FIU Law Review

Volume 13 | Number 6 Article 16

2019

The Challenges of Cryptocurrency Asset Recovery

Andrew W. Balthazor
J.D. candidate, 2019, Florida International University (FIU) College of Law, abalt009@fiu.edu

Online ISSN: 2643-7759

Recommended Citation
Andrew W. Balthazor, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. Rev. 1207 (2019).
Available at: https://ecollections.law.fiu.edu/lawreview/vol13/iss6/16

THE CHALLENGES OF CRYPTOCURRENCY ASSET RECOVERY

Andrew W. Balthazor*

ABSTRACT

Cryptocurrencies, like Bitcoin, present challenges to plaintiffs seeking to recover these digital assets. No third-party intermediaries are involved in cryptocurrency transactions, and there is no controlling authority that can revoke or avoid a transaction once completed. The possessor of a cryptocurrency's private key—its password—has total and exclusive control over the account's assets. These digital assets cross jurisdictional boundaries without impediment. The features of cryptocurrencies make it easy for defendants to judgment-proof themselves and make these assets difficult to recover after a court has entered judgment. This comment explains cryptocurrency features relevant to asset recovery, explores pre- and post-judgment procedures as applied to cryptocurrencies, and suggests ways to mitigate the risks of this potentially difficult-to-recover asset.

* J.D. candidate, 2019, Florida International University (FIU) College of Law; United States Military Academy, B.S. 1999. For help with my research for this article I would like to thank Professor Thomas Baker of the FIU College of Law, who sent me numerous articles regarding Bitcoin; my colleague Eve Peres Torres, whose assistance researching cryptocurrency cases was invaluable; my colleague and Law Review editor Lauren Odom, who provided very useful substantive feedback; and Professor Howard Wasserman of the FIU College of Law, who advised me regarding content and organization.

I. INTRODUCTION

Paul Vernon of Cryptsy, a Florida-based cryptocurrency exchange, stole more than 11,000 bitcoins in 2014 and fled to China.[1] Affected customers filed a class action suit in the United States District Court for the Southern District of Florida.[2] The court ordered a default judgment against Vernon, declaring the stolen bitcoins the property of the plaintiff class.[3] But the plaintiffs have been unable to recover the stolen currency.[4] They know where the funds are located: in bitcoin addresses, similar in function to a bank account.[5] But the victims cannot access the funds associated with those addresses without the private keys: strings of characters that grant access to those bitcoin addresses.[6] The prevailing plaintiffs do not know the private keys—and do not know anyone else who would know them—with the exception of the thief, Vernon.[7]

Courts are limited in their power to force the illegitimate wielder of a private key to return stolen cryptocurrency, due to the qualities of this intangible asset.[8] Cryptocurrencies' only real-world footprint are the private keys granting access to the funds, and then only if the private key is stored somewhere tangible.[9] Cryptocurrencies ignore physical borders, transaction quantity limits, or other traditional currency controls. And cryptocurrency transactions, once completed, are essentially irreversible due to the lack of a

1 Angela Morris, *Judge Orders $30 Million in Bitcoin to Be Returned in Cryptocurrency Class Action*, MIAMI DAILY BUS. REV., Aug. 3, 2017, at A1, *available at* https://advance.lexis.com/api/permalink/e067ba8f-6e83-4192-a430-dcc793182938/?context=1000516.

2 *Id.*

3 Final Default Judgment at 1–2, Liu v. Project Inv'rs, No. 9:16-cv-80060 (S.D. Fla. July 27, 2017), ECF No. 123 [hereinafter Liu Final Default Judgment].

4 Morris, *supra* note 1.

5 *See* Liu Final Default Judgment, *supra* note 3, at 2.

6 *See* Morris, *supra* note 1.

7 *Id.* Cryptsy's receiver hired a former employee to perform a tracing analysis of Vernon's theft, concluding that Vernon transferred cryptocurrencies to digital wallets under Vernon's control. Affidavit of Nicholas Mullesch (August 5, 2016) at 6–7, *Liu*, 9:16-cv-80060 (attachment # 1 to the plaintiffs' motion for entry of final default judgment) [hereinafter Mullesch Affidavit].

8 *See* Morris*, supra* note 1.

9 Max I. Raskin, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. 969, 975 (2015).

controlling authority that can undo transactions.[10] Digital currencies are freely transferrable from one digital wallet to another without need for a bank or other third-party intermediary, unlike conventional currencies or securities.[11] Cryptocurrency is under the sole control of whomever has the private key to a bitcoin address; only the person possessing the private key of a receiving account has any power over the funds received.[12]

This new "digital gold" is particularly attractive to thieves, who need only purloin the private key to gain control of hundreds of millions of dollars in virtual wealth.[13] Private keys are vulnerable to both cyber and traditional theft.[14] Thieves no longer need be concerned about physically breaking and entering property, or fleeing a jurisdiction with their ill-gotten gains; they simply need access to a private key for mere moments to complete a cryptocurrency heist.[15] And once a thief with a private key transfers digital funds, those criminal transactions cannot be undone unless the recipient account's private key holder can be identified.[16]

The only method to return stolen cryptocurrency is to gain control of the private key associated with the bitcoin address in which the currency stored, which may be impossible. Bitcoin addresses are often anonymous.[17] And because a thief can transfer the funds to an account controlled by a physically-distant person, that person—even if identifiable—may be out of reach by whatever court asserted jurisdiction over the stolen cryptocurrency litigation.[18] In such a situation only the physical assets within the jurisdiction of appropriate courts would be subject to a court's judgment. Even assuming the cryptocurrency thief had reachable assets, their value may be insignificant compared to the value of the stolen currency.

Vernon's Cryptsy victims faced this problem. They knew who possessed the stolen currency, and which bitcoin addresses contained their

10 *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN PROJECT, 1, http://bitcoin.org/bitcoin.pdf.

11 *See* Nakamoto, *supra* note 10, at 1.

12 Raskin, *supra* note 9, at 975.

13 Cryptocurrency values are volatile, but at the time of writing this the value of Vernon's stolen 11,325 bitcoins was approximately US $142 million. *bitcoin (USD) Price*, COINDESK, https://www.coindesk.com/price/ (last visited Mar. 13, 2018) [hereinafter COINDESK *bitcoin Price*].

14 *See* Raskin, *supra* note 9, at 977.

15 *See id.* at 989.

16 *See* Nakamoto, *supra* note 10, at 1.

17 *See* Nakamoto, *supra* note 10, at 6.

18 *See* Raskin, *supra* note 9, at 998.

stolen bitcoins.[19] But Vernon had fled to China, [20] leaving behind real-world assets worth less than two percent of the value of the stolen bitcoins.[21] Vernon ignored the court's jurisdiction, failing to respond to the action in any way. [22] Out of the country and out of reach, the court was powerless to force Vernon to return or to surrender his ill-gotten gains.[23]

Cryptocurrency's value and susceptibility to theft will attract criminals at an ever-increasing rate. At least 10% of Bitcoin—the most prevalent cryptocurrency in the world—has been stolen and recirculated.[24] Cryptocurrencies are volatile but maintain significant real-world value. Motivated thieves are creatively applying criminal schemes designed to illicitly transfer this digital wealth.[25] The lack of any method to undo a cryptocurrency heist or provide an effective remedy to victims means that once cryptocurrencies are lost, they may be lost forever.

This comment identifies the challenges presented by applying conventional judgment enforcement and asset recovery procedures to cryptocurrencies. It begins by providing relevant background regarding cryptocurrencies. This includes cryptocurrency properties, how cryptocurrencies interact with the financial system, and some common characteristics of cases where quantities of cryptocurrency are held by defendants or are subject to judgment. The comment then explores the efficacy of existing asset recovery procedures applied to cryptocurrencies, including procedures intended to prevent defendants from moving or hiding assets, and why in many situations such procedures are unsatisfactory. Finally, this comment suggests ways to mitigate the risks of an unsatisfactory recovery when dealing with defendants possessing cryptocurrency.

II. UNDERSTANDING CRYPTOCURRENCY

Understanding the abstract characteristics of cryptocurrencies is necessary to appreciate the limitations of asset recovery procedures as applied to bitcoin. What follows is an introduction to the relevant features of

19 Morris, *supra* note 1; *see* Liu Final Default Judgment, *supra* note 3, at 2.

20 Second Amended Class Action Complaint at 10, Liu v. Project Inv'rs, No. 9:16-cv-80060 (S.D. Fla. filed Jan. 9, 2017) (basing the allegation on Vernon's ex-wife's filings pursuant to their divorce, which was contemporaneous with Vernon's theft from Cryptsy and its customers) [hereinafter Liu Complaint].

21 *See id.* at 10–11 (basing allegations of Vernon's net worth on Vernon's affidavit filed pursuant to his divorce: less than $2 million).

22 *See* Liu Final Default Judgment, *supra* note 3, at 1.

23 Morris, *supra* note 1.

24 *See* Raincoaster, *Ten Percent of All Bitcoin in Circulation was Just Stolen*, THE CRYPTOSPHERE (Feb. 9, 2015), https://thecryptosphere.com/2015/02/09/ten-percent-of-all-bitcoin-in-circulation-was-just-stolen/.

25 *See* Raskin, *supra* note 9, at 998 & n.217.

cryptocurrencies and how these assets interact with the real world. This includes a presentation of characteristics common to cases involving recovery of digital currencies. The properties of cryptocurrencies and the characteristics of cryptocurrency cases work in concert to make it difficult to recover these novel assets.

