Steve Leimberg's Estate Planning Email Newsletter - Archive Message #3354

Date: **23-Nov-26**

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

Subject: **Shukla, Saini, Tietz, Shenkman & Blattmachr: Blockchain as Estate Planning Infrastructure - A Fully Developed Analytical Framework for Advanced Practitioners**

"Against this backdrop, the integration of technological infrastructure into estate planning may at some point not be optional. Blockchain technology, properly understood, offers a framework capable of addressing many of these vulnerabilities. The objective of this article is to examine in some detail how blockchain, and specifically the concepts of decentralization, cryptographic hashing, and conditional execution, may enhance estate planning systems by improving evidentiary reliability, facilitating asset discovery, reducing disputes, and enabling new forms of intergenerational communication. The potential power of these blockchain characteristics make it worthwhile for practitioners to begin to learn of these concepts and monitor how the law evolves with respect to them so that they can, as appropriate incorporate them as options in their estate planning practices."

Ishan Shukla, Deepak Saini, Thomas Tietz, Martin Shenkman and Jonathan Blattmachr provide members with commentary on how blockchain technology, and in particular cryptographic hashing, can be used to verify the existence and integrity of wills, trusts and other estate planning documents, and on what that means for lost wills, fraud, asset discovery and milestone-based communication with heirs.

Ishan Shukla is Co-Founder and Head of Strategy at BlockWill, a digital-inheritance platform that helps individuals and families record, protect, and transfer digital and traditional assets to their heirs. He writes and speaks frequently on the coming wave of private wealth transfer and the gap between on-chain assets and the legal frameworks needed to pass them on. His e-mail address is ishanshukla@blockwill.io.

Deepak Saini is the Founder and Chief Executive Officer of BlockWill, a digital estate-planning platform incorporated in the Dubai International

Financial Centre (DIFC). BlockWill uses zero-knowledge encryption and blockchain-backed verification to help clients protect and transfer cryptocurrency, digital accounts, property, and critical documents to their beneficiaries. He works with family offices and wealth managers on the secure succession of digital wealth. His e-mail address is deepaksaini@blockwill.io.

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

Martin M. Shenkman, CPA, MBA, PFS, AEP (distinguished), JD, is an attorney in private practice in Fort Lee, New Jersey and New York City whose practice concentrates on estate planning. He is the author of 44 books and more than 1,300 articles and is an editorial board member of Trusts & Estates Magazine. He holds a B.S. from the Wharton School, an MBA from the University of Michigan, and a law degree from Fordham University School of Law.

Jonathan G. Blattmachr is Editor-in-Chief and Co-Founder of InterActive Legal, a Principal in ILS Management, LLC, and a retired member of Milbank Tweed Hadley & McCloy LLP and of the Alaska, California and New York Bars. He is a Fellow and former Regent of the American College of Trust and Estate Counsel and a recipient of Bloomberg Tax & Accounting's Leonard L. Silverstein Award. He graduated cum laude from Columbia University School of Law and received his A.B. in mathematics from Bucknell University.

Here is their commentary:

EXECUTIVE SUMMARY:

Against this backdrop, the integration of technological infrastructure into estate planning may at some point not be optional. Blockchain technology, properly understood, offers a framework capable of addressing many of these vulnerabilities. The objective of this article is to examine in some

detail how blockchain, and specifically the concepts of decentralization, cryptographic hashing, and conditional execution, may enhance estate planning systems by improving evidentiary reliability, facilitating asset discovery, reducing disputes, and enabling new forms of intergenerational communication. The potential power of these blockchain characteristics make it worthwhile for practitioners to begin to learn of these concepts and monitor how the law evolves with respect to them so that they can, as appropriate incorporate them as options in their estate planning practices.

COMMENT:

Introduction

Practitioners are struggling to keep up with the pace of technological change. Many estate planning practitioners have still not adapted document generation systems and rely on more manual document preparation methods. Some firms still have components of their practices that are paper based instead of digital, while other firms have migrated to a fully paperless virtual model. In addition, many practitioners are struggling, and some even resisting, the use of AI in a fully integrated manner in their practices. Cybersecurity issues continue to grow and threaten practitioners. Blockchain is yet another technology that practitioners need to start learning about now. As with all other estate planning tech, ignoring these developments may only put the firm or practitioner further behind the technology curve which will reduce their ability to be profitable and to attract and keep clients.

