

THE INADEQUACY OF EQUITABLE REMEDIES FOR BLOCKCHAIN FRAUD

*Joan Heminway**

INTRODUCTION	1145
I. A SPECTRUM OF BLOCKCHAIN FRAUD—FRAUD ON BLOCKCHAINS & FRAUD USING BLOCKCHAINS	1150
II. TRADITIONAL CIVIL REMEDIES FOR BLOCKCHAIN FRAUD	1155
<i>A. Existing Remedial Landscape</i>	1155
<i>B. Where Equitable Remedies Fall Short</i>	1161
1. Difficulties in Obtaining and Enforcing Equitable Remedies	1162
2. Deficient Efficacy of Equitable Remedies	1166
III. POTENTIAL INNOVATIONS IN BLOCKCHAIN FRAUD PREVENTION	1168
CONCLUSION	1173

* Rick Rose Distinguished Professor of Law and Director of the Clayton Center for Entrepreneurial Law, The University of Tennessee Winston College of Law. Brown University (A.B., 1982); New York University School of Law (J.D., 1985). I am grateful to Russ Weaver for the invitation to present this research at the 2025 Remedies Discussion Forum at the University of Public Service in Budapest, Hungary.

[T]he threat of cyberattacks and blockchain exploits is increasing at an alarming rate. Existing legislation—and related case law—was not written with such technologies, actions, or behavior in mind, leading to considerable uncertainty. . . . [A]ddressing the issue of potential legal recourse is as timely as it is consequential.¹

INTRODUCTION

Blockchains are all around us, even if we do not always see them. Smart contracts—computer code that executes transactions on blockchains²—are helping to run businesses and effectuate the funding of businesses and projects of various kinds. “Blockchain is revolutionizing the supply chain, food distribution, financial services, government, retail, and more.”³ It can be used to supply automated organizational governance for a variety of enterprises through decentralized autonomous organizations commonly known as DAOs.⁴ It enables funding from new audiences for nonprofits, political campaigns, creative enterprises, athlete name, image, and likeness rights, and more.⁵ Blockchain technology—especially the use of permissionless public

¹ Michael Conklin et al., *Legal Recourse for Victims of Blockchain and Cyber Breach Attacks*, 23 U.C. DAVIS BUS. L.J. 135, 179 (2023).

² For a more fulsome definition, see, for example, Carla L. Reyes, *Emerging Technology’s Language Wars: Smart Contracts*, 2022 WIS. L. REV. FORWARD 85, 92-94.

³ *What Is Blockchain for Business?*, IBM, <https://www.ibm.com/think/topics/blockchain-for-business> [https://perma.cc/MV9B-4QYN] (last visited May 19, 2025).

⁴ See, e.g., Carla L. Reyes, *Autonomous Business Reality*, 21 NEV. L.J. 437, 447 (2021) (“A DAO is computer software, distributed across a ‘peer-to-peer network, incorporating governance and decision-making rules.’”).

⁵ See, e.g., Brian L. Frye, *The Art of the Token*, 5 STAN. J. BLOCKCHAIN L. & POL’Y 238 (2022) (describing the use of NFTs as and in creative enterprises); Joan MacLeod Heminway, *Non-Investment Finance in an NFT World*, in THE CAMBRIDGE HANDBOOK FOR THE LAW AND POLICY FOR NFTS (Nizan Packin ed., 2024) (describing the use of NFTs in funding nonprofits and political campaigns); Joan MacLeod Heminway, *NILs on Blockchains: The Good, The Bad, And Avoiding The Ugly*, 26 TRANSACTIONS: TENN. J. BUS. L. 91 (2025) (describing various uses of blockchains in the context of actual and potential collegiate athlete name, image, and likeness arrangements).

blockchains⁶—is a growing part of business and personal life in the United States and around the world.

Both business entities and individuals interact with blockchains. Blockchains are the digital home of cryptocurrencies (like Bitcoin and Ether) and other digital assets, including NFTs—non-fungible tokens, unique digital assets that denote ownership of something. Cryptocurrencies may be used as forms of payment in certain routine commercial transactions. Commonly categorized as personal property under U.S. law, digital assets may require reflection in financial statements, trusts, wills, divorce settlements and decrees, and more. Smart contracts are not necessarily legally enforceable as contracts, but they can be a viable substitute for traditional contracting, especially in simple transactions that benefit from immutability and mechanization. As a result, lawyers of all kinds need to be or become familiar with blockchain technology. It is ostensibly a matter of professional responsibility.⁷

Yet, describing a blockchain can be somewhat difficult to do, whether undertaken in the written or spoken word. The technical aspects are important to a complete understanding of the concept.⁸ That complete understanding should be, but frequently is not, sought or attained by lawmakers and policymakers engaging with blockchain related legislation, regulation, and judicial decision-making.⁹ The matters addressed in this Article do not, however, require that the reader have a comprehensive technical definition of blockchain technology or smart contracts. Rather, given this Article's narrow focus on the need to provide for more, and more efficacious, remedies for frauds conducted on or using blockchains,

⁶ Although there are different kinds and taxonomies of blockchains, this Article generally addresses only those blockchains that are openly available to the public without the need to get access permission.

⁷ See MODEL RULES OF PRO. CONDUCT r. 1.1, cmt. 8 (A.B.A. 2016) (“To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . .”).

⁸ Many reputable sources can provide that technical explanation. See, e.g., Carla L. Reyes, *Law's Detrimental Reliance on Intermediaries*, 92 GEO. WASH. L. REV. 1343, 1354-57 (2024).

⁹ See Reyes, *supra* note 2, at 87-88 (describing a legislative misunderstanding of smart contracts).

it is sufficient that the reader understand certain key attributes of blockchains important to that thesis.

Blockchains allow people to participate in a network of computers through software that enables participants to engage in transactions that are automatically recorded and immutable and to verify the transactions of other network participants.¹⁰ The verification process is transparent and decentralized—occurring across the network of participating computers.¹¹ Blockchain transactions are therefore able to be tracked and traced by participants. Participant assets are stored in an account or a digital wallet that has a specific address. Their transactions are associated with (and are identifiable by reference to) the participant’s wallet address. However, those wallets are associated with unique identifying numbers, not names.¹²

However, despite the open, communal nature of public blockchains and the relative transparency of blockchain

¹⁰ See, e.g., Veronica Lark, *Building Blocks of Privacy: Why the Third-Party Doctrine Should Not Be Applied to Blockchain Transactions*, 74 FED. COMM. L.J. 353, 357-58 (2022) (“Blockchain is a decentralized network comprised of a system of computer node participants that record transactions on a shared, immutable ledger.”); Carla L. Reyes, *Emerging Technology’s Language Wars: Cryptocurrency*, 64 WM. & MARY L. REV. 1193, 1210 (2023) (“Blockchain technology, one type of distributed database known broadly as distributed ledger technology (DLT), allows parties that remain unknown to each other to transact on a peer-to-peer basis by using networked computers to reach consensus about the state of a ledger of transactions shared between them.” (footnote omitted)).