A. Bitcoin: The Original Cryptocurrency

Cryptocurrencies are mediums of exchange that exist as a compilation of digital transactions. The first and most widely used such currency is Bitcoin.[26] All succeeding cryptocurrencies are based on the same technology underpinning Bitcoin, and they share many of the same features.[27]

In 2008,[28] Satoshi Nakamoto[29] proposed Bitcoin as a peer-to-peer system for exchanging value independent of any central authority.[30] Nakamoto sought to create a system that would eliminate the need for a trusted intermediary to negotiate payments.[31] Such a system would allow "non-reversible payments," theoretically reducing transaction costs.[32] It would also eliminate the need for merchants to gather information from customers, a need that exists only when merchants must submit the payment information to a traditional third-party payment processor for verification of funds.[33]

1. Operational Features

Bitcoin has many features that serve to remove it from the sphere of control of government. The owner of bitcoins has complete control over her digital wealth, and no outside force can take bitcoins from an owner who maintains integrity of their ownership.[34] Bitcoin is decentralized and democratic by design, operating without any central authority that can

26 *FAQ*, BITCOIN PROJECT, https://bitcoin.org/en/faq (last visited Feb. 19, 2018) [hereinafter BITCOIN *FAQ*]. Throughout this Comment, the word Bitcoin is capitalized when it is used as the name of the Bitcoin software itself. Lowercase type is employed when referring to individual units of value.

27 *See* BITCOIN *FAQ*, *supra* note 26.

28 *See* Raskin, *supra* note 9, at 971.

29 The identify of Satoshi Nakamoto is a mystery. *See id.* at 974 n.31. *But see* BLOOMBERG, *Self-Proclaimed Inventor of Bitcoin Accused of Swindling $5 Billion in Cryptocurrency*, FORTUNE (Feb. 27, 2018), http://fortune.com/2018/02/26/craig-wright-bitcoin/.

30 *See* Nakamoto, *supra* note 10, at 1.

31 *Id.*

32 *Id.*

33 *Id.*

34 *See* Raskin, *supra* note 9, at 977.

enforce its will on users; any changes to the Bitcoin system are only implemented by majority consent of all worldwide users running the software.[35] Transactions ignore political borders, are irrevocable absent the consent of the possessor, and ownership of bitcoins is anonymous. Because of the software's mechanics, it is practically impossible for any government, or any group, to control Bitcoin.[36]

The units of exchange of the Bitcoin system are bitcoins, an entirely digital resource controlled only by those who generate or receive them.[37] There are no physical "coins."[38] Instead, bitcoins are associated with an address.[39] Each address has its own alphanumeric designation, serving a function like a bank account number.[40] Knowing a bitcoin address allows anyone to deposit funds into it. But to use the digital funds associated with a bitcoin address, one must also possess the private key, which is a different alphanumeric string of characters.[41] Only the possessor of an address's private key may make withdrawals—outgoing payments.[42]

Bitcoin's backbone is a distributed digital ledger known as a blockchain.[43] The Bitcoin blockchain contains a complete record of all transactions.[44] Determining the "account balance" for a Bitcoin address is done by adding all incoming and outgoing transactions associated with the address.[45] The Bitcoin blockchain, which stores the digital ledger of transactions, is a distributed database.[46] It is distributed in the sense that many copies of the same database reside on every computer running the Bitcoin software.[47] If a user attempts to send bitcoin from an address, the Bitcoin algorithm validates that the user has the correct private key and the requisite

35 *See* BITCOIN *FAQ*, *supra* note 26.

36 *See* Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L.J. 139, 144–45 (2016) (describing as "preposterous" the idea that any one group could accumulate the computing power necessary to reverse transactions or make unilateral changes to the software).

37 *See* Raskin, *supra* note 9, at 975–78.

38 There are physical bitcoins that are gag gifts or "conversation pieces," but they are extraneous to the Bitcoin system itself. *See* Nermin, Hajdarbegovic, *10 Physical Bitcoins: The Good, the Bad and the Ugly*, COINDESK (Sep. 14, 2014, 4:15 PM), https://www.coindesk.com/10-physical-bitcoins-good-bad-ugly/.

39 *See* Raskin, *supra* note 28, at 975.

40 *Id.*

41 *Id.*

42 *Id.*

43 *Id.*

44 *See* Nakamoto, *supra* note 30, at 2.

45 *See* Raskin, *supra* note 28, at 975.

46 *Id.*

47 *See* BITCOIN *FAQ*, *supra* note 26.

bitcoins available for the transaction.[48] Every computer running the Bitcoin software conducts this validation on its copy of the distributed database.[49] The validating computers compare their results via the internet.[50] Transactions are only processed if the majority of the computers running the software agree a transaction is valid.[51] As the software processes transactions, the transactions are added to the distributed ledger in batches known as blocks, lengthening the chain of transactions maintained by every copy of the distributed database: the blockchain.[52]

Without numerous computers running the Bitcoin software, the system would be vulnerable to control by a single entity with sufficient computer resources.[53] The decentralized ledger model only works because Bitcoin has an integrated feature that encourages broad adoption of the software: bitcoin mining.[54] Bitcoin mining is operating the Bitcoin software as a validating computer, processing bitcoin transactions. To incentivize broad adoption of the Bitcoin software by computers for validating transactions, bitcoin mining generates new bitcoins for the bitcoin miner, adding to the global supply.[55] Miners may also earn transaction fees paid by those conducting transactions.[56]

Conducting Bitcoin transactions only requires that a user have access to the software and be connected to the internet.[57] She then may freely transfer the digital assets to other Bitcoin addresses if the software validates those transactions.[58] Geographic or political borders are irrelevant; transactions cross jurisdictions limited only by the reach of the internet.

Adding transactions to the blockchain is essentially irrevocable.[59] Adding a new transaction that reverses the effect of a transaction is possible, but only the possessor of a private key can do so. Without the private key, the majority of the computers attempting to validate the transaction would interpret the transaction as invalid. However, a single person or group could gain majority control of computers running the cryptocurrency software and

48 *See* Raskin, *supra* note 9, at 975–76.

49 *See* BITCOIN *FAQ*, *supra* note 26.

50 *Id.*

51 *Id.*

52 *Id.*

53 *See* Nakamoto, *supra* note 30, at 8.

54 *See id.* at 4.

55 *Id.*

56 *Id.*

57 *See* BITCOIN *FAQ*, *supra* note 26.

58 *See id.*

59 *See* Nakamoto, *supra* note 30, at 1.

then "validate" any transactions they wished.[60] This type of "51% attack" is impractical to execute if the cryptocurrency software is running on sufficient numbers of computers.[61] Asserting control over the Bitcoin software like this is impractical, given the large number of computers running the Bitcoin software.[62] It is exactly this type of attack that bitcoin mining is designed to prevent, by encouraging users to run the software to mine coins.

Accordingly, Bitcoin users cannot remove or reverse transactions if made by accident or fraud. The received bitcoins are fully under the control of the person who possesses the private key associated with the recipient bitcoin address. The recipient is the only person who can return the funds. There is no appeal and no authority to turn to that can help.

A consequence of Bitcoin's blockchain—its distributed ledger, stored on every computer running the Bitcoin software—is that all Bitcoin transactions are public.[63] Knowing a Bitcoin address allows one to know every incoming and outgoing bitcoin transaction associated with the address.[64] Ownership of a Bitcoin address is anonymous within the blockchain. This anonymity carries a substantial caveat:

> [T]he anonymity is by no means perfect. Security experts call it pseudonymous privacy, like writing books under a nom de plume. You can preserve your privacy as long as the pseudonym is not linked to you. But as soon as somebody makes the link to one of your anonymous books, the ruse is revealed.[65]

The distributed ledger allows tracing of bitcoin back to its generation, by following the trail of Bitcoin addresses through which the bitcoin has traveled.[66]

Bitcoin's features support its design: to be a digital currency operating outside the control of any central authority.[67] The Bitcoin system's mining-

60 *See id.* at 4.

61 *Compare* Daniel Cawrey, *Are 51% Attacks a Real Threat to Bitcoin?*, COINDESK (June 20, 2014, 6:42 AM), https://www.coindesk.com/51-attacks-real-threat-bitcoin/ (discussing the improbability of a 51% attack on Bitcoin), *with* Kai Sedgwick, *Verge is Forced to Fork After Suffering a 51% Attack*, BITCOIN.COM (Apr. 5, 2018), https://news.bitcoin.com/verge-is-forced-to-fork-after-suffering-a-51-attack/ (reporting the successful 51% attack on a smaller, less-used cryptocurrency).

62 *See* BITCOIN *FAQ*, *supra* note 26.

63 *Bitcoin Transactions Aren't as Anonymous as Everyone Hoped*, MIT TECH. REV.: EMERGING TECHNOLOGY FROM THE ARXIV (Aug. 23, 2017), https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/ [hereinafter ARXIV].

64 *Id.*

65 *Id.*

66 *See* Adam Ludwin, *How Anonymous is Bitcoin? A Backgrounder for Policymakers*, COINDESK (Jan. 25, 2015, 8:45 AM), https://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/.

67 *See* Nakamoto, *supra* note 30, at 1.

incentive model expands the number of validating nodes checking transactions and maintaining copies of the distributed ledger. The decentralized spread of the Bitcoin network, its autonomous consensus-based transaction validation algorithm, and its lack of a centralized controlling authority prevents any one group or government gaining control over the Bitcoin network.

2. Security Features

Bitcoin is subject to theft like any other asset.[68] The Bitcoin system's decentralization and cryptographic-based security help maintain the system's integrity. But individual bitcoin accounts are only as secure as the possessor's private key.

