Northwestern Journal of Technology and Intellectual Property

Volume 16 | Issue 4 Article 1

2019

THROW AWAY THE KEY, OR THE KEY HOLDER? COERCIVE CONTEMPT FOR LOST OR FORGOTTEN CRYPTOCURRENCY PRIVATE KEYS, OR OBSTINATE HOLDERS

Andrew M. Hinkes
New York University School of Law and Leonard N. Stern School of Business

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

THROW AWAY THE KEY, OR THE KEY HOLDER? COERCIVE CONTEMPT FOR LOST OR FORGOTTEN CRYPTOCURRENCY PRIVATE KEYS, OR OBSTINATE HOLDERS

Andrew M. Hinkes

May 2019 VOL. 16, NO. 4

Copyright 2019 by Northwestern University Pritzker School of Law
Northwestern Journal of Technology and Intellectual Property

Volume 16, Number 4 (2019)

THROW AWAY THE KEY, OR THE KEY HOLDER? COERCIVE CONTEMPT FOR LOST OR FORGOTTEN CRYPTOCURRENCY PRIVATE KEYS, OR OBSTINATE HOLDERS

Andrew M. Hinkes[1]

ABSTRACT—Most cryptoassets natively function as bearer instruments. Whoever controls the private key for a given cryptoasset wallet generally controls the assets held by that wallet. In a civil or criminal action or as part of a governmental investigation, parties may be ordered to disclose their private keys or to transfer cryptoassets controlled by those private keys. However, people forget things and lose things, including extremely important things. Parties may lose private keys, and thereby lose control of their assets; parties acting in bad faith, or due to ideological motivation, may claim that "lost" or "forgotten" private keys prevent them from complying with disclosure or turnover orders. Determining whether claims of lost or forgotten private keys are genuine or are bad faith attempts to protect assets will be a challenge for courts, forcing them to confront complex, technology-specific evidence and requiring that they determine whether that loss is *bona fide* or tactical "self-created impossibility." Courts may likewise find that traditional contempt sanctions are insufficient to compel a motivated contemnor to comply with disclosure or turnover orders. To avoid expensive, time-consuming evidentiary hearings on contempt, parties and courts should consider *ex ante* measures, including standing orders and injunctive relief that would require disclosure of and prevent the loss of private keys once financial condition becomes relevant to any claim or defense in litigation. Legislators could create novel contempt sanctions that leverage the unique features of cryptoassets to lien sufficiently identifiable cryptoassets at issue. New laws could create registries listing identifiable cryptoassets subject to turnover orders (similar

[1] Andrew M. Hinkes is an Adjunct Professor of Law, New York University School of Law, New York University Stern School of Business; J.D., University of Miami School of Law, A.B. (History), Washington University in St. Louis. My thanks to David Yermack, Max Raskin, Peter Van Valkenburgh, Jerry Brito, Darren Sandler, Nelson "Romero" Rosario, Addison Cameron-Huff, Marco Dell'Erba, Chris DeRose, Joshua Unseth, Editor-in-Chief Anne Monjar, the staff and hardworking students with the Northwestern University Journal of Technology and Intellectual Property, and to Michelle Hinkes for her infinite patience, encouragement, support, and love. Any errors, mistakes, omissions, or misapprehensions found herein are my own.

to state UCC registries), use the infrastructure and legal obligations imposed upon regulated intermediaries by the Bank Secrecy Act and Office of Foreign Asset Controls, or modify existing state law writs to direct state-regulated financial intermediaries to seize those identifiable cryptoassets pending further court order. Although these new sanctions would destroy the fungibility of the cryptoassets at issue and reduce their commercial value, they would also create new, efficient incentives. The lien against identifiable cryptoassets would have no impact on parties who actually lose their private key but would facilitate recovery of cryptoassets taken without authorization in a hack or theft. Finally, the threat of a lien that would adversely impact the value of the specific implicated cryptoassets would reduce the incentive for a bad faith contemnor to defy a turnover order and instead encourage compliance.

INTRODUCTION

The financial and legal worlds have struggled to adapt to the sudden popularity of cryptoassets like Bitcoin and Ethereum.[2] Although much of the legal concern created by cryptoassets has focused on the implications of their sale, trading, and use for fundraising, cryptoassets are now widely held and will inevitably challenge certain procedural aspects of the traditional justice system as a result of their eccentricities in form and function.

Cryptoassets are generally digital instruments created and transacted by software operated on a decentralized network of computers that are designed to remove legally accountable intermediaries from transactions between system participants.[3] This distributed structure complicates, but does not prevent, the exercise of power over those assets by courts.[4] Cryptoasset owners control their assets via cryptographically-generated credentials known as private keys that are typically kept secret.[5] Although a range of technologies exists to back up private keys, if a private key is not backed up and is subsequently forgotten, lost, or stolen, a cryptoasset owner may irrevocably lose control of his cryptoassets, which may include irreplaceable, unique, non-fungible assets.

[2] Although there is significant variety in the functionality, intended purpose, legal classification, and distribution model of various cryptoassets, "cryptoassets" will be used herein to refer to all varieties of cryptoasset systems that use public/private key encryption to control those underlying assets, unless a meaningful distinction calls for the use of a more specific term.

[3] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/8PAA-PQ9E] ("What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.")

[4] In particular, the SEC has taken a technology agnostic approach in a variety of its settlement agreements related to the cryptoasset ecosystem. *See generally In re* Zachary Coburn, File Release No. 3-18888 at 3 (Sec. Exch. Release No. 84553 (Nov. 8, 2018), https://www.sec.gov/litigation/admin/2018/34-84553.pdf [https://perma.cc/5KFT-UD2V])(finding the technical structure of a smart contract running on the Ethereum blockchain immaterial to the conclusion that the system was an unregistered securities exchange); Report of Investigation Pursuant to Section 21(a) of the Sec. Exch. Act of 1934: The Dao, Release No. 81207 at 1, 11 (Sec. Exch. Comm'n. 81207 (July 25, 2017), *available at* https://www.sec.gov/litigation/investreport/34-81207.pdf [https://perma.cc/5FL5-L2VQ]) (holding that the decentralized structure of unregistered, unexempted offering of investment contracts did not impact the analysis under the *Howey* test or its conclusion that Dao Tokens sold were an improper unregistered securities offering).

[5] Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 239 (2018) ("A person who owns or possesses Bitcoin controls it with a long, complex encryption key . . . ") Most private keys used are summary or compressed versions of private keys. *See infra* note 120 ("A person ultimately controls their Bitcoin or other cryptocurrency by way of a much longer private key."). *See generally Private Key*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Private_key [https://perma.cc/S8DA-TZMD].

These novel features complicate the exercise of power by courts to compel disclosure of private keys, enforce cryptoasset turnover orders, or attach or execute against cryptoassets.[6] Courts should understand how users control their cryptoassets to appropriately identify situations where parties have, in good faith, lost their private keys,[7] and situations where users lie about lost private keys or intentionally "lose" their private keys to render compliance with turnover orders impossible, and to craft appropriate sanctions for each case. Courts should understand what evidence constitutes "all reasonable efforts to comply"[8] with a turnover order and what evidence supports a legal conclusion of bad faith self-created impossibility.

Courts use coercive contempt sanctions to compel compliance with their orders if compliance is possible or if compliance is rendered impossible by the actions of the party charged with compliance. These sanctions may include indefinite incarceration. However, given the ease by which a private key may be secreted, even the harsh sanction of incarceration may be insufficient to convince a truly motivated contemnor to comply with a court order. Incarceration may be insignificant if a fortune in safely secured assets awaits after a contemnor's inevitable release. Likewise, cryptoasset holders may resist or invent complicated technical excuses to ignore a turnover order based upon an ideological belief that cryptoassets should be self-sovereign and coercion-resistant. Moreover, a party may invoke the Fifth Amendment, thereby introducing complicated constitutional issues, as a defense to turnover orders; depending on the specific requirements of the turnover order, compliance may be considered to be a testimonial act. These assertions may protect the private key holder where the order requires the turnover of a private key to evidence the key holder's legal culpability, or where the private key itself is to be discovered but should not prevent a court from compelling a user to use (as opposed to disclose) their private key to effectuate a transfer of cryptoassets.

However, it is unlikely that sanctioning a contemnor will result in the regeneration or re-discovery of a truly lost private key. Courts instead should embrace a two-part strategy; first, they should act to prevent private

[6] Court orders that require a party to turn over a private key or to turn over assets controlled by a private key will be referred to herein as "turnover orders" unless there is a material distinction in the type of order, for which a more specific term will be used.

[7] *See* Joseph Young, *How a Cryptocurrency Investor Lost $60 Million in Bitcoin and Never Got it Back*, CCN (May 27, 2018), https://www.ccn.com/how-a-cryptocurrency-investor-lost-60-million-in-bitcoin-and-never-got-it-back/ [https://perma.cc/6FJH-BUYF] (recounting the plight of Jesse Howells who lost 7500 bitcoins by throwing away the thumb drive holding his private keys).

[8] *See infra* notes 113–14.

key loss, and second, they should impose new sanctions tailored to the specific control issues associated with cryptoassets.

Courts could enter injunctions requiring private key holders to escrow a backup of their private keys with their counsel or with third parties once the private key or cryptoassets controlled thereby are at issue in litigation. Courts could also introduce standing orders requiring preservation of private keys at the commencement of an action implicating asset discovery or when cryptoassets become at issue in litigation.

Even these proactive measures, however, cannot prevent claims of lost keys. Courts should address these novel assets with novel expressions of existing court power. The focus of these contempt sanctions should shift from coercing compliance by the contemnor to acting directly upon the cryptoassets at issue. Courts should leverage the blockchain public ledger maintained by cryptoasset systems and the ability to identify cryptoassets associated with the contemnor to impose a new kind of lien against identifiable cryptoassets subject to a turnover order that may cause those cryptoassets to be seized or frozen when transacted through regulated intermediaries. State or federal regulators could create new registries that would put transacting parties and intermediaries on notice of the lien against those cryptoassets and require regulated money transmitters to identify and seize transactions of those cryptoassets. New laws could likewise criminalize transactions of those liened cryptoassets. Alternatively, states may create new writs of attachment and facilitate service of these writs upon state-regulated money transmitters through a state regulator, which would compel all regulated entities to seize transactions of liened cryptoassets pending further court order. These strategies would not harm a party who actually lost their private keys, but would disincentivize contemnors from acting in bad faith to tactically claim private key loss and potentially may enable the recovery of stolen cryptoassets. These new contempt sanctions would efficiently and effectively use rebalanced incentives to accomplish the goal of contempt: to encourage compliance with the court's order.

Part I of this article will discuss the unique attributes of possession and ownership of cryptoassets, including wallets, keys, and the mechanics of cryptoasset transactions. Part II will discuss the use of coercive contempt in the context of orders requiring the production of private keys and turnover of cryptoassets. Part III will address problems in the use of traditional contempt sanctions to compel compliance with turnover orders. Finally, Part IV will discuss new proactive measures and novel contempt sanctions to compel the production of cryptoassets.

I. WALLET SOFTWARE AND KEYS

Wallets[9] are software created by third parties or the developer(s) of a given cryptoasset system that allow users to control credentials used to transfer assets created by that system to other users.[10] Keys are lengthy strings of numbers reduced by algorithms to strings of numbers and letters generated by the cryptoasset wallet software that allow users to direct transactions of assets on that cryptoasset system.[11] Cryptoasset private keys are randomly generated by the wallet software executing a cryptographic hash function against a randomly generated number.[12] Public keys, sometimes called public addresses, are generated by wallet software by executing a cryptographic hash function against the private key.[13] Public keys are displayed on the system's blockchain, i.e. a public ledger that records transactions between users, but information linking a given transaction to an identifiable person or entity is generally hidden or not provided.[14] Private keys allow their holder to "sign" transactions to "spend," i.e. authorize transactions of cryptoassets.[15] Initiation of a transaction is evidence of the party's use, knowledge, and control (although perhaps not exclusive control) of the private key at that time. That a transaction has occurred, however, does not evidence the identity of the person who controls that private key, unless the public key associated with that private key is publicly known to belong to a given person or entity, and is known to be in that person or entity's exclusive control at the time of that

[9] This paper will focus upon public distributed blockchain systems, using Bitcoin as the primary example. These systems are distributed and generally lack a central point of control. Private or permissioned blockchains generally have a central administrator who will respond to court process and thus many of the issues detailed herein do not apply to assets on those private or permissioned systems.

[10] *See generally Wallet*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Wallet [https://perma.cc/7772-HGLC]. *See also* Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at p. 15 https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf)("[Convertible virtual currency] wallets are interfaces for storing and transferring [convertible virtual currencies].")[https://perma.cc/3F98-GY22].

[11] *See generally Private Key*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Private_key [https://perma.cc/S25N-762T].

[12] *Id.*

[13] *See Address*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Address [https://perma.cc/WFJ2-RHTK].

[14] NAKAMOTO, *supra* note 3, at 6.