Estate planning is undergoing a fundamental transformation. For centuries, the practice has relied on formal paper legal instruments as the exclusive mechanism for transmitting wealth and implementing client intent. Wills, trusts, beneficiary designations, and related documents have formed the core architecture of the discipline. While those instruments remain indispensable, the conditions under which they operate have changed. For example, PDF copies of documents in some instances are acceptable. The Uniform Electronic Wills Act provides: (4) “Record” means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.” Sec. 3 states: “An electronic will is a will for all purposes of the law of this state. The law of this state applicable to wills and principles of equity apply to an electronic will, except as modified by this [act].” This reflects the growing legal acceptance of electronic rather than purely paper records and may provide

an argument for a foundation for documents on the blockchain.[1] Remote and electronic signing of documents is slowly making inroads[2] But the estate planning legal environment may change even faster and more dramatically. Modern wealth is no longer confined to tangible property or local jurisdictions. It is increasingly digital, global, fragmented across platforms, and increasingly susceptible to technological risks that traditional legal structures were never designed to address.[3]

During Covid numerous exceptions for electronic and remote signing were enacted to deal with the urgency of being able to permit clients to sign documents in that environment. During the COVID-19 pandemic, estate planners were compelled to adapt longstanding document execution practices to unprecedented restrictions on in-person meetings. This led to emerging state emergency orders, remote notarization initiatives, electronic witnessing procedures, drive-through signings, outdoor signings, video-supervised executions, and other techniques designed to preserve the validity of estate planning documents while protecting public health. Those laws, even if temporary, demonstrated that legal systems could adapt traditional execution formalities to technological and practical realities without abandoning core safeguards against fraud, undue influence, and lack of capacity. The pandemic thus accelerated acceptance of electronic and remote execution methods and helped establish a foundation for broader modernization of estate planning practice.[4]

The consequence is that estate planning today faces a structural mismatch. The legal system continues to depend on written documents as the primary evidence of intent, yet those documents exist within an environment characterized by unprecedented exposure to loss, manipulation, and uncertainty. These risks are not merely theoretical; they arise repeatedly in practice and often result in disputes that undermine both family relationships and carefully constructed plans.

Natural disasters have repeatedly demonstrated the vulnerability of paper-based estate planning systems. Hurricanes, floods, fires, and other catastrophes have destroyed original wills and related records, creating significant probate complications when a decedent's original testamentary documents cannot be located. Following Hurricane Sandy, New York courts confronted precisely this issue. In *Matter of Certoma*, the Surrogate's Court admitted a copy of a will after concluding that the original had been destroyed by Hurricane Sandy rather than revoked by the testator. The case illustrates both the fragility of paper documents and the

legal complexity and expense that can result when original estate planning documents are lost due to forces beyond the testator's control. The ability to preserve authenticated digital copies may therefore provide an additional layer of protection against the risks posed by natural disasters.[5]

Against this backdrop, the integration of technological infrastructure into estate planning may at some point not be optional. Blockchain technology, properly understood, offers a framework capable of addressing many of these vulnerabilities. The objective of this article is to examine in some detail how blockchain, and specifically the concepts of decentralization, cryptographic hashing, and conditional execution, may enhance estate planning systems by improving evidentiary reliability, facilitating asset discovery, reducing disputes, and enabling new forms of intergenerational communication. The potential power of these blockchain characteristics make it worthwhile for practitioners to begin to learn of these concepts and monitor how the law evolves with respect to them so that they can, as appropriate incorporate them as options in their estate planning practices.

The Structural Weakness of Document-Centric Planning

Traditional estate planning rests on a relatively simple premise: that a properly executed document will be available, authentic, and accepted as evidence of intent at the time it is needed. This assumption underlies the entire system of testamentary transfers. Using lifetime trusts as opposed to wills may reduce this problem but the original trusts will still need to be maintained and accessed.