Theft by manipulating the Bitcoin algorithm itself is unlikely, due to Bitcoin's decentralized consensus-based model.[69] Bitcoin is only transferred if the transaction is validated by a majority of the computer nodes running the Bitcoin software; invalid transactions are rejected.[70] New bitcoins, generated by miners, are validated and added in a way that is impossible to replicate artificially.[71] Persons attempting to adjust the computer code underlying the software and inject counterfeit transactions would find their transactions invalidated by the majority of the computer nodes running unadulterated versions of the software.[72] Double-spending of the same digital currency, or counterfeit creation of bitcoins, is thus impossible.[73]

Complex mathematical equations founded on cryptography protect bitcoins possessed by individual owners, hence the name: cryptocurrency.[74] Bitcoins associated with a bitcoin address can only be spent by those who

68 *See* Raskin, *supra* note 9, at 989.

69 *See* Nakamoto, *supra* note 10, at 8.

70 *See id.* at 3.

71 *See id.* at 4.

72 *See id.* at 2.

73 See *id.*

74 *See* BITCOIN *FAQ*, *supra* note 26.

possess that address's private key.[75] It is theoretically impossible to crack a private key.[76] Bitcoin has no password recovery tools.[77]

Private keys are the one Achilles heel of the Bitcoin system. Thieves can steal private keys, providing unfettered access to the associated digital assets.[78] Owners protect and store private keys in a variety of ways.[79] Some go low-tech: private keys written down on paper.[80] Hard-copies of private keys are impervious to cybertheft. Others store their private keys on offline digital devices, likewise making them immune to hacking.[81] Some owners with substantial cryptocurrency assets under their control may split up their private keys, placing different parts of the same key in separate locations.[82] This prevents a single theft from compromising their digital hoard, deterring thieves from attempting what would require a series of coordinated heists. There are several digital wallet software options which can store numerous private keys.[83] These digital wallets are themselves protected by additional layers of encryption, passcodes, and multi-factor authorization.[84] For example, one bitcoin owner wears a ring with an embedded code that grants him access to his digital wallet.[85] Digital wallets are stored either on remote servers or locally, providing a tradeoff between convenience and security.[86]

75 Raskin, *supra* note 9, at 975.

76 *See* BITCOIN *FAQ*, *supra* note 26; *see also* Matthew Sparkes, *The £625m Lost Forever - The Phenomenon of Disappearing Bitcoins*, THE TELEGRAPH (Jan. 23, 2015), https://www.telegraph.co.uk/technology/news/11362827/The-625m-lost-forever-the-phenomenon-of-disappearing-Bitcoins.html ("Security expert Bruce Schneier once ruled out an attempt to crack a 256-bit key, of the type used by Bitcoin, by referring to the laws of physics: such is the magnitude of the problem. Even an impracticably large computer consuming all the energy outputted by the sun couldn't count the number of possible combinations in several decades.").

77 *See* BITCOIN *FAQ*, *supra* note 26 ("[L]ost bitcoins remain dormant forever because there is no way for anybody to find the private key(s) that would allow them to be spent again.").

78 Raskin, *supra* note 9, at 989.

79 *See id.* at 990–91 (describing storing private keys on paper stored in safety deposit boxes, in the cloud, or on hard drives).

80 *Id.* at 990.

81 *Securing Your Wallet*, BITCOIN PROJECT, https://bitcoin.org/en/secure-your-wallet (last visited Feb. 19, 2018) [hereinafter BITCOIN *Wallet*].

82 *See, e.g.*, *Secure Bitcoin Storage*, COINBASE, https://www.coinbase.com/security (last visited Jan. 1, 2018) [hereinafter COINBASE *Bitcoin Storage*] (describing how Coinbase, one of the largest cryptocurrency exchanges in the world, secures its "bitcoin geographically in safe deposit boxes and vaults around the world").

83 BITCOIN *Wallet*, *supra* note 81.

84 *Id.*

85 Max Raskin, *Meet the Bitcoin Millionaires,* BUSINESSWEEK (Apr. 12, 2013, 12:41 PM), http://www.businessweek.com/articles/2013-04-10/meet-the-bitcoin-millionaires.

86 BITCOIN *Wallet*, *supra* note 81.

B. Cryptocurrency Exchanges

Bitcoin has thus far failed to displace conventional payment systems and currencies.[87] The purpose of Bitcoin was to act as a medium of exchange outside the control of governmental central banks, placing financial assets completely within the domain of the owner.[88] Achieving this purpose required widespread adoption by merchants. But widespread adoption has not happened.[89] Purveyors of goods and services are reluctant to accept bitcoin payments because of the asset's volatility, high transaction fees, and slow transaction times.[90] Traditional payment systems are comparatively cheaper and faster and conventional fiat currency is a more predictable store of value.

If Bitcoin is not replacing other currencies or payment systems, it must intersect with conventional currencies for people to make meaningful use of their assets.[91] Some owners transact bitcoins for traditional currencies by locating interested parties using message boards or websites.[92] This practice can be cumbersome and prone to problems. It may take time to find another person who meets desired terms. And because Bitcoin transactions are peer-to-peer and do not involve a third party, any transaction is fraught with the risk that if you send your bitcoins to another they may simply abscond with the currency and disappear.[93]

Cryptocurrency exchanges offer a place to buy or sell cryptocurrencies for conventional currencies.[94] They attract a high volume of traders, like a stock exchange.[95] Many exchanges operate like a third-party escrow service; the two traders exchange their assets with the exchange, and only once the exchange has received the assets from both parties does the exchange release funds to their respective new owners.[96] Cryptocurrency exchanges operate by charging a per-transaction fee and work with a variety of different digital and

87 Christopher, *supra* note 36, at 152 (observing that bitcoins are not a functional currency because they are not used by enough people for bitcoins to be a medium of exchange).

88 *See* Nakamoto, *supra* note 10, at 1.

89 Christopher, *supra* note 36, at 152.

90 *Id.*

91 *See* Christopher, *supra* note 36, at 151.

92 *See* BITCOIN *FAQ*, *supra* note 26; *e.g.*, LOCALBITCOINS.COM (last visited Feb. 19, 2018).

93 *See* BITCOIN *FAQ*, *supra* note 26; *e.g.*, Hallie Detrick, *Someone Stole 7 Bitcoins from Apple Co-Founder Steve Wozniak*, FORTUNE (Feb. 27, 2018), http://fortune.com/2018/02/27/apple-steve-wozniak-bitcoin-theft/ ("Wozniak sold the bitcoins to someone who paid for them with a credit card. The credit card transaction was then cancelled before it cleared, leaving him with nothing to show for [it]. The credit card number turned out to be stolen . . . .").

94 *See* BITCOIN *FAQ*, *supra* note 26.

95 Christopher, *supra* note 36, at 151.

96 *Id.*

fiat currencies. Cryptocurrency exchanges maintain fiat currency accounts for their operations, as well as bitcoin and other cryptocurrency addresses as necessary.

Cryptocurrency exchanges provide convenient methods to exchange digital and conventional currencies using online accounts.[97] These exchange-managed accounts serve the same functions as digital wallets. And like digital wallets, owners may protect cryptocurrency exchange accounts with encryption, passcodes, and multi-factor authorization.[98]

Exchanges add vulnerabilities to the cryptocurrency ecosystem by providing additional avenues of attack for thieves:[99] the assets held by the individual owners (accessible via their exchange-managed account), and the assets held by the exchange itself.[100] Cryptocurrency exchanges are vulnerable to cybertheft because exchanges must be online to conduct cryptocurrency transactions.[101] Mt. Gox was the largest cryptocurrency exchange in the world until it began collapsing in 2013.[102] It lost 850,000 bitcoins due to hacking.[103] Exchanges mitigate the risk of cybertheft by keeping some portion of their digital assets offline, using private keys stored away from the internet.[104] Cryptocurrency exchanges are also prone to familiar white-collar crimes: embezzlement and fraud.[105] Vernon's Cryptsy customers learned this the hard way, when he embezzled the entirety of his exchange's assets to accounts under his personal control.[106]

---

97 *See, e.g.*, *How to Buy Bitcoin*, COINBASE, https://www.coinbase.com/buy-bitcoin (last visited Dec. 20, 2018).

98 *See, e.g.*, *How Can I Make My Account More Secure?*, COINBASE: SUPPORT, https://support.coinbase.com/customer/en/portal/articles/1447997-how-can-i-make-my-account-more-secure- (last visited Dec. 20, 2018).

99 Steve Stecklow, Alexandra Harney, Anna Irrera & Jemima Kelly, *Special Report: Chaos and Hackers Stalk Investors on Cryptocurrency Exchanges*, REUTERS (Sept. 29, 2017, 6:55 PM), https://www.reuters.com/article/legal-bitcoin-exchanges-risks/special-report-chaos-and-hackers-stalk-investors-on-cryptocurrency-exchanges-idUSKCN1C42JV ("These exchanges, which match buyers and sellers and sometimes hold traders' funds, have become magnets for fraud and mires of technological dysfunction . . . .").

100 *See* Jason Tashea, *What's Actually Happening When a Cryptocurrency Gets Hacked?*, ABA J. (Feb. 28, 2018, 12:32 PM), http://www.abajournal.com/lawscribbler/article/whats_actually_happening_when_a_cryptocurrency_gets_hacked/?utm_source=feeds&utm_medium=rss&utm_campaign=site_rss_feeds.

