ACTEC Law Journal

Volume 48 | Number 1 Article 5

9-1-2022

Privacy in Plain Sight: How Blockchain Assets and Decentralized Technology Can Increase Privacy in Inheritance

Tye J. Cressman

Privacy in Plain Sight: How Blockchain Assets and Decentralized Technology Can Increase Privacy in Inheritance

*Tye J. Cressman**

I. Introduction and Central Question

The first Bitcoin currency was minted in 2009, giving rise to a new and exciting class of assets.[1] In the years since, this asset class has expanded to include other cryptocurrencies, fungible tokens that operate much like cryptocurrencies, and non-fungible tokens (NFTs) that operate in many different ways.[2] Collectively, this class of assets can be referred to as "Blockchain Assets," since ownership of the underlying asset and transaction history is all stored on decentralized ledgers, referred to as *blockchains*.[3]

Owner privacy was immediately hailed as a primary benefit of the technology's decentralized nature.[4] The claim was paradoxical on its face, since all transactions on blockchain networks are public, albeit anonymous.[5] That paradox gifts us several questions when regarding the obligations typically required of a fiduciary in the post-mortem context, be it Trustee or Executor. These questions become even more interesting when we consider the increasing popularity of Decentralized Autonomous Organizations (DAOs, for short), which permit individuals to anonymously organize via blockchain networks, and are increasingly used by blockchain financial entities as a stand-in for traditional corpo-

---

* Certified in Elder Law by the National Elder Law Foundation.

1 *See* Usman W. Chohan, *A History of Bitcoin*, *in* Discussion Paper Series: Notes on the 21st Century 1, 9 (2022).

2 *See id.* at 3, 6, 18.

3 Adam Hayes, *Blockchain Facts: What is It, How it Works, and How it Can be Used*, Investopedia (Sept. 18, 2022), https://www.investopedia.com/terms/b/blockchain.asp [https://perma.cc/Q756-ZQWM]. The reader should be aware that many separate blockchains exist, each comprised of separate blocks of date and possessing unique characteristics. *See* Chohan, *supra* note 1, at 7. This paper involves most prominently the Bitcoin blockchain and the Ethereum blockchain.

4 *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 6 (2009), https://bitcoin.org/bitcoin.pdf.

5 *See id.*

rate structures.[6] This article seeks to explore the blockchain privacy paradox within the context of inheritance planning possibilities presented by Blockchain Assets and, secondarily, ask how this developing technology may impact the role of post-mortem fiduciary, as it pertains to inheritance of Blockchain Assets.

II. Blockchain Assets, Explained

The challenge of Blockchain Assets, for many estate planners, is simply understanding the underlying elements of this asset class. The value of achieving such understanding cannot be overstated: with Bitcoin currency alone achieving current market capitalization of $450,000,000,000 USD and more than 81,000,000 unique owners,[7] it is clear that many people are allocating resources to this asset type.[8]

The term "Blockchain technology" can be somewhat off-putting, so readers are invited to use the analogy of their local courthouse to understand how blockchain ledgers interact with each other. The courthouse has various offices, all of which are public and accessible. Within those offices are multiple individual ledgers of information, including (1) deeds in the Register's Office, (2) real estate tax filings in the Assessment Office, and (3) boundary descriptions in the Planning Office. Because many people own real estate, pay real estate taxes, and your county reviews boundary descriptions, the individual files within the file cabinets of those offices will often correlate and verify each other. The information contained in those offices is stored in ledgers, regularly updated by courthouse personnel.

Now let's make this courthouse a bit more efficient (and accurate). For a moment, pretend that every time a deed is recorded, that change is *immediately* reported to every office in the courthouse and must verify the accuracy of its details with all of those offices. If any office cannot verify the accuracy of the deed, the transaction does not happen. If the accuracy of the deed is true across the board, the entire courthouse is updated immediately and automatically. All offices accept the change as true.

---

[6] *See* Nathan Reiff, *Decentralized Autonomous Organization (DAO)*, Investopedia (July 11, 2022), https://www.investopedia.com/tech/what-dao/ [https://perma.cc/UXN4-R9UG].

