultaneously about tax reporting, technological control, fiduciary governance, and transfer tax doctrines. Traditional estate planning often assumes that ownership can be evidenced by title, account registration, assignment documents, entity records, or custodial statements.

Digital assets complicate that assumption because practical control may depend less on formal legal documentation and more on who can cause a blockchain transaction to occur. Digital assets include cryptocurrencies and other assets recorded on a blockchain, which is a distributed digital ledger that tracks ownership and transfers. A blockchain transaction is the digital equivalent of signing and delivering a transfer document: it is the electronic instruction that moves an asset from one wallet or account to another and permanently records on the blockchain. However, unlike a traditional bank transfer, the ability to initiate the transaction generally depends on possession of cryptographic credentials, often referred to as private keys. As a result, the person with legal authority under a will, trust, power of attorney, or court appointment may not be the person with practical control over the asset. For estate planners, the critical issue is often not merely who owns the asset, but who has the ability to initiate and authorize a blockchain transaction and thereby move, transfer, or access it.

The result is a planning environment in which legal form and technological power may diverge. A client may sign an assignment purporting to transfer cryptocurrency yet still retain the only private key capable of moving the asset. Someone may be named as fiduciary, yet lack any practical ability to access the crypto-assets because that person does not know the private key. A family member may possess technical access yet hold no formal fiduciary office. These mismatches can affect income tax compliance, gift completion, estate inclusion risk, fiduciary responsibility, and practical asset preservation.

The issues are especially important because digital assets are no longer merely speculative curiosities held in small amounts by technologically adventurous investors. Some individuals hold substantial cryptocurrency positions. Others operate businesses that conduct a meaningful portion of their revenue and expense activity on-chain. Still others participate in decentralized organizations, token economies, staking, mining, or other blockchain infrastructure. Advisers who serve affluent families, entrepreneurs, executives, and technology-oriented clients should expect these issues to arise with increasing frequency.

A recurring theme is that cryptocurrency planning cannot be reduced to standard estate planning concepts or paperwork. A trust agreement, assignment, limited liability company (“LLC”) operating agreement, or gift letter may be necessary, but those documents alone may be insufficient if they do not address the technical reality of control which for crypto assets

usually involves having the “key” to effectuate transfers of the cryptocurrency involved. Conversely, a technically effective transfer may create practical risks if the fiduciary control structure is poorly designed (e.g., a friend as trustee is the only person with knowledge of a private key for a crypto-wallet). The planning challenge is to harmonize the legal and technological dimensions so that the intended transfer is respected while the assets remain protected and accessible to the proper fiduciaries.

COMMENT:

Forms of Digital Asset Holdings

Before analyzing tax or transfer issues, the adviser should understand what the client actually holds and how the client uses it. Digital asset clients tend to fall into a few overlapping categories, and the distinction matters because each presents different tax, compliance, and estate planning concerns. A client may be:

- a long-term investor who buys and holds;
- an active trader who moves in and out of positions frequently;
- a collector of non-fungible tokens;
- the operator of a business that transacts on-chain using stablecoins (these are a type of cryptocurrency designed to maintain a generally stable value by being pegged to an asset like the U.S. dollar);
- a participant in a decentralized organization (this is a decentralized organization governed by its participants instead of by a more traditional board of directors’ type arrangement). A common form is a Decentralized Autonomous Organization (“DAO”) where decisions are made by voting on the block;
- participate in a token economy (this is an economic arrangement based on a blockchain token, and it governs how tokens are created, distributed, used, governed, rewarded, and traded. Tokens may be used for payment, voting, ownership, etc.)
- a participant in staking or mining infrastructure.

These roles are not mutually exclusive. The same client may be an investor, a trader, a company founder, and a staking participant at once, and the plan must, therefore, account for each activity the client conducts.

What unites these categories is that the actual control of a digital asset depends less on legal title than on technological access and control. That difference may have profound implications to estate planning. Every holding lives at a blockchain address, and the ability to move the asset depends on who holds the private key associated with that address. A wallet address, or public key, lets others observe activity at that address but confers no control. The private key is the authority to initiate transactions. Whoever holds the private key can move the asset, regardless or of what title documents, account statements, or assignments say. This distinction drives nearly every issue that follows, from reconstructing a trader's tax history to completing a gift to a trust or an individual.

Income Tax Implications

Digital asset income tax reporting requires classification of both the asset and the transaction. A trader moving in and out of the same cryptocurrency may generate a substantial amount of short-term gain or loss. Rapid turnover may leave little opportunity for long-term holding periods. A client who trades extensively may have a return dominated by short-term results even if the client views the activity as part of a longer-term investment strategy.

The analysis may become more complicated when the assets are non-fungible tokens (“NFTs”). NFT activity may resemble trading cards, collectibles, artwork, digital memberships, or speculative tokens, depending on the asset and the rights attached to it. NFTs are unique digital identifying records on a blockchain used to prove ownership or rights associated with a specific digital or physical asset. But, unlike cryptocurrencies where any unit is interchangeable with any other, each NFT is unique. Some clients may trade NFTs in large volumes because they view the activity as analogous to collecting and trading cards. The monetary amounts can nevertheless be significant. A digital image or membership token may be purchased at a cost that is well below its current value. It may later be sold for substantially greater amounts during a period of market enthusiasm.