In reality, however, the system is far more fragile. Estate planners routinely encounter the following problems:

- Documents may be lost. Whether due to fire, flood, poor storage practices, or simple human error, original instruments frequently cannot be located when needed. Consider the growth in the number of severe natural disasters and the impact on estate planning documents as illustrated above.
- Documents may be destroyed. In some cases, destruction is accidental. In others, it may be deliberate, particularly where competing parties seek to alter distributions.
- Documents may be altered. Modifications may be subtle or overt, but even minor changes can have significant legal consequences.

- Documents may be replaced or superseded. New instruments may appear that conflict with prior versions, raising questions of authenticity, undue influence, or fraud.

These risks are magnified in the context of elder financial abuse. Vulnerable individuals may be manipulated into executing new documents, perhaps under conditions that are difficult to reconstruct after death.

The legal system has developed mechanisms to address these issues. Courts may admit copies of wills where the original is lost, provided sufficient evidence is presented. Witness testimony, circumstantial evidence, and forensic analysis may all play a role.[6] However, these solutions may sometimes be uncertain, time-consuming, and expensive. Consider the impact of the thousands of wills destroyed on 9/11 held by New York law firms. Admission of a copy of a paper wills relies heavily on human recollection and judicial interpretation rather than the objective verification that blockchain may provide. The 9/11 disaster became a powerful practical argument for redundant storage, digitization, off-site backups, and preservation of copies. That theme aligns closely with the point about blockchain-supported preservation of testamentary records. Recognize that the application of blockchain in these applications is new and will evolve over time. But that should not mean avoiding it; rather, it should instead suggest learning about the technology and adapting it as each practitioner feels comfortable, and as more guidance develops.

Blockchain: A New Model of Record Integrity

Blockchain technology introduces a fundamentally different paradigm for recordkeeping. Rather than relying on a single authoritative record maintained by a central party, such as an original signed paper will in an attorney's physical will vault, blockchain systems maintain identical copies of a ledger across a distributed network of participants. Each entry in the ledger is verified through computational processes and cryptographically linked to the previous entry.

For example, an estate planning attorney could generate a cryptographic hash of a client's signed will and record that hash on the blockchain. Years later, if the original will were lost in a flood, fire, hurricane, or office disaster, a copy can be compared to the blockchain record. If the hashes match, the blockchain provides some evidence that the copy is identical to the document that existed when the blockchain entry was made. Because each block is linked to the preceding block through cryptographic hashes, any attempt to retroactively alter the record would be readily detectable. The

other elements of proving a lost will still have to be met, but the blockchain evidence may be helpful to that effort.

The effect of this structure is to create immutability. Once a record is added to the blockchain, it cannot be altered without invalidating the subsequent chain of records. Because the ledger exists simultaneously across multiple independent systems, any attempt to modify a prior entry is immediately detectable due to inconsistency with the rest of the network. Contrast this with the above paper will. The elderly and infirm client is taken to a new lawyer by a predator and a new will is signed and retained by the new attorney. Will anyone even know of the prior will or prior attorney?

> An analogy that may be useful for practitioners is to consider blockchain as a universal, continuously updated ledger that exists in thousands of synchronized copies. Imagine that every major law firm, bank, trust company, court, and title company maintained an identical copy of the same ledger and updated it simultaneously whenever a new entry was added. If someone attempted to alter an entry on one copy, the alteration would immediately become apparent because that version would no longer match the thousands of other copies. Blockchain operates in a similar manner. Rather than depending on a single institution to maintain the authoritative record, the system relies on a network of participants that collectively validate and store the information. Each new entry is mathematically linked to previous entries through cryptographic techniques that function much like a digital fingerprint. If someone attempts to change a historical record, the digital fingerprint changes as well, making the alteration detectable. The integrity of the system is therefore maintained not by placing trust in a single custodian, law firm, bank, or governmental agency, but by the ability of the network as a whole to verify that all copies remain consistent with one another. From an estate planning perspective, this is one of blockchain's most significant attributes: it can create a durable, tamper-evident record that is not dependent on the preservation of a single original document or the continued existence of any particular repository.