[7] *See Historical Data for Bitcoin*, CoinMarketCap, https://coinmarketcap.com/currencies/bitcoin/historical-data/ [https://perma.cc/FPQ3-FKS3] (showing Bitcoin's overall achievements in the current markets).

[8] *See* Raynor de Best, *Bitcoin (BTC) Blockchain Size as of July 11, 2022*, Statista (July 27, 2022), https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ [https://perma.cc/BG2W-BFQA]. Note this represents only wallets created through www.blockchain.com. *Id.* When combined with other custodial and non-custodial wallets, the actual number is likely several multiples of this.

Notice how the offices function together as links on a chain of information. The courthouse offices are *blocks*, and the interlocking verification of information creates a chain of shared accuracy between them that is automatic and constantly updated.[9] It's a blockchain, and it's easier to understand than many people think, at least on a basic level.[10]

Central to the issue of privacy is that ownership of financial assets typically requires significant information about an owner, while ownership of Blockchain Assets does not.[11] For example, investing in a mutual fund or purchasing stock will require disclosure of considerable personal information before ownership can take place. Ownership of Blockchain Assets is typically recorded on an owner-specific ledger that is identified by a unique 26 to 35-character series of numbers and letters. [12] This alphanumeric sequence is all that identifies a user's wallet individually. There are no names, addresses, telephone numbers, social security numbers, or other identifying information associated with the individual owner. This personalized (and relatively anonymous) ledger is often referred to as an owner's "wallet," although that term can be misleading.

Certain companies that assist users in acquiring Blockchain Assets may require customers to provide information in a manner similar to traditional financial institutions.[13] These are sometimes referred to as "custodial" wallets[14] and obviously reduce the significant privacy enjoyed by owners maintaining a "non-custodial" ledger of their own creation.

Any blockchain asset transaction is public in nature, albeit identified only by the alphanumeric wallet identifier. Each time a transaction involving any blockchain asset takes place, it is a public transaction, able to be seen by anyone with access to the internet.[15] However, unless an-

---

9 *See* Paul Gambles, *Even Bitterer Coins & Unstable Coins*, MBMG GRP. (May 23, 2022), https://mbmg-group.com/article/even-bitterer-coins-unstable-coins [https://perma.cc/E5NG-Y6M6] (Examples provided were translated to the courthouse analogy).

10 *See id.*

11 *See* Jorge B. Bernabe et al., *Privacy-Preserving Solutions for Blockchain: Review and Challenges*, 7 IEEE ACCESS 164908, 164908-09 (2019).

12 Kai Sedgwick, *Everything You Should Know About Bitcoin Address Formats*, BITCOIN.COM, (Feb. 18, 2019), https://news.bitcoin.com/everything-you-should-know-about-bitcoin-address-formats/ [https://perma.cc/4JSW-6WQL].

13 *See* Nakamoto, *supra* note 4, at 6.

14 *See, e.g.*, *Custodial vs. Non-Custodial Wallets*, CRYPTO APIs (June 22, 2022), https://cryptoapis.io/blog/92-custodial-vs-non-custodial-wallets#:~:text=with%20a%20custodial%20wallet%2C%20a,of%20platforms%20providing%20custodial%20wallets [https://perma.cc/2WK2-CPCG].

15 *See* Nakamoto, supra note 4, at 6. Popular websites such as *www.blockchain.com/explorer* provide a running list of all blockchain asset transactions, separable by the different currency or token being transacted. BLOCKCHAIN.COM, http://www.blockchain.com/explorer [https://perma.cc/V854-D3ED].

other person knows the exact character identifier for a wallet address partaking in a transaction, it is essentially anonymous.[16]

Numerous websites track ongoing Blockchain Asset transactions and make them readily available for view.[17] This real-time ability to observe transactions has led, in a very short time, to a complex decentralized finance industry that permits lending, borrowing, and price exchange arbitrage for various cryptocurrencies and tokens.[18] As a result, any interested party is able to know what is taking place, but does not know who the other transacting parties are unless a party's public wallet address is known to others.[19]