If an NFT is treated as a collectible, that classification may affect the tax consequences of a long-term capital gain on its sale. This point is important because the client’s intuitive view of the asset may not match the tax classification. A client may think in terms of digital culture, community

access, or speculation, while the tax analysis may require a more conventional categorization.

The active trader presents one of the clearest examples of the difference between traditional tax compliance and digital asset tax compliance. In the conventional setting, a taxpayer may provide brokerage statements, Forms 1099, and supporting documents. The adviser matches proceeds, basis, holding period, and character. In the digital asset setting, the taxpayer may have used multiple exchanges, multiple self-custodied wallets, decentralized applications, NFT platforms, and stablecoin rails (rails are analogous to wire or ACH (automated clearing house) parameters; stablecoin rails are the use of stablecoins to transfer money and settle transactions over blockchain).

Virtually all income tax forms now ask about whether or not the taxpayer received digital assets as a reward, award or payment for property or services or sold, exchanged or otherwise disposed of a digital asset or a financial interest in a digital asset. This is no longer an issue that practitioners can avoid.

Treasury recently issued Revenue Procedure 2026-20 which addresses the tax status of state law trusts holding digital assets.

Recordkeeping

The problem is not necessarily that data is unavailable. On a public blockchain, transaction detail is generally available and complete. The challenge is volume, aggregation, and interpretation. A blockchain can show that a wallet sent or received a quantity of a digital asset at a particular time. That fact alone does not necessarily determine the taxpayer's basis, holding period, tax character, purpose, or whether the transaction was a purchase, sale, exchange, transfer between wallets, payment for services, or some other event.

The adviser must often begin by identifying the client's exchanges and wallets. If the client only traded on a centralized exchange, the reporting may be comparatively easier. If the client also maintained wallets outside the exchange, additional work is required. The adviser may trace transfers from exchange accounts to off-exchange wallets and then examine interactions between those wallets and other addresses. This process can produce a map of related wallet activity, but that map still requires interpretation.

Earlier years in the cryptocurrency market may present additional difficulties. Some exchanges failed, became inaccessible, or maintained records that are no longer readily available. In those cases, advisers may need to make judgment calls based on available data. More recent years may involve better exchange records and more systematic reporting, but high-volume activity remains complex. A complete ledger does not automatically produce a correct income tax return.

Exchanges serve as on-ramps and off-ramps between the traditional financial system and blockchain networks. A client may transfer dollars to an exchange, buy digital assets, move those assets to a self-custodied wallet, later return assets to an exchange, sell them, and withdraw dollars. Each of those steps may create records that identify the taxpayer, the exchange account, and potentially related wallet addresses.

Exchange reporting may allow taxing authorities to associate named taxpayers with wallet addresses. Once the wallet address is known, blockchain analytics may permit review of related activity. Data analytics and artificial intelligence are tools that taxing authorities are using to sift through and track digital asset transactions. In addition, starting with the 2025 tax year, the IRS is requiring custodial brokers to file information returns (Form 1099-DA) reporting the details of digital asset transactions.

This reality undermines the assumption that cryptocurrency activity is too complex for tax authorities to evaluate. It may be complex, but much of it is mathematical, deterministic, and capable of analysis with appropriate tools. Advisers should therefore counsel clients based on the expectation that substantial on-chain activity may be traceable, particularly where centralized exchanges are involved. That all means that clients and their advisers should assume all activity can be audited.

Stablecoin Transactions

Stablecoin transactions raise different issues. (A stablecoin is a crypto currency that maintains a constant relationship with other “currency” such as the US dollar.) In a blockchain-enabled business, stablecoins may be used to pay invoices, contractors, or developers. These payments are generally not investment transactions. They may be part of the business revenue and expense cycle. The adviser should understand whether stablecoins are being used to receive income, pay expenses, compensate service providers, or move value between platforms. Moving value between platforms could mean moving stablecoins between different

exchanges (e.g., Coinbase, Kraken, Binance, Gemini). It might also mean moving assets between other types of custodial and non-custodial arrangements.

For example, a business may transfer stablecoins from one exchange to another, move them from an exchange to a self-custodied wallet, or transfer them to a custodial platform that provides trading, lending, staking, or treasury-management services. These transfers may not represent a change in economic ownership, but they can affect custody, security, recordkeeping, operational risk, and the ability of fiduciaries or successors to locate and access the assets.

Wallets, Public Keys, And Private Keys

The distinction between public and private keys is central to estate planning. Public information provides visibility but no control. A fiduciary, adviser, or taxing authority may be able to observe the activity of a wallet without having any ability to move the digital assets. Conversely, a person who holds the private key may be able to move the assets even if formal legal documents say another person or entity owns them.