For estate planning, this will be transformative. It creates the possibility of a record of client intent that is not dependent on a single physical document,

location, or custodian. Instead, it exists as a verified, tamper-evident record accessible across time and geography.

Hashing and the Concept of the Document Fingerprint

The practical application of blockchain to estate planning depends on the concept of “hashing”. A hash function is a mathematical process that takes a document of any length, whether a two-page power of attorney or a one-hundred-page trust agreement, and converts it into a fixed-length string of characters. That string is commonly described as a digital fingerprint. Although the fingerprint may appear to be nothing more than a random series of letters and numbers, it serves an important evidentiary function because it is uniquely tied to the contents of the document from which it was created. A hash is thus somewhat analogous to a person’s fingerprint: it can be used to identify a document with extraordinary precision, but it cannot be used to reconstruct the document itself.

Several characteristics of hashing are particularly important for estate planners. First, the fingerprint is unique to the exact contents of the document. For example, if a signed will is converted into a scanned PDF document whose hash is generated on the date of execution, that hash will correspond to that specific version of the will and no other. Second, the process operates in only one direction. A hash can be created from the document, but someone who possesses only the hash cannot reverse the process and recreate the will, trust, or other legal instrument. This is important because sensitive estate planning documents can be authenticated without publicly disclosing their contents.

Third, even the smallest change to a document produces an entirely different hash value. If a testator’s surname is corrected, a beneficiary designation is changed, or even a single comma is added or deleted, the resulting hash will be dramatically different. This feature makes hashes useful as evidence of document integrity. If an attorney generates a hash of a client’s will on the date the will is executed, and years later a copy of that will is presented for probate, the hash of the scanned PDF copy of the will generated earlier provides the timestamped immutable evidence that this document was created at a particular date & time, which when compared to the original Will proves the document’s authenticity. If the electronic document is produced before the Court, it provides strong evidence that the copy is identical to the document that existed when the original hash was created on the blockchain. If the hashes do not match, it indicates that the

document has been altered, intentionally or inadvertently, sometime after the original record was made.

A practical analogy may help. Imagine that when a will is signed, the attorney creates a detailed inventory of every character, word, space, punctuation mark, and formatting element contained in the document and compresses that information into a unique identification number. That identification number is then securely recorded. Years later, even if the original will has been lost in a fire, flood, hurricane, cyberattack, or other disaster, the attorney can compare the identification number generated from the surviving copy to the previously recorded number. If they match exactly, that is powerful evidence that the copy is the same document that existed at the earlier point in time. Hashing therefore provides a mechanism for verifying authenticity and integrity without requiring the original document itself to remain continuously available.

In a blockchain-based system, the hash of a document, not necessarily the document itself, may be recorded on the blockchain together with a date and time stamp. Because blockchain records are distributed across many participants and protected by cryptographic safeguards, later alteration of that record becomes extremely difficult. For estate planners, the practical value is not that blockchain replaces wills, trusts, or traditional execution formalities. Rather, blockchain may provide an additional means of proving that a specific document existed in a particular form at a particular point in time and that its contents have not subsequently been altered.

These properties make hashing a potentially useful tool for verifying document integrity. By calculating the hash of a document at a specific point in time and recording that hash on a blockchain, practitioners create a permanent, time-stamped record of that document's exact contents.

Example: Consider the risks of multiple wills and poor document control in Aretha Franklin's estate. After her death, it was initially believed she had died intestate (without a will) but later multiple handwritten wills were discovered in various locations and with conflicting provisions. Litigation followed over which document constituted her valid will, and courts were required to determine which writing reflected her final testamentary intent. Consider alternatively the impact if each will had been posted confidentially to the blockchain with a hash or fingerprint preventing alteration. Each such posting would have a date stamp. Would that have avoided litigation? Even if not, it may have limited [7]the scope, costs and family damage.

The document itself does not need to be stored on the blockchain. Instead, it can remain private, stored in a secure repository. At any later time, the document can be re-hashed and compared to the original fingerprint. If the two match, the document has not been altered. If they differ, the document has been changed.