101 *See, e.g.*, Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014, 6:30 AM), https://www.wired.com/2014/03/bitcoin-exchange/.

102 *Id.*

103 *Id.*

104 *See, e.g.*, COINBASE *Bitcoin Storage*, *supra* note 82.

105 *See, e.g.*, Morris, *supra* note 1.

106 *See id.*

III. ENFORCING JUDGMENTS AGAINST DEFENDANTS WITH CRYPTOCURRENCY

A party seeking to recover cryptocurrency faces two sets of challenges. Prior to judgment there is a risk that a defendant may attempt to judgment-proof themselves, preventing enforcement of a judgment debt by concealing or transferring digital assets in such a way that may make the cryptocurrency difficult to locate after a court enters judgment. And post-judgment, a defendant may find herself frustrated by the fact that only the wielder of a private key may control the use of cryptocurrency funds; not all wielders give up that exclusive control willingly. Only certain pre-judgment and post-judgment remedies are applicable to cryptocurrencies. Some are more useful than others, and a few are not applicable at all.

There have been relatively few civil actions involving cryptocurrency. These cases include commercial disputes, fraud, bankruptcy actions where the debtor possesses cryptocurrency, and actions against insolvent companies in receivership.[107] Many of these cases involve contracts for cryptocurrency services or mining computers.[108] Others involve theft or fraud.[109] These cases

107 *See, e.g.*, CFTC v. McDonnell, No. 18-cv-00361, 2018 BL 76558, at *1 (E.D.N.Y. Mar. 6, 2018) (virtual currency fraud); Complaint at 1–2, SEC v. Montroll, No. 1:18-cv-01582 (S.D.N.Y. Feb. 21, 2018) (securities fraud); Complaint at 31-38, Kleiman v. Wright, No. 9:18-cv-80176 (S.D. Fla. Feb. 14, 2018) (alleging conversion and misappropriation) [hereinafter Kleiman Complaint]; Class Action Complaint at 1–2, Paige v. Bitconnect Int'l PLC , No. 3:18-cv-00058 (W.D. Ky. Jan. 29, 2018) (alleging Ponzi and pyramid schemes); SEC v. Plexcorps, No. 17-cv-07007, 2017 BL 448742, at *1 (E.D.N.Y. Dec. 14, 2017) (securities fraud); Class Action Complaint at 1, Rensel v. Centra Tech, Inc., No. 1:17-cv-24500 (S.D. Fla. Dec. 13, 2017) (alleging securities fraud); Audet v. Fraser, No. 3:16-cv-00940, 2017 BL 364322, at *1 (D. Conn. Oct. 11, 2017) (alleging securities fraud); Liedel v. Coinbase, Inc., No. 16-81992-CIV, 2017 BL 184681, at *1 (S.D. Fla. June 1, 2017) (aiding and abetting a third party's breach of fiduciary duty); Alexander v. BF Labs Inc., No. CV 14-2159, 2016 WL 6581460, at *1 (D. Kan. Nov. 7, 2016) (breach of contract); Greene v. Mizuho Bank, Ltd., 206 F.Supp. 3d 1362, 1369-70 (N.D. Ill. 2016) (tortious interference and fraudulent concealment relating to collapse of a cryptocurrency exchange); Morici v. Hashfast Techs. LLC, No. 5:14-CV-00087, 2015 WL 4880670, at *1 (N.D. Cal. Aug. 14, 2015) (breach of contract and fraud); FTC v. BF Labs Inc., No. 4:14-CV-00815, 2014 WL 7238080, at *1 (W.D. Mo. Dec. 12, 2014) (breach of contract); Meissner v. BF Labs Inc., No. 13-2617, 2014 WL 2558203, at *1 (D. Kan. June 6, 2014) (breach of contract); TradeHill, Inc. v. Dwolla, Inc., No. C-12-1082, 2012 WL 1622668, at *1 (N.D. Cal. May 9, 2012) (enforcing arbitration agreement involving cryptocurrency services).

108 *See* cases cited *supra* note 107.

109 *See, e.g.*, Liu Final Default Judgment, *supra* note 3, at 1–2 (embezzling from a cryptocurrency exchange); Order for Entry of Default Judgment at 1, SEC v. Garza, No. 3:15-cv-01760 (D. Conn. May 29, 2017) (operating a Ponzi scheme) [hereinafter Garza Default Judgment]; Hussein v. Coinabul, LLC, No. 14-cv-05735, 2014 BL 358914, at *1 (N.D. Ill. Dec. 19, 2014) (promising gold or silver in exchange for bitcoin, and not delivering); Lenell v. Advanced Mining Tech., Inc., No. 14-cv-01924, 2014 WL 7008609, at *1 (E.D. Pa. Dec. 11, 2014) (fraud involving failure to delivery mining machines); SEC v. Shavers, No. 4:13-cv-416, 2014 BL 259471, at *1 (E.D. Tex. Sept. 18, 2014) (running a bitcoin Ponzi scheme).

are useful to illustrate the challenges facing attorneys seeking to recover from a defendant who holds digital currencies.

A. Pre-Judgment Remedies

Ensuring a defendant has funds reachable by judgment enforcement mechanisms is sometimes necessary to ensure satisfaction of judgments. Judgment-proofing techniques prevent enforcement of judgment debts designed to render any judgment difficult or impossible to collect from the debtor.[110] For example, a defendant may place assets in the possession of a business entity or person whose assets are not subject to any potential liability arising from the defendant's conduct.[111] Or a defendant may move assets—and possibly herself—to a foreign jurisdiction that does not give legal force to domestic judgments.[112]

Pre-judgment remedies are available to prevent a defendant from executing some judgment-proofing tactics. However, a plaintiff seeking purely monetary damages generally cannot ask a court to control a defendant's assets before judgment.[113] This restriction is inapplicable if there are claims for equitable relief,[114] such as specific performance or replevin, or if there is a statutory basis for rescinding a fraudulent sale of a security.

If the facts of the case allow, plaintiffs seeking the return of their cryptocurrency may allege a claim for replevin to ensure that equitable pre-judgment remedies are available.[115]

1. Preliminary Injunctions, Generally

Courts may preliminarily enjoin a defendant to prevent her from moving assets to avoid judgment. Preliminary injunctions require notice to the adverse party and an opportunity for the adverse party to be heard.[116] In certain situations, the court may grant preliminary relief without notice to the

110 *See* Lynn M. LoPucki, *The Death of Liability*, 106 YALE L.J. 1, 14 (1996).

111 *Id.* at 20–23, 30–32.

112 *Id.* at 32–33.

113 *See* Grupo Mexicano de Desarrollo S.A. v. All. Bond Fund, Inc., 527 U.S. 308, 321 (1999) (following "the well-established general rule that a judgment establishing the debt was necessary before a court of equity would interfere with the debtor's use of his property"). *But see* Deckert v. Independence Shares Corp., 311 U.S. 282, 290 (1940) (preliminary injunction of money assets proper where defendant "was insolvent and its assets in danger of dissipation or depletion").

114 *See Desarrollo*, 527 U.S. at 324–25.

115 *See, e.g.*, Kleiman Complaint, *supra* note 107, at 34–35 (alleging replevin claim for the return of approximately $10 billion in bitcoins).

116 *See* FED. R. CIV. P. 65(a).

other party on a showing of sufficient urgency by the party seeking the injunction.[117] A plaintiff must "establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest."[118] Proving irreparable harm also means proving that monetary damages are inadequate to compensate for the injury.[119] Courts sometimes grant preliminary relief when plaintiffs show a defendant is effectively insolvent and will be unable to satisfy money judgments.[120]

A plaintiff may be able to show imminent irreparable injury if a cryptocurrency defendant signals their intentions that they are preparing to hide or move assets. Signals of such an intention may include: liquidating or gifting real-world assets;[121] establishing accounts at foreign cryptocurrency exchanges; making exaggerated or oscillating claims to disguise bad faith conduct;[122] and reporting hacks or other interruptions of their business activity.[123] This conduct, combined with the features of cryptocurrency that make it difficult for a court to control and which enable fraud,[124] may be sufficient to show likely irreparable harm unless a defendant's conduct is enjoined.

Imminent irreparable harm may also be shown if the defendant signals they are likely to ignore litigation altogether. Cryptocurrency is rooted in anti-authoritarian ideals; the idea of a currency uncontrollable by any government is attractive to those with an anarchistic bent. Some defendants manifest this ideology during litigation by failing to meaningfully respond to court orders or rules of procedures. Occasionally such a defendant will hire an attorney, only for that attorney to withdraw as counsel after a period of time, citing difficulties working with the defendant.[125] Eventually, the court

117 FED. R. CIV. P. 65(b)(1).

118 *See* Winter v. Natural Res. Def. Council, Inc., 555 U.S. 7, 20 (2008).

119 *See* eBay Inc. v. MercExchange, LLC, 574 U.S. 388, 391 (2006).

120 *See* Deckert v. Indep. Shares Corp., 311 U.S. 282, 290 (1940).

121 *See, e.g.*, Liu Complaint, *supra* note 20, at 7–9.

122 *See, e.g.*, SEC v. Shavers, No. 4:13-cv-416, 2014 BL 259471, at *3–*6 (E.D. Tex. Sept. 18, 2014) (finding that the defendant made increasingly incredible claims as to how he was able to pay "profits" in what was actually a Ponzi scheme, in order to attract new investors to sustain the scheme).

123 *See, e.g.*, Liu Complaint, *supra* note 20, at 7–9.