The private key is therefore the practical equivalent of control. The analogy to a safe is useful but incomplete. A physical safe may sometimes be opened by a locksmith, court order, drilling, or other physical intervention. A cryptocurrency wallet without the required private key may be inaccessible in a way that has no traditional analogue. If the necessary key material is lost, no court, custodian, fiduciary, or beneficiary may be able to restore access. That presents a unique, dangerous and potentially financially ruinous risk of loss. What if the only person knowing the private key becomes incompetent or dies?

Way to Embody a Private Key

There are many different ways to confirm, safeguard or embody a private key. These concepts are important for planners to understand as these may be relevant to a client seeking to make a completed gift or other transfer of crypto. It is also important to know how the crypto can be safeguarded after transfer (e.g. by a trustee).

- The owner could print the private key or seed phrase on paper. That might be referred to as a paper wallet. If that was done then if the purported transferor still has a copy of that paper have they parted

with dominion and control? How can a trustee safeguard such physical evidence especially in a virtual environment?

- Similar to paper is when the owner engraves or stamps their seed phrase onto stainless steel or titanium plates. The question is similar to that of paper. Has the purported transferor retained a copy of the information?
- A seed or recovery phrase (e.g. 24 words) may be created so that it is mathematically linked to the wallet's private key. Again, how can that be protected and safeguarded? How can the transferee, or advisor, know that the purported transferor has not retained the information to control the crypto?
- Another approach is using a physical device called a hardware wallet. The device itself is not the key. Rather, it securely stores and uses the private key for signing transactions. Similar issues as to completed gift, control and safeguarding the physical wallet must be considered.

This feature changes the adviser’s questions. It is not enough to ask who owns the asset. It is also necessary to ask who can move it, who has the private key, whether anyone else has a copy, whether the key is stored securely, whether the key can be recovered, and whether the person with key access is acting in a fiduciary capacity. These concepts are explored further below.

The Completed Gift Problem

One of the most technically demanding estate planning issues is how to make a completed gift of cryptocurrency. The traditional transfer tax concept is a familiar one. A donor must part with dominion and control over the transferred property in order for the transfer to be regarded as complete. With conventional assets, this requirement is usually implemented through transfer of title, change of account registration, delivery, assignment, or transfer to a trustee or custodian.

Cryptocurrency complicates the doctrine because technical control may remain with the donor even after paper ownership changes. If the donor is the only person who knows the private key to the wallet holding the cryptocurrency, the donor can still move the assets. However, that practical power may be inconsistent with the assertion that the donor has relinquished dominion and control.

The concern is not that the donor could act in a manner that is inconsistent with the purported transfer. The concern is that the donor retains the practical ability to act. Under a completed gift analysis, retained power may matter even if the donor has promised contractually not to use it. A donor who retains the private key may be able to sell, transfer, spend, or otherwise dispose of the cryptocurrency. That retained ability raises questions about whether the gift has been completed.

The problem is analogous in practical terms to a trust brokerage account only up to a point. A donor may transfer stock to a trust account at a brokerage firm. If the trustee controls distributions and withdrawals, and the donor cannot remove value for personal benefit, the donor may have relinquished control even if the donor remains involved as an investment adviser or investment trustee with limited powers. The brokerage platform enforces the distinction between investment authority and distribution control. Cryptocurrency self-custody lacks that built-in institutional gatekeeper unless one is deliberately created.

An assignment of cryptocurrency to an LLC may appear to provide a solution because it fits familiar planning patterns. The client signs an assignment of the wallet or digital assets to the LLC. The client then transfers LLC interests to an irrevocable trust. The documents resemble conventional planning for closely held assets. The problem is that the documents may not alter the private-key reality. Again, as with the analogy above to an investment account, real estate held by an LLC can only be transferred by those controlling the LLC, not the transferor.

If the original owner continues to hold the private key, the LLC may be the nominal owner, but the original owner may remain the only person capable of moving the asset, or one of those who can. The LLC manager, trustee, or donee may have legal claims, but practical control could remain with the purported donor. For cryptocurrency, that distinction may be decisive.

This analysis suggests that advisers should avoid assuming that an assignment alone effects a completed gift. The adviser should ask whether the donee, trustee, LLC manager, custodian, or other fiduciary has actual control over the digital asset. If not, the transfer may be vulnerable to challenge or may fail to accomplish its intended tax objective.

The assignment problem also creates administrative risk. If the donor dies and no one else knows the private key, the assignment may be of limited practical value. The fiduciary may have paperwork showing ownership but

no ability to access the assets. Another possible risk is if the donor retains the key and later becomes incapacitated, acts improperly, or shares the key insecurely, the assets may be lost or misappropriated.

Direct Transfer To A Trustee-Controlled Wallet

A more technically safe approach may be for the trustee or other appropriate fiduciary to create a new wallet, control the private key, and for the donor to transfer the cryptocurrency to that wallet. In that structure, the donor does not retain the private key to the relevant recipient wallet. The donor has caused an on-chain transfer to a wallet controlled by the fiduciary. That structure more closely aligns the legal transfer with the technological transfer of control.