This approach resolves a central tension in estate planning: the need to preserve confidentiality while ensuring authenticity. Only the fingerprint is public; the document remains private. Yet its integrity is independently verifiable.

Also, if the attorney involved prefers to hold the original will in the law firm's will vault that can be done, and a copy posted to the blockchain where the fingerprint is public to assure no tampering. But the copy of the will and all its terms remain private. If the attorney involved is skeptical of posting to the blockchain and does not do so, and if that attorney continues to hold the original signed will, what risk exists?

Evidentiary Implications: From Subjective Proof to Objective Verification

The introduction of blockchain-based hashes has significant implications for evidentiary practice. Traditional probate disputes often turn on questions of authenticity and intent, with courts relying on testimony and circumstantial evidence to resolve conflicts.

A blockchain hash provides a new form of evidence. It establishes that a document existed in a specific form at a particular time and that its contents have not been altered since that time. This adds an objective, mathematical dimension to what has historically been a subjective inquiry.

Consider the familiar scenario of a lost will. A practitioner may present a copy and seek admission based on witness testimony and other evidence. A corresponding blockchain hash might strengthen this argument by demonstrating that the copy matches a document that was recorded at the relevant time.

Similarly, where competing documents are presented, the existence of a blockchain record for one version but not the other may become a significant evidentiary factor. While not dispositive, it would influence the assessment of authenticity. And likely over time law will develop that will define and refine the evidentiary weight to be given.

Fraud, Undue Influence, and the Problem of Late-Stage Documents

The risks associated with fraudulent wills and undue influence are well known. What is new, and worrisome, is the ease with which convincing documents can be created using modern technology. Digital tools, and increasingly artificial intelligence, enable the production of documents, and even videos, that appear authentic but may not reflect the true intent of the decedent.

Blockchain-based recordkeeping may offer a mechanism to reduce these risks. By recording a document's fingerprint following execution, a baseline may be established. Any subsequent document can be evaluated against that baseline.[8]

If a later document emerges without a corresponding history of recorded hashes, or if its fingerprint differs from that of a previously recorded document, questions arise regarding its legitimacy. A cryptographic hash provides evidence that a later copy is identical to the version that was originally hashed. This does not eliminate the need for legal analysis, but it provides some evidentiary anchor.

A hash may thus help establish:

- existence of a document at a point in time;
- integrity of a document;
- that a later copy matches an earlier version;
- that a file has not been altered after hashing.

But a hash cannot independently establish:

- testamentary capacity;
- due execution;
- freedom from undue influence;
- nonrevocation;
- testamentary intent.

Thus, blockchain hashes may be helpful even if they cannot address all potential issues, and even as the law continues to develop.

As to nonrevocation, blockchain evidence may provide additional support for the argument that a will was not revoked. If the attorney and client establish a practice that any revocation, amendment, codicil, or replacement will is to be accompanied by a corresponding blockchain entry, the absence of any later blockchain record reflecting such action may

constitute evidence consistent with continued validity of the original instrument. For example, if a hash of a will was recorded on a blockchain at execution and the blockchain thereafter contains no record of a later will, codicil, or revocation document, that absence may support the contention that the original instrument remained operative. However, blockchain evidence would not by itself conclusively establish nonrevocation, as a testator might revoke a will through legally effective means without creating a corresponding blockchain record. Accordingly, blockchain evidence should generally be viewed as corroborative evidence rather than as a substitute for the traditional proof required under applicable lost-will statutes and probate law.

The absence of a subsequent blockchain entry reflecting a later will, codicil, or revocation may be analogous to the absence of evidence that a client returned to counsel to modify an estate plan. While not conclusive, it may constitute circumstantial evidence supporting an inference of continued testamentary intent.

Beyond the Will: A System of Interrelated Documents

A critical insight for practitioners is that estate planning is not defined by a single document. In most cases, a client's intent is expressed through a network of instruments, each governing a different aspect of asset disposition.

These may include revocable trusts, irrevocable trusts, entity agreements, beneficiary designations, and letters of instruction. Each document may be subject to modification over time, and conflicts may arise among the various versions.