[15] *Id.* at 2 ("Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin."). Signing the transfer submits the proposed transaction to the miners who will verify the transaction. *See* Mauro Conti, et al., *A Survey on Security and Privacy Issues of Bitcoin*, 20 IEEE COMM. SURV. TUTORIALS 3416, 3418 (2018) http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8369416&isnumber=8540503 [https://perma.cc/C2JK-GQMR]. This verification by miners records the transaction on the blockchain and causes the value at issue in the transaction to be recorded as transferred from transferor to transferee.

transaction. Because transactions of cryptoassets are generally immediate and irrevocable, users hold their private keys confidential.[16] Any person who controls a private key can access and control the assets associated therewith; a thief who steals a private key may immediately transfer the assets controlled by that private key to another wallet.[17]

Although a user-to-user transaction is recorded on the system's blockchain, a user may transfer cryptoassets controlled by a given wallet by communicating her private key to another user.[18] Such a transfer does not appear on a blockchain or otherwise create any record or "paper trail." Although possession of a private key is control of the assets associated with that wallet,[19] mere possession is not equivalent to ownership of those assets; a party may possess a private key but lack legal title or "the best claim" to the assets controlled by that private key.[20] This may occur when a private key is stolen, when cryptoassets are subject to liens, or when a party holds one of several private keys in a multi-signature configuration wallet.

A. Types of Wallets

Cryptoasset wallets vary among their features and physical form. The most common types of wallets are digital, externalized, third-party-hosted, brain wallet/incorporeal, and multiple signature wallets.

[16] *See, e.g.*, ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 41 (2014) ("In simple terms, a transaction tells the network that the owner of a number of bitcoins has authorized the transfer of some of those bitcoins to another owner. The new owner can now spend these bitcoins by creating another transaction that authorizes transfer to another owner, and so on, in a chain of ownership."). Nakamoto recommends using new public and private keys for each transaction to provide additional identity protection. NAKAMOTO, *supra* note 3, at 6 ("As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner.").

[17] Under those circumstances, if the user who suffered the loss can identify the thief, that user still has limited recourse; they may ask nicely, use self-help, file a police report, or seek civil monetary relief, but cannot by any system operation reclaim those assets. *See generally* Timothy B. Lee, *Lawsuit Illustrates Bitcoin's Chargeback Problem*, ARS TECHNICA (Mar. 7, 2012), https://arstechnica.com/tech-policy/2012/03/lawsuit-illustrates-bitcoins-chargeback-problem [https://perma.cc/46SP-NHJ4].

[18] The author expects that this means of conveying value will be most often used by parties seeking to transfer assets without detection.

[19] To "hold a private key" has been defined in multiple states' Digital Signature Acts to mean "to be authorized to utilize a private key." *See, e.g.*, MINN. STAT. § 325K.01(14) (2018). This definition is not universal, and it addresses authority to use the key without explicitly addressing the ownership of the underlying data associated with the private key.

[20] Although possession of private keys is generally conflated with ownership, ownership is a function of legal title, not mere control. Byrne has suggested that cryptocurrency system assets could be viewed as a matter of contract rights among participants in those networks or as an asset for which title exists. Preston Byrne, *What Do You Legally "Own" with Bitcoin? A Short Introduction to Krypto-property*, PRESTON BYRNE (Nov. 23, 2018), https://prestonbyrne.com/2018/11/23/what-do-you-legally-own-with-bitcoin/ [https://perma.cc/B9MA-994X]. Case law supports claims of ownership over pure information. *See, e.g.*, *Int'l News Serv. v. Associated Press,* 248 U.S. 215, 216 (1918).

A typical cryptoasset wallet is software that is downloaded and installed on an internet-connected computer. Users access their cryptoassets by inputting their private key or a password derived from that private key into the wallet software. Users may use any software wallet compatible with the cryptoasset system at issue; in most cases access is not device or software instance reliant.

Externalized wallets are physical or virtual objects that include a private key written, engraved, saved, embedded, or otherwise represented exclusively in that object. These vary in form from writing on paper,[21] to instruments that resemble currency,[22] to art,[23] to external computer storage devices.[24] Typically the private key is not otherwise saved, and the private key stored in or on the externalized wallet must be input into software to access the cryptoassets controlled thereby. "Hardware wallets" are external storage devices that hold the private key and require the user to connect the device to an internet-connected computer, and then to input a saved access credential into software to access the cryptoassets associated with the stored private key.[25]

Specialized key structures, known as multiple signature or "multisig" wallets,[26] split the private key into N sub-keys where some subset M of N keys are required to spend cryptoassets controlled by that wallet.[27] Multisig wallets are often used when cryptoasset ownership or control is intended to be shared, to secure cryptoassets by holding multiple sub-private keys in

[21] *Paper Wallet*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Paper_wallet [https://perma.cc/774W-VCA5].

[22] Ariella Brown, *What's a Casascius Coin?*, COINDESK (May 9, 2013, 4:14 PM), https://www.coindesk.com/whats-a-casascius-coin [https://perma.cc/CPE7-PH8U].

[23] Lynx Art Collection (@LynxCollection), TWITTER, https://twitter.com/LynxCollection [https://perma.cc/XPZ3-WKJY].

[24] *Hardware Wallet*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Hardware_wallet [https://perma.cc/4LLE-J6J4].

[25] *See id*. Examples of hardware wallets include devices sold by Ledger, Trezor, KeepKey. *See generally* Myrto Arapinis, et. al., A 2018, A Formal Treatment of Hardware Wallets in Financial Cryptography and Data Security - 23RD INTERNATIONAL CONFERENCE, FC (Feb. 18, 2019). Financial Cryptography and Data Security 2019, St Kitts, Saint Kitts and Nevis, 18/02/19, (analyzing security aspects of multiple hardware wallets).

[26] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 11 (2016).

[27] *See Multisignature*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Multisignature. [https://perma.cc/2R2B-E2DH]; *see also* Abigail J. Farmer & Cory Elizabeth Tyszka, *Virtual Currency Estate Planning, Bit By Bit*, 40 ACTEC L.J. 249, 250, 265 (2014), *What is Multisig and What Can It Do?*, COINCENTER, https://coincenter.org/entry/what-is-multi-sig-and-what-can-it-do (last accessed 4/21/19) ("A P2SH address can support arbitrary sets of N keys, any M of which are required to transact — this is commonly referred to as 'M-of-N.'").[https://perma.cc/QPY7-XH28].

different locations,[28] or as a governance tool to prevent unexpected or unintended transactions.[29]

Online exchanges have contributed to the widespread popularity of cryptoassets by allowing 24 hour a day, seven days a week trading of an ever-expanding group of cryptoassets in an under-regulated or unregulated environment. Although these exchanges are generally used to trade cryptoassets, they are frequently misused as a form of simplified remote storage.[30] There are generally five distinct types of exchanges. First and most common are custodial exchanges that commingle their customers' assets in non-differentiated cryptoasset wallets and maintain their own records of customer deposit, trading, and withdrawal activity. Customers access these exchanges via the Internet using exchange-issued usernames and passwords. The legal rights associated with the deposit of cryptoassets into these exchanges vary widely, and are usually established by clickwrap agreements.[31] Customers who store assets on these third party exchanges forfeit direct control over their cryptoassets and instead rely on the exchange's operators to protect their cryptoassets from external and internal threats.[32] The second type of exchange holds its users' assets in user-segregated wallets.[33] Some exchanges allow their users to control their

[28] M. Rosenfeld, Comment to *What are Multi-Signature Transactions?*, STACK EXCHANGE: BITCOIN, http://bitcoin.stackexchange.com/questions/3718/what-are-multi-signature-transactions [https://perma.cc/NVA7-SAPR].

[29] Pamela Morgan, *Using Multi-Signature Accounts for Corporate Governance*, Empowered Law (May 2014), https://empoweredlaw.files.wordpress.com/2014/05/multi-signatureaccountsforcorporate governance1.pdf [https://perma.cc/DB99-NML7].

[30] This is a terrible idea for a number of reasons. *See generally* Andrew Hinkes, *On Centralized Custodial Crypto-currency Exchanges and Other Terrible Ideas*, Mmedium (Aug. 6, 2016), https://medium.com/@drewhinkes/on-centralized-custodial-crypto-currency-exchanges-and-other-terrible-ideas-1cb3f9ca5410; [https://perma.cc/7ur7-meqz]; Rachel Wolfson, *Why Centralized Cryptocurrency Exchanges Make Terrible Custodians for Crypto Assets*, Forbes (Nov. 7, 2018, 12:00 PM), https://www.forbes.com/sites/rachelwolfson/2018/11/07/why-centralized-cryptocurrency-exchanges-make-terrible-custodians-for-crypto-assets/#11e87e222e18. [https://perma.cc/xnx5-97p2].

[31] *See, e.g.*, Coinbase User Agreement, https://www.coinbase.com/legal/user_agreement?locale=en-US [https://perma.cc/B9LG-WJJR] .

[32] Sacharoff, *supra* note 5, at 239 ("Or they will outsource the responsibility to hold onto the keys to an institution such as Coinbase and use a password to access their Coinbase account."). Leaving assets on an exchange may be tempting to a user; by relying on a custodian, users can avoid downloading and operating a separate instance of wallet software for each asset they own on a machine they own and operate, and avoid the need to remember a private key for each type of asset's wallet software.

[33] Certain crypto asset exchanges that are regulated as options exchanges, such as LedgerX, are required to segregate each user's assets under CFTC regulation. *See, e.g.*, COMM. FUTURES TRADING COMM'N, LEDGERX LLC RULES 52, https://www.cftc.gov/sites/default/files/idc/groups/public/@otherif/documents/ifdocs/ledgercdcoappa-22017.pdf [https://perma.cc/ZD4N-6C3U] (discussing segregated customer collateral accounts).

cryptoassets using their private keys.[34] Certain online exchanges referred to as decentralized exchanges[35] function like centralized exchanges but operate certain parts of their order fulfilment function over a decentralized system. These decentralized exchanges may or may not include central actors to accept court process.[36] However, most online exchanges are incorporated businesses[37] and are likely to respond to court orders to provide user data,[38] freeze assets, and to turn over its users' cryptoassets.[39] Finally, outsourced custody services are offered by companies that hold cryptoassets for their customers in exchange for payment pursuant to express contracts.[40]

"Brain wallets" or incorporeal wallets allow control of cryptoasset wallets to be held exclusively in the mind of its owner.[41] Brain wallets use an algorithm that generates a private key from a password or seed phrase

[34] *See, e.g.*, CRYPTOBRIDGE, http://crypto-bridge.org [https://perma.cc/2Y7G-D5WQ].

[35] Lindsay X. Lin, *Deconstructing Decentralized Exchanges*, STAN. J. BLOCKCHAIN L. & POL'Y (Jan. 5, 2019), https://stanford-jblp.pubpub.org/pub/deconstructing-dex[https://perma.cc/4D8F-9Z5V].

[36] *Cf. In re* Zachary Coburn, File No. 3-18888 Zachary Coburn*,* Exch. Act Rel. 84553 (Nov. 8, 2018) (documenting the SEC's cease and desist order against Coburn who "controlled" a decentralized crypto exchange market which operated as software on a decentralized network of nodes on the Ethereum blockchain).

[37] *See* BARBARA D. UNDERWOOD, VIRTUAL MARKETS INTEGRITY INITIATIVE REPORT 8 (2018), https://ag.ny.gov/sites/default/files/vmii_report.pdf [https://perma.cc/J376-9PN4].

[38] United States v. Coinbase, Inc., No. 17-CV-01431-JSC, 2017 WL 5890052, at *7 (N.D. Cal. Nov. 28, 2017); Coinbase, *supra* note 31 (Coinbase reserves the right to refuse to process or cancel any pending Digital Currency Transaction as required by law or in response to a subpoena, court order, or other binding government order or to enforce transaction limits).

[39] *See* Sacharoff, *supra* note 5, at 239.

[40] Various strategies have been used to provide custody of cryptoassets as a service. Some vendors, such as Xapo, function like banks and will hold assets for third-parties pursuant to express contracts. XAPO, http://xapo.com [https://perma.cc/87XV-S974?type=image]. Others like Bitgo provide custody through a multisig wallet. BITGO, http://www.bitgo.com [https://perma.cc/YPL3-3CA6]. Finally, trust companies like Northern Trust that previously provided custody services for regulated financial products have recently offered similar service offerings to custody of cryptoassets. NORTHERN TRUST, https://www.northerntrust.com [https://perma.cc/AJW3-Q9BA]. Each of these types of external custodians are incorporated entities that will generally respond to court-issued process. The Wyoming Legislature recently passed Wyoming Senate File 0125, SEA NO. 0039, which authorizes banks to voluntarily provide custodial services for digital assets consistent with the Securities and Exchange Commission's qualified custodian requirements, effective as of July 1, 2019. *See* 39 S. Res. 65th Leg., Gen.Sess. (Wyo.2019).*See also* discussion of regulatory burdens associated with the operation of so called "hosted wallets" where the hosting wallet has "has total independent control over the value (although it is contractually obligated to access the value only on instructions from the owner)" at Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001, at p. 15-16, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf [https://perma.cc/3F98-GY22].

[41] Max I. Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. 969, 998 (2015).

that is memorized by the owner or user.[42] The holder of a brain wallet password can transfer control of assets by communicating the passphrase to another person, which would allow the transferee to regenerate the wallet and to access the cryptoassets associated with that private key.[43]

Although there are meaningful variations among wallet technologies, unless the wallet type used involves a third-party custodian or a physical object, a party seeking to obtain turnover of cryptoassets or to establish that a given party has control of cryptoassets held in a specific wallet will need to obtain the private key from that party. In that sense, most cryptoasset wallets are either hosted and controlled by a third party, or function like brain wallets.

B. Automated Transactions of Cryptocurrency

Certain cryptoasset systems allow users to pre-set transactions to occur in the future. Bitcoin, for example, allows users to use nLockTime to pre-set transactions to be submitted for verification on a time and date in the future.[44] These transactions may be valid when set but only become effective and cause a transaction to be submitted for verification if there are sufficient assets associated with the transferor wallet to fund the intended transaction and if the system reaches a given block height or system time.[45] The private key holder is not required to do anything at the time the transaction is submitted for verification.