124 *See supra* Section 0 and Part 0; *see also* Bitconnect Preliminary Injunction, *supra* note 158, at 7. *See generally* Scott Isaacson, *The Bamboozling Bite of Bitcoin: Bitcoin Doesn't Make White Collar Crime Possible, but It Does Make It Easier!*, UTAH B.J., July-August 2017, at 32–33.

125 *See, e.g.*, Motion to Withdraw as Attorney for Defendants at 2, *Hussein*, No. 14-cv-05735 (N.D. Ill. filed Feb. 2, 2015) (defendants failing to meet obligations to attorneys and systemic failures to communicate); Motion to Withdraw as Attorney for Defendants at 3, Lenell v. Advanced Mining Tech., Inc., No. 14-cv-01924 (E.D. Pa. Jan. 12, 2015) (defendants did not pay attorneys); Unopposed Motion to

determines the defendant is ignoring the court and renders a default judgment upon the plaintiff's motion.[126] Plaintiffs showing that the defendant is likely to ignore court proceedings may be able to persuade the court that preliminary injunctive relief is necessary to ensure that a defendant does not hide assets in an attempt to judgment-proof themselves.

Two forms of preliminary injunctive relief warrant discussion in the cryptocurrency asset recovery context: (1) asset freeze orders—court orders preventing the disposal or shifting of assets—and (2) receiverships—placing a business entity or assets under the control of a court-appointed receiver.

2. Asset Freeze Orders

Courts may order a party to not sell or transfer assets under the control using an asset freeze order, a form of preliminary junctive relief. The party requesting the asset freeze must monitor for violations of the order. If a party violates the order, they may inform the court, and the court will order the enjoined party to show cause why she should not be held in contempt.

Asset freeze orders may include cryptocurrency assets.[127] Defendants could only dispose of cryptocurrency assets at the risk of contempt of court. However, a plaintiff would need to know the bitcoin addresses of the frozen cryptocurrencies to monitor for violations of the freeze order. An advantage of the blockchain's public distributed ledger is that a plaintiff armed with the knowledge of the bitcoin addresses can determine the timing, amounts, and destination accounts of any cryptocurrency transactions.

Plaintiffs successfully persuaded a court to issue a preliminary injunction in *Greene v. MtGox Inc.*, requiring defendants to freeze assets, preserve data, and other ancillary remedies.[128] The case arose from plaintiffs seeking recovery of their lost funds due to the hacking and subsequent collapse of the Mt. Gox cryptocurrency exchange.[129] Mt. Gox and the bank it

Withdraw as Counsel for Defendants at 1, *Shavers*, No. 4:13-cv-416 (E.D. Tex. Aug. 29, 2014) (defendants dismissing attorney).

126 Liu Final Default Judgment, *supra* note 3, at 1 (failing to respond to court); Garza Default Judgment, *supra* note 109, at 1 (failing to respond to court); Motion for Default Entry at 1, Audet v. Garza, No. 3:16-cv-00940 (D. Conn. Feb. 23, 2017) (requesting default judgment against some defendants who failed to respond to complaint); Order of Default Judgment at 1, *Hussein*, No. 14-cv-05735 (N.D. Ill. Jul. 6, 2015), (failing to "appear, plead, or otherwise defend in this action"); *Lenell*, No. 14-cv-01924 (noting in the docket that all documents served on defendants are returned undeliverable).

127 *See, e.g.*, Order Freezing Assets and Granting Other Ancillary Relief at 3, *Shavers*, No. 4:13-cv-416 (E.D. Tex. July 23, 2013) [hereinafter Shavers Freeze Assets Order].

128 *See* Temporary Restraining Order at 4–6, No. 1:14-cv-01437 (N.D. Ill. entered Mar. 11, 2014).

129 *See supra* notes 102–103 and accompanying text.

used for fiat currency transactions were in Japan.[130] Plaintiffs argued that the defendants were effectively insolvent and would be unable to satisfy a money judgment, and that allowing the defendant to liquidate any other assets—for example, transferring assets to the personal ownership of its operators—would cause irreparable harm.[131] Plaintiffs also argued that allowing a foreign entity to preferentially dissipate assets at the expense of domestic consumers would be to support a policy where foreign companies may feel free "to cheat and steal from U.S. consumers with impunity."[132] The court agreed.[133]

The fact that defendants are in the process of selling cryptocurrency is not sufficient to prove irreparable harm. In *MacDonald v. Dynamic Ledger Solutions, Inc.*, the court denied injunctive relief in a case involving substantial amounts of cryptocurrency.[134] Plaintiffs alleged that the defendants were looting a company by liquidating massive amounts of cryptocurrency and converting the assets into fiat currency, and that this conduct would prevent them from adequate compensation in the event they prevailed in their case.[135] The court held that simply converting cryptocurrency into conventional cash equivalents would not prevent the plaintiffs from recovering under a favorable judgment, because there was no evidence that the defendants were disposing the proceeds of the cryptocurrency sales.[136]

Freeze orders may be ineffective applied to defendants undeterred by the threat of contempt for violating the order. This is what occurred in *Securities and Exchange Commission v. Shavers*.[137] In that case, the court ordered Shavers' assets frozen, and ordered him to turn over all records so that the SEC could account for his assets and prevent probable loss.[138] Shavers never turned over the records.[139] When the court held a show cause hearing why Shavers should not be held in contempt—a year after the freeze

130 Motion for Temporary Restraining Order & Preliminary Injunction at 22, *Greene*, No. 1:14-cv-01437 (N.D. Ill. Mar. 4, 2014) [hereinafter Greene TRO Motion].

131 *See id.* at 19-21; *see also* Deckert v. Indep. Shares Corp., 311 U.S. 282, 290 (1940) (preliminary injunction of money assets proper where defendant "was insolvent and its assets in danger of dissipation or depletion").

132 Greene TRO Motion, *supra* note 130, at 22.

133 *See* Temporary Restraining Order, *supra* note 128, at 2.

134 No. 3:17-cv-07095, 2017 BL 456346, at *1 (N.D. Cal. Dec. 20, 2017).

135 *Id.* at *3.

136 *Id.* at *4 ("The conversion of some portion of the volatile cryptocurrency assets into more stable currency is unlikely to jeopardize MacDonald's ability to recover the 18.145 Ethereum he contributed (or its equivalent economic value) should he ultimately prevail.").

137 No. 4:13-cv-416, 2014 BL 259471, at *14–16 (E.D. Tex. Sep. 18, 2014).

138 Shavers Freeze Assets Order, *supra* note 127, at 1.

139 Order to Show Cause at 1, *Shavers*, No. 4:13-cv-416 (E.D. Tex. Apr. 24, 2014) [hereinafter *Shavers* Show Cause Order].

order had been issued—Shavers claimed to have "loaned" over 200,000 Bitcoin to an anonymous person.[140] He then claimed to have deleted all records of the transaction, including the sending Bitcoin addresses under his control.[141] It only takes a moment to transfer cryptocurrencies. Shavers had a year, and thus plenty of opportunity to transfer his cryptocurrency, worth approximately $1 billion.[142]

3. Receiverships

Plaintiffs may request appointment of a receiver as a method of controlling a defendant's assets, before or after judgment.[143] Receivers are court-appointed trustees that, *inter alia*, manage entities or assets when the owners pose the risk of liquidating their assets for their own personal benefit, and when the requesting party has a right or interest in the assets.[144] Requesting receivership as a preliminary equitable remedy is subject to the same restrictions as other preliminary injunctive relief, including the requirement of a showing of irreparable harm.[145]

A receiver may oversee cryptocurrency assets like any other asset. This requires either control of the private key that accesses the cryptocurrency, or the defendant transferring the cryptocurrency to accounts under the receiver's exclusive control pending resolution of the litigation.[146]

4. Avoiding Fraudulent Transfers

Plaintiffs unable to meet the requirements for a preliminary injunction may seek avoidance of fraudulent transfers. Fraudulent transfer acts create statutory causes of action to remedy the situation where defendants attempt to dispose of assets that would otherwise be subject to a possible judgment.[147]

---

140 *Shavers*, 2014 BL 259471, at *11.

141 *Id.*

142 *See* COINDESK *bitcoin Price*, *supra* note 13.

143 *See* FED. R. CIV. P. 66.

144 *See, e.g.*, FLA. STAT. § 607.1432(1), (3) (2018).

145 *See supra* Section 0.

146 Cryptsy was under control of a court-appointed receiver after Vernon had liquidated some portion of the company's assets and fled the country. But the receiver never had control of the company's bitcoin addresses. Vernon maintained that control and was stealing funds from those addresses even after the receiver took control of Cryptsy. Liu Complaint, *supra* note 20, at 9–10; Mullesch Affidavit, *supra* note 7, at 2–7 ("It appears that Mr. Vernon has transferred, and continues to transfer, a large amount of coins traceable back to Cryptsy wallets to new addresses beyond the Receiver's control after the Receiver's appointment.").