III. Decentralized Autonomous Organizations, Explained

As originally envisioned by Vitalik Buterin, Ethereum blockchain co-founder, a Decentralized Autonomous Organization ("DAO") is an entity where the membership collectively makes decisions, based on an agreed-upon decision-making model.[20] In many ways, a DAO can mimic "the legal trappings of a traditional company . . . but using only cryptographic blockchain technology for enforcement."[21] Currently, such organization models are used for many purposes, often to manage decentralized finance, such as MakerDAO[22] or Aave Protocol.[23] However, numerous other applications exist. The underlying characteristic of each is that members vote on proposals governing the organization and actions within the organization, and that membership is evidenced by token ownership rather than stock.[24]

---

16 *See* Nakamoto, *supra* note 4, at 6.

17 *See, e.g.*, *Where to Track Cryptocurrency Transactions?*, Bitstamp (Aug. 5, 2022), https://www.bitstamp.net/learn/blockchain/where-to-track-cryptocurrency-transactions/ [https://perma.cc/CC5J-XSQP].

18 *See The Continued Growth of Decentralised Finance*, BCB Grp. (Mar. 15, 2022), https://www.bcbgroup.com/the-continued-growth-of-decentralised-finance [https://perma.cc/C9GN-8ECJ].

19 *See* Nakamoto, *supra* note 4, at 6.

20 Vitalik Buterin, *Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform*, Ethereum (2022), https://ethereum.org/en/whitepaper/ [https://perma.cc/67FV-RKCE].

21 *Id.*

22 *The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System*, MakerDAO, https://makerdao.com/en/whitepaper/#abstract [https://perma.cc/U38N-YVAF].

23 *Aave Document Hub*, Aave, https://docs.aave.com/hub/ [https://perma.cc/MU4C-CZBG].

24 *See* David Shuttleworth, *What Is A DAO and How Do They Work?*, Consensys Blog (Oct. 7, 2021), https://consensys.net/blog/blockchain-explained/what-is-a-dao-and-how-do-they-work/ [https://perma.cc/SM9L-A7DL].

As mentioned above, many decentralized finance operations are being organized as DAOs. These organizations carry out complex decentralized finance operations, such as lending and borrowing assets, and so the capabilities of the organization can be similar to those of a traditional finance company.[25] Instead of a shareholder agreement, however, the rules of the organization (such as governance and voting) are coded to the blockchain.[26] Like other blockchain processes, participation can be anonymous because membership is tied only to token ownership — as opposed to name and Social Security Number — depending on the DAO.[27]

Liability considerations for DAO membership are developing rapidly and are mostly uncertain at the present time. At least one state, Wyoming, has granted legal company status to DAOs, which provides some framework for their treatment under state law.[28] In the case of Wyoming, this allows qualifying DAOs to limit liability of members if the DAO is formed as a Limited Liability Company, rather than treatment as a general partnership.[29] Other organizations, such as the dYdX Foundation, seek treatment as Non-U.S. Trusts for DAO formation.[30]

What is clear from the above examples is that a DAO could: (1) receive and hold Blockchain Assets; (2) engage in financial transactions according to protocols established by membership; and (3) distribute Blockchain Assets to other ledgers/wallets. More so, these actions seem able to be carried out with the typical anonymity enjoyed by Blockchain Asset owners. While the concept is largely unexplored, the question estate planning attorneys must ask themselves is: why can't a DAO serve as a Trustee?

IV. The Problem and the Promise of Blockchain Assets, as it Pertains to Privacy

Blockchain Assets do not lend themselves to traditional administration approaches because of their decentralized nature. First, while an owner's ownership of Bitcoin is evidenced on the owner's ledger (his or her personal wallet), there is not necessarily any central authority which

---

25 *See AAVE Protocol Whitepaper V2.0*, at 1 (Dec. 2020), https://cryptorating.eu/whitepapers/Aave/aave-v2-whitepaper.pdf.

26 *See* Shuttleworth, *supra* note 24.