Smart contracts may also be used to "pre-load" a transaction to be executed in the future. The term "smart contract" in this context means code that controls a cryptoasset wallet that, depending on external data reported to that code, may or may not execute a given transaction.[46] This allows the smart contract to "break escrow" and transact value to another

[42] *Id.* at 998 n.215.

[43] *Id.* at 998 n.216. ("Because '[e]ach owner transfers the coin to the next by digitally signing a hash . . . and that digital signature is the passphrase generating the brain wallet.'"); *see also*, NAKAMOTO, *supra* note 3, at 2.

[44] *nLockTime*, BITCOIN WIKI (Feb. 17, 2019, 4:50 PM), https://en.bitcoin.it/wiki/NLockTime [https://perma.cc/8UQ6-9TRP]; *Protocol Documentation*, BITCOIN WIKI (Dec. 26, 2018, 3:12 PM), https://en.bitcoin.it/wiki/Protocol_documentation#tx [https://perma.cc/J7DV-S8CH].

[45] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 63 (July 19, 2016).

[46] Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (Sept. 1, 1997), https://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=
First [https://perma.cc/F3MD-93DF]; *A Primer on Smart Contracts*, LABCFTC 2, 4 (Nov. 27, 2018), https://www.cftc.gov/sites/default/files/2018-11/LabCFTC_PrimerSmartContracts112718.pdf [https://perma.cc/AES8-CVJX] ("[A] 'smart contract' is a set of code . . . [that a]llows self-executing computer code to take actions at specified times and/or based on reference to the occurrence or non-occurrence of an action or event. . . .").

wallet upon the report of the occurrence of some external event.[47] Typically, smart contracts require an intentional transfer of cryptoassets into the smart contract wallet but do not require the transferor to sign a transaction with that user's private key when the smart contract itself executes and transacts cryptoassets to another public key address.[48] Both nLockTime transactions and smart contracts may be used to conceal or delay a transfer of cryptoassets to a third party.[49]

A multisig wallet or smart contract may be configured to create a "dead man's switch," wherein a smart contract or other software may act as a third party that will periodically check if the private key holder is "alive,"[50] and if not, "throw the switch" and submit a transaction of cryptoassets controlled by that wallet to another wallet without the need for a human third party's intervention.[51] However, a dead man's switch may fail if the software relied upon also fails, is hacked, or if the underlying system is forked.[52] A dead man's switch may be used to passively transact cryptoassets in case of "duress" that prevents the settlor of the switch from confirming their vitality.

[47] Michael Bacina, *When Two Worlds Collide: Smart Contracts and the Australian Legal System*, 21 J. INTERNET L. 15, 19 (2018); Jenny Cieplak & Simon Leefatt, *Smart Contracts: A Smart Way to Automate Performance*, 1 GEO. L. TECH. REV. 417, 423 (2017) ("An oracle is a third-party information services provider that will digitally 'sign' a transaction, attesting to the occurrence of specific conditions."). For example, a smart contract may cause the transfer of assets upon a specific date or upon the reporting of the outcome of a sporting event or political election to that smart contract by an oracle.

[48] It is unclear who "owns" assets held by a smart contract that has not yet executed. It can be inferred that each of the potential recipients of the value who may potentially receive that value, depending on the report from the oracle, has a contingent right to those assets.

[49] Consider a smart contract wallet holding 50 bitcoins that were transacted to that smart contract wallet public address by A, which smart contract code holds those bitcoins until Oracle 1 reports some data X, wherein depending on X, the bitcoin may be transferred to public addresses controlled by either A or B. The parties assume that oracle 1 will report data X fairly and truthfully. If A and whoever controls oracle 1 conspire, those assets can be held in a smart contract that appears to be arms-length, but which will transact the 50 bitcoin back to A at A's direction. Or, in a different version of this hypothetical, consider that irrespective of X, B has agreed to hold the 50 bitcoin for A as its undisclosed agent until litigation is concluded in exchange for some other benefit. Or, in a different version of this hypothetical, the condition to be reported by oracle 1 never occurs and can never be reported.

[50] Such a "vitality check" may be accomplished by software that sends an email on a regular interval that that requires a response by a date and time to abstain from initiating a transaction.

[51] *What Is Bitcoin and How Does It Fit into Estate Planning*, TINDALL, GASK, BENTLEY LAWYERS (June 6, 2014), https://tgb.com.au/news-features/what-is-bitcoin-and-how-does-it-fit-into-estate-planning/ [https://perma.cc/DGA7-PXG9].

[52] *See* Jingnan Huo, *Lawyer Says Dead Man's Switch Not Best Option for Digital Asset Inheritance*, COIN TELEGRAPH (Oct. 28, 2017), https://cointelegraph.com/news/lawyer-says-dead-mans-switch-not-best-option-for-digital-asset-inheritance [https://perma.cc/PHA5-2EPD] (recognizing Ethereum as the likely candidate to facilitate these transactions, but noting its youth and the recent DAO hack that caused a hard fork).

C. Implication of Lost/Forgotten Private Keys

Private keys generally cannot be recovered if lost or forgotten.[53] Unlike most financial instruments which function through or with the cooperation of an intermediary, there is usually no central entity in control of a cryptoasset system that can replace or restore a lost private key, or otherwise provide access to the cryptoassets associated with a lost or forgotten private key.[54] These systems do not feature a central actor who can respond to a turnover order; a court will not receive a response if it attempts to subpoena information from, for example, the Bitcoin network.[55] As discussed *supra*, some cryptoasset users leave their assets on centralized third-party exchanges that may respond to court process, but this is the exception, not the rule. The loss of a private key may subject assets controlled by that key to immediate immobilization and permanent illiquidity.[56]

Certain systems and service providers allow users to backup private keys, or to regenerate private keys if they are lost using a "seed phrase" which is typically a combination of sixteen English language words which, if input into the appropriate software, will recover that user's private key.[57] While helpful, seed phrases may be stolen and lost too, so the issues discussed herein remain.

[53] S. Eskandari et al., *A First Look at the Usability of Bitcoin Key Management,* "A first look at the usability of bitcoin key management," Workshop on Usable Security (USEC) at 2 (2015), https://arxiv.org/pdf/1802.04351.pdf [https://perma.cc/T7XS-QM6F] ("However, if access to such a password is lost, online services generally offer account recovery mechanisms (e.g., based on email). No such recovery mechanism exists for self-managed cryptographic keys.")

[54] *Id. See generally James Howells Searches for Hard Drive with £4m-worth of Bitcoins Stored*, BBC (Nov. 28, 2013), https://www.bbc.com/news/uk-wales-south-east-wales-25134289 [https://perma.cc/WQW9-P9V4]. Users relying on hosted third-party wallets, however, may have recourse. *See* discussion, *supra*, in Section I(A).

[55] Although many argue this point, cryptocurrency systems generally tout themselves as "decentralized" but actually reallocate authority and power typically reposed in a single party to different actors or groups of actors within those systems. This decentralization complicates, but does not eliminate, the ability to identify parties responsible for the actions of a given software network. *See generally* Adem Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*, FIN. CRYPTOGRAPHY & DATA SEC., arXiv:1801.03998 (2018); Angela Walch, *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, CRYPTOASSETS: LEGAL & MONETARY PERSPS. (forthcoming) (offering a comprehensive examination of the potentially misleading claims of "decentralization" in the context of public network cryptocurrency systems).

[56] The assets associated with private keys do not "disappear" when private keys are lost. The party who lost the key loses control of the asset. Eric (Rick) S. Rein & John Guzzardo, *The Trustee and the Bitcoin Identifying and Recovering International Cryptocurrency Assets*, AM. BANKR. INST. J., 34 (August 2018) ("[W]ithout the complete private key, no court or legal authority can manipulate ownership of a blockchain asset. . . .").

[57] *Seed Phrase*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Seed_phrase [https://perma.cc/DBF6-TDUM].

A private key may be held in numerous places (i.e. by being externalized and held concurrently in a user's pocket and safe deposit box) and may be held by more than one person at any given time, each of whom by virtue of possession has equal access to all assets held in that wallet. A private key may be claimed to be lost or forgotten, only to be "found," remembered, or rediscovered years later. Assuming that the cryptoassets at issue retain commercial value, "lost" or "forgotten" private keys that are recovered years later may be an effective way to secret value.

D. Orders Requiring Production of Private Keys or Transfer of Cryptoassets

Courts may order parties to divulge their private key or to transfer cryptoassets controlled by a private key in a variety of situations. Orders or writs allow parties to discover assets in post-judgment collection matters.[58] Assets are routinely disclosed in discovery conducted in marriage dissolution actions,[59] probate litigation,[60] or in actions where financial status is an element of a party's claim or defense[61] such as accounting claims,[62] claims related to profit sharing in a business dispute,[63] claims where punitive damages are at issue,[64] fraudulent transfer actions,[65] or in bankruptcy-related matters.[66] Courts may order[67] parties to turn over private

[58] Rule 69(a)(2) of the Federal Rules of Civil Procedure provides that "[i]n aid of the judgment or execution, the judgment creditor . . . may obtain *discovery* from any person—including the judgment debtor—as provided in these rules. . . ." FED. R. CIV. P. 69(a)(2) (emphasis added). Discovery is used "to find out about assets on which execution can issue or about assets that have been fraudulently transferred or are otherwise beyond the reach of execution." 12 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 3014 (2d ed.1997).

[59] *See* Walton v. Walton, 537 So. 2d 658, 659 (Fla. Dist. Ct. App. 1989).

[60] *See* In re Estate of Sauey, 869 So. 2d 664, 665 (Fla. Dist. Ct. App. 2004).

[61] *See Friedman v. Heart Inst. of Port St. Lucie,* 863 So. 2d 189, 194 (Fla. 2003) ("[W]here materials sought by a party 'would appear to be relevant to the subject matter of the pending action,' the information is fully discoverable.") (quoting *Epstein v. Epstein,* 519 So. 2d 1042, 1043 (Fla. Dist. Ct. App. 1988)).

[62] *See, e.g.*, *Fla. Gaming Corp. of Del. v. Am. Jai-Alai, Inc.,* 673 So. 2d 523, 524 (Fla. Dist. Ct. App. 1996).

[63] *See, e.g.*, Aspex Eyewear, Inc. v. Ross*,* 778 So. 2d 481, 482 (Fla. Dist. Ct. App. 2001).

[64] Gersh v. Anglin, No. CV 17-50-M-DLC-JCL, 2019 WL 265800 (D. Mont., Jan. 18, 2019) (sustaining an interrogatory in discovery requesting disclosure of opposing party's cryptoasset holdings).

[65] A judgment creditor "is entitled to 'utilize the full panoply of federal discovery measures' provided for under federal and state law to obtain information from parties and non-parties alike, including information about assets on which execution can issue or about assets that have been fraudulently transferred." GATX Corp. v. Appalachian Fuels, LLC, No. CIV.A. 09-41-DLB, 2011 WL 4015573, at *8 (E.D. Ky. Sept. 9, 2011) (quoting Magnaleasing, Inc. v. Staten Island Mall*,* 76 F.R.D. 559, 561 n.1 (S.D.N.Y. 1977)).

[66] *See* 11 U.S.C. § 521 (2014) ("The debtor . . . shall . . . unless the court orders otherwise . . . file a schedule of assets and liabilities. . . ."); Rein & Guzzardo, *supra* note 56, at 64 ("With a cooperative

keys where establishing the identity of a party in control of cryptoassets or who initiated or received a transfer of cryptoassets is relevant and material.[68] Courts in criminal actions may also order private keys to be produced or cryptoassets to be transferred to evidence control of a certain cryptoasset wallet,[69] in forfeiture matters to seize assets,[70] or to prove the location or disposition of certain identifiable cryptoassets.[71]

II. ENFORCING ORDERS: THE LAW OF COERCIVE CONTEMPT

Under our common law system,[72] courts have the inherent power to enforce their own orders.[73] An individual's refusal to decrypt a data source

debtor (or adverse party), the private key will simply be turned over to the trustee at the § 341 meeting in order to access the virtual wallet and liquidate the cryptocurrency through the exchange platform.")

[67] Because a private key in plain text may be copied or memorized and used to access assets by anyone who can read it, a private key disclosure order should limit access to the recorded private key to parties who are bound by legal duties of confidentiality. Exposed keys have resulted in theft of cryptoassets, including theft by law enforcement officers in the course of an active investigation. *See generally* Cyrus Farivar & Joe Mullin, *Stealing Bitcoins with Badges: How Silk Road's Dirty Cops Got Caught*, ARS TECHNICA (Aug. 17, 2016, 5:00 AM), https://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught/ [https://perma.cc/J2MD-ZP72]. Key disclosure orders should require private keys to be provided to the court under seal, or provided to court-appointed fiduciaries, only, along with an affidavit by the producing key holder asserting that the affiant is the only person known to hold the private key and the only person known to affiant to execute transactions using that private key. This would prevent claims that others had control of the cryptoassets at issue.

[68] For instance, discovery may be taken to identify a transferee in a fraudulent transfer action. *See, e.g.*, In re: Cont'l Capital Inv. Services Inc., Bankruptcy Adv. Pro. No. 03-3370, Adv. Pro. No. 06-3505, MEMORANDUM OF DECISION AND ORDER REGARDING MOTION TO COMPEL, D.E. # 94 (Bankr. N.D. Ohio. Mar. 6, 2009).