Blockchain infrastructure allows each of these documents to be independently hashed and recorded. As changes occur, new fingerprints are generated and appended to the chain. The result is a chronological record of the entire planning process.

This versioning capability may be particularly valuable. It allows practitioners and courts to reconstruct the evolution of a plan, providing context for interpreting intent and potentially resolving disputes.

Dynamic Planning in a Changing World

One of the most significant limitations of traditional estate planning is its static nature. Documents are often updated infrequently, even as the client's circumstances change.

Blockchain-enabled systems allow for more dynamic planning. Lists, instructions, and even certain documents can be updated regularly, with each update recorded as a new entry. This creates a living record that evolves with the client's life.

Such a system does not replace formal legal instruments, but it may complement them by providing a more granular, continuously updated record of intent.

Asset Discovery: Existence, Location, and Access

In practice, one of the greatest challenges in estate administration is simply identifying and accessing assets. The problem may be divided into three questions: does the asset exist, where it is located, and how it can be accessed.

Failure to answer any of these questions can result in assets being overlooked or lost. This problem is particularly acute with digital assets, which may not leave a paper trail.

Blockchain-based systems can store structured inventories addressing these issues. Each version of the inventory is recorded, creating a verified history of assets, locations, and access mechanisms.

This approach not only facilitates administration but also provides evidence of what assets existed at a given time, which may be relevant in disputes.

Tangible Personal Property: A Potential Source of Conflict

Disputes over tangible personal property can be the most emotionally charged in estate administration. Items of sentimental or financial value often become points of contention, particularly when documentation is unclear. Traditional approaches rely on lists, either incorporated by reference or maintained informally. These lists are vulnerable to the same risks as other documents: loss, destruction, and manipulation.

Hashing these lists and recording them may provide a more reliable system. Each version is preserved, and the operative version can be identified with certainty.

Trigger Mechanisms and Conditional Distribution

Another important concept is the use of trigger mechanisms. Information and instructions can be released upon the occurrence of specified events, such as death or incapacity.

The role of the trigger person is distinct from that of a fiduciary. This individual confirms that the triggering event has occurred but does not necessarily have access to the underlying information.

This separation enhances both privacy and security. It ensures that sensitive information is not prematurely disclosed while still enabling timely execution.

Example: A mother creates three separate digital letters of instruction for her daughter. The first contains family history, expressions of love, and guidance concerning the family's values and traditions and is released upon the mother's death. The second contains more sensitive information about family relationships, health history, and the mother's reasons for structuring her estate plan in a particular manner. The mother believes that this information may be better understood after the passage of time, so it is programmed to be released five years after her death. The third letter addresses the daughter's future inheritance, financial responsibilities, and long-term stewardship of family wealth and is released only when the daughter attains age fifty. A designated trigger person, perhaps the family's attorney, accountant, or trust protector, merely verifies that the applicable triggering event has occurred. The trigger person does not have access to the contents of the letters and cannot alter them. Once the specified condition is satisfied, the system automatically releases the appropriate communication.

The later letters might address subjects that many clients are uncomfortable discussing during life and be designed to be released at appropriate ages or life milestones:

- Why one child received a larger inheritance.
- Explanation of a family business succession plan.
- Information regarding an adopted child, donor conception, or other sensitive family matter.
- Explanations of discretionary trust provisions.
- Guidance to future trustees or beneficiaries.
- Family investment philosophy and philanthropic goals.
- Medical, genetic, or health information that may become relevant later.

Security: Moving Beyond Passwords

Traditional security methods have well-documented limitations. Passwords are vulnerable, and even two-factor authentication can be compromised.

More advanced methods, including biometric verification and hardware security keys, provide stronger protection. As estate planning increasingly intersects with digital assets, such measures become essential.

Milestone-Based Communication and the Transmission of Values

Estate planning is not only about wealth transfer but also about the transmission of values. The ability to deliver communications at specific milestones, as illustrated above, provides a new dimension to planning.

Letters, videos, and other messages can be preserved and delivered when beneficiaries reach certain ages or events. This creates a structured approach to intergenerational communication.