This approach may support the argument that the donor has relinquished dominion and control. The donor can no longer move the transferred cryptocurrency unless the fiduciary permits or participates in a later transaction.

However, this structure creates a separate practical problem. If the trustee alone controls the private key, the trustee may be able to misappropriate the assets. Fiduciary duties may provide legal recourse, but recourse may be inadequate if the assets are moved quickly, transferred across chains or platforms, or placed beyond practical recovery.

This risk is not unique to cryptocurrency. A dishonest trustee can also misuse traditional trust assets. But cryptocurrency can make the consequences more immediate and difficult to reverse. There may be no bank fraud department, transfer agent, or custodian capable of freezing or reversing the transaction. Once assets are transferred on-chain, recovery may be difficult or impractical.

The adviser must therefore solve two problems at the same time. The donor must give up sufficient control to complete the gift, and the structure must prevent any single fiduciary or key holder from having unchecked ability to misappropriate or lose the assets.

In some instances, a client may feel that the trustee is sufficiently honest and, therefore, they are not worried. If that is the case, the advisor may choose to document that decision in the event that a problem later arises. But even if that is the case what of the successor trustee? Will naming an institutional trustee solve the problem? Will the intended institutional trustee be willing to hold cryptocurrency with sole control over the private key?

Custodial Trust Accounts And The Brokerage Analogy

Another possible solution is the use of a custodial platform capable of maintaining accounts in the name of a trust or other entity. If a trust account can be established with a digital asset custodian, the custodian may provide institutional controls similar to a brokerage account. The trustee may be recognized as the person authorized to manage or withdraw assets, and the donor may lack unilateral access. A digital asset custodian is generally a third-party institution that holds digital assets and the related access credentials on behalf of clients, providing security, account controls, transaction authorization procedures, and recordkeeping. In many respects, it functions much like a traditional securities custodian, except that it is safeguarding cryptocurrencies and other digital assets rather than stocks and bonds.

The brokerage analogy is important. For example, if a donor transfers shares of Apple stock from an individual brokerage account to a trust brokerage account, the transfer may be straightforward. The donor directs the transfer, the trust becomes the account owner, and the trustee controls distributions and withdrawals. The donor may retain investment advisory input in some structures, but the donor does not control the removal of assets for personal benefit.

A digital asset custodian may replicate some of these features if it recognizes trust accounts, verifies fiduciary authority, and controls withdrawals through institutional procedures. That model may be attractive for clients who do not want self-custody. It may also be more familiar to trustees, advisers, accountants, and tax preparers.

The custodial model is not free from risk. Some digital asset holders prefer self-custody precisely because they distrust exchanges or centralized platforms. Others prefer the sanitized experience of a custodian because they do not want responsibility for private keys. The planning choice should reflect the client's risk tolerance, the sophistication of the fiduciaries, the value of the asset, and the need for administrable controls.

For estate planning purposes, the key question is whether the custodial arrangement effectively prevents the donor from retaining control while permitting the trustee or fiduciary to administer the assets. If that balance is achieved, the custodial model may be one of the more practical approaches for gifts of cryptocurrency to trusts.

Self-Custody And Multi-Signature Wallets

For clients who prefer self-custody, multi-signature wallets may provide a more nuanced solution. A multi-signature wallet requires more than one authorization to initiate a transaction. Instead of one person holding unilateral control, multiple participants must act together. The structure can be designed so that any specified number of participants out of a larger group can authorize a transfer.

A common example is a two-of-three structure multiple signature wallet. Three participants are, for example, designated. Perhaps any two of the named persons can authorize a transaction. No single participant can move the assets alone. Other thresholds are possible, such as three-of-five. The planning significance is that control can be distributed amongst fiduciaries or trusted parties while preserving redundancy if one participant becomes unavailable. The challenge is how this mechanism will be implemented if each of three named people are given 1/3rd of the private key.

The concept is analogous to a safe requiring multiple keys to get in it. The analogy is useful, although the digital version may be less forgiving. If a physical safe cannot be opened, there may be destructive means to access it (like a break in). If a cryptocurrency wallet requires two signatures and only one required key remains available, there may be no practical method to recover the assets. Simply put, the value of the wallet could be lost.

Multi-signature wallets may help address the concern that one trustee could misuse the private key. If the wallet requires two of three approvals, no single trustee or key holder can act alone. The likelihood of misappropriation may be reduced because collusion would be required. At the same time, the structure can tolerate the loss or unavailability of one participant if the remaining two can still act.

However, multi-signature arrangements may raise difficult completed gift questions if the donor is one of the required or potential signatories. If the donor retains a signing role, the donor may have some continuing control and may even have veto power over a transfer. If the donor’s signature is necessary for all transactions, the donor may have retained a blocking power. Even if the donor cannot act alone, the donor may prevent others from acting. The consequences of that retained power should be carefully considered before including the donor in the signing group.

For an estate planning and transfer tax audience, practitioners should consider that the law is still developing. Thus, these raise potential concerns that require analysis.