¹¹ See, e.g., Lark, *supra* note 10, at 358 (“[M]ultiple computer nodes have authority to update the record on the ledger The nodes are essentially a network of computers that compete to complete mathematical equations under a given consensus protocol, and the computer that does this this [sic] computation correctly, and the most quickly, posts the entry into the ledger”); Christa J. Laser, *Legal Issues in Blockchain, Cryptocurrency, and Non-Fungible Tokens (NFTs)*, 102 NEB. L. REV. 761, 766 (2024) (“[B]lockchain ledgers are . . . verified by a distributed network of devices called nodes. Nodes may be owned by thousands of different people or entities who use a consensus protocol to agree on the content of the ledger.” (footnote omitted)).

¹² See, e.g., *Address*, COINMARKETCAP, <https://coinmarketcap.com/academy/glossary/address> [https://perma.cc/GVX4-CPJW] (last visited June 7, 2025) (“Most blockchain addresses are difficult for humans to read, as they take the form of long random strings of letters and numbers. . . . Even though addresses are public, most of the addresses are anonymous (or rather, pseudonymous) as the person owning the address does not usually have their real name associated with it.”).

transactions, blockchains are not fully fraud resistant.¹³ Individual blockchain participants may perpetrate fraud on blockchains, but fraud may also be conducted in a systematized way through collective action. Blockchain fraud is a business, and market entrants of various kinds have emerged to support this nefarious element of modern commerce.¹⁴

In fact, fraud on blockchains, while relatively rare (when compared to the overall volume and value of transactions), is increasing in volume and complexity, encouraged by industry partners that are supplying tools to assist fraudsters.¹⁵ Published data indicate that blockchain usage continues to trend upward, although its use still lingers at relatively low global population rates.¹⁶ However, public reports reveal that the dollar volume of

¹³ Lynnise Phillips Pantin, *Financial Inclusion, Cryptocurrency, and Afrofuturism*, 118 NW. U. L. REV. 621, 664 (2023) (“Cryptocurrencies, like any other technology, are not immune to hacks and attacks. While blockchain technology is considered secure due to its cryptographic algorithms and decentralized nature, cryptocurrencies have been the target of several attacks in the past.” (footnote omitted)).

¹⁴ See CHAINALYSIS, THE 2025 CRYPTO CRIME REPORT 61-66 (2025), <https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf> [<https://perma.cc/6V38-49JZ>] (describing the evolving “ecosystem” for blockchain fraud); Sanjeev Bhasker, Alexandra D. Comolli & Olivia Zhu, *Carpe Crypto: Prosecuting Cases Involving Digital Assets and Blockchain Technology*, 70 DEP’T JUST. J. FED. L. & PRAC. 105, 105 (2022) (“[C]riminals today exploit digital assets and blockchain technology on a mind-boggling level. They do so as the supporting technologies evolve at an incredible rate, leading to even more creative opportunities for illicit use.” (footnote omitted)).

¹⁵ See, e.g., CHAINALYSIS, *supra* note 14, at 4 (noting that cryptocurrency is estimated to constitute less than 1% of the total volume of cryptocurrency transactions, but that the illicit blockchain addresses in 2024 may receive an aggregate of \$50 billion dollars); *id.* at 55 (“Operations like Huione Guarantee, a peer-to-peer (P2P) marketplace, offer a host of illicit services that support pig butchering scamming operations and serve as a one-stop-shop for scammers’ needs. These services range from the technology infrastructure required to initiate scams to money laundering services for obfuscating illicit activity and cashing out.”).

¹⁶ See, e.g., Naveen Kumar, *Blockchain Statistics 2025: Adoption Rate & Usage*, DEMANDSAGE (May 12, 2025), <https://web.archive.org/web/20250602115923/https://www.demandsage.com/blockchain-statistics/> [<https://perma.cc/4M35-NZTZ>] (“More than 560 million people worldwide use Blockchain.”); TRIPLE A, THE STATE OF GLOBAL CRYPTOCURRENCY OWNERSHIP IN 2024, at 3 (“6.8% of the global population owns crypto. This amounts to 562 million people.”); Joran Tuwiner, *79+ Blockchain Statistics, Facts, and Trends (2024)*, BUY BITCOIN WORLDWIDE (Sep. 10, 2023), <https://buybitcoinworldwide.com/blockchain-statistics/> [<https://perma.cc/RV5A-V3RL>] (reporting 80,025,125 blockchain users as of December 21, 2021, and that “2.8% of the world’s population is already using blockchain”).

cryptocurrency transactions also continues to increase, making blockchains growing targets for fraudulent activity.¹⁷

In recent years, cryptocurrency has become increasingly mainstream. Although illicit activity on-chain previously revolved heavily around cybercrime, cryptocurrency is now also being used to fund and facilitate all kinds of threats, ranging from national security to consumer protection. As cryptocurrency has gained greater acceptance, illicit on-chain activity, too, has become more varied. For example, some illicit actors primarily operate off-chain, but move funds on-chain for laundering.¹⁸

At some level of fraudulent activity, current and future benefits of blockchain technology will be compromised.

To preserve blockchain's actual and potential social, financial, and economic value, policymakers, the practicing bar, and blockchain consumers must familiarize themselves with the blockchain fraud environment and ensure that conduct regulation and enforcement efforts and outcomes properly balance innovation and regulation. Appropriately designed fraud enforcement efforts, including the resulting remedies, are a component piece of the puzzle. This Article offers a window into blockchain fraud and describes and evaluates both the equitable remedies that are assessed against those who commit fraud on blockchains and related proposals for reform. It principally focuses on these issues through a U.S. lens. However, international perspectives are introduced in places, and some observations also may have purchase in other jurisdictions or internationally.