Authenticity in the Era of Deepfakes

The rise of artificial intelligence introduces new risks. Audio and video recordings can be manipulated convincingly. Hashing provides a mechanism to verify authenticity, ensuring that such communications can be trusted.

Professional Implications: The Risk of Inaction

A final point is the broader implication for the profession. Technology will continue to evolve, and clients will expect solutions that address modern risks.

Practitioners who fail to engage with these developments risk being displaced by those who do. The integration of technological infrastructure is likely to become a defining feature of advanced estate planning.

Conclusion

Blockchain represents an opportunity to strengthen the infrastructure underlying estate planning. By providing immutable, verifiable records, it addresses many of the weaknesses inherent in traditional systems.

For sophisticated practitioners, the challenge is to integrate these tools thoughtfully, preserving the strengths of established doctrine while enhancing reliability and adaptability.

Appendix: An Important Note on "How Blockchain Protects Your Will"

When your original will is scanned, that scan (PDF) is hashed and recorded on the blockchain exactly once. Think of the hash as a unique digital fingerprint: it belongs to that specific file, created at that specific moment, and it can never be altered.

One subtlety worth understanding: if you were to scan the same physical will again later, the new scan would produce a *different* fingerprint, even though it's the same document. That's why only the original scan is anchored on the blockchain, and why it becomes the single, permanent point of reference.

This gives you protection in two situations:

Scenario 1: The original will still exists. The blockchain fingerprint proves that the PDF is the exact document created on a specific date and time. It can be compared with the physical will word for word, character for character, confirming the will is genuine and unaltered.

Scenario 2: The original will is lost or destroyed. Even without the physical document, the blockchain fingerprint still proves that this PDF existed in exactly this form on that date and time. The digital copy stands as tamper-proof evidence of what the will said and when it was recorded.

In short: the blockchain doesn't store your will itself, it stores undeniable proof of *what* the will said and *when* it existed. Whether the paper survives or not, the truth of the document does.

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

Ishan Shukla
Deepak Saini
Thomas Tietz

Martin Shenkman
Jonathan Blattmachr

CITE AS:

LISI Estate Planning Newsletter #3354 (November 23, 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**.

CITATIONS:

1. *Uniform Electronic Wills Act* § 2(4), § 3 (Unif. L. Comm'n 2019).
2. *Uniform Electronic Wills Act* §5 (Unif. L. Comm'n 2019).
3. Wesley Brandi & Deborah Hoffman, Digital Assets and Estate Planning: Preventing and Resolving Trust and Probate Challenges, Prob. & Prop., Jan./Feb. 2026, American Bar Association.
4. Martin M. Shenkman, Jonathan G. Blattmachr, Andrew Wolfe & Thomas A. Tietz, On the Slow Return to the New Normal and Different Approaches to Signing/Executing Estate Planning Documents, Steve Leimberg's Estate Planning Newsletter No. 2794 (May 11, 2020); Martin M. Shenkman, Jonathan Blattmachr, Andrew Wolfe & Thomas Tietz, Different Approaches to Signing/Executing Estate Planning Documents, Steve Leimberg's Estate Planning Newsletter No. 2799

(June 11, 2020); Martin M. Shenkman, Jonathan Blattmachr, Andrew Wolfe & Thomas Tietz, Different Approaches to Signing/Executing Estate Planning Documents, Steve Leimberg's Estate Planning Newsletter No. 2803 (July 1, 2020).

5. Matter of Certoma, 55 Misc. 3d 908, 51 N.Y.S.3d 385 (Sur. Ct. Queens Cnty. 2017).
6. New York law, SCPA § 1407 permits probate of a lost or destroyed will if the proponent can establish: (1) that the will was not revoked, (2) that it was duly executed, and (3) the contents of the will can be proven through a copy or other competent evidence.
7. Reid Kress Weisbord & David Horton, "Why a Handwritten Will Found in Aretha Franklin's Couch Got R-E-S-P-E-C-T from a Jury," The Conversation (July 13, 2023).
8. Federal Rule of Evidence 902(14) recognizes authentication of copied electronic data through a process of digital identification, such as a cryptographic hash.

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

Click Here for Special LISI Member Discounts on Webinars and eBooks