147 Grupo Mexicano De Desarrollo v. Alliance Bond Fund, 527 U.S. 308, 322 (1999) ("[T]here is absolutely nothing new about debtors' trying to avoid paying their debts, or seeking to favor some

Such acts authorize courts to avoid fraudulent transfers, force the return of assets, implement a receivership, or allow the use of other remedies as appropriate.[148]

Forcing the avoidance of a fraudulent cryptocurrency transfer may be difficult, even if one can identify the recipients of the transferred bitcoins. This is because the transferred funds are under the sole control of whomever possesses the private key of the recipient account.[149] However, if a defendant relies on third parties for parts of her bitcoin transfers—such as cryptocurrency exchanges—or can identify the actual recipient, then a plaintiff may be able to seek fraudulent transfer remedies against those parties, if the party is within the court's jurisdiction.[150]

B. Post-Judgment Enforcement

Generally, enforcement of civil liabilities begins with the entry of a judgment.[151] The judgment creditor then requires a court's writ of execution to enforce the judgment.[152] That writ of execution empowers local law enforcement to levy—seize and sell property—to satisfy the judgment.[153] A judgment creditor may also pursue writs of garnishment or attachment, granting the creditor a right to some or all of the judgment debtor's wages, property, or other debt owing in satisfaction of the judgment debt.[154] These writs may be served directly on the debtor, or on employers or banks to force the payment of judgment debts.[155] If the judgment creditor prevailed on a replevin claim, then she may use a writ of replevin to have local law enforcement seize and return the property at issue to the creditor.[156]

Cryptocurrencies are tailor-made to resist control by external authorities, and this limits the efficacy of certain judgment enforcement

creditors over others—or even about their seeking to achieve these ends through 'sophisticated . . . strategies.' The law of fraudulent conveyances and bankruptcy was developed to prevent such conduct . . . ." (quoting *id.* at 338 (Ginsburg, J., dissenting))).

148 *See, e.g.*, FLA. STAT. § 726.108 (2018).

149 *See supra* Section 0.

150 *See, e.g.*, Complaint at 7–12, Kasolas v. Lowe, No. 3:15-ap-03011 (Bankr. N.D. Cal. filed Feb 17, 2015).

151 LoPucki, *supra* note 110, at 13.

152 FED. R. CIV. P. 69(a)(1).

153 *See, e.g.*, FLA. STAT. § 56.21 (2018).

154 *See, e.g.*, FLA. STAT. § 77.01 (2018).

155 *See generally* FED. R. CIV. P. 64(b) (listing available civil remedies for seizing property); Carrie A. Tendler, Jef Klazen & Michael A. Sanfilippo, *United States*, *in* GETTING THE DEAL THROUGH: 1 ASSET RECOVERY 2018 (2014), Lexis 2018-1 GTDT: Asset Recovery (listing asset recovery options available in civil cases).

156 *See, e.g.*, FLA. STAT. § 78.01 (2018).

mechanisms when the possessor resists surrendering the cryptocurrency.[157] Whereas wages may be garnished by serving a writ of garnishment on an employer, or a bank account may be seized by a writ of attachment served on a bank, there are no analogous third parties that can grant control over cryptocurrency.[158]

Several judgment enforcement procedures may be effective to recover cryptocurrency from judgment debtors: levy, replevin, judgment liens, and receiverships.[159] The limited usefulness of contempt against cryptocurrency defendants as an ultimate enforcement mechanism is also discussed.

1. Execution, Levy, and Replevin

Judgment creditors may seize and sell property to satisfy a judgment, pursuant to a writ of execution, by levy.[160] A creditor levies property by providing local law enforcement the court's writ of execution and the identity and location of property subject to levy.[161] The local law enforcement levying the property, often the sheriff, will then sell at auction the seized property to satisfy the judgment debt.[162]

Plaintiffs succeeding on a claim for replevin—a demand for the return of wrongfully taken property—may enforce the judgment in a manner similar to execution and levy. However, instead of the sheriff selling property to satisfy a money judgment, the sheriff returns the replevied property to the rightful owner.[163]

Cryptocurrency may be seized, pursuant to a levy or writ of replevin,[164] by taking the private key, granting control over the assets. This requires the judgment creditor locating the private key, informing the sheriff, and the sheriff taking the private key from its possessor. Seizure may be impractical if a judgment debtor does not disclose a private key's location pursuant to discovery. Independently locating a private key may be difficult, because a

157 *See supra* note 30 and accompanying text.

158 *See, e.g.*, Memorandum in Support of Motion for Preliminary Injunction at 7, Paige v. Bitconnect Int'l PLC, No. 3:18-cv-00058 (W.D. Ky. filed Jan. 29, 2018) (arguing that the jurisdiction's attachment statute would be impractical or impossible to apply against cryptocurrencies), *granted* (W.D. Ky. Feb. 9, 2018) [hereinafter Bitconnect Preliminary Injunction].

159 See section 0, *supra*, for analysis of receiverships applied to cryptocurrency defendants.

160 *See, e.g.*, FLA. STAT. § 56.27 (2018).

161 *See, e.g.*, *How to Collect a Judgment in Florida*, FLA. DEP'T OF STATE, http://dos.myflorida.com/sunbiz/forms/judgment-lien/collect-judgment/ (last visited Apr. 8, 2016) ("The sheriff's department will not locate the property for you.").

162 *See, e.g.*, FLA. STAT. § 56.27 (2018).

163 *See, e.g.*, FLA. STAT. § 78.01 (2018).

164 *See, e.g.*, Kleiman Complaint, *supra* note 107, at 34–35 (alleging replevin claim for the return of approximately $10 billion in bitcoins).

private key may be stored on a device, a piece of paper, memorized, or even divided up and placed in multiple locations.[165] Even if the private key is seized, the sheriff would need to transfer the funds to another bitcoin address to prevent theft. Otherwise, a third party with access to a copy of the private key could prevent the sale or return of the seized cryptocurrency by shifting the funds out of the bitcoin address associated with the seized private key. Because cryptocurrency is relatively new, a judgment creditor would need to instruct local law enforcement what exactly is being seized and how to protect it post-seizure so they may dispose of the property successfully.

2. Judgment Liens

Tangible personal property may become subject to a lien upon execution of a judgment.[166] Jurisdictions vary in how a judgment creditor may enforce their rights against a judgment debtor's assets, but generally the lien is a creation of a possessory interest in the liened property.[167] Unless a statute provides otherwise, judgment liens are not enforced against innocent purchasers—those that have no notice of the lien—as a matter of equity.[168] In such a circumstance, a lien creditor would need to avoid the transfer of the property under a fraudulent transfer act or similar statute.[169]

Cryptocurrencies are subject to judgment liens in jurisdictions that allow such liens on personal property. Courts addressing the issue treat bitcoins as tangible personal property, controlled by a private key that is capable of manifestation.[170] Accordingly, judgment liens may allow a judgment creditor to recovery cryptocurrency from a judgment debtor, possibly by enforcing a lien against third parties to whom the judgment debtor transferred bitcoins.

The Bitcoin blockchain allows the tracing of bitcoin transactions.[171] Using the public distributed ledger that is the backbone of Bitcoin, one can track the transfer of bitcoins from address to address.[172] Knowing the owner

165 *See supra* Section 0 (describing how private keys are stored).

166 *See* David Gray Carlson, *Critique of Money Judgment Part Three: Restraining Notices*, 77 ALB. L. REV. 1489, 1502 (2014).

167 *See id.* at 1502–03.

168 *See* D.C. v. Lyon, 161 U.S. 200, 206–07 (1896).

169 *See, e.g.*, FLA. STAT. § 726.108 (2018).

170 *See* Raskin, *supra* note 9, at 983.

171 *See* MIT TECH. REV., *supra* note 63, at 3–4 and accompanying text; *see also supra* text accompanying note 64; *supra* text accompanying note 65; Ludwin, *supra* note 66, at 3 and accompanying text.

172 *See* MIT TECH. REV., *supra* note 63, at 3–4 and accompanying text; *supra* text accompanying note 64.

of an address allows tying these transaction records to a person.[173] Users of the infamous Silk Road discovered that their online transactions were traceable, and that there was no way to erase these records embedded in the blockchain.[174] Silk Road was an online black-market clearinghouse for illicit goods that accepted bitcoins as payment for anything from drugs to assassinations.[175] Determining the bitcoin addresses used by Silk Road allowed criminal investigators to trace transactions through the blockchain to accounts used by Silk Road customers.[176]

A plaintiff can use Bitcoin's traceability to enforce judgment liens against third parties who acquire illicit bitcoins from the judgment debtor,[177] but tracing bitcoin transactions is difficult and requires some forensic computing expertise. Tracing transactions from a Bitcoin address to a person requires knowing the identity of a Bitcoin address's owner.[178] Bitcoin address services that list some identifying information exist, but they rely on third parties manually submitting reports of Bitcoin addresses.[179] Such haphazard databases will be imperfect and incomplete tools for identifying owners.

Furthermore, Bitcoin users now take measures to obscure their digital trail. People learned from Silk Road and developed "best practices" to make tracing transactions difficult. One such practice is to create many Bitcoin addresses, limiting the use of one Bitcoin address to one incoming transaction.[180] Users can also "tumble" their outgoing bitcoin transactions, combining transactions together using intermediaries to digitally launder cryptocurrency.[181] Tumbling allows users to place their funds in a combined address, managed by a third party. That third party then distributes the funds to their final destination for each respective customer. Without the internal

173 *See* MIT TECH. REV., *supra* note 63, at 2–4 and accompanying text; *supra* text accompanying note 65.

174 *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.

175 Andy Greenberg, *Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges*, WIRED (Feb. 4, 2015, 3:57 PM), https://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict/.

176 *Id.*

177 Counsel for the plaintiffs victimized by Vernon's cryptocurrency theft proposed just such an approach: "I believe we are going to keep tracking down the users and trace the bitcoin through the blockchain, and when someone tries to move some of it, we will hopefully locate the person."" Morris, *supra* note 1.

178 Greenberg, *supra* note 174.

179 *See, e.g.*, BITCOIN WHO'S WHO, http://bitcoinwhoswho.com/ (last visited Jan. 3, 2018).