[69] In an analogous matter, see United States v. Apple MacPro Computer, 851 F.3d 238, 241 (3d Cir. 2017), cert. denied sub nom. Doe v. United States, 138 S. Ct. 1988 (2018) (seeking to establish ownership and control of hard drives known to contain child pornography for the purpose of establishing criminal liability).

[70] COMISKY, FELD & HARRIS, Tax Fraud and Evasion, Volume 2 (Thomson Reuters/Tax & Accounting, 1994, with updates through September 2018) (online version accessed on Checkpoint (www.checkpoint.riag.com).

[71] See *supra* note 70, wherein decryption of a data source was sought to confirm the location of contraband which formed the basis for the criminal charges.

[72] Unlike common law legal systems, code law systems from the "Continental Legal tradition" view a party's failure to comply with a court's order as a private matter to be enforced by the parties, as opposed to our system that views such a failure as an affront and challenge to the Court's power, and which has for centuries permitted courts to "vindicate the court's authority or its dignity" through contempt orders. *See generally* Carlo Vittorio Giabardo, *Disobeying Courts' Orders—A Comparative Analysis of the Civil Contempt of Court Doctrine and of the Image of the Common Law Judge*, 10 J. Civ. L. Stud. 35, 40 (2018).

[73] Chambers v. NASCO, Inc., 501 U.S. 32, 44 (1991) (quoting Ex parte Robinson, 86 U.S. 505, 510 (1873)); Paul A. Grote, *Purging Contempt: Eliminating the Distinction between Civil and Criminal Contempt*, 88 WASH. U. L. REV. 1247, 1250 (2011) ("[P]ower of contempt is inherent in the courts and would have been vested in the courts in the absence of a specific legislative grant."); *see also* Michaelson v. U.S. *ex rel*. Chicago, St. P., M. & O. Ry. Co., 266 U.S. 42, 65 (1924) ("That the power to

may have dire consequences in other contexts;[74] in the context of a failure to comply with a turnover order, the likely consequence is contempt of court.[75] Although the history of the jurisprudence underlying contempt is hardly a picture of clarity,[76] contempt used to coerce future compliance with a court order is regarded as civil contempt.[77] The theory behind coercive contempt is that court orders must be followed, or consequences should issue.[78] Those consequences in the case of coercive contempt answer the question of "What happens to me if I don't?"[79]

A clear order that provides appropriate notice to the party obligated to comply is a predicate to the entry of a contempt sanction.[80] To obtain a contempt order, the proponent of contempt brings a motion against the party charged with compliance with a Court order seeking the imposition of contempt for non-compliance, and the party charged with compliance is entitled to notice and an opportunity to be heard before the motion is ruled upon.[81] The court, after considering evidence, must find that the party charged with compliance with the court's order has the present ability to comply and has willfully refused to do so.[82] Coercive sanctions are not

punish for contempts is inherent in all courts, has been many times decided and may be regarded as settled law. It is essential to the administration of justice.").

[74] *See* Tom Davidson, *Wife 'Burns Husband Alive After He Refused to Give Her His Phone Password'*, UK DAILY MIRROR (Jan. 17, 2019), https://www.mirror.co.uk/news/world-news/wife-burns-husband-alive-after-13871070 [https://perma.cc/P5GZ-MKJU].

[75] "The court for the district where compliance is required . . . may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it." FED. R. CIV. P. 45(g); *see also* 17 AM. JUR. 2d *Contempt* §§ 41, 166 (1990) (In civil contempt, the court attempts to coerce the defiant party into complying with an order by imposing fines and/or jail time that can be avoided by complying with the underlying order.).

[76] *See generally* Grote, *supra* note 73, at 1250 (analyzing the history of contempt and proposing to eliminate the distinction between civil and criminal contempt).

[77] Int'l Union v. Bagwell, 512 U.S. 821, 829 (1994); *see also* Turner v. Rogers, 564 U.S. 431, 441–42 (2011) ("Civil contempt differs from criminal contempt in that it seeks only to 'coerc[e] the defendant to do' what a court had previously ordered him to do.") (quoting Gompers v. Bucks Stove & Range Co., 221 U.S. 418, 442 (1911)); Grote, *supra* note 73, at 1257 ("A civil contempt is designed to coerce the contemnor into compliance.").

[78] Giabardo, *supra* note 72, at 38 ("[T]he rationale of coercive means is to make non-compliance with the judicial order less convenient than compliance.")

[79] Doug Rendleman, *Disobedience and Coercive Contempt Confinement: The Terminally Stubborn Contemnor*, WASH. & LEE L. REV. 48, 185, 188 (1991).

[80] *In re* Keller, 568 B.R. 118 (B.A.P. 9th Cir. 2017) ("For contempt, the moving party must show by clear and convincing evidence the contemnors violated a specific and definite order of the court.").

[81] *Turner*, 564 U.S. at 442 ("[W]here civil contempt is at issue, the Fourteenth Amendment's Due Process Clause allows a State to provide fewer procedural protections than in a criminal case."); Akridge v. Crow, 903 So. 2d 346, 350 (Fla. Dist. Ct. App. 2005) ("[S]uch fundamental fairness includes notice and an opportunity to be heard.").

[82] *See, e.g.*, Gregory v. Rice, 727 So. 2d 251, 254 (Fla. 1999) ("The court must then evaluate the evidence and determine whether the alleged contemnor has the present ability to pay the support and has willfully refused to do so."); *Notes: Indefinite Confinement as a Coercive Measure by Courts*, 1

available "when it is clearly established that the alleged contemnor is unable to comply with the terms of the order."[83] Once the proponent of contempt establishes a *prima facie* case, the burden of production shifts to the alleged contemnor, who must then come forward with evidence to show inability to comply with the court's order.[84]

The mere assertion of inability to comply is insufficient.[85] "In order to succeed on the inability defense . . . [the prospective contemnor] must . . . establish that he has made in good faith all reasonable efforts to meet the terms of the court order he is seeking to avoid."[86] The court will review evidence under the clear and convincing standard.[87] The trial court determines the credibility of the evidence when determining whether to discharge contempt or whether to impose penalties for failure to comply with the order.[88] The court must find based on evidence that the contemnor has the ability to comply but has failed to do so.[89] Then the court must conclude that the entry of a contempt sanction is appropriate. The order imposing contempt must provide the contemnor with the ability to purge the contempt.[90]

REGENT U. L. REV. 77, 90 (1991) ("Where the contemptuous act did not occur in the presence of the court, the offender has the right to offer evidence and argument in his defense.").

[83] *See Hicks ex rel. Feiock v. Feiock, 485 U.S. 624, 638 n.9 (1988).*

[84] *See, e.g.*, BANKR. EVID. MANUAL § 301:38 (2018 ed.) (collecting citations); United States v. Rylander, 460 U.S. 752, 757 (1983); *In re* Lawrence, 279 F.3d 1294, 1297 (11th Cir. 2002); In re Taggart, 548 B.R. 275 (B.A.P. 9th Cir. 2016) ("[On motion to hold a party in contempt], [t]he moving party has the burden of showing by clear and convincing evidence that the contemnors violated a specific and definite order of the court. The burden then shifts to the contemnors to demonstrate why they were unable to comply.") (quoting *In re* Bennett, 298 F.3d 1059, 1069 (9th Cir. 2002)).

[85] Huber v. Marine Midland Bank, 51 F.3d 5, 10 (2d Cir. 1995) (citing Donovan v. Sovereign Security, Ltd., 726 F.2d 55, 59 (2d Cir. 1984)); United States v. Hayes, 722 F.2d 723, 725 (11th Cir. 1984).

[86] *Commodity Futures Trading Comm'n v. Wellington Precious Metals, 950 F.2d 1525, 1529 (11th Cir. 1992)* (citations omitted).

[87] F.T.C. v. Kuykendall, 371 F.3d 745, 756 (10th Cir. 2004) (citing Reliance Ins. Co v. Mast Constr. Co., 159 F.3d 1311, 1315 (10th Cir. 1998)).

[88] In *Wellington Precious Metals, 950 F.2d at 1530,* the trial court ". . . found [contemnor's] explanations unworthy of belief." *See also In re* Howald, 877 F.2d 849, 850 (11th Cir. 1989) (stating the court must make individualized determination of possible future compliance).

[89] Huber v. Marine Midland Bank, 51 F.3d 5, 10 (2d Cir. 1995) ("[I]f he offers no evidence as to his inability to comply . . . or stands mute, he has not met his burden.") (internal quotations omitted).

[90] Int'l Union v. Bagwell, 512 U.S. 821, 828 (1994) (quoting Gompers v. Bucks Stove & Range Co., 221 U.S. 418, 442 (1911)) ("In these circumstances, the contemnor is able to purge the contempt and obtain his release by committing an affirmative act, and thus 'carries the keys of his prison in his own pocket.'").

While courts have considerable discretion in their choice of remedies for contempt,[91] courts should never exercise more than "the least possible power adequate to the end proposed."[92] Coercive sanctions "'cannot be any greater than necessary to ensure such compliance' and may not be so excessive as to be punitive in nature."[93] In fashioning an appropriate remedy, courts must consider "the nature of the harm and the probable effect of alternative sanctions."[94]

Trial courts typically only consider the use of conditional incarceration as a contempt sanction once other methods to secure compliance have been considered.[95] To fashion an appropriate remedy, a court should consider: "(1) the harm from noncompliance; (2) the probable effectiveness of the sanction; (3) the financial resources of the contemnor and the burden the sanctions may impose; and (4) the willfulness of the contemnor in disregarding the court's order."[96] Typically, incarceration sanctions are only ordered after less severe alternatives have failed or have been deemed doomed to fail.[97] It must be possible for the contemnor to comply with the coercive contempt order;[98] the contemnor is said to possess the "keys to his own cell" and generally is incarcerated to imprisonment until the contempt is purged.[99]

E. Arguments of Inability to Comply and Evidence of Self-Created Impossibility

As noted *supra*, to avoid contempt,[100] the putative contemnor must provide evidence that the party charged with compliance made "in good

[91] *In re* Managed Care*,* 756 F.3d 1222, 1240 (11th Cir. 2014) (quoting Howard Johnson Co. v. Khimani, 892 F.2d 1512, 1519 (11th Cir. 1990) ("A district court has 'broad discretion in fashioning civil contempt sanctions.'").

[92] United States v. United Mine Workers of Am., 330 U.S. 258, 332 (1947).

[93] *In re Jove Eng'g, Inc. v. I.R.S., 92 F.3d at 1558* (quoting *Citronelle–Mobile Gathering, Inc. v. Watkins, 943 F.2d 1297, 1304 (11th Cir.1991)*). Incarceration runs a high risk of becoming punitive. *See In re Duggan, 133 B.R. 671, 671–74 (Bankr. D. Mass. 1991)*. Contempt sanctions also risk becoming incarceration for debt, which is prohibited. *See* Myron Fink, *Basic Issues in Civil Contempt*, 8 N.M. L. Rev. 55, 71 (1978).

[94] *In re* 1990's Caterers Ltd., 531 B.R. 309, 319 (Bankr. E.D.N.Y. 2015) (citing In re *Chief. Exec. Officers Clubs,* 359 B.R. at 536).

[95] Combs v. Ryan's Coal Co., 785 F.2d 970, 981 (11th Cir. 1986).

[96] *United Mine Workers,* 330 U.S. at 258.

[97] *In re* Tate, 521 B.R. 427, 429 (Bankr. S.D. Ga. 2014).

[98] Fink, *supra* note 93, at 60 ("[P]unishment for civil contempt is not really punishment since the party imprisoned can control his incarceration by doing the required act.").

[99] *See Hicks ex rel. Feiock v. Feiock, 485 U.S. 624, 649 (1988)*; Penfield Co. v. SEC, 330 U.S. 585, 595 (1947); Gompers v. Bucks Stove and Range Co., 221 U.S. 418, 441–42 (1911).

[100] Other defenses besides impossibility may be asserted to avoid contempt, including, for example, the invalidity of the subject order. *See In re* Novak*,* 932 F.2d 1397, 1401 n.6 (11th Cir.1991); *see*

faith all reasonable efforts" to meet the terms of the court order that party is attempting to avoid.[101] A contemnor may successfully assert a complete defense of impossibility where compliance with the order is actually impossible.[102] However, courts are likely to be skeptical of claims of fortunes irrevocably lost by the only party who had the ability to control it.[103] So-called self-created impossibility does not excuse non-compliance.[104] The burden to produce sufficient evidence that compliance is impossible remains on the putative contemnor.[105] In the case of a turnover order, a putative contemnor asserting impossibility as a defense will be required to provide evidence of the circumstances that led to the loss of that private key.[106]

To establish impossibility, the "alleged contemnor[] . . . must establish: (1) that they were unable to comply, explaining why 'categorically and in detail,' and (2) that their inability to comply was not 'self-imposed,'; and (3) that they made 'in good faith all reasonable efforts to comply.'"[107] This evidence shall be considered on a case by case basis.[108] The "all reasonable efforts" requirement is interpreted strictly.[109] The

also United States v. United Mine Workers of Am., 330 U.S. 258, 295 (1947). However, this article focuses only on the claim that the party charged with compliance is unable to comply because of the loss of the private key.

[101] *See In re* Lawrence, 279 F.3d at 1300 (citing *United States v. Roberts,* 858 F.2d 698, 701 (11th Cir. 1988)).

[102] *See Rylander*, 460 U.S. at 757; United States v. Bryan, 339 U.S. 323, 330–331 (1950).

[103] *See In re Lawrence*, 279 F.3d at 1298 (citing *F.T.C. v. Affordable Media,* 179 F.3d 1228, 1241 (9th Cir. 1999)). The court also pointedly observed that, "[w]hile it is possible that a rational person would send millions of dollars overseas and retain absolutely no control over the assets, we share the district court's skepticism." *Id*.