The consequences of that retained power in a multi-signature arrangement should be carefully evaluated before including the donor in the signing group. Depending on the facts and applicable law, a retained ability to block or influence transactions could raise questions as to whether the donor has fully relinquished dominion and control over the transferred property. That, in turn, may create uncertainty regarding whether a completed gift has occurred, whether the asset should remain subject to inclusion in the donor's gross estate, whether the trust may be treated as a grantor trust for income tax purposes, or whether the donor's retained rights could affect asset protection or creditor analyses. The significance of any retained signing authority will depend on the scope of the power, the number and identity of the other signatories, and whether the donor can exercise meaningful practical control over the asset after the transfer.

A safer approach for completed gift purposes may require that the donor not be a signatory and not hold any key material that can authorize transactions. Control should instead rest with trustees, investment trustees, trust protectors, designated fiduciaries, custodians, or other persons whose roles are consistent with the intended transfer tax treatment. The precise structure should be coordinated with the trust terms and fiduciary appointments.

Threshold Design And Fiduciary Governance

Threshold design is a central planning decision. A one-of-one wallet is simple but concentrates risk. A two-of-two wallet requires unanimity but creates access risk if either participant becomes unavailable. A two-of-three wallet introduces redundancy and reduces single-person control. A three-of-five wallet may further reduce collusion risk, but it may also increase administrative complexity. But in those latter scenarios, the mechanics of the mechanism must be worked out.

The correct threshold depends on the amount involved, the reliability and sophistication of the participants, the expected frequency of transactions, and the client’s tolerance for operational complexity. A buy-and-hold Bitcoin investor may not need frequent wallet activity. A trust holding actively traded digital assets may require more agile authorization procedures. A

trust that stakes assets or uses decentralized applications may require additional operational capacity.

The trust instrument or ancillary governance document should address who may serve as a signer, whether signers are fiduciaries, how signers may be removed, how successors are appointed, and what happens if a signer dies, becomes incompetent, refuses to cooperate, loses key material, or becomes untrustworthy. These provisions are critical because the technology may not solve governance problems on its own.

If a two-of-three wallet loses one signer, the remaining two *may* (will depending on the legal arrangement terms) still be able to move assets. But the structure has lost redundancy. The remaining fiduciaries should be required to reconstitute the wallet or move the assets to a new wallet with a restored signer group. For example, the remaining two signers may establish a new two-of-three wallet with a replacement participant and transfer the assets to that new wallet. The governance documents should require prompt action so that a temporary loss of redundancy does not become a permanent risk.

The plan should also address records. The fiduciaries should maintain documentation of wallet addresses, authorization structures, signer identities, custody procedures, and transaction approvals. Without records, successors may not know which wallet holds assets, who must sign, or how authority is exercised.

The Fiduciary Risk Of Key Control

Cryptocurrency creates a sharper version of a familiar fiduciary problem. Trustees, investment trustees, and other fiduciaries are expected to control trust assets for beneficiaries. But if one person has sole access to a private key, that person may have the practical ability to steal or lose the assets. Legal duties, and traditional trust safeguards, may not prevent the loss and post-loss remedies may be inadequate.

This risk may cause institutional fiduciaries to hesitate before accepting responsibility for self-custodied cryptocurrency. Holding a private key is not the same as holding a statement for a brokerage account. The fiduciary must secure the key, prevent unauthorized access, maintain recovery processes, and avoid operational mistakes. A fiduciary who is not technically competent may expose the trust to unacceptable risk.

Individual fiduciaries present a different set of risks. A family member or friend may be trustworthy but lack technical sophistication. A technically sophisticated person may understand wallets and keys but may not understand fiduciary duties. A spouse may be considered as a trustee or signer, but marital dynamics and divorce risk may make that choice problematic in some plans. The proper selection of fiduciaries and signers is therefore a substantive planning decision, not merely an administrative detail.

The planning documents should distinguish between investment authority, distribution authority, custody authority, and technical signing authority. These roles may overlap, but they need not be identical in a directed trust structure. A person who can participate in a multi-signature wallet may be serving in a fiduciary capacity. The document should clarify the role so that authority, duty, compensation, liability, and succession are addressed.

The adviser should also consider whether signers should be bonded, insured, compensated, indemnified, or subject to standards of care specific to digital assets. These drafting issues cannot be resolved in the abstract, but the practical need to address them is clear. A plan that names signers without defining their responsibilities may create uncertainty.

The central planning tension is clear.

If the donor retains the only private key, the gift may not be complete. If the donor gives the key entirely to one trustee, the gift may be more complete but the asset may be exposed to trustee misuse or loss. If the donor divides control among several participants and remains one of them, the donor may retain a blocking or participatory control right. Might that make the transfer of cryptocurrency to the trust an incomplete gift? If the donor is excluded entirely, the client may feel uncomfortable relying on others.

This tension is not unique to cryptocurrency, but cryptocurrency may make it more nettlesome. Traditional trust planning often separates beneficial enjoyment, investment management, and distribution control. Digital asset planning adds another layer: transaction authority on the blockchain. The plan should specify not only who has legal authority but also who has the technical ability to exercise that authority.