27 *See id.*

28 Joshua T. Lewis & Robert L. Zeglarski, *Wyoming Paves Way for DAO Legal Company Status*, Frost Brown Todd LLC (Aug. 2, 2021), https://frostbrowntodd.com/wyoming-paves-way-for-dao-legal-company-status/ [https://perma.cc/RJ88-HAE5].

29 *Id.*

30 *See Legal Framework for Non-U.S. Trusts in Decentralized Autonomous Organizations*, dYdX Found., (Mar. 15, 2022), https://dydx.foundation/blog/legal-framework-non-us-trusts-in-daos [https://perma.cc/A7SW-3S2F].

manages this ledger. In the event an owner of Blockchain Assets holds those assets in a non-custodial wallet, there is no management organization. Thus, even if a fiduciary is appointed for the deceased owner's assets, there is no entity who can authorize transfer, other than the deceased owner or someone holding the person's password or passphrase.[31]

But maybe we don't need a fiduciary here—at least, in the traditional sense. After all, Blockchain Assets are computer code, which is more flexible than fiat currency. Vitalik Buterin has described one of the applications of cryptocurrency as "digital assets being directly controlled by a piece of code implementing arbitrary rules . . . ."[32] The "arbitrary rules" programmed into such cryptocurrency code are often referred to as "smart contracts."[33] Such smart contract programming should make it feasible to program inheritance protocols directly into the code of various cryptocurrencies and tokens.[34]

A simple example may help illustrate this point. Assume that an owner of 100 Ether (the native Ethereum blockchain currency) holds his Ether in a non-custodial ledger/wallet that is programmed to distribute that Ether to a *different* ledger/wallet if the owner fails to access his ledger/wallet at least once every 60 days. Again, his ledger/wallet is just a coded function that is programmed to the decentralized blockchain network. The user in this example does, in fact, die, and after 60 days, his Ether is distributed automatically to the recipient ledger/wallet. The programmed function is complete, the transaction has occurred, and the blockchain ledger has been updated publicly, showing that 100 Ether was transferred on a specific date from ledger #000x123 to ledger #000x128.

While Bitcoin is more basic in its functionality, various other cryptocurrencies and tokens possess the complexity to have this exact function encoded *directly into the asset itself*.[35] In either example (an encoded ledger/wallet function or when the asset itself is coded with

---

31 *See* Nathaniel Rich, *Ponzi Schemes, Private Yachts, and a Missing $250 Million in Crypto: The Strange Tale of Quadriga*, VANITY FAIR, (Nov. 22, 2019), https://www.vanityfair.com/news/2019/11/the-strange-tale-of-quadriga-gerald-cotten [https://perma.cc/8EMG-CQRF].

32 Buterin, *supra* note 20.

33 *See id.*

34 *See, e.g.*, Toshendra Kumar Sharma, *Best Performing Languages to Build Smart Contracts*, BLOCKCHAIN COUNCIL (June 23, 2022), https://www.blockchain-council.org/blockchain/best-programming-languages-to-build-smart-contracts/ [https://perma.cc/JJ37-EQY5]. *See also Digital Inheritance, Secured: Providing the Management, Protection, and Distribution of Digital Assets to Designated Shareholders*, INHERITI, https://inheriti.com/ [https://perma.cc/X8PY-GYFL]. Several companies are presently experimenting with this type of programming. *Id.*

35 *See* Buterin, *supra* note 20.

inheritance protocols), there is no person or entity responsible for effecting the transaction, although there would appear to be a natural beneficiary. The automatic nature of this distribution feels somewhat similar to beneficiary designations that allow certain assets to avoid probate, however the transfer would happen without any financial company or custodian required to approve the transaction.

Finally, as introduced earlier, it seems inevitable that DAOs will begin fiduciary management of Blockchain Assets for decedents since they already do so for living persons. Certainly, DAOs currently engaging in decentralized finance increasingly resemble traditional financial institutions. More interesting may be the ability of smaller groups of people – a family, for example – to create DAOs to manage family investments and inheritance, specific to their inheritance planning desires. Based on what is presently available, it does not seem far-fetched to create a DAO whose governance protocols resemble those of a multigenerational trust. The major difference is that the participants are identified only by unique public wallet addresses.