To achieve its purpose, this Article proceeds in three additional parts before briefly concluding. First, it offers a brief primer on blockchain fraud—what it is, in general. Next, it offers an overview of civil remedies for blockchain fraud, focusing on both the overall remedies environment and the insufficiency of equitable remedies as an important part of that environment.

¹⁷ See, e.g., Kumar, *supra* note 16 (“The blockchain market has steadily grown over the years. Its market value increased from \$4.19 billion in 2020 to \$26.91 billion last year.”); Tuwiner, *supra* note 16 (“The global blockchain market will be worth \$1,431.54 billion by 2030, growing at a CAGR of around 85.9% from 2022-2030.”).

¹⁸ CHAINALYSIS, *supra* note 14, at 2.

Finally, this Article offers observations on reforms that hold promise to better address blockchain fraud both *ex ante* and as a means of better ensuring the availability and enforceability of equitable remedies.

I. A SPECTRUM OF BLOCKCHAIN FRAUD—FRAUD ON BLOCKCHAINS & FRAUD USING BLOCKCHAINS

Blockchain fraud can take many forms, but fraudulent actors principally use blockchain technology to engage in unlawful behaviors in two principal ways: as an essential environment for their schemes or as a tool for their use in obtaining and hiding movement of the resulting financial gain.¹⁹ In the first case, fraud originates and relies on blockchains. For example:

- ❖ NFT originators and promoters may make unauthorized use of art created by others;
- ❖ promoters may offer and sell copycat or otherwise bogus NFTs;
- ❖ promoted blockchain NFT or investment platforms may impersonate valid platforms, be mere façades, or involve fly-by-night promoters engaged in schemes to lure in unsuspecting collectors or investors whose funds are then absconded with (a scheme often referred to as a rug pull);
- ❖ digital asset Ponzi and pump-and-dump schemes may be executed on blockchain platforms;
- ❖ sellers or promoters of NFTs or blockchain business finance may make material misrepresentations or misleadingly withhold significant information from purchasers or investors who rely on those misrepresentations or omissions; and

¹⁹ See WILLIAM MAGNUSON, BLOCKCHAIN DEMOCRACY: TECHNOLOGY, LAW AND THE RULE OF THE CROWD 100 (2020) (“[W]hen people say that the blockchain has a crime problem, they are generally saying one of two things: blockchain is a *target* of criminals, in that it is being stolen by them, and blockchain is a *currency* of criminals, in that it is being used by them.”); see also Pantin, *supra* note 13, at 664 (“Investors have been harmed in various ways, including by cybercrime and ransomware. In addition, many retail investors have been falling prey to simple phishing attempts and other ‘hacks.’”).

- ❖ wallets holding valuable digital assets may be hacked by blockchain participants who identify and take advantage of coding errors or other security lapses.²⁰

Alternatively, a fraudster using blockchain technology as a tool to execute on the financial aspects of their scheme may receive and launder ill-gotten gains from frauds obtained off the blockchain through ransomware, bribery, or other criminal activities.²¹ Fraud relating to the promotion or conduct of transactions in cryptocurrencies is the most public and widely recognized blockchain fraud.²²

Those who follow international news coverage undoubtedly remember the collapse of cryptocurrency exchange and hedge fund high-flyer FTX Trading Ltd. (“FTX”) in 2022. In brief, FTX represented that the assets of cryptocurrency investors trading through its FTX.com platform were held in custody by FTX when their assets were being redeployed by FTX for use by an affiliated firm, Alameda Research LLC, and by FTX founder Samuel Bankman-Fried.²³ Public and private enforcement actions relating to the FTX fiasco are ongoing, but the U.S. Commodities Futures Trading Commission won a \$12.7 billion judgment against FTX and Alameda in August 2024.²⁴ Other large cryptocurrency fraud

²⁰ See, e.g., CHAINALYSIS, *supra* note 14, at 7-8 (describing general types of and trends in cryptocurrency fraud); Carol R. Goforth, *How Nifty! But Are NFTs Securities, Commodities, or Something Else?*, 90 UMKC L. REV. 775, 776 (2022) (“[A]rtists wake up to find that their art is being packaged and sold as NFTs by unauthorized third parties.”); *id.* (mentioning as common NFT frauds “sites that imitate legitimate NFT platforms; NFT platforms that do not really exist; counterfeit or fraudulently created NFTs; fake giveaways or airdrops of NFTs; and impersonation of platforms and brands on social media”).

²¹ See generally CHAINALYSIS, *supra* note 14, at 10-21 (describing ransomware trends, types, processes, examples, and more); Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security*, 18 N.Y.U. J.L. & BUS. 391 (2022) (describing ransomware attacks and their connection to cryptocurrencies and money laundering).

²² See, e.g., Pantin, *supra* note 13, at 665 (“Cryptocurrency scams account for a greater percentage of losses than any other type of payment method.”).

²³ See Press Release, CFTC, CFTC Charges Sam Bankman-Fried, FTX Trading and Alameda with Fraud and Material Misrepresentations (Dec. 13, 2022), <https://www.cftc.gov/PressRoom/PressReleases/8638-22> [<https://perma.cc/44AY-NHVD>].

²⁴ See Press Release, CFTC, CFTC Obtains \$12.7 Billion Judgment Against FTX and Alameda (Aug. 8, 2024), <https://www.cftc.gov/PressRoom/PressReleases/8938-24> [<https://perma.cc/3S72-TF4L>].

claims include lending fraud involving Digital Currency Group Inc. and its subsidiaries Genesis Global Holdco LLC, Genesis Global Capital LLC, and Genesis Asia Pacific Pte. Ltd. (together with others)²⁵ and the 2016 Bitfinex hacking and money laundering scandal.²⁶ “The recent publicized failures of cryptocurrency issuers, exchanges, and hedge funds demonstrate the risky nature of the ecosystem, as billions of dollars have disappeared overnight with little remedy or recourse for investors.”²⁷

In a May 2025 speech, Caroline Crenshaw, one of the five commissioners of the U.S. Securities and Exchange Commission (“SEC”), offered a sobering assessment of fraud involving cryptocurrencies.