A well-designed trust structure may use an irrevocable trust, a trustee who controls distributions, an investment fiduciary or adviser who directs investment policy, and a multi-signature wallet controlled by fiduciaries or technical signers who are not the donor. The donor may provide

information, preferences, or nonbinding guidance, but should not retain the practical ability to move the assets if completed gift treatment is desired.

The structure should also account for the possibility that beneficiaries or fiduciaries may need access after the donor's death or incapacity. The plan should avoid placing all knowledge in the donor's head or all access in the donor's devices. A technically complete transfer that becomes inaccessible because no one can find the wallet or key material may fail the family even if it succeeds doctrinally.

Staking And Ongoing Administration Inside A Trust

Some digital assets are inert from an income-generation standpoint, while others may be staked or otherwise used to generate rewards.

Staking is a method by which certain blockchain networks are secured through financial commitments. A participant locks digital assets into the network as collateral and, in exchange, may receive rewards for helping validate transactions and maintain network integrity. The staked assets (see below) are placed at risk because the participant may suffer economic penalties if network rules are violated. As a result, staking can transform an otherwise passive digital asset holding into an income-producing asset that may require ongoing fiduciary oversight, valuation, accounting, and tax reporting. If this is done, do the fiduciaries involved have the expertise to conduct these activities, or to monitor someone who is hired to do so?

Staking is a method by which certain blockchain networks are secured through financial commitments. A participant locks digital assets into the network as collateral and, in exchange, may receive rewards for helping validate transactions and maintain network integrity. The staked assets are placed at risk because the participant may suffer economic penalties if network rules are violated. Some blockchain protocols may impose penalties, sometimes referred to as "slashing." If a validator improperly validates transactions, signs conflicting versions of the blockchain, remains offline for extended periods, fails to perform required validation functions, or otherwise fails to comply with the protocol's operational requirements, penalties may apply. Thus, staking can transform an otherwise passive digital asset holding into an income-producing asset that may require ongoing fiduciary oversight, valuation, accounting, and tax reporting. It may change the income tax status as well. Advisers and fiduciaries should consider whether they possess the technical expertise necessary to evaluate staking risks. Where specialized expertise is lacking, prudent

administration may require the retention and oversight of qualified technical advisers, much as a trustee might retain investment, tax, or valuation professionals in other complex contexts.

Example: Assume your client owns $1,000,000 of Ethereum. Instead of simply holding the Ethereum as a passive investment, the owner may choose to "stake" it. Staking involves committing, or locking, Ethereum into the network's validation system. The owner may operate a validator directly or, more commonly, delegate the Ethereum staking to a third-party validator that performs the technical functions required by the network. In return for helping support the operation and security of the blockchain, the owner may receive additional Ethereum as compensation. Economically, this is somewhat analogous to earning interest on a bond or dividends on an investment, although the legal, tax, and economic characteristics are different. If the staking is delegated the income would be the difference between the staking fee and the cost charged by the firm handling the responsibilities.

To understand staking, it is helpful to understand what the blockchain network is attempting to accomplish. Unlike a bank, brokerage firm, or other centralized institution, many blockchain networks do not rely on a single trusted party to maintain transaction records. Instead, the network must continually determine whether transactions are valid and whether the ledger accurately reflects asset ownership. The network therefore needs a mechanism for confirming and recording transactions in a trustworthy manner.

For example, suppose John sends five Ether to Jane. Before the transaction can be permanently recorded, the network must confirm a variety of matters. Did John actually own the five Ether he is attempting to transfer? Did John already transfer those same Ether to someone else? Is the transaction properly authorized? Does the transaction comply with the network's rules? Should the transaction be added to the official record of ownership maintained by the blockchain? Validators participate in answering these questions and thereby in maintaining the integrity of the system.

In a proof-of-stake system such as Ethereum, validators are selected in part based on cryptocurrency that has been committed, or staked, to the network. The staked assets function as a form of economic collateral. Because the validator has assets at risk, the validator is incentivized to act honestly and follow the network's protocol. If a validator improperly

validates transactions, attempts to approve conflicting versions of the blockchain, remains unavailable for extended periods, or otherwise violates protocol requirements, the network may impose penalties that reduce the amount of cryptocurrency staked. This penalty mechanism is one of the ways in which the network seeks to promote accurate recordkeeping and discourage misconduct.

The estate planning implications can be significant. A trust that merely holds Ethereum as an investment may resemble a trust holding marketable securities. By contrast, a trust that stakes Ethereum is participating in an ongoing operational activity that generates rewards, incurs risks, and may require specialized monitoring. Fiduciaries may need to evaluate validator performance, review staking arrangements, monitor the risk of network penalties, account for rewards received, address valuation issues, and obtain appropriate tax reporting. Questions may also arise as to whether the trustee possesses sufficient expertise to oversee the activity directly or whether specialized digital asset advisers should be retained. In that regard, staking may create fiduciary considerations more analogous to overseeing an operating investment or specialized financial strategy than merely holding a passive asset.