[104] *See* S.E.C. v. Solow, 682 F. Supp. 2d 1312, 1329 (S.D. Fla.), *aff'd,* 396 F. App'x 635 (11th Cir. 2010) (citing *In re Lawrence*, 279 F.3d at 1300); Pesaplastic, C.A. v. Cincinnati Milacron Co., 799 F.2d 1510, 1521 (11th Cir. 1986); *see also In re Power Recovery Systems, Inc., 950 F.2d 798, 803 (1st Cir. 1991)* (a party may defend contempt and failure to comply on the grounds that compliance was impossible; self-induced inability, however, does not meet the test).

[105] *See Rylander*, 460 U.S. at 755.

[106] *See In re* Luma Camera Serv., Inc., 157 F.2d 951, 953 (2d Cir. 1946), *rev'd sub nom.* Maggio v. Zeitz, 333 U.S. 56 (1948). Contemnors may puzzle over how they can prove they do not have their private key with evidence: "[I]t is difficult to prove a negative by documentation. That is generally true." Huber v. Marine Midland Bank, 51 F.3d 5, 11 (2d Cir. 1995). However, as discussed below, circumstantial evidence will be critical in the court's inquiry.

[107] *In re* Lawrence, 251 B.R. 630, 652 (S.D. Fla. 2000), *aff'd,* 279 F.3d 1294 (11th Cir. 2002) (internal citations omitted).

[108] *See* Maggio v. Zeitz, 333 U.S. 56, 75 (1948) ("Of course we do not attempt to lay down a comprehensive or detailed set of rules on this subject. They will have to be formulated as specific and concrete cases present different aspects of the problem.").

[109] The Eleventh Circuit strictly construes the "all reasonable efforts" requirement of the impossibility defense; substantial, diligent, or good faith efforts are not sufficient to rebut a prima facie showing of noncompliance. *See In re Lawrence,* 279 F.3d at 1297; *United States v. Roberts,* 858 F.2d 698, 701 (11th Cir. 1988); United States v. Hayes*,* 722 F.2d 723, 725 (11th Cir. 1984) (holding district

putative contemnor must evidence taking efforts reasonably necessary to purge the contempt.[110]

A given contemnor's motivation for non-compliance may vary–some contemnors may have inadvertently lost their keys and in "good faith" lack the ability to comply, while other contemnors may tactically fake inability to comply, and still other contemnors may believe that their non-compliance is necessary on ideological grounds to prevent a greater harm. Contemnors may believe that cryptoassets should be censorship- and collection-resistant,[111] and that court orders are a form of censorship to be resisted.[112] Contemnors may claim to be supporting an ethical or moral conviction by refusing to obey.[113] Such contemnors may believe that by

court abused its discretion when it held an alleged contemnor showing "some effort" to comply with court order was sufficient to rebut moving party's prima facie case); *see also F.T.C. v. Affordable Media,* 179 F.3d 1228, 1241 (9th Cir. 1999) ("In the asset protection trust context, moreover, the burden on the party asserting an impossibility defense will be particularly high because of the likelihood that any attempted compliance with the court's orders will be merely a charade rather than a good faith effort to comply."); *Oliner v. Kontrabecki,* 305 B.R. 510, 520 (N.D. Cal. 2004) ("The burden is on a contemnor to demonstrate 'categorically and in detail' why they were unable to comply with an order of the court.").

[110] *See In re* Tate, 521 B.R. 427, 444–45 (Bankr. S.D. Ga. 2014) ("Finally, Tate did not present any evidence that he has made 'all other efforts reasonably necessary to recover the property of the estate' as required by . . . the Contempt Order. Tate provided no evidence that he has attempted to recover the portion of the funds supposedly loaned to friends and relatives.); *see also Hayes,* 722 F.2d at 725–26 (contemnor ordered to produce financial records did not make all reasonable efforts "'merely by adducing evidence that he requested the documents (even diligent requests involving trips to Switzerland), when it appears that he [had] greater leverage at his disposal").

[111] *Cf.* Winkelvoss Captial Funds v. Shrem, No. 18-cv-8250, Memorandum Order (S.D.N.Y.Nov 19, 2018) ("Stating the fact that defendant invests some of his assets in cryptocurrency (which does not make them judgment – proof) . . . does not constitute a showing that he lacks sufficient assets.").

[112] For example, "[b]itcoin is a seizure-resistant digital asset with a transparent and incorruptible monetary policy, which provides the base, intrinsic (if you want to call it that) value proposition that attracts holders." Kyle Torpey, *3 More Lies Bitcoin Skeptics Tell Themselves*, FORBES (Jan. 30, 2018), https://www.forbes.com/sites/ktorpey/2018/01/30/3-more-lies-bitcoin-skeptics-tell-themselves/1 [https://perma.cc/JHE3-AGHR]. "The features of programmable money enabled by novel computer science and cryptography are: Seizure-Resistant Store of Value—cryptocurrencies as a cryptographically secured, seizure-proof, and government censorship resistant digital asset are a clear utility," Electric Capital, *Programmable Money*, MEDIUM (June 14, 2018), https://medium.com/@ElectricCapital/programmable-money-79e16dc7bfca [https://perma.cc/8ELF-RN83]. This assumption is belied by the extensive history of sovereign nations seizing cryptoassets. *See generally* Nikhilesh De, *The Bulgarian Government is Sitting on $3 Billion in Bitcoin*, COINDESK, https://www.coindesk.com/bulgarian-government-sitting-3-billion-bitcoin [https://perma.cc/F24F-MM8K]; Larry Cermak, *Analysis: The U.S. Has Seized Nearly 200,000 Bitcoins to Date, Global Confiscations are Up to 453,000*, BLOCK (Nov. 7, 2018), https://www.theblockcrypto.com/2018/11/07/analysis-the-u-s-has-seized-nearly-200000-bitcoins-to-date-global-confiscations-are-up-to-453000/ [https://perma.cc/BV77-F7WW].

[113] Rendleman, *supra* note 79, at 203 (discussing ideological, religious, ethical, and fear-based motivations for non-compliance with court orders).

holding out, they clear a path for others to similarly resist.[114] Some contemnors may seek to create a precedent of resisting orders followed by subsequent release from coercive imprisonment to empower others to resist similar orders.[115]

Although a desire to create precedent may influence a court's evaluation of evidence, such motivation would be improper; contempt orders are not intended to create future precedent or to discourage future disobedience by future contemnors.[116] However, it is foreseeable that others similarly situated may observe a Court's treatment of a contemnor claiming a lost private key and be guided by the outcome.[117] Advocates of cryptoassets as a coercion-resistant asset class may look to the contemnor as a test case or view the contemnor as a martyr for suffering sanctions to protect their claimed "right" to hold cryptoassets despite a turnover order.[118] However, unlike many social causes, it is unlikely that refusing to comply with a court order to hide financial assets will engender broad sympathy, no matter the form of technology used.[119]

If the court finds based upon evidence that the impossibility is self-created, the court may find the contemnor in contempt and impose a sanction.[120] The court's fact finding must be a considered and precise exercise; failing to enforce a court order based upon lies, or ordering the incarceration of a party who actually lacks the ability to comply with the court's order are both improper and potentially dangerous outcomes.

[114] See, for example, Morgan v. Fortich, 546 A.2d 407 (D.C. Cir. 1988), wherein Morgan unsuccessfully refused to obey an order to produce her daughter claiming that her ex-husband sexually abused the child in prior visitations and that her disobedience was necessary to avoid the more significant harm of child abuse.

[115] Susan Apel, *Custodial Parents, Child Sexual Abuse, and the Legal System: Beyond Contempt*, 38 AM. U. L. REV. 491, 525 (1989) ("[R]ecalcitrance then results in imprisonment, but real recalcitrance results in release.").

[116] Rendleman, *supra* note 79, at 201.

[117] *Id.* at 203 n.97 (collecting cases where contemnor disobedience is based upon the contemnor's ideological motivations).

[118] *Id.* at 203 n.98; *In re* Dohrn, 560 F. Supp. 179, 180 n.4 (S.D.N.Y. 1983); Linda S. Beres, *Civil Contempt and the Rational Contemnor*, 69 IND. L.J. 723, 753 (1994).

[119] *Cf.* Beres, *supra* note 122 at 753 n. 87 (noting instances where contemnors were released from incarceration where their non-compliance was a result of upholding organized crime's code of silence, obtaining the fruits of illegal activities, and furthering friendships with political activists).

[120] *See In re Lawrence*, 279 F.3d at 1300 (quoting Pesaplastic, C.A. v. Cincinnati Milacron Co., 799 F.2d 1510, 1521 (11th Cir. 1986)) ("Even if we were to find that Lawrence had set forth sufficient evidence of impossibility, we must agree with the trial court that Lawrence's claimed defense is invalid because the asserted impossibility was self-created. We previously have held that, 'where the person charged with contempt is responsible for the inability to comply, impossibility is not a defense to the contempt proceedings.'").

Some courts may conclude that all claims of impossibility due to the contemnor's loss of her own private keys are self-created impossibility, meriting the imposition of sanctions. Although this may compound the financial injury already suffered by some contemnors,[121] the policy behind this conclusion is sound. To suggest otherwise would encourage tactical claims of lost keys. For those courts, the inquiry will end there, and their subsequent labors will focus on identifying an appropriate sanction as discussed in sections III and IV.

Some courts may wish to distinguish between inadvertent "good faith" loss and tactical "bad faith" loss and impose different sanctions for each.[122] In drawing a distinction, these courts will be required to draw conclusions from evidence, including testimony and circumstantial evidence obtained from computers, witnesses, experts, and third parties. A simple claim that the contemnor cannot and will not comply is insufficient and unavailing.[123]

In the case of a lost private key, the contemnor would be required to provide evidence beyond self-serving testimony that the private key is lost, and that the loss was not tactical or strategic to avoid compliance with the court's order. Such evidence would typically include evidence of the circumstances behind the claimed loss, evidence that the loss was not intentional, and that the party charged with compliance has made in good

[121] Many will bristle at the thought of losing a fortune in cryptoassets because of a faulty memory or poor data hygiene, and later being punished in the form of sanctions for the same ineptitude.

[122] *Inability to Comply with Judgment or Order as Defense to Charge of Contempt*, 120 A.L.R. 703 (citing Spear v. McDermott, 926 P.2d 228, 236–37 (N.M. App. 1996) ("When there is genuine inability to comply with court order, even if the inability is self-created, it is complete defense to coercive contempt sanction such as incarcerating person indefinitely or imposing daily fine; however, such inability is not a defense to compensatory sanction such as one-time compensatory fine or sentence of imprisonment to punish contemnor or compensate for harm done")). Discussion of compensatory contempt is beyond the scope of this article.

[123] *See* Beres, *supra* note 122, at 734 ("Thus, while a contemnor's assertion that he will never comply may be a necessary condition for release, it rarely will be sufficient."). Evidence that the private key is lost, with nothing more, evidences only recalcitrance. Judges may persist in disbelief if they find the contemnor's claims incredible. *See generally* Maggio v. Zeitz, 333 U.S. 56, 75–76 (1948) ("Of course, if he offers no evidence as to his inability to comply with the turnover order, or stands mute, he does not meet the issue"); SEC v. Huffman, 996 F.2d 800, 803 (5th Cir.1993) (the court is not bound to accept unsubstantiated, self-serving testimony as true); U.S. *ex rel.* Thom v. Jenkins, 760 F.2d 736, 740 (7th Cir. 1985) (testimony insufficient to meet burden when self-serving, self-contradictory, confusing, and uncorroborated); Lopiparo v. United States, 216 F.2d 87, 91 (8th Cir. 1954) (Corporate president who failed to produce corporate books and records claiming inability to access records held in contempt; court rejected excuse that president was unable to find books and records); *In re* Cal. Motors, Inc., 122 F. Supp. 885, 887 (E.D.N.Y. 1954) (Court rejected respondent's claim of inability to turn over money at issue where respondent could not "satisfactorily explain his inability to turn over the fund . . . "); In re Sussman, 85 F. Supp. 570, 572 (S.D.N.Y. 1949)(Court rejected debtor's evidence indicating that debtor had no assets and lived on borrowed money, but otherwise did not address funds already determined to be in debtor's possession at the time of bankruptcy filing, finding that debtor's " . . . explanation of his inability to turn over the money is not sufficient").

faith all reasonable efforts to comply. Evidence of "all reasonable efforts" made in "good faith" to comply will likely include evidence of contemnor's efforts to recover the private key, testimony as to the circumstances of the loss, attempts to locate saved electronic versions or backups of the private key, attempts to use backups, attempts to restore the wallet using a seed phrase, forensic examination of remnants on the hard drive of the computer or device that hosted the wallet software previously used by the contemnor,[124] and evidence provided by forensic experts of efforts to recover the private key.[125] The contemnor could also offer evidence that either (a) no transactions occurred since the private key was lost, or (b) that subsequent transactions occurred that evidence that another party is controlling the private key.[126] Although a contemnor may argue that she did not have use or control of a given public address, forensic experts may trace cryptoasset transfers or identify the parties interacting with certain identifiable cryptoassets.[127] Likewise, if contemnor claims to be the victim of a hack, the contemnor must show some evidence of the hack, including the circumstances and timing of the loss associated with that hack, and contemnor's response to the hack. [128]

[124] For instance, if the user operated a full bitcoin node, the wallet.dat file should be present on the hard drive of that computer and may be a source of forensic information sufficient to recover a private key. Similarly, files in the install and related profile directories may contain information sufficient to recover a key. Useful forensic data may not be available for all cryptoassets; transactions made using privacy-enabled assets like Monero or Zcash may be significantly more difficult to trace.