180 *See* Chris Pacia, *Innovations that Enhance Bitcoin Anonymity*, BITCOIN NOT BOMBS (Feb. 5, 2014), http://www.bitcoinnotbombs.com/innovations-that-enhance-bitcoin-anonymity/ (suggesting that the problems of a publicly viewable transactions can be "largely mitigated by treating all Bitcoin addresses as one-time use addresses.").

181 *See* Jeff John Roberts, *Inside Uncle Sam's Secret Bitcoin Hoard*, FORTUNE (Feb. 21, 2018), http://fortune.com/2018/02/21/government-forfeiture-bitcoin-auction/.

records of the third-party tumbler, an outside observer cannot tell whose funds are going to which account. This makes it nearly impossible to determine where the bitcoin is being spent.[182] And some newer cryptocurrencies, based on the fundamental bitcoin technology, increase the privacy of transactions by making it more difficult to use their blockchains to trace transactions.[183] The rise of these privacy-focused cryptocurrencies is a response to the traceability of the original bitcoin software.

Courts are not likely to enforce judgment liens on innocent third parties acquiring illicit bitcoin, even if there were reliable methods to trace bitcoin transactions to identifiable people, because of the problem of notice in the quasi-anonymous digital currency context.[184] Enforcing judgment liens against third parties generally requires that the third party have notice of the lien prior to acquisition of the property in question.[185] There is no mechanism for putting potential bitcoin transferees on notice that the bitcoin they are acquiring may have a clouded digital title. A lien holder would have to independently put potential bitcoin transferees on notice based on their knowledge of the judgment debtor's relationships. But, because cryptocurrencies freely cross jurisdictions, there is no reason to expect that a judgment debtor would limit their transactions to their known contacts.

Judgment liens could serve to recover stolen cryptocurrency amid certain conditions. Plaintiffs must identify likely third-party recipients of the judgment debtor's digital assets, based on information discovered about the defendant's financial dealings. Plaintiffs must serve those third parties notice of a judgment lien on the cryptocurrency. The plaintiffs then will have to identify transactions between the defendant's cryptocurrency accounts and the noticed third parties. If the plaintiffs identify such transactions, and the third parties are in a jurisdiction that will give force to the plaintiffs' judgment lien,[186] then the plaintiffs may recover from that third party.

3. Contempt of Court

Civil asset recovery procedures are only effective if they are enforceable against defendants. Defendants who do not comply with court orders are

182 *Id.*

183 *Id.*; Lucinda Shen, *Bitcoins Worth $4.7 Million Seized in Fake ID Case*, FORTUNE (Feb. 9, 2018) ("[C]riminals are gravitating toward other cryptocurrencies such as Litecoin or Monero instead of Bitcoin, as investigators grow more savvy with tracking [Bitcoin]."); Greenberg, *supra* note 174 ("[N]ewer digital currencies like Monero and Zcash . . . promise far greater privacy by default.").

184 *See* D.C. v. Lyon, 161 U.S. 200, 206–07 (1896).

185 *Id.*

186 Certain foreign jurisdictions do not enforce domestic judgments. LoPucki, *supra* note 110, at 32–33.

subject to contempt of court. For example, if person refused a subpoena ordering that a bitcoin private key be turned over, the court could hold them in contempt.[187]

Contempt may be civil or criminal, with differing sanctions.[188] Civil contempt sanctions are designed to compensate the wronged party or coerce obedience with the court's orders.[189] Civil sanctions may include monetary fines or preventing the offending party from disputing related issues in the case.[190] Criminal contempt is reserved for punishing willful disobedience of the court's authority or when the underlying conduct is criminal.[191] Criminal contempt sanctions may include fines and prison.[192] Typically, an alleged offender has an opportunity to show cause why they should not be found in contempt.[193] However, imprisonment is not generally used in the United States to enforce the repayment of debts, including enforcing court orders necessary to collect those debts.[194]

Contempt is only effective at coercing compliance with court orders if the defendant wishes to avoid potential contempt sanctions. A defendant may ignore monetary sanctions if they feel they have more to lose by cooperating with court orders than by being held in contempt.

Some defendants possessing cryptocurrency became suddenly and unexpectedly wealthy due to the rapidly increasing value of these assets. Defendants with immense digital assets in proportion to conventional assets are more likely to risk contempt rather than expose their digital wealth to potential seizure.[195]

Securities Exchange Commission v. Shavers illustrates how contempt is ineffective against defendants with large digital holdings.[196] In 2011, Trendon Shavers set up a Ponzi scheme disguised as a bank.[197] He accepted

187 *See* FED. R. CIV. P. 45(g) ("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.").

188 Elizabeth G. Patterson, *Civil Contempt and the Indigent Child Support Obligor: The Silent Return of Debtor's Prison*, 18 CORNELL J.L. & PUB. POL'Y 95, 102 (2008).

189 *Id.* at 102–03.

190 *Id.*

191 *Id.*

192 *Id.* at 103.

193 *Id.*

194 *See* LoPucki, *supra* note 110, at 9.

195 *See generally* SEC v. Shavers, No. 4:13-cv-416, 2014 BL 259471 (E.D. Tex. Sept. 18, 2014) (illustrating one of the only examples of a contempt order issued relating to a cryptocurrency case, where the defendant apparently protected approximately 200,000 bitcoins by ignoring court orders to disclose his accounts, freeze assets, and repatriate funds).

196 *See generally id.*

197 *Id.* at *1.

bitcoin investments in return for incredible interest rates, as high as 3,641% annually.[198] At one point during the scheme, Shavers had accumulated "about seven percent of all the Bitcoin that was in public circulation at the time."[199] In 2012, he apparently siphoned off around 200,000 Bitcoin, deleted most records of his transactions, and declared the scheme defunct.[200] In its civil case against Shavers, the SEC requested and received a court order instructing Shavers to freeze his assets, to repatriate any assets he had transferred away, and to give a full accounting of his assets (digital and otherwise) and other discovery to the SEC for its case.[201]

Shavers did not comply with the court order.[202] Shavers claimed that the 200,000 stolen Bitcoin were lent to an anonymous person whom he had never met and could not identify.[203] He stated that he could not provide any other information about this fantastic transaction, because he had deleted all related records.[204]

The court shared the SEC's incredulity over these allegations and ordered Shavers to show cause why he should not be held in contempt.[205] In the show cause order, the court limited its threatened contempt sanctions to preventing Shavers from admitting evidence that would (essentially) allow him to win his case.[206] This was not sufficient to persuade Shavers to cooperate. Eventually, the court ordered summary judgment against Shavers because he simply had no credible facts to dispute the SEC's claims.[207] The court ordered him to pay over $40 million, mostly in disgorgement to compensate his victims.[208] Shavers' 200,000 lost Bitcoin are worth approximately two billion dollars.[209] That amount of money at stake may

198 U.S. Atty's Office for S.D.N.Y., *Texas Man Sentenced for Operating Bitcoin Ponzi Scheme*, U.S. DEP'T JUST. (July 21, 2016), https://www.justice.gov/usao-sdny/pr/texas-man-sentenced-operating-bitcoin-ponzi-scheme. The United States convicted Trendon Shavers of the theft of 146,000 Bitcoin and sent him to prison in a case parallel to his Securities and Exchange Commission civil case. *Id.*

199 *Id.*

200 *Shavers*, 2014 BL 259471, at *7.

201 Shavers Freeze Assets Order, *supra* note 127, at 1.

202 *See* Shavers Show Cause Order, *supra* note 139, at 1 ("It appears that Shavers has willfully refused to comply with: (a) the Court's August 5, 2013 Order Freezing Assets and Granting other Ancillary Relief; (b) the Court's August 29, 2013 Order; and (c) his discovery obligations in this litigation.").

203 *Shavers*, 2014 BL 259471, at *11.

204 *Id.*

205 *See* Shavers Show Cause Order, *supra* note 139, at 1.

206 *Id.* at 2.

207 *See Shavers*, 2014 BL 259471, at *7 ("Shavers' claims concerning the lending activity he supposedly undertook . . . are not possible based on the record evidence in this action.").

208 *Id.* at *12.

209 *See* COINDESK *bitcoin Price*, *supra* note 13.

explain why contempt may not be effective against a defendant whose wealth is largely digital and easy to hide.

IV. MITIGATING CRYPTOCURRENCY ASSET RECOVERY CHALLENGES

Plaintiffs may improve their chances at recovering cryptocurrency assets by incorporating lessons learned from other cases mixed with an application of common sense. This includes extensive and stealthy pre-complaint investigations and partnering with law enforcement or regulatory agencies when possible.

A. Pre-Complaint Investigations

Attempting to recover cryptocurrency from a defendant may be difficult, but sufficient preparation prior to a complaint can improve your chances of successful recovery. Because cryptocurrencies can be transferred almost instantly, avoiding giving a defendant notice is important.

A lot of useful information can be gleaned prior to filing a complaint. If plaintiffs transferred bitcoins to the defendant, they will have some records that show the defendant's receiving bitcoin addresses. Employing appropriate forensic cryptocurrency experts may allow tracing of bitcoin transfers from the defendants' bitcoin addresses, mapping the defendants' usual spending patterns.[210] This is helpful to mitigate against a defendant's bad faith destruction of records, transfers of assets, and to establish the identity of his normal vendors, if notice to those vendors of a judgment lien were ever required.[211]

If pre-complaint investigations uncover evidence of crimes or securities law violations, then that information may be provided to the appropriate agency for action. Involving those agencies increases the chances of successful cryptocurrency asset recovery.