Crypto presents certain novel risks—including those related to hacks and the prevalence of crypto as a method of payment for illicit activity. This last year alone saw a 66 percent increase in total fraud-related crypto losses—primarily affecting individuals over the age of 60 [U]nique challenges with custody, conflicts of interest, disclosure, and market integrity remain unresolved—despite the pressure for widespread crypto adoption and experimentation.²⁸

Overall, Commissioner Crenshaw expressed concern about the impact of current deregulatory forces on cryptocurrency fraud and related misconduct, a factor to be considered in designing appropriate responses to cryptocurrency and other blockchain frauds.²⁹

²⁵ See *Genesis LOC's Two Major Lawsuits Against DCG, Barry Silbert, and a Network of Insiders Now Available to the Public*, BUS. WIRE (May 19, 2025, at 15:45 ET), <https://www.businesswire.com/news/home/20250519165640/en/Genesis-LOCs-Two-Major-Lawsuits-Against-DCG-Barry-Silbert-and-a-Network-of-Insiders-Now-Available-to-the-Public> [https://perma.cc/ZG7Q-L9SK].

²⁶ See *2016 Bitfinex Hack*, U.S. ATT'Y OFF.: D.C. (Oct. 29, 2024), <https://www.justice.gov/usao-dc/2016-bitfinex-hack> [https://perma.cc/M5E5-3LSD].

²⁷ Pantin, *supra* note 13, at 668.

²⁸ Caroline A. Crenshaw, Comm'r, SEC, A Reckless Game of Regulatory Jenga - Remarks at “SEC Speaks” (May 19, 2025).

²⁹ *Id.* (“Failing to appreciate and address these risks and complexities destines us to repeat hard lessons with high stakes as crypto becomes increasingly entangled with traditional finance.”).

Given that blockchain technology has been adopted and is gaining in popularity in a variety of professional and personal settings and that blockchain fraud and other misconduct involve many different behaviors, fashioning an appropriate regulatory environment is complex and fraught with some peril. Indeed, as Commissioner Crenshaw references in her speech, the current focus at the SEC is on positive, pro-innovation regulation rather than enforcement efforts intended to curb wrongdoing.³⁰ But more fundamentally, at the outset of his second presidential term, Donald Trump issued an executive order that focused on the promotion of digital assets.³¹ On April 7, 2025, Deputy Attorney General Todd Blanche issued a memorandum to all employees in the U.S. Department of Justice disbanding the department's National Cryptocurrency Enforcement Team and offering guidance on the department's pursuit of criminal enforcement efforts relating to digital assets.³²

Executive Order 14178 tasks the Justice Department and others with “protecting and promoting” (1) “the ability of individual citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution”; and (2) “fair and open access to banking services for all law-abiding individual citizens and private-sector entities alike.” In response to those taskings, the Justice Department will stop participating in regulation by prosecution in this space. Specifically, the Department will no longer target virtual currency exchanges, mixing and tumbling services, and offline wallets for the acts of their end

³⁰ *Id.* (“In the past four months, we’ve used guidance to walk away from rules and upend longstanding practice. . . . In particular, our statements on . . . crypto-related issues are the equivalent of a wink and nod intended to convey that we do not plan to rigorously apply our laws in certain, specific situations.”).

³¹ Exec. Order No. 14178, 90 Fed. Reg. 8647 (Jan. 23, 2025).

³² Memorandum from Todd Blanche, Deputy Att’y Gen., to All Department Employees, Ending Regulation by Prosecution (Apr. 7, 2025) (on file with the U.S. Department of Justice); *see also* Devlin Barrett, *Justice Dept. Disbands Cryptocurrency Enforcement Unit*, N.Y. TIMES (Apr. 8, 2025), <https://www.nytimes.com/2025/04/08/us/politics/doj-disbands-crypto-unit.html> [https://perma.cc/5BTY-SCHF] (noting the disbanding of “a unit in the Justice Department that was responsible for investigating cryptocurrency crimes” and the Deputy Attorney General’s instructions “to narrow the focus of cryptocurrency investigations to crimes like fraud, drug trafficking and terrorism”).

users or unwitting violations of regulations—except to the extent the investigation is consistent with the priorities articulated in the following paragraphs.³³

The Blanche memorandum does note that prosecutions will continue for certain primary criminal conduct on or involving blockchains.³⁴ In addition, the head of the SEC's Crypto Task Force, SEC Commissioner Hester Peirce, has asserted continued investor protection as the SEC engages in its deregulation efforts.³⁵ However, the tempering of public enforcement activity designed to encourage and guide lawful conduct may portend a shift in enforcement emphasis toward private civil litigation.

Thus, although cryptocurrency and other blockchain fraud may be—and are—pursued in criminal and civil public enforcement actions, the subsequent parts of this Article focus on private civil fraud claims. More specifically, the remainder of it outlines and evaluates existing civil remedies for blockchain fraud and offers preliminary suggestions on enhanced and additional remedies that could be designed to guide lawful behaviors more skillfully and successfully and to deter or punish wrongful conduct more effectively. The principal critical focus is on equitable remedies, although damages remedies are also addressed to a limited extent.

³³ Memorandum from Todd Blanche to All Department Employees, *supra* note 32, at 1.

³⁴ *Id.* at 2 (“Prosecutors shall prioritize cases that hold accountable individuals who (a) cause financial harm to digital asset investors and consumers; and/or (b) use digital assets in furtherance of other criminal conduct, such as fentanyl trafficking, terrorism, cartels, organized crime, and human trafficking and smuggling.”).

³⁵ See, e.g., Hester M. Peirce, Comm’r, SEC, New Paradigm: Remarks at SEC Speaks (May 19, 2025) (“The Commission—consistent with its investor protection mission—will continue to vigorously pursue *securities* fraud, including in cases that involve crypto, but the Commission’s statutory authority does not cover fraud and scams of every kind.”); Hester M. Peirce, *The Journey Begins*, U.S. SEC. & EXCH. COMM’N (Feb. 4, 2025), <https://www.sec.gov/newsroom/speeches-statements/peirce-journey-begins-020425> [<https://perma.cc/G6U4-3Y8G>] (“[T]he Task Force wants to travel to a destination where people have great freedom to experiment and build interesting things, and which will not be a haven for fraudsters. . . . As the Task Force works to help develop this regulatory framework, it will give careful consideration to antifraud protections.”).

II. TRADITIONAL CIVIL REMEDIES FOR BLOCKCHAIN FRAUD

Given the relatively recent advent of blockchain technology, it may seem odd to refer to remedies for blockchain fraud as “traditional.” Truthfully, however, the use of that word—traditional—signals the problem and opportunity this Article is designed to address. Remedies for blockchain fraud offer little in the way of novelty, despite the complex technological innovation that commerce on blockchains represents.