[125] For example, www.walletrecoveryservices.com offers a service to assist with private key recovery. WALLET RECOVERY SERVICES, https://walletrecoveryservices.com [https://perma.cc/L3N2-L7LP]. This service requires the wallet user to provide basic information regarding the private key. *See generally* Mark Frauenfelder, *'I Forgot My Pin': An Epic Tale of Losing $30,000 in Bitcoin*, WIRED (Oct. 29, 2017), https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/ [https://perma.cc/PQN5-A9MP]; Conor Blenkinsop, *How to Recover Your Wallet if Your Private Keys are Lost*, COINTELEGRAPH (Nov. 16, 2018), https://cointelegraph.com/news/how-to-recover-your-wallet-if-your-private-keys-are-lost [https://perma.cc/3FTR-PSZC].

[126] Courts should carefully examine such evidence; a claim that a hacker used a stolen private key after the date of the claimed loss of the private key to transact offered as evidence of the hack could be a disguised nLockTime transaction set by the contemnor prior to the date of the claimed "loss." *See* discussion *supra*.

[127] *See* Andy Greenberg, *Your Sloppy Bitcoin Drug Deals Will Haunt You For Years*, WIRED (Jan. 26, 2018), https://www.wired.com/story/bitcoin-drug-deals-silk-road-blockchain/ [https://perma.cc/N9LY-LLL2]; Jeff John Roberts, *To Catch a Bitcoin Thief, Call These Detectives*, FORTUNE (June 27, 2018), http://fortune.com/2018/06/27/bitcoin-detective-zcash-cryptocurrency [https://perma.cc/X47T-ZUDA] ("Chainalysis can identify clusters of wallets tied to criminal activity, enabling law enforcement to look for other online clues to connect them to a real-life identity."); *see also infra* note 132.

[128] This evidence may be in the form of an expert forensic report, expert testimony, or evidence demonstrating diligent response to the hack when detected, such as a police report, a timely submitted insurance claim, and other similar documents.

Cooperation to identify transactions that could subsequently be recovered would also show the contemnor's good faith. In the circumstance of a pre-set nLockTime transaction or pre-funded smart contract, the contemnor may contact the prospective transferee and either seek to compel them to turn over the cryptoassets when received or identify the transferee to the court.[129] A contemnor's failure or refusal to do so evidences bad faith, as it strains credibility to suggest that the contemnor pre-funded a transaction to transfer value to a third party, yet does not know that third party.[130]

In determining the credibility of the contemnor's evidence, the court should look to badges of fraud used in various states' Uniform Fraudulent Transfer Act statutes to identify "red flags that would tend to evidence strategic or tactical key loss."[131] Those badges may be used as objective factors to infer the circumstances underlying the claimed loss of private key from the evidence before the court. Among various factors specified in the Uniform Fraudulent Transfer Act, the court should consider as "red flags" evidence that the assets controlled by the private key at issue were actually transferred to an insider, were transferred but still retained within the control of the contemnor, or were concealed. In addition, the court should consider evidence that (1) the contemnor was threatened with suit prior to the loss of the private key, (2) the loss of the private key resulted in the loss of all or substantially all of the contemnor's assets, (3) the loss of the private key occurred in order to obscure or avoid detection, (4) the loss of the private key rendered the contemnor insolvent, and (5) the loss of the private key occurred shortly before or after a substantial debt was incurred. If there is evidence to support these "badges of fraud," the court may find that the evidence provided by the contemnor lacks credibility, or evidences tactical or intentional loss of private keys.

The proponent of contempt who seeks to establish that the private key loss is tactical or intentional would not be required to submit evidence to establish prior use of the private key; that evidence is determined by the turnover order and is *res judicata*.[132] However, the proponent of contempt

[129] The court could then enter appropriate orders to compel the transferee to turn over the assets at issue.

[130] *See In re Lawrence*, 251 B.R. at 652 n.18 ("The Debtor has testified that he voluntarily established the Alleged Trust in 1991. Since the provisions which he now relies upon in order to substantiate his inability to comply with the Turn Over Order were of his own creation, he may not claim the benefit of the impossibility defense.").

[131] *See generally* Uniform Fraudulent Transfer Act, FLA. STAT. § 726.105(2) (2018) (as adopted by Florida).

[132] In re Sussman, 85 F. Supp. 570, 572 (S.D.N.Y. 1949)(Findings based on evidence which gave rise to the initial turn over order were *res judiciata* and " . . . the bankrupt may not go behind that order

may provide evidence to show that the loss was premeditated. Such evidence would include transactions with others that can be identified on the cryptoasset system's blockchain, banking records evidencing the purchase of cryptoassets via exchange or money services business,[133] or evidencing the receipt of funds from vendors that convert cryptoassets to fiat currency. Forensic evidence suggesting that assets were loaded into smart contracts or nLockTime transactions shortly before the claimed loss would suggest premeditation or an intentional claim of loss. Likewise, forensic examination of transactions prior to the purported loss may reveal transfers to insiders, or to other wallets controlled by the contemnor. Other evidence that may suggest tactical or purposeful loss includes if a contemnor failed to attempt to obtain technical assistance in an attempt to restore the private key around the time the loss was discovered, if there was loss or destruction of computers or devices previously used to access the contemnor's wallet, or if there was an intentional "wiping" of data or stripping of data sources from those devices.[134] Similarly, conversion of cryptoassets into a privacy enabled cryptoasset may also evidence attempt to circumvent tracing.[135]

At least one court has considered evidence on a motion to hold a party charged with compliance with a turnover order in contempt, albeit in a different context. In *U.S. v. Apple MacPro Computer*,[136] a criminal court sought to compel a defendant to unencrypt a hard disc drive that was suspected to hold child pornography. Defendant, when ordered to enter passwords to decrypt his external hard drives, entered several incorrect passwords during the forensic examination "and stated that he could not remember the passwords."[137] The trial court held the defendant in contempt of court for willfully disobeying its order to decrypt the external hard drives. The trial court found the defendant's testimony not to be credible

and show that the Referee was in error"), Maggio v. Zeitz, 333 U.S. 56, 66 (1948) (turnover order is res judicata and is not subject to collateral attack in the contempt proceedings).

[133] These purchase records are critical, as most purchases of cryptoassets occur with a regulated entity providing cryptoassets in exchange for fiat currency payment. These records, and discovery to be taken from that regulated entity, will typically be used by a forensic consultant as the starting point for their forensic tracing. Rein & Guzzardo, *supra* note 56, at 64 ("In cases where the debtor attempts to conceal the existence of a virtual wallet, a trustee might be able to discover evidence from the debtor's 'traditional' financial records (account or credit card statements) of the debtor 'cashing in' or 'cashing out' on that platform.").

[134] *See In re Lawrence*, 251 B.R. at 652 (voluntary acts of the contemnor that facially appear calculated to avoid turnover evidence bad faith).

[135] See note 182, *infra*, discussing privacy enabled cryptoassets.

[136] United States v. Apple MacPro Computer, 851 F.3d 238, 241 (3d Cir. 2017), *cert. denied sub nom*. Doe v. United States, 138 S. Ct. 1988 (2018).

[137] *Id.* at 243.

and "found that [Defendant] remembered the passwords needed to decrypt the hard drives but chose not to reveal them because of the devices' contents."[138] At the hearing conducted on the Government's motion seeking the entry of contempt, defendant put on no evidence. The Court ruled in favor of the Government and entered contempt sanctions. On appeal, the Third Circuit Court of Appeals found that the government provided sufficient evidence to support contempt, including: testimony by defendant's sister evidencing that defendant formerly memorized passwords to his data sources, from a detective who testified that defendant did not provide his password at the time because he wanted to prevent the police from accessing his computer, and that defendant did not previously assert an inability to remember the passwords. The Third Circuit affirmed the entry of contempt.[139]

F. How Long May a Contemnor Be Incarcerated Pursuant to a Coercive Contempt Sanction?

Courts have held that there is "no temporal limitation on the amount of time that a contemnor can be confined for civil contempt when it is undisputed that the contemnor has the ability to comply with the underlying order."[140] Thus, incarceration for coercive contempt may continue indefinitely, as long as the court determines that the sanction maintains its coercive effect.[141] A court may incarcerate the contemnor as a coercive sanction for civil contempt, so long as "the contemnor is able to purge the contempt and obtain his release by committing an affirmative act."[142] Confinement may last as long as the contemnor's lifetime.[143]

[138] *Id.*

[139] *Id.* at 249.

[140] United States v. Harris, 582 F.3d 512, 517 (3d Cir. 2009) (citing Int'l Union v. Bagwell, 512 U.S. 821, 828 (1994)). However, the duration of incarceration may be limited for certain types of contempt; the Federal Recalcitrant Witness Statute caps incarceration for refusal to testify at trial or grand jury at eighteen months. 28 U.S.C. § 1826 (2012).

[141] *Chadwick v. Janecka*, 312 F.3d 597, 608 (3d Cir. 2002) ("The meaning of the statement in *Bagwell* that a contemnor may be held 'indefinitely until he complies' is perfectly clear. The phrase 'until he complies' sets the point in time when confinement must cease. The term 'indefinitely' describes the length of confinement up to that point, namely, a period 'having no exact limits,' because the end point (the time of compliance) cannot be foretold."); Rendleman, *supra* note 79, at 196 n.56 (1991) (citing *In re* Griffin, 677 F. Supp. 26, 28 (D. Me. 1988)) ("[H]olding that confinement must continue as long as a judge is satisfied that coercive sanction might produce intended result."); *The Coercive Function of Civil Contempt*, 57 U. CHI. L. REV. 120, 122 (1965) ("[C]onfinement may continue until compliance.").

[142] *In re* 1990's Caterers Ltd., 531 B.R. 309, 319 (Bankr. E.D. N.Y. 2015) (quoting *Bagwell*, 512 U.S. at 828–29 (internal citations and quotation marks omitted)).

[143] *See* Uphaus v. Wyman, 360 U.S. 72, 82 (1959); Penfield Co. v. S.E.C., 330 U.S. 585, 594 (1947); *In re* Nevitt, 117 F. 448, 449 (8th Cir. 1902); Culver City v. Superior Court, 241 P.2d 258, 261–

However, the power to incarcerate must be limited, given its "awesome potential for abuse."[144] Civil contempt is determined by a single judge, using considerably less due process than provided in a criminal matter.[145] As the decision to release a contemnor from incarceration is fact and judge specific, the common law test for when a contempt sanction has lost its coercive effect may result in seemingly illogical or absurd outcomes.[146]

A contemnor's term of incarceration may be for an indefinite period but must remain coercive.[147] Courts typically periodically reassess whether there remains a realistic possibility the contemnor will yield to the coercive effect of the sanction.[148] In such cases, trial courts will consider, among other things, the passage of time, the fungible quality of the assets subject to turnover and the likelihood of the contemnor further misbehaving upon release.[149] The key to the inquiry is the contemnor's ability to comply. [150]

A judge's determination of whether a contempt sanction has lost its coercive effect is basically unreviewable.[151] However, multiple courts have released contemnors after lengthy incarcerations based upon the perceived

62 (Cal. 1952); City of Vernon v. Superior Court, 241 P.2d 243, 245 (Cal. 1952); *see also* Moskovitz, *Contempt of Injunctions, Civil and Criminal*, 43 COLUM. L. REV. 780, 801, 802–02; Comment*, Equity-Contempt-Duration of Imprisonment*, 36 MICH. L. REV. 1016, 1018 (1938).

[144] Rendleman, *supra* note 79, at 190; *The Coercive Function of Civil Contempt*, *supra* note 145, at 133 ("[C]oercive imprisonment is a powerful judicial tool for the enforcement of court orders. On occasion it can, however, be too powerful.").

[145] *Id.*

[146] *Id.* at 210 ("Dr. Elizabeth Morgan declined to release her daughter to the child's father because she feared sexual abuse; she spent twenty-five months in a District of Columbia jail, seven months longer than a thug who refused, under grant of immunity, to identify criminals.").

[147] *Wellington Precious Metals, 950 F.2d at 1530* ("[W]hen civil contempt sanctions lose their coercive effect, they become punitive and violate the contemnor's due process rights."); *see Gompers, 221 U.S. at 442*.

[148] *See In re Lawrence, 279 F.3d at 1301* ("If the bankruptcy judge determines that, although Lawrence has the ability to turnover the Trust *res,* he will steadfastly refuse to do so, the judge will be obligated to release Lawrence because the subject incarceration would no longer serve the civil purpose of coercion."); *United States v. Rylander*, 460 U.S. 752 (1983) (finding when a contemnor provides evidence they are no longer able to comply, the incarceration would be punitive and presumably convert to a criminal contempt or give grounds for application to discharge the contempt sanction).

[149] Maggio v. Zeitz, 333 U.S. 56, 66 (1948).

[150] *Id.* at 72 (noting that jailing someone for omitting an act the individual is powerless to do would make contempt proceedings purely punitive).