B. Using Law Enforcement and Regulatory Agencies

If the defendant or her digital assets arise out of criminal conduct, it makes sense to cooperate with law enforcement or regulatory agencies at the earliest stage possible. This will minimize the opportunity for defendants to relocate digital assets or take measures to prevent disclosure of private keys. If the defendant's conduct violates laws enforced by regulatory agencies,

210 *See* Greenberg, *supra* note 174, at 2.

211 *See supra* note 185 and accompanying text.

then those agencies have statutory tools that make them effective at preventing cryptocurrency defendants from moving their wealth using preliminary injunctive relief, including receivers supported by forensic computing consultants, asset freezes, and expedited discovery procedures. Law enforcement agencies have investigative methods and are able to exercise a degree of control over a defendant's person and their property that are unavailable to civil plaintiffs and increases their efficacy in recovering stolen cryptocurrency.[212]

Additionally, national law enforcement agencies have a better opportunity to attain discovery of foreign defendants' assets, if the defendant stores private keys or other assets abroad:

> The United States has more than 70 mutual legal assistance treaties (MLATs) with foreign nations that concern the sharing of evidence. MLATs are typically employed by the US to pursue its own law enforcement interests and are not directly available to private litigants. Nevertheless, coordination with US authorities can be used in pursuit of information. If the government does make such a request, then private litigants can utilise US discovery mechanisms to attempt to obtain information after information is produced in response to the MLAT request.[213]

Cooperating with law enforcement thus has benefits to civil plaintiffs in cases involving domestic or foreign defendants, where those defendants are also suspects in crimes.

Law enforcement agencies such as the FBI and DEA are much more effective at recovering illicitly procured digital assets than plaintiffs relying on civil actions alone. Law enforcement agencies do not need to wait on court ordered contempt proceedings to force a suspect to disclose their assets or provide access to their cryptocurrency.[214] These agencies are becoming more familiar with where to locate private keys, or how to convince a suspect to surrender their private keys; law enforcement can threaten liberty in a way civil plaintiffs cannot.[215] The agencies transfer assets to law enforcement

212 *See, e.g.*, Criminal Complaint at 1–14, U.S. v. Kim, No. 1:18-cr-00107 (N.D. Ill. Feb. 15, 2018) (illustrating the ability of law enforcement to covertly collect information about a suspect's activities, including copies of text messages, that are not readily available to civil plaintiffs).

213 Tendler, Klazen & Sanfilippo, *supra* note 155, at 5.

214 *E.g.*, United States v. 50.44 Bitcoins, No. ELH-15-3692, 2016 BL 171855, at *1–*3 (recommending that the Bitcoins be forfeited to the United States). *See generally* Raskin, *supra* note 9, at 980–83 (describing two criminal cases where the court ordered seizure of cryptocurrency assets).

215 Shen, *supra* note 183 (reporting that law enforcement is growing increasingly adept at tracking Bitcoin transactions); Roberts, *supra* note 181, at 3 ("In private-key cases, the only way law enforcement can quickly obtain the Bitcoin is if the suspect reveals the key.").

controlled bitcoin addresses, divesting access from the former possessor.[216] After the coin is seized, victims may apply to the Department of Justice for restitution.[217]

In 2013, federal law enforcement agents suspected Ross Ulbricht of operating Silk Road.[218] Silk Road was a multi-million-dollar digital clearinghouse for drugs and other illegal goods and services.[219] When they arrested Ulbricht in a San Francisco library, they seized his laptop before he had an opportunity to lock it and consequently recovered his bitcoin private keys, giving the agents access to about 175,000 Bitcoins.[220] Such a dramatic seizure simply has no analog in the civil asset recovery toolbox.

Certain regulatory agencies, such as the Securities and Exchange Commission, Federal Trade Commission, or the Commodities Futures Trading Commission possess special tools to recover cryptocurrency assets from defendants who violate laws under their purview. These agencies can secure preliminary relief in situations where that relief may be unavailable to private litigants. For example, the SEC, as a "statutory guardian charged with safeguarding the public interest in enforcing the securities laws," has a lower burden to meet to secure preliminary relief in cases involving securities law violations.[221] The SEC does not need to show that irreparable harm would result in the absence of the requested preliminary relief.[222] Instead, the SEC need only "make a *prima facie* showing that a defendant has violated the federal securities laws."[223] Additionally, this different preliminary injunctive burden for regulatory agencies allows them to secure *ex parte* preliminary relief in contexts where a court would deny that relief to standard civil

216 *See* Raskin, *supra* note 9, at 982–83.

217 *See* Roberts, *supra* note 181, at 9.

218 *Id*. at 2–3.

219 *Id.*

220 *Id.*

221 Emergency Motion for Order to Show Cause, Asset Freeze, & Other Ancillary Relief at 9, SEC v. Shavers, No. 4:13-cv-00416 (E.D. Tex. July 23, 2013) (citing SEC v. Mgmt. Dynamics, Inc., 515 F.2d 801, 808 (2d Cir. 1975)); *see also* SEC v. Plexcorps, No. 17-cv-07007, 2017 BL 448742, at *2 (E.D.N.Y. Dec. 14, 2017).

222 *Mgmt. Dynamics*, 515 F.2d at 808–09 ("[T]he standards of the public interest not the requirements of private litigation measure the propriety and need for injunctive relief." (quoting Hecht Co. v. Bowles, 321 U.S. 321, 331 (1944)).

223 Emergency Motion for Order to Show Cause, Asset Freeze, & Other Ancillary Relief, *supra* note 221, at 10 (citing CFTC v. Muller, 570 F.2d 1296, 1300 (5th Cir. 1978); *see also* Aaron v. SEC, 446 U.S. 680, 700–01 (1980) (interpreting the statutory basis for the SEC's showing required to establish preliminary injunctive relief); 15 U.S.C. §§ 77t, 78u (2012).

plaintiffs. Similar standards apply to the injunctions sought by the Federal Trade Commission[224] or the Commodities Futures Trading Commission.[225]

Regulatory agencies, taking advantage of their lower burden to secure preliminary injunctive relief, are employing a multi-part strategy to prevent defendants from hiding cryptocurrency. In *SEC v. Arise Bank*, the Commission filed a motion to appoint a receiver for Arise Bank on the same day as they filed their complaint, alleging securities fraud involving cryptocurrencies.[226] The court granted the order *ex parte*, limiting the risk that Arise Bank would transfer cryptocurrencies to potentially unreachable accounts.[227] The next day the SEC filed a sealed motion requesting appointment of cybersecurity and forensic experts in support of the receiver;[228] this motion was granted the same day, also under seal.[229] This strategy appeared to be successful, because after several days the SEC stated that the case may proceed unsealed and then filed an amended complaint with numerous documents supporting their allegations.[230] Civil plaintiffs, required to prove irreparable harm, may not be able to make the requisite showing to achieve these same results under similar facts.[231]

V. CONCLUSION

Cryptocurrency asset recovery poses challenges surmountable under the right conditions. Covert pre-complaint investigation may produce the facts necessary to present plaintiffs' claims to law enforcement or regulatory agencies, entities which have more tools to prevent possible judgment proofing strategies. Educating the court about the qualities of cryptocurrency

224 *See* 15 U.S.C. § 53(b) (2012); *see also, e.g.*, Stipulated Interim Order at 1, FTC v. BF Labs, Inc., No. 4:14-cv-00815-BCW (W.D. Mo. Oct. 2, 2014).

225 *See* 7 U.S.C. § 13a-1(a) (2012); *see also, e.g.*, CFTC v. McDonnell, No. 18-cv-00361, 2018 BL 76558, at *14 (E.D.N.Y. Mar. 6, 2018).

226 Complaint, SEC v. Arise Bank, No. 3:18-cv-00186-M (N.D. Tex. Jan. 25, 2018); Emergency Ex Parte Motion to Temporarily Seal Docket & Proceedings, *Arise Bank*, No. 3:18-cv-00186-M; Emergency Ex Parte Motion for Temporary Restraining Order, Preliminary Injunction, Asset Freeze, Appointment of Receiver, Document Preservation Order, Order to Make Accounting & Other Emergency & Ancillary Relief, *Arise Bank*, No. 3:18-cv-00186-M.

227 Ex Parte Orders Granting Emergency Ex Parte Motions, *Arise Bank*, No. 3:18-cv-00186-M.

228 Sealed Motion to Employ Kroll Cyber Security as Forensic Expert & Investigative Consultant, *Arise Bank*, No. 3:18-cv-00186-M.

229 Sealed Order Granting Sealed Motion to Employ Kroll Cyber Security as Forensic Expert & Investigative Consultant, *Arise Bank*, No. 3:18-cv-00186-M.

230 *See* Order to Unseal Case, Amended Complaint & Amended Documents, *Arise Bank*, No. 3:18-cv-00186-M.

231 *See* MacDonald v. Dynamic Ledger Solutions, Inc., No. 3:17-cv-07095, 2017 BL 456346, at *1 (N.D. Cal. Dec. 20, 2017) (denying a temporary restraining order because plaintiffs failed to show irreparable harm).

that make it difficult to recover if a defendant moves assets or hides the location of private keys may justify preliminary injunctive relief to prevent irreparable harm. Courts should consider that cryptocurrencies are uniquely suited to evade control by design when balancing the equities and likelihood of injury. Finally, extensive factual investigation of a defendant's cryptocurrency network and business contacts will afford plaintiffs the best chance to recover under fraudulent transfer statutes or using judgment liens.