Indeed, while the need for efficacious blockchain fraud remedies is clear, their availability is limited. Focusing on cryptocurrency, one commentator notes this paradox:

[C]ryptocurrency owners are vulnerable to scams and wide fluctuations in price with little to no recourse, particularly in the digital marketplace. According to the FTC, cryptocurrency fraud cost investors \$1.205 billion in 2022. By contrast, credit card fraud amounted only to \$185 million. Cryptocurrency scams account for a greater percentage of losses than any other type of payment method. There is no immediate remedy or recourse for victims of cryptocurrency scams or fraud.³⁶

Understanding the existing remedial landscape, imperfect as it may be, is an essential starting point in fashioning more effective alternatives.

Although blockchains and their participants are multinational and blockchain transactions (and related fraud) cross borders, the objective of this Article is not to address transnational claims, enforcement, or remedies. Accordingly, in this part, references are to U.S. law and regulation, unless otherwise noted. Commentary, however, incorporates the observations and wisdom of both U.S. and non-U.S. observers.

A. *Existing Remedial Landscape*

Experts typically advise victims of blockchain fraud to first report the fraud to appropriate government law enforcement authorities or related regulatory agencies.³⁷ These official

³⁶ Pantin, *supra* note 13, at 665 (footnotes omitted).

³⁷ Goforth, *supra* note 20, at 798 (“[F]or consumers who are defrauded, reporting the problem is a good first step.”); *Cryptocurrency Investment Fraud*, FED. BUREAU OF

enforcement agents are undoubtedly better resourced to investigate and pursue fraud claims than individuals.³⁸ Evidence gathered in these investigations may prove useful in later public or private enforcement proceedings.³⁹

However, it may be difficult to identify enforcement authorities governing specific types of fraud due to blurred boundaries of authority, and the resources of enforcement authorities may not be sufficient to respond adequately to blockchain fraud. Digital assets may be classified as securities, commodities, or other personal property, making the locus of regulatory authority unclear.⁴⁰ Investigations can be complex; tracing transactions and legal identities on blockchains may require the use of technologies and expertise that may not be

INVESTIGATION, <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud> [<https://perma.cc/R4V9-B8N7>] (last visited Mar. 17, 2026) (“If you feel that you are a victim of a cryptocurrency investment fraud, stop sending any money to the suspected criminals, file a report at FBI’s Internet Crime Complaint Center”); Suyash Raizada, *Top Ways to Recover Funds from Crypto Scam in 2026*, BLOCKCHAIN COUNCIL (May 17, 2026), <https://www.blockchain-council.org/cryptocurrency/top-5-ways-to-recover-funds-from-crypto-scam/> [<https://perma.cc/SSV9-DEJ8>] (“Once you have gathered the necessary evidence, it is crucial to report the cryptocurrency scam to the appropriate authorities. Taking prompt action will increase the likelihood of recovering your funds and help prevent others from falling victim to the same scam.”).

³⁸ See Goforth, *supra* note 20, at 782 (“Enforcing judgments can also be particularly problematic for private plaintiffs. Official agencies of the United States have international treaties and cooperation agreements to fall back on, while individual plaintiffs have no such assurance of assistance. Agencies are also familiar with this kind of problem, while many litigators (particularly from smaller firms) may not be.” (footnote omitted)).

³⁹ See, e.g., *United States v. Approximately Five Hundred Forty-One Thousand Nine Hundred Fifty-Three Dollars & Zero Cents (\$541,953.00) Seized from JP Morgan Chase NA Acct. No. XXXXXXXXXX Held in the Name of Jiawig Trade Inc.*, No. 23-CV-9585, 2025 WL 1029431, at *2 (E.D.N.Y. Feb. 10, 2025), *report and recommendation adopted*, No. 23-CV-9585, 2025 WL 923412 (E.D.N.Y. Mar. 27, 2025) (noting that “[l]aw enforcement officers were able to track several victims’ funds to a bank account maintained at JP Morgan Chase NA”).

⁴⁰ On the federal level, however, as a rule, blockchain fraud can be reported on one of two government websites. *Learn Where to Report a Scam*, USA.GOV, <https://www.usa.gov/stop-scams-frauds> [<https://perma.cc/RH47-6YFQ>] (last visited June 7, 2025) (for general reports); *Welcome to the Internet Crime Complaint Center*, INTERNET CRIME COMPLAINT CTR. (IC3), <https://www.ic3.gov/> [<https://perma.cc/HD7M-WDD2>] (last visited June 7, 2025) (for criminal complaints).

available to local—or even federal—enforcement officials.⁴¹ Moreover, investigation and enforcement of blockchain fraud often involves cross-border activity, given the inherently international capacity of blockchain transactions. Fraudsters, platforms, exchanges, and fraud victims may be organized or residents in different jurisdictions, which introduces additional layers of complexity.⁴² Finally, the pursuit of wrongdoers through government enforcement ultimately requires the affirmative exercise of investigative and prosecutorial discretion, meaning that the path to recovery and justice is uncertain. And even if enforcement efforts are successfully undertaken, they may result in the assessment of specific penal sanctions (including incarceration or fines) rather than redress for fraud victims (although redress is possible in some cases).⁴³

Accordingly, while reporting blockchain fraud to law enforcement is an appropriate starting point for victims (and a potentially essential step in achieving recompense for those who do not have the resources to perform an investigation on their own),⁴⁴ it is not typically sufficient to serve the fraud victim's

⁴¹ See Joan MacLeod Heminway & Cody Dethlefs, *The Fraud Remains the Same . . . or Does It?*, 55 STETSON L. REV. 507, 531 (2026) (“[E]nforcement agents face certain novel challenges in bringing blockchain wrongdoers to justice. These challenges include general technological barriers, the relative anonymity of blockchain participants, and the multi-jurisdictional nature of blockchain activity.”).

⁴² See *id.*; see also Goforth, *supra* note 20, at 782 (“[I]ndividual plaintiffs must also be able to assert jurisdiction over the persons associated with any fraud. . . . While some platforms are based in the United States, there is no guarantee that it will be simple to obtain jurisdiction over all of them. Obtaining jurisdiction over international operations is not easy for individual plaintiffs.”); Raizada, *supra* note 37 (“Cryptocurrencies transcend physical borders, making it challenging to determine jurisdiction in cases of scams. The decentralized nature of blockchain technology, which powers cryptocurrencies, further complicates matters. Jurisdictional issues arise when identifying the location of the scammer, determining the applicable laws, and initiating legal action.”).