V. The Future of Blockchain Asset Inheritance

Earlier in this article, we introduced the analogy of the local courthouse as a blockchain, with its row offices functioning as individual blocks of information. Returning to that example, consider how similar deeded property is to Blockchain Assets, in the context of embedded inheritance planning. Deeds reserving life estates unto the Grantor, for example, create self-extinguishing rights that allow real property to pass upon death. How long until a Bitcoin owner's ledger/wallet can effectively name beneficiaries? And how long before that process becomes commonplace and user-friendly? Whatever the answers to those questions may be, it is clear we are about to witness a substantial development in inheritance planning, largely by necessity.

Whether DAOs begin to engage in post-mortem fiduciary activities is yet to be seen, but the prospect raises more than a few questions. Specifically, how is jurisdiction acquired over a group of anonymous individuals known only by usernames, some of which may or may not live in the United States? While companies are incorporated in a place, and often hold assets in a place over which jurisdiction can be acquired, DAOs do not so easily lend themselves to that jurisdictional reach.[36] DAOs seeking incorporation can acquire some benefits of limited liability for DAO members through incorporation according to state require-

---

36 *See* Stephen D. Palley, *Determining Jurisdiction When a DAO is Sued*, CoinDesk, (Sept. 11, 2021, 8:17 AM), https://www.coindesk.com/markets/2016/05/22/ [https://perma.cc/P32Z-8NV2].

ments (as in the Wyoming DAO LLC), but the tradeoff is loss of privacy since significant disclosures are required.[37] Some commentators suggest that, in the absence of any recognized legal entity structure, a general partnership structure would be applied by a Court, offering no liability protection to individual members.[38] Alternatively, a Court could treat a DAO designed for inheritance purposes as a constructive trust and require DAO members to carry out normal fiduciary duties.[39] It seems unlikely that DAOs are an easy tool to sidestep the fiduciary rules and liability concerns of the traditional trustee role. However, the prospects of an individual or family holding Blockchain Assets in a DAO whose members are intended inheritors of the assets is a fascinating prospect and bears some resemblance to well-established Family Limited Partnership-style arrangements. The notable difference is that DAO members might only be identified by cryptographic code, rather than their names and social security numbers.

VI. Conclusion

At the onset, we asked whether the public nature of blockchain transactions could be reconciled with an individual's concern for privacy. The anonymity provided by blockchain transactions appears to far outweigh the public nature of decentralized transactions, which should please most privacy enthusiasts. However, the inheritance questions posed are less easily answered.

Specifically, the technology currently exists to permit blockchain encoding to automatically distribute Blockchain Assets to an owner's beneficiary, although it is currently happening only in limited scenarios with just a handful of companies in the market. Whether such code-based solutions begin operating as "beneficiary designations" for Blockchain Assets is yet to be seen but appears to be very possible.

Finally, decentralized organizations operating anonymously among many users are a fascinating prospect for fiduciary administration. The privacy offered by a DAO's fiduciary administration of assets may win over privacy enthusiasts who own substantial Blockchain Assets. However, the same concerns that affect current fiduciaries (liability and fiduciary duties) would appear to apply still to these new organizations. DAO members would have to consider whether they all inherit liability associated with any negative action that would occur which would likely

---

[37] *See* Jordan Teague, *Starting a DAO in the USA? Steer Clear of DAO Legislation,* Defiant (June 7, 2022), https://thedefiant.io/starting-a-dao-in-the-usa-steer-clear-of-dao-legislation/ [https://perma.cc/X9E8-K57J].

[38] *See* Palley, *supra* note 36.

[39] *See* William Swadling, *The Fiction of the Constructive Trust, in* 64 Current Legal Problems 399, 405-06 (George Letsas et al. eds., 2011).

discourage participation. As such, the promise of a Decentralized Autonomous Trustee remains just a promise for now.