Historically, some blockchain networks used a different model known as "proof of work." Under that approach, miners, rather than validators, performed the transaction verification function using computing power and substantial electricity consumption. Proof of stake replaces much of that computational competition with economic commitments from validators who place cryptocurrency at risk in exchange for the opportunity to earn rewards. Might staking activity cause the trust to cross from passive investment management into an active trade or business, thereby creating additional fiduciary, income tax, accounting, reporting, and administrative issues?

- Could staking income be characterized differently from passive investment income?
- Does the trustee have sufficient expertise to evaluate validator risk?
- Are specialized advisers required?
- How should staking rewards be accounted for?
- How should the activity be reported for income tax purposes?

Could the trust be viewed as conducting a business activity rather than merely holding an investment? For trust administration, staking raises practical questions.

- Who decides whether to stake?
- Who evaluates the risk of loss if the validator or participant fails to act properly?
- Who has authority to delegate staking activities? How are rewards tracked and reported?
- How are expenses accounted for?
- If the trust uses a custodian, does the custodian provide staking services?
- If the trust self-custodies, who has the technical ability to stake or unstake assets?

Some of the above considerations might be addressed in the governing trust document.

Mining, And Ongoing Administration Inside A Trust

Mining differs from staking which was described above in both function and operation. Instead of committing cryptocurrency as collateral, a mining operation uses specialized computer equipment to perform complex and massive calculations to verify transactions and add new blocks to the blockchain. When a miner successfully participates in creating a new block, the miner may receive newly issued cryptocurrency and transaction fees as compensation.

Consider a trust that owns Bitcoin. The trust could simply hold the Bitcoin as a passive investment, much as it might hold stock or bonds. Alternatively, the trustee might decide to participate in Bitcoin mining. To do so, the trust could purchase specialized mining computers, contract for electricity, obtain hosting facilities, hire technical service providers, and continually monitor the operation. The trust could then earn income, if successful, from mining rewards rather than solely rely on appreciation in the value of the cryptocurrency.

To understand mining, it is helpful to understand the problem the blockchain is trying to solve. The network must continuously verify transactions as discussed above. For example, if John transfers one

Bitcoin to Jane, the network must determine whether John actually owns the Bitcoin, whether the transaction has been properly authorized, and whether John is attempting to spend the same Bitcoin in another transaction. Mining is one of the mechanisms used to confirm these transactions and maintain a reliable and secure ledger of ownership.

In a proof-of-work system such as Bitcoin, miners compete by devoting computing power to solving complex mathematical problems. The first miner to successfully solve the required calculation earns the right to add the next block of transactions to the blockchain and receive a reward. Because participating requires substantial investment in computers, facilities, maintenance, and electricity, mining may more closely resembles an operating business than a passive investment activity.

The estate planning implications may be important. A trust that merely owns cryptocurrency is generally holding an investment asset. A trust that operates or participates in mining activities may be conducting a business and all the operational risks those entail. Trustees may need to determine whether the governing instrument authorizes such activities, whether participation is consistent with fiduciary investment standards, whether specialized advisers should be retained, and whether the activity creates additional accounting, tax reporting, regulatory, or business-management obligations.

Mining presents a different operational model involving hardware, electricity, and infrastructure. A trust holding a passive cryptocurrency investment is one thing. A trust operating or participating in mining infrastructure is another. Fiduciaries may need to evaluate whether the activity is an appropriate trust investment, whether it constitutes an operating business, and whether the trust instrument provides sufficient authority.

These issues demonstrate that cryptocurrency planning cannot end with the transfer. Administration may be ongoing and technically demanding. A trust that receives digital assets may need accounting systems, valuation processes, tax reporting procedures, cybersecurity controls, signing policies, and protocols for interacting with exchanges or custodians.

Blockchain Technology Also Has Broader Applications In Estate Planning

Practitioners should consider maintaining, or having the client maintain, an immutable record of personal instructions, letters of instruction, or

information intended to accompany estate planning documents. The concept is not necessarily to place the entire document publicly on a blockchain. Rather, the blockchain may serve as a system of record to prove that information has not been altered.

This concept may be especially relevant for tangible personal property. Family disputes often arise over items of emotional significance, such as watches, jewelry, art, family heirlooms, and other personal effects. These disputes may involve more emotion than monetary value. A will may list items, but that approach can become outdated. A separate list may be incorporated by reference, but disputes may arise over whether the list is current, authentic, or altered.

A blockchain-based record could, in concept, help establish provenance, timing, and integrity. If a client updates instructions regarding tangible property, a system that records the change in a tamper-evident manner may reduce later disputes. The beneficiaries may still argue about interpretation or fairness, but the evidentiary question of which instruction was last validly recorded may be easier to answer.

Tokenization Of Real-World Assets Is Another Emerging Area

Tokenization involves creating a digital token that represents ownership or rights in an underlying asset. Examples include tokenized shares of stock and the possibility of tokenizing personal property such as a watch.

For estate planning, tokenization could theoretically allow a client to identify a particular item and associate ownership or transfer instructions with a token. For example, a token could represent a specific watch, and instructions could specify which beneficiary should receive that token or the underlying property. The blockchain could serve as a system of record for the asset's representation and transfer history.