⁴³ See Goforth, *supra* note 20, at 797 (“In some cases, an order of disgorgement may be made and the funds may be reserved to compensate victims.”); Raizada, *supra* note 37 (“In some cases, reporting a scam can also lead to compensation or reimbursement for victims.”).

⁴⁴ See Goforth, *supra* note 20, at 797 (“Even if there is no action on the agencies’ own initiative, this does not mean that consumers should not take advantage of the presence of potential regulators. . . . Because government agencies use these reports to track patterns of illicit behavior, these reports can be quite important. The agencies may even take legal action, although consumers should know that this may not result in them recovering any money that they have lost.”); Raizada, *supra* note 37

needs or desires.⁴⁵ As is true for victims of financial and property fraud conducted outside the blockchain context, those who lose cryptocurrencies or other digital assets in blockchain fraud typically want to stop the misconduct (if it is still in process) and recover their funds or property. As a result, absent recovery of funds or assets through law enforcement efforts, the most appropriate avenues for relief are civil claims requesting legal and equitable remedies, including injunctive relief, rescission of any fraudulent transactions, or restitution. Defendants in these claims may include both the fraudsters themselves and the platforms, exchanges, or other intermediaries involved or used in the fraudulent scheme.

Generally, the most useful remedy for victims of crypto fraud is to bring a proprietary claim against the fraudsters and, depending on the circumstances, against the exchange. As a proprietary claim rather than a personal claim, the victim benefits from familiar advantages including priority in insolvency, the ability to recover the property itself or an equitable lien for the amount the property was worth when it was taken (which may be beneficial in a volatile market) and recovery from subsequent transferees.⁴⁶

Damages and related penalties also may be available for specific statutory or common law wrongs within the scope of blockchain fraud.⁴⁷

Although legal actions may be brought individually, individual private actions can be expensive.

(“Reporting a cryptocurrency scam can also help you recoup your losses. The sooner you report it, the better the chances of authorities being able to track down the scammers and recover any stolen funds.”).

⁴⁵ See *id.* (“Although it doesn’t assure fund recovery, it’s also best to report the cryptocurrency scam to your area’s designated law enforcement authorities.”).

⁴⁶ Gretel Scott, *Remedies for Victims of Crypto Fraud*, BUTTERWORTHS J. INT’L BANKING & FIN. L., Aug./Sep. 2023, at 539 (commenting on this phenomenon from an English law perspective).

⁴⁷ See, e.g., *Bishop v. Defendant “1”*, No. 23-CV-24376-RAR, 2024 WL 4635126 (S.D. Fla. May 30, 2024) (awarding treble damages under the federal Racketeer Influenced and Corrupt Organizations Act); *Kozlar v. Blammo, Ltd.*, 759 F. Supp. 3d 543, 546 (S.D.N.Y. 2024) (recommending a \$644,400.10 award in damages, together with pre-judgment interest at a 9% statutory rate).

[T]he difficulty and costs of bringing a private fraud claim are not insignificant. One source suggests that smaller law firms generally charge \$100-300 per hour, “while larger, more powerful firms with in-demand attorneys may charge as much as \$500 per hour.” As any lawyer will tell you, the more complicated the case, the more hours of time that will need to be spent in litigating, and, regrettably, fraud cases can be extremely complicated. Crypto fraud, which may or may not involve securities laws issues in addition to elements associated with common law fraud, adds unique issues which may require even more attorney hours. There are also a range of court costs that are likely to be incurred. Many individual plaintiffs will be unable to afford those kinds of expenses.⁴⁸

Accordingly, class actions may be more cost-effective for many individual victims of blockchain fraud. Having said that, class action processes may present collective action impediments and take time to develop, establish, and manage. Also, the aggregate amount of any pecuniary remedy is likely to be reduced substantially by the payment of contingency fees and related expenses to plaintiffs’ legal counsel. Finally, blockchain terms of use may require users to waive their rights to class action litigation (perhaps accompanied by an arbitration provision).⁴⁹

Nevertheless, both public and private blockchain fraud enforcement actions have been brought, and equitable and legal remedies have been successfully pursued and awarded. Although there are relatively few reported opinions to date, as these actions proceed to reported decisions, we can learn much from the claims that are brought and the remedies that are requested and awarded. A few sample cases illustrate important aspects of this litigation environment.

For example, on the public enforcement side, the CFTC brought a legal action in May 2022 alleging that Eddy Alexandre

⁴⁸ Goforth, *supra* note 20, at 781.

⁴⁹ See, e.g., Skye Witley, *Cryptocurrency Theft Lawsuits Diminish Amid Rise in Cybercrime*, BLOOMBERG L. (Feb. 15, 2024), <https://www.bloomberglaw.com/product/blaw/bloomberglawnews/privacy-and-data-security/BN%200000018d-a92b-de43-a5ed-bdef65560001> [https://perma.cc/4FAN-ZAJ6] (quoting advice to general counsels to “ensure their ‘terms and conditions have an arbitration provision and a no class action provision,’ because courts generally uphold those”).

operated investment club EminiFX, Inc. fraudulently, in a way that resembled a Ponzi scheme.⁵⁰ The CFTC was successful in obtaining an *ex parte* statutory restraining order freezing certain portions of the defendants' assets and appointing a receiver to oversee customer assets possessed or controlled by Eddy Alexandre, holding them for later distribution to defrauded investors.⁵¹ As of January 2025, the total value of assets under the receiver's control was approximately \$153 million.⁵² The CFTC also has successfully brought claims resulting in awards of injunctive relief, restitution, and monetary penalties.⁵³

The emergency temporary restraining order request of the plaintiff in *Patel v. "Defendant 1"*⁵⁴ offers insights into private enforcement in response to blockchain fraud. The plaintiff was induced by defendants into downloading a fraudulent app that mimicked an actual cryptocurrency exchange.⁵⁵ The plaintiff used the app to transfer cryptocurrency to an account that then enabled the defendants to move the cryptocurrency into accounts for their own benefit.⁵⁶ The plaintiff retained the services of a forensic cryptocurrency tracing firm that identified the accounts in which his cryptocurrency was being held.⁵⁷ He filed a legal action claiming conversion, unjust enrichment, imposition of constructive trust and disgorgement of funds, and conspiracy and, shortly thereafter, filed an *ex parte* Emergency Motion for Temporary Restraining Order, seeking to freeze the defendants' assets in the identified accounts.⁵⁸ The court granted the motion, noting that the plaintiff "provided specific facts . . . showing that immediate

⁵⁰ *Commodity Futures Trading Comm'n v. Alexandre*, No. 22-CV-3822, 2025 WL 252435, at *1 (S.D.N.Y. Jan. 21, 2025).

⁵¹ *Id.* at *1-2.

⁵² *Id.* at *2.

⁵³ *See, e.g., Commodity Futures Trading Comm'n v. Ochi*, No. 21-11615, 2025 WL 871137 (D. Mass. Mar. 19, 2025) (awarding injunctive relief, restitution, and monetary penalties); *Commodity Futures Trading Comm'n v. My Big Coin Pay, Inc.*, No. 18-CV-10077, 2025 WL 1021899 (D. Mass. Feb. 6, 2025) (granting injunctive relief and restitution).

⁵⁴ No. 3:23cv24651, 2024 WL 4919639 (N.D. Fla. Jan. 11, 2024).

⁵⁵ *Id.* at *1.

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ *Id.* at *2.

and irreparable loss will result absent the TRO and Patel does not currently know the Defendants' true identities.”⁵⁹

*Bishop v. Defendant “I”*⁶⁰ provides another example of private enforcement—one in which one fraudster has been identified and was served but failed to appear in court.⁶¹ Other defendants were unable to be identified and served.⁶² In that legal action, the plaintiff alleged that the defendant, together with co-conspirators, engaged in cryptocurrency fraud and conversion through which they stole over \$900,000 of cryptocurrency.⁶³ Specifically, as part of a broad global fraud network, the defendant allegedly persuaded the plaintiff to deposit cryptocurrency on a sham electronic platform, from which the defendant moved the plaintiff's cryptocurrency to wallets and accounts controlled by the defendant.⁶⁴ Claims included violation of the Racketeer Influenced and Corrupt Organizations Act (“RICO”),⁶⁵ as well as Georgia law causes of action for conversion, unjust enrichment, breach of fiduciary duty, and conspiracy.⁶⁶ The court found that the plaintiff established both entitlement to a constructive trust and the existence of a conspiracy, awarded a default judgment to the plaintiff for treble damages under RICO, and ordered the establishment of a constructive trust and disgorgement of the plaintiff's funds.⁶⁷

B. Where Equitable Remedies Fall Short

The availability of equitable remedies for blockchain fraud is an essential component of a healthy, fair, and safe blockchain transactional market. The market for blockchain transactions depends on the trust of participants in just and equitable

⁵⁹ *Id.* at *3.

⁶⁰ No. 23-CV-24376, 2024 WL 4635126 (S.D. Fla. May 30, 2024).

⁶¹ *Id.* at *1.

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.* at *2 (“Plaintiff alleges that Defendant and her co-conspirators operate a sophisticated global internet cryptocurrency fraud and conversion scheme. Pursuant to this scheme Defendant continually contacted Plaintiff via electronic means, induced him to interact with a fraudulent electronic platform, and converted Plaintiff's cryptocurrency.”).

⁶⁵ 18 U.S.C. §§ 1961-68 (2024).

⁶⁶ *Bishop*, 2024 WL 4635126, at *1.

⁶⁷ *Id.* at *2-4.

treatment as transactional counterparties. Blockchain participants who are fraudulently separated from their digital assets are unlikely to continue to engage in blockchain transactions if they are unable to effectively stop, rescind, or receive restitution for those fraudulent transactions. Thus, traditional equitable remedies serve an important public policy function in supporting blockchain commerce. As noted in Part III.A, some cryptocurrency fraud claims may and do result in awards of equitable remedies, even if judgments ultimately may not be enforceable.⁶⁸

Yet, as necessary as traditional equitable remedies are to sustaining blockchain market integrity, they are alone insufficient to the task for at least two reasons. The first relates to process barriers to obtaining and enforcing court judgments awarding the desired remedies. The second stems from the suboptimal impact of equitable remedies on larger, core market actors—platforms and exchanges. These shortcomings of equitable remedies may dissuade aggrieved fraud victims from reporting blockchain fraud or bringing related claims for relief. Fraud, left unaddressed, is likely to compromise the vitality of blockchain commerce.

1. Difficulties in Obtaining and Enforcing Equitable Remedies

Obtaining and enforcing equitable remedies on blockchains can be challenging.⁶⁹ Blockchain users enjoy pseudonymity.⁷⁰

⁶⁸ See, e.g., Joe Dickerson, *Why Do 80% of Judgments Remain Uncollected?*, ABA J. (Apr. 2, 2020, at 13:55 CT), <https://www.abajournal.com/voice/article/why-do-80-of-judgments-remain-uncollected> [<https://perma.cc/9A2M-JYR4>] (“80% of the U.S. civil money judgments, year after year, continued to be unenforced, leaving the victims of fraud and malfeasance unable to recover/collect the money the courts have ruled is rightfully their money.”).

⁶⁹ Maayan Perel, *Digital Remedies*, 35 BERKELEY TECH. L.J. 1, 6 (2020) (“Remedies that compel action or inaction—that is, equitable remedies—generally create great difficulties for courts in ascertaining and ensuring compliance; digital remedies heighten these issues.” (footnote omitted)); Samuel N. Weinstein, *Blockchain Neutrality*, 55 GA. L. REV. 499, 542 (2021) (“Another general enforcement challenge blockchain poses stems from its decentralized nature, which could make it tricky to effectively remedy unlawful conduct undertaken on these networks. Enforcing injunctions against an organization controlled by a disparate group of pseudonymous users may be difficult.”).

⁷⁰ See *supra* note 12 and accompanying text; see also Weinstein, *supra* note 69, at 541 (“Blockchain users sometimes protect their identities using pseudonyms, which may make identifying them for purposes of legal sanctions difficult.”).