[151] Wellington Precious Metals, 950 F.2d at 1531 (11th Cir. 1992) (citing Simkin v. United States, 715 F.2d 34, 38 (2d Cir. 1983) (finding that in determining whether a civil contempt sanction has lost its coercive effect, the trial judge has virtually unreviewable discretion)); *see also* Commodity Futures Trading Comm'n v. Armstrong, 284 F.3d 404, 406–07 (2d Cir. 2002).

lack of effect of continued incarceration.[152] Although the initial factual assessment giving rise to incarceration has a *res judicata* effect,[153] the court may revisit the evidence, examine the contemnor's ability to comply at present, "articulate its present belief, and terminate coercive confinement."[154]

In the context of a lost private key, if the key is lost and a party has sought to recover it through diligent investigation, including the examination of the wallet and with the assistance of experts, incarceration may never have a coercive effect. This draws into question the use of the sanction of incarceration for self-created impossibility and suggests that where the evidence shows that a private key is lost in "good faith," other sanctions may be more appropriate, as argued in sections III and IV. However, where the evidence shows that the loss of the private key is tactical or in bad faith to avoid compliance with the order, incarceration sanctions may still be appropriate.[155]

G. What If the Contemnor Invokes Their Fifth Amendment Right Against Self-Incrimination as a Basis to Refuse to Comply?

Federal courts have found no inherent Fifth Amendment self-incrimination violations with ordering an individual to unencrypt a hard-drive.[156] Notwithstanding, a contemnor may invoke her Fifth Amendment right against self-incrimination, and, on that basis, refuse to comply with a court's order. This claim of right under the Fifth Amendment is not evidence and will not meet the burden of compliance or provide evidence

[152] *See In re* Lawrence, 279 F.3d 1294 at 1301 (explaining that the trial court will be obligated to release the incarcerated contemnor if it concludes that he will steadfastly refuse to comply with the court's order even though he retains the ability to comply); United States v. Harris, 582 F.3d 512, 522 (3d Cir. 2009) (DuBois, J., concurring opinion) (discussing Delaware state court judge's order directing the release of H. Beatty Chadwick from incarceration after more than 14 years—what the authors believe is the longest term of incarceration civil contempt to date—despite finding that the contemnor had the present ability to comply with an order directing him to deposit $2.5 million with the court, which concluded that the contempt order had lost its coercive effect given the contemnor's continued refusal to comply).

[153] Rendleman, *supra* note 79, at 195. *See also supra*, note 136.

[154] *Id.*

[155] *See supra* note 138.

[156] Raskin, *supra* note 41, at 999 n.222 (citing United States v. Fricosu, 841 F. Supp. 2d 1232, 1236 (D. Colo. 2012) (recapitulating the "[t]he small universe of decisions dealing with the Fifth Amendment issues implicated by compelling a witness or defendant to provide a password to an encrypted computer or otherwise permit access to its unencrypted contents"); United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (finding a Fifth Amendment violation because defendant's divulging his password was a testimonial communication); *In re* Boucher, No. 2:06-MJ-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009) (finding no Fifth Amendment violation because defendant's decryption of a hard-drive was not incriminating testimonial evidence).). *See generally* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 96 TEXAS L. REV. 767.

of impossibility of performance.[157] However, the impact of this claim of right depends on the nature of the order at issue. If the order only requires the contemnor to use the private key, then the testimonial aspect of compliance is limited to the implied statement that the suspect knows the password.[158] In that circumstance, according to Professor Kerr, where the movant can show that the party subject to the order knows the password, "the assertion is a foregone conclusion and the Fifth Amendment poses no bar to the enforcement of the order."[159] If the order requires the private key to be communicated, which would be direct testimony,[160] the foregone conclusion doctrine does not apply and the Fifth Amendment may protect the contemnor from her obligation under the order to provide that testimony.[161] This may have broader implications befitting further analysis given that decrypting a cryptoasset wallet implicates access to monetary value (as opposed to other forms of data), and suggests ongoing association with acts described on the ledger of transactions conducted using public key addresses associated with that private key.[162] Orders requiring a contemnor to use a private key, rather than to reveal a private key in writing, will not be defeated or mooted by a claim under the Fifth Amendment by the contemnor, assuming the proponent of the order has established by competent evidence that the contemnor has the private key.[163]

[157] *See* United States v. Rylander, 460 U.S. 752, 758 (1983) ("But while the assertion of the Fifth Amendment privilege against compulsory self-incrimination may be a valid ground upon which a witness . . . declines to answer questions, it has never been thought to be in itself a substitute for evidence that would assist in meeting a burden of production.").

[158] Kerr, *supra* note 155, at 778 ("Entering a password that unlocks a device has a testimonial component: It testifies that the person knows the password that unlocks the device."). An order that requires a party to transfer cryptoassets is different from an order that requires a party to produce a private key. A user may transfer cryptoassets by using their private key without disclosing that private key to a third party. An order that requires turnover of a private key functionally provides evidence that the party disclosing has the private key, and shares control of the assets controlled by that private key with anyone else who has knowledge of that private key.

[159] *Id,* at 767.

[160] Brief of Amicus Curiae Professor Orin Kerr in Support of Neither Party at 5, Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019) (No. SJC-12564), 2018 WL 5269423.

[161] *See supra* note 157.

[162] The implications of the Fifth Amendment invocation protecting information which is the equivalent of bearer forms of value, and the potential for abuse of compelled production are important, but beyond the scope of this note.

[163] As discussed *supra*, such evidence will typically be established by evidence of payment of fiat to obtain cryptoassets from conventional bank records and from experts who will use forensic tools to establish that Listed Cryptoassets, as defined and discussed in Section IV herein, are controlled by the public and private key at issue.

III. PROBLEMS IN THE USE OF TRADITIONAL COERCIVE CONTEMPT SANCTIONS

Because cryptoasset systems are optimized for rapid, irreversible asset transaction, generally are not conducted through centralized intermediaries who will respond to court process,[164] and leave a relatively sparse and novel forensic record, a claim of lost private keys may be an instance in which immediate use of a strong sanction is prudent.[165]

Although some have suggested that traditional contempt sanctions should be used to compel compliance with orders compelling production of a private key,[166] it is unclear whether coercive incarceration is an effective sanction in this context.[167] In the case of a lying contemnor who has hidden a private key, that contemnor may be content to wait out a contempt sanction, and upon the court determining that contempt is no longer having a coercive effect,[168] immediately access their stored wealth using their secreted private key, provided they are willing to tolerate temporary deprivation of liberty and to bear market and technology risk.[169] The threat of (and reality of) long term incarceration may compel compliance by some contemnors, but incarceration may not be sufficient motivation for contemnors who have large amounts of cryptoasset value or who are ideologically motivated to resist.[170]

Those contemnors may know that their assets are protected and may be either passed to another while incarcerated or held indefinitely until they

[164] Any cryptoassets maintained by an incorporated third party could be discovered using typical court process, including subpoenas and writs.

[165] Contempt incarceration is appropriate when less severe sanctions would lack the force necessary to compel compliance. *See Commercial Banking Co. v. Jones,* 148 B.R. 353, 359 (M.D. Ga. 1992) (holding coercive incarceration should be ordered when the contemnor has an established history of noncompliance and the circumstances indicate less severe sanctions would lack the force necessary to coerce compliance).

[166] Rein & Guzzardo, *supra* note 56, at 34, 64.

[167] Beres, *supra* note 122, at 724 ("In most cases, however, a rational individual faced with a court order never will comply after serving a period of incarceration. He either will comply immediately or not at all . . . . . . In general, belated compliance will occur only where an individual lacks perfect information at the time of his original decision to disobey the court order.").

[168] *See In re* Lawrence, 279 F.3d at 1301 ("If the bankruptcy judge determines that, although Lawrence has the ability to turn over the Trust *res,* he will steadfastly refuse to do so, the judge will be obligated to release Lawrence because the subject incarceration would no longer serve the civil purpose of coercion.").

[169] The contemnor who decides to "hold out" bears the risk that their cryptoassets will diminish in value, that the software system that enables those assets to be transacted may cease to be operational, that she may be hacked, or that the cryptoasssets may be forked to another asset, all of which would impact the commercial value of those secreted assets.

[170] Beres, *supra* note 123, at 754 ("[T]he more stubborn a contemnor appears, the more likely he is to be released and thus the lower his expected jail term.").

are released. A wily contemnor would not transfer assets "on chain" while in custody, as that transfer can easily be detected and may give rise to additional adverse consequences.[171] However, it would be trivial for a contemnor to write her private key on a piece of paper and hand that paper to another person, or to "encode" it in an email message, or to whisper it to a visitor, and by doing so transfer control of her assets to another person without creating an obvious or detectable record of the transfer. Likewise, hardware wallets or physical wallets may be "lost," only to be found years later. That a large amount of value may be at issue suggests that harsher penalties may be required as the contemnor may have sufficient incentive to wait through whatever incarceration is imposed to recover both his liberty and substantial amounts of concealed property.[172] Under those circumstances, a contemnor may have no incentive to comply, and may decide that ten to fifteen years in prison is a price worth paying to preserve a safely hidden fortune waiting for the contemnor upon release.[173]

Thus, mere incarceration may be insufficient. Given how easily a private key may be communicated, the court may wish to restrict that contemnor's ability to share the private key during incarceration by restricting a contemnor's ability to communicate. A court may order full surveillance of all of a contemnor's communications while incarcerated, including telephone calls, writings, text messages, email communications, and in-person communications to ensure that a contemnor does not pass a

[171] Failing to disclose assets in bankruptcy, for example, may jeopardize the debtor's opportunity to have her debts discharged, result in the loss of a claim, or give rise to criminal perjury charges. *See In re* Colvin, 288 B.R. 477, 483 (Bankr. E.D. Mich. 2003) (debtor's failure to disclose tax refund resulted in loss of exemption over that refund); *In re* Kasal, 217 B.R. 727, 739 (Bankr. E.D. Pa.1998), *aff'd sub nom.* Casey v. Kasal, 223 B.R. 879 (E.D. Pa. 1998) (debtor denied discharge of debts for "knowing and fraudulent" failure to disclose assets and misleading asset disclosures). *See also* fn 18, *supra*.

[172] Armstrong v. Guccione, 470 F.3d 89, 111 (2d Cir. 2006) ("The Court's statement in *Maggio* can be viewed as an 'inference that may be drawn under most circumstances when a contemnor, despite long confinement, fails to comply with an order . . . Thus, in most cases, after a certain period, the inference that the contemnor is unable to comply becomes overwhelming.'") (internal citations omitted). Armstrong's case, however, is not the ordinary case. Fifteen million dollars is a life-altering amount of money. We think that the value of the concealed property is a significant factor to the extent that it would lead the contemnor to conclude that the risk of continued incarceration is worth the potential benefit of securing both his freedom and the concealed property. *See* Armstrong, 284 F.3d at 406 ("True, Armstrong has been confined for more than two years, but the length of confinement must be viewed in the light of the value of the concealed property, which is unusually great."). (the parenthesis in this footnote appear off)

[173] Jonathan Lane, *Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation*, 8 CHARLESTON L. REV. 511, 555–56 (2014) ("[N]o level of regulation will definitively enable the government to compel a defendant to provide memorized private key information that is not stored in any tangible medium.").

private key to another.[174] Of course, persistent surveillance implicates considerable intrusion of the contemnor's privacy and would require extraordinary effort by the state. However, courts order surveillance over parties in circumstances including where conduct at issue would give rise to offenses punishable by more than one year of imprisonment,[175] and incarcerated parties have limited privacy rights.[176] Given that any form of communication can be used to communicate a private key or seed phrase to a third party, full surveillance of an incarcerated contemnor may be necessary to prevent or, at minimum, detect such efforts by the contemnor. While even full surveillance of the contemnor may not prevent that contemnor from transferring a private key to another person, such surveillance may narrow the population of prospective transferees for future proceedings to recover transfers or for aiding and abetting violation of the court's order.

However, rather than wait for a contemnor to fail to comply with an order or impose expensive and dystopian means to attempt to coerce compliance or prevent further violations of turnover orders, courts and counsel should proactively adapt their strategies around these new assets.

IV. New Paradigms Call for New Solutions: Adapting Contempt Sanctions to Cryptoassets

Courts and parties should treat these new assets in new ways; instead of arguing over evidence of loss of private keys, courts and parties should take steps to avoid private key loss, or to address the claimed loss of a private key at the earliest possible instance.

H. Proactive Measures to Prevent Private Key Loss

First, courts or parties may impose an express duty to preserve private keys. Parties in litigation, upon the occurrence of an event, filing, or ruling that gives rise to a right for a party to take discovery of a party's financial condition or assets, to seek disclosure of a private key, or to attach or

[174] Ignoring the question of whether this full surveillance is possible, from a practical perspective, courts, legislators, and prison officials may be loath to fund and build a panopticon to punish a small class of imprisoned contemnors.

[175] Standards for Electronic Surveillance of Private Communications § 2-4.4, Am. Bar Ass'n (2017), https://www.americanbar.org/groups/criminal_justice/publications/criminal_justice_section_archive/crimjust_standards_private1/#part44 [https://perma.cc/XC59-KDXA] ("An application for an order authorizing electronic surveillance should be permitted only for the investigation of offenses which are punishable by more than one year imprisonment and have been designated by the legislature as serious enough to justify the intrusiveness of the surveillance.").

[176] Inmates generally do not have a reasonable expectation of privacy. *See* Hudson v. Palmer, 468 U.S. 517, 530 (1984).

execute against a party's assets, should immediately seek the entry of an affirmative injunction[177] against the party in possession of the private key to obligate that party to (a) direct those assets to a third party actor or system that can "recover" those assets for their owner if the key is subsequently lost, or (b) provide a record of or backup of the private keys to their counsel, and to notify those parties of severe sanctions if that private key is lost (or as may be appropriate, if value is transacted out of that wallet[178]) thereafter. Proactive measures may avoid the need to argue over circumstantial evidence of potential bad faith spoliation or loss of assets while also giving courts the predicate to impose punitive sanctions for violations of the court's injunction, including evidentiary presumptionsand potentially striking claims and defenses.