Tokenization should not be confused with legal effectiveness. A token representing a watch is only meaningful if the legal system, custodians, family members, or fiduciaries recognize the token as controlling or evidentiary. The practical utility of tokenization depends on the relationship between the digital record and the legal ownership of the underlying asset.

Practical Checklist For Advisers

- Identify the category of client. Is the client primarily an investor, active trader, DAO or token participant, operating business, staking participant, mining participant, or some combination of these roles?

- The adviser should inventory exchanges, wallets, custodians, tokens, NFTs, stablecoins, staking arrangements, mining activities, and any blockchain-enabled business operations. The inventory should distinguish between assets held on centralized platforms and assets held in self-custody.
- The adviser should determine who has private keys, where key material is stored, whether backups exist, whether anyone else has copies, and whether key access is consistent with the client's legal documents. This inquiry should be handled carefully because unnecessary disclosure of private keys can itself create risk.
- For proposed gifts, the adviser should analyze whether the donor will retain any practical ability to move the cryptocurrency after the transfer. If the donor retains the private key, the transfer may be vulnerable. If the donor remains a required signer, the donor may be retaining a blocking power. If the donor remains one of several optional signers, the retained control should be evaluated carefully (e.g., does the power make the gift incomplete).
- The adviser should consider whether a custodial trust account, a trustee-controlled wallet, a multi-signature wallet, or a hybrid structure is appropriate. The decision should reflect the amount involved, the client's philosophy regarding self-custody, the sophistication of fiduciaries, expected trading frequency, staking or operational needs, and tolerance for platform risk. If a multi-signature structure is used, the adviser should coordinate the wallet threshold with the legal governance structure. The documents should identify signers, define their roles, establish succession processes, require reconstitution if redundancy is lost, and address liability and standards of conduct.
- The adviser should ensure that income tax reporting systems are in place. A trust or entity receiving digital assets may inherit the need to track basis, holding period, rewards, transfers, and transaction character. Gift planning should not be separated from tax compliance.
- The adviser should also consider whether the client's estate plan includes instructions for locating digital assets after death or incapacity. The instructions should provide sufficient information for fiduciaries to identify assets without exposing private keys to unauthorized persons.

Tax Developments

Practitioners should be alert for new guidance and changes in the law, but need to be cautious about putting too much weight on proposals. A number of bills have made significant progress in Congress only to then stall. The recent Clarity Act is example: despite advancing substantially and going through a series of bipartisan changes, it failed to clear the Senate. Given the current political environment in Washington, no one can predict with much confidence whether any particular tax proposal will ultimately become law or, if it does, whether the final legislation will resemble the current proposal.

Conclusion

Cryptocurrency and digital assets require a more integrated planning process than many traditional assets. Legal ownership, tax reporting, custody, fiduciary governance, and technological control must be aligned. If any component is missing, the plan may fail as a tax matter, an administrative matter, or a practical matter.

The completed gift issue illustrates the larger point. A donor cannot rely solely on an assignment or entity transfer if the donor retains the private key that controls the cryptocurrency. Conversely, simply handing complete key control to one fiduciary may create unacceptable practical risk. Custodial platforms and multi-signature wallet structures may provide workable paths, but they require careful legal and technical design.

Digital asset planning is likely to become more common as cryptocurrency holders age, as digital wealth increases, and as blockchain-based business models expand. Advisers who understand both the legal doctrines, the technological mechanics and the estate and income tax implications will be better positioned to identify risks, design practical structures, and help clients transfer value in a manner that is both legally coherent and operationally secure.

The central lesson is that cryptocurrency planning must respect the reality of control. Whoever can move the asset has practical power over it. Estate planning documents should not ignore that reality. They should be drafted and implemented so that the legal plan and the blockchain mechanics point in the same direction.

HOPE THIS HELPS YOU HELP OTHERS MAKE A *POSITIVE* DIFFERENCE!

Karolis Matulis
Martin Shenkman
Thomas Tietz
Christine Pronek
Jonathan Blattmachr

CITE AS:

LISI Estate Planning Newsletter #3345, (October 27, 2026) at http://www.leimbergservices.com. Copyright © 2026 Leimberg Information Services, Inc. (**LISI**) Reproduction in Any Form or Forwarding to Any Person Prohibited - Without Express Permission. Our agreement with you does not allow you to use or upload content from **LISI** into any hardware, software, bot, or external application, including any use(s) for artificial intelligence technologies such as large language models, generative AI, machine learning or AI system. This newsletter is designed to provide accurate and authoritative information regarding the subject matter covered. It is provided with the understanding that **LISI** is not engaged in rendering legal, accounting, or other professional advice or services. If such advice is required, the services of a competent professional should be sought. Statements of fact or opinion are the responsibility of the authors and do not represent an opinion on the part of the officers or staff of **LISI**.

HELP US HELP OTHERS! TELL A FRIEND ABOUT OUR NEWSLETTERS.

Click Here for Special LISI Member Discounts on Webinars and eBooks