Tracing transactions in digital assets and freezing a defendant's assets on and off blockchains require diligence (often assisted by forensic technology and skilled intermediaries), expert legal advice, and at least a modicum of luck.⁷¹ Assets may have been laundered and impossible to locate.⁷² Moreover, "if a purchaser wishes to sue the seller of an NFT rather than the platform (which is more probable)," one scholar notes, "the first problem is accurately identifying who the seller is (especially given that fake and imitation sites have sprung up)."⁷³

Indeed, a review of reported cases reveals that individuals participating in blockchain fraud who conduct their unlawful activities solely or principally on an actual or sham Internet platform can be hard to identify and bring to justice in court. Many orders are entered *ex parte* because defendant identities have not yet been determined;⁷⁴ legal action against certain

⁷¹ See, e.g., Sophia Dudgeon, Note, *Service of Process Via NFT Airdrops: The Pathway to Private Litigation for Injured Web3 Plaintiffs*, 42 CARDOZO ARTS & ENT. L.J. 467, 499 (2024) ("Identifying a wallet address containing stolen digital assets is not an easy task, especially after the coins or tokens have been swapped in a crypto mixer like Tornado. Without a team of in-house algorithm tracing specialists or a cooperative and security-focused crypto exchange, individual plaintiffs who do not possess the skills required to track blockchain activity might feel defeated as soon as they realize funds have been stolen from them.").

⁷² Joshua Fairfield, *Crypto-Counterfeiting*, 15 WM. & MARY BUS. L. REV. 497, 545 (2024) ("Crypto-counterfeiters are likely to try to launder their ill-gotten gains quickly by using tumblers, which arrange transactions intended to wash duped currency clean from their wrongful origins and thus into the blue water of the general token economy for a given chain."); Samantha B. Larkin, *Lipstick on a Slaughtered Piggybank: Civil RICO Against "Pig Butchering" Cryptocurrency Investment Schemes*, 30 ROGER WILLIAMS U. L. REV. 1, 45 (2025) ("Recovery may not be possible . . . , especially if the crypto has been converted into cash or lost on the darknet.").

⁷³ Goforth, *supra* note 20, at 782.

⁷⁴ E.g., Patel v. Defendant "1", No. 3:23CV24651, 2024 WL 4919639, at *3 (N.D. Fla. Jan. 11, 2024)

("[T]he Court enters the TRO without notice to the Defendants because Patel provided specific facts in his verified First Amended Complaint showing that immediate and irreparable loss will result absent the TRO and Patel does not currently know the Defendants' true identities."); *Astrove v. Doe*, No. 22-CV-80614, 2022 WL 2805315, at *3 (S.D. Fla. Apr. 22, 2022) ("Notice was not provided to Defendant JOHN DOE prior to entry of this Order because his identity is presently unknown to Plaintiff. The Court will separately consider a request from Plaintiff to engage in expedited discovery through which Plaintiff intends to obtain from the recipient cryptocurrency exchanges listed above Defendant JOHN DOE's identity, including a physical and/or electronic address at which Defendant JOHN DOE can be contacted about the claims asserted against him in this lawsuit.").

unidentified defendants may even be dismissed.⁷⁵ These impediments undoubtedly discourage many defrauded blockchain users from bringing legal actions against many blockchain fraudsters.

As a result, defendants most likely to be held liable for fraud conducted on or using blockchains are those who directly and personally promote cryptocurrency investments or other blockchain participation off-chain and blockchain firms, including platforms and exchanges. Blockchain platforms and exchanges may be defendants and are most certainly important to the efficacy of equitable remedies when they are awarded.

[T]he cases show that victims are most successful in enforcing where their assets can be traced to an exchange (these also being the cases that victims seem most prepared to litigate). Exchanges may be willing to comply with court orders against fraudsters, but . . . victims should be careful how they frame any proprietary claims against exchanges.⁷⁶

The extent to which platforms and exchanges will be held legally responsible for different types of blockchain fraud remains uncertain, however.

Overall, courts may be inadequate forums for achieving meaningful relief for blockchain fraud victims.⁷⁷ The very substance of blockchain fraud claims can be complex. For this and other reasons, relief provided through litigation—especially private litigation—can be slow.⁷⁸ Even if conventional early-stage

⁷⁵ *E.g.*, Bishop v. Defendant “1”, No. 23-CV-24376, 2024 WL 4635126, at *1 (S.D. Fla. May 30, 2024) (“Unable to identify and serve Defendants John Does 1–20, Plaintiff voluntarily dismissed them from the action.”).

⁷⁶ Scott, *supra* note 46, at 542.

⁷⁷ Amy J. Schmitz, *Resolving NFT and Blockchain Disputes*, 6 STAN. J. BLOCKCHAIN L. & POL’Y 156, 171 (2023) (“Most commentators and practitioners realize that blockchain-related disputes do not belong in court.”); *id.* at 188 (“The jurisdictional and coding issues alone indicate that the traditional judicial *forum* does not fit the blockchain *fuss*.”). Actions brought in administrative law courts may provide more advantages, however. See Goforth, *supra* note 20, at 781 (“While serving as head of the SEC’s Division of Enforcement, Andrew Ceresney ‘identified a number of advantages of administrative proceedings, including faster decisions, the use of specialized factfinders, and more flexible evidentiary rules.’ Private plaintiffs cannot rely on these advantages.” (footnote omitted)).

⁷⁸ See, *e.g.*, Goforth, *supra* note 20, at 781 (“[R]elying on private litigation to provide sufficient redress for fraud ignores the reality that any remedy will likely be a

injunctive relief or asset freezes are legally available, for example, that relief may not be able to be obtained in time to secure the accounts and wallets in which unlawfully obtained digital assets reside and through which they may be traded. Digital assets can be transferred in a matter of seconds and can move between blockchains.⁷⁹ Moreover, by the time digital assets are secured, their value may have decreased substantially.⁸⁰ As a result, even a judgment awarding appropriate, useful equitable remedies may fall short in achieving its objectives because legal action to effectuate those remedies may come too late. Putative fraud plaintiffs may be further disincentivized in bringing fraudulent actors to justice by the protracted nature of litigation.

In general, equitable remedies cannot consistently serve their aim in treating victims of blockchain fraud justly because they may be difficult or impossible to obtain and enforce. Some defrauded blockchain participants may seek and be granted equitable relief. However, enforcement may then be impeded by difficulties in tracing assets (if asset tracing has not already occurred as a predicate for granting the requested relief) and locating and identifying key fraudulent actors.

long time coming and is dependent on determinations by factfinders who are unlikely to be familiar with the intricacies of cryptoassets.”).

⁷⁹ See *Patel v. Defendant “1”*, No. 3:23CV24651, 2024 WL 4919639, at *2 (N.D. Fla. Jan. 11, 2024) (noting that the plaintiff “has shown that irreparable harm will ensue absent a TRO, considering the speed with which cryptocurrency transactions are made, as well as the anonymous nature of those transactions”); *Astrove v. Doe*, No. 22-