Courts could standardize this practice by issuing standing orders or local rules to require parties to backup and retain private keys at the initiation of litigation or with the filing of claims or defenses implicating parties' financial condition. These rules or orders would expressly create a duty to retain or duty to back up private keys, similar to duties to preserve evidence that generally arise in litigation when the parties reasonably anticipate litigation.[179] Although a party could trigger the same obligation by serving a discovery request upon the party to be charged with production of the private key, this strategy would likely require additional litigation over discovery objections. Injunctions, local rules or standing orders would also lay a clearer path for the imposition of adverse inferences, striking claims, defenses, and similar spoliation-type sanctions, and eliminate surprise claims that private keys providing access to cryptoassets at issue have been "lost."

I. New Contempt Sanctions

Although proactive measures may eliminate surprise and reduce the opportunity for a party to tactically claim private key loss, these proactive measures cannot prevent all fraudulent claims of lost private keys nor recover truly lost keys. No matter the strategy or sanction, court power over the contemnor can only seek to motivate the contemnor to comply.

[177] Rendleman, *supra* note 79, at 189 ("Injunctions are preventive and individualized remedies to protect citizens' rights that judges cannot compensate with money.").

[178] A user may send cryptoassets from wallet to wallet, or public key address to public key address without losing possession or control of that asset, but so doing complicates subsequent efforts to recover those assets.

[179] *See* Hynix Semiconductor Inc. v. Rambus Inc., 645 F.3d 1336 (Fed. Cir. 2011); Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311 (Fed. Cir. 2011); Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497, 521 (D. Md. 2010). It may be argued that the existing duty to preserve evidence would apply in this case.

Courts should consider using new sanctions that focus on the unique attributes of the assets at issue. Instead of relying upon sanctions that seek to compel contemnors to comply, courts could instead act directly on the assets at issue by exercising power over intermediaries who facilitate transactions of the assets subject to court orders without the contemnor's cooperation.[180]

J. State or Federal Cryptoasset Registries

Unlike cash, many cryptoassets[181] are non-fungible and thus identifiable, either by sender public key address,[182] or by transaction output[183] in the case of Bitcoin-based systems. Courts could use these attributes to impose a novel form of lien against the cryptoassets at issue. State legislatures could create public key registries, akin to state secured transaction registries,[184] wherein courts could "add" public key addresses, discrete transaction outputs, or both (Listed Cryptoassets) for identifiable assets associated with the wallets known to be used by parties that are charged with compliance with turnover orders. A so-called Listed Cryptoasset Registry (LCR) would provide actual notice to the public that Listed Cryptoassets found thereon are subject to turnover orders. State law could then require regulated money services businesses to cross reference the LCR before permitting any transaction, to seize any transactions including Listed Cryptoassets, and to report that seizure to the listing court for further order. State law could prohibit other parties from entering into

[180] Once contempt has been established, a district court has "broad discretion to fashion an appropriate coercive remedy . . . based on the nature of the harm and the probable effect of alternative sanctions." EEOC v. Local 28, 247 F.3d 333, 336 (2d Cir. 2001) (quoting N.A. Sales Co. v. Chapman Industries Corp., 736 F.2d 854, 857 (2d Cir. 1984)).

[181] Certain cryptoasset systems, like Zcash, Monero, Beam, and Grin include native features that provide additional transactional privacy for their users. This additional transactional privacy complicates tracing of these assets. Some cryptoasset users intentionally obscure their transactions by using protocols that provide additional privacy, like coinjoin, or services like mixers or tumblers that commingle transactions to provide additional privacy. Tokenized versions of securities are distinct from these assets as lost securities may be replaced by the issuer, and issuers of tokenized securities will typically respond to valid court process. Those asset types and transaction types are excluded from the analysis and proposals suggested herein.

[182] Although best practices suggest never reusing public keys, and new public keys can be generated for each transaction by hierarchical deterministic wallets, no wallet software mandates this practice and it is foreseeable that sloppy users may reuse public keys. *See generally Address reuse,* BITCOIN WIKI, https://en.bitcoin.it/wiki/Address_reuse [https://perma.cc/W4UL-2KGA].

[183] All transaction outputs are identifiable. Identifiable unspent transaction outputs, called "UTXOs," are increments of Bitcoin value that have not yet been spent by their holder. *See generally Unspent Transaction Output, UTXO*, BITCOIN, https://bitcoin.org/en/glossary/unspent-transaction-output [https://perma.cc/NKJ3-ND2E].

[184] *See, e.g.*, *Welcome to the Florida Secured Transaction Registry*, FLORIDA SECURED TRANSACTION REGISTRY, https://www.floridaucc.com/uccweb/ [https://perma.cc/Q4RJ-96KF].

transactions including Listed Cryptoassets[185] and impose criminal penalties for violations.[186]

This strategy would require state by state legislative enactment. State regulated money services businesses may claim that referencing multiple lists of transaction outputs and public key addresses before permitting a customer transaction is unduly burdensome. However, comparing transaction public key addresses or transaction outcomes would be a simple task for a smart contract, which reduces the prospective burden on regulated intermediaries.[187] Alternatively, this registry could be created at the federal level by legislation that requires compliance by all intermediaries registered with the Financial Crimes Enforcement Network, which would centralize the Listed Cryptoassets into a single list.

Advocates for the censorship-free use of cryptocurrencies will likely read this proposal as antithetical to the purpose of cryptocurrency. However, neither the Nakamoto whitepaper nor the cypherpunk manifesto[188] suggest that violation of the law for personal gain is a core value or motivation underlying the creation of cryptocurrencies.

K. Use BSA-created Infrastructure

Alternatively, courts could impose a lien on Listed Cryptoassets by creating a list that would be regularly circulated using the infrastructure created by the Bank Secrecy Act[189] in a manner similar to the Office of Foreign Asset Control's (OFAC) Specially Designated Nationals and Blocked Persons list (SDN),[190] which precludes regulated entities from engaging in transactions of value, including cryptoassets,[191] from listed public addresses, including cryptoasset public key addresses.[192]

[185] The same "blacklisted" Listed Cryptoassets Registry could be mandated to be added as a screening criterion at the wallet level.

[186] States could also amend their statutes criminalizing transactions in stolen property to include Listed Cryptoassets found on that state's LCR.

[187] Polymath, for example, uses smart contracts that restrict transactions at the token level by referencing whitelists that determine whether a transaction is permitted. *See generally* Pablo Ruiz, *Everything You Always Wanted to Know About Restricting Token Transfers But Were Afraid to Ask*, POLYMATHNETWORK (June 7, 2018), https://blog.polymath.network/all-you-ever-wanted-to-know-about-restricting-token-transfers-827009d649b7 [https://perma.cc/7EFH-E6M2].

[188] Eric Hughes, *A Cypherpunk Manifesto*, ACTIVISM.NET (Mar. 9, 1993), https://www.activism.net/cypherpunk/manifesto.html [https://perma.cc/B7RY-KPY2].

[189] *See generally* 31 U.S.C.§ 310 (2012) *et seq*.

[190] *See generally Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists*, DEP'T OF TREASURY, https://www.treasury.gov/resource-center/sanctions/sdn-list/pages/default.aspx [https://perma.cc/T4MZ-RMEW].

[191] *Id.*

[192] Andrew Hinkes & Joe Ciccolo, *OFAC's Bitcoin Blacklist Could Change Crypto*, COINDESK (Mar. 24, 2018), https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

However, OFAC's SDN list was created due to national security concerns, and enforcement of turnover orders are unlikely to qualify as national security issues.[193] Likewise, the SDN list is only updated on a monthly basis, which is unlikely to be sufficient given the speed at which cryptoassets travel.

L. Modify Existing State Law Writs of Attachment

Alternatively, courts could issue modified writs of attachment that would direct state regulated money services businesses to freeze or seize transactions including Listed Cryptoassets. Procedurally, the proponent of contempt would be required to serve the writ upon the various intermediaries who may be asked to facilitate transactions including Listed Cryptoassets. This approach would burden parties to identify and individually serve each regulated intermediary which may potentially facilitate transfers of Listed Cryptoassets. Legislation could require state regulators to maintain a public list of contact information for regulated intermediaries for service of process, or to create a central "hub" that would permit streamlined service of process upon a single entity that would qualify as service upon all state-registered intermediaries. The contemplated writ would require the regulated entities to serve a response that would indicate if the intermediary has processed any transactions including the Listed Cryptoassets, to provide information related to those transactions, to seize any transactions including the Listed Cryptoassets, and to update the court with additional replies if they seize any transactions including those Listed Cryptoassets. When a regulated intermediary reports that they have frozen or seized a Listed Cryptoasset, the court could order that intermediary to transact those cryptoassets to the proponent of the contempt, and the court would by order remove that asset from the LCR, functionally removing the "mark" from those assets, and permitting the

[https://perma.cc/VLS2-LDD9] ("What happens if you receive a transaction from a listed digital currency address? It is possible that the received coins would then be 'tainted' as being linked back to a listed individual or entity, and that your identity and digital currency address may then be added to the OFAC list."); OFAC FAQs: Sanctions Compliance, DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx [https://perma.cc/N975-LXED].

[193] Terrorism and Financial Intelligence, DEP'T OF THE TREASURY, https://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx [https://perma.cc/A3VQ-FT2L] ("The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.").

party receiving those cryptoassets to take them free and clear of any cloud on title.[194]

Each of the above proposals would have the effect of "marking" those transaction outcomes or assets held by designated public key addresses so that they are distinct from other similar assets. This would practically destroy the fungibility of those assets and make those marked assets less useful, less marketable, and likely less valuable. Subsequent purchasers of those assets or lenders offered those assets as collateral would reject those transactions as a result of the lien.

Of course, this lien or "marking" system would potentially implicate the rights of third parties who may receive those assets as part of an arms-length transaction and who would believe that they are *bona fide* purchasers of those cryptoassets. The law enacted to create the lien could provide for the purported owner, recipient of the seized cryptoassets, or both to receive notice and an opportunity to contest the seizure prior to the turnover of those assets. These priority contests would be handled by courts like other lien priority matters.

This new approach to contempt strikes an elegant balance. It does not harm a contemnor who actually lost her private key, because the cryptoassets associated with a lost private key will not be transacted and therefore marking them, and by so doing destroying their fungibility, causes no harm. Barring unforeseen technical innovation, those assets will forever remain illiquid and un-negotiable. However, this approach may allow a party to recover cryptoassets transacted by a thief or hacker using a stolen private key, and may result in the identification of the hacker or thief. Likewise, marking or imposing a lien on cryptoassets would harm a lying contemnor who intends to profit from the secreted assets by significantly impairing their value and transactability. This strategy also potentially allows a court to catch a lying contemnor violating the turnover order. All of these factors disincentive future contemnors from tactically claiming private key loss and "waiting out" an incarceration sanction with the expectation that valuable assets will be available upon release.[195] Finally, this sanction may allow the proponent of contempt to recover cryptoassets regardless of the contemnor's cooperation.

Unlike typical contempt sanctions, these new strategies do not seek to compel the contemnor to take some action to comply with the turnover

[194] *See, for example*, 11 U.S.C. § 363(f) (2012), which allows property to be sold "free and clear" of other property interests under specific conditions.

[195] There would likely emerge a "black market" for these encumbered cryptoassets; reducing fungibility may drive these assets out of the system of regulated intermediaries, or out of the United States' jurisdiction.

order; as a result they may be preferable to coercive imprisonment of the contemnor on policy grounds as well.[196] Although these new strategies could be viewed as independent remedies, they are consistent with typical civil contempt remedies as they directly benefit the opposing party and seek to effectuate the court's orders.[197]

CONCLUSION

Cryptoassets are now commonly held and are marketed to integrate with, and in some instances, to replace traditional financial products. As these assets approach ubiquity, parties in litigation and courts will be challenged to exercise power over cryptoassets. Given that actual control of considerable wealth frequently exists as ephemeral and easily communicated data, recalcitrant parties may be incentivized to hide, through omission or non-disclosure, the credentials needed to access that value, and may conveniently claim to have lost private keys. These contemnors may be willing to "wait out" a contempt sanction after resisting an order that requires disclosure or the use of private keys to execute a transaction if they know that their cryptoassets will be available to them after their inevitable release.

Courts have wide latitude to fashion remedies for contempt, provided that, in the civil context, those remedies are not punitive and are intended to coerce compliance. However, where bearer forms of data is equivalent to value and there are a variety of means to communicate that data to third parties, even the drastic sanctions of open-ended incarceration with full surveillance of all communications suggested in this article may be insufficient to coerce a truly motivated contemnor to comply with a turnover order, or to prevent that contemnor from violating the order. Instead, parties and courts should enter proscriptive disclosure injunctions that require backups of private keys to be made and retained, which would both reduce the likelihood of tactical claims of lost private keys and provide the legal predicate for severe sanctions for noncompliance or subsequent loss. Courts should also look to new types of sanctions that leverage the capabilities of cryptoasset systems, including new laws that can compel regulated intermediaries to lien, identify and seize transfers of implicated cryptoassets. Maybe, if courts act directly against the cryptoassets at issue, they may not need to imprison contemnors at all;

[196] *The Coercive Function of Civil Contempt*, *supra* note 143, at 129 ("[W]hen a complainant can effectively proceed by ordinary attachment or garnishment proceedings, policy dictates that the coercive remedy should not be available.").

[197] Grote, *supra* note 73, at 1256.

maybe courts don't need to throw away the contemnors with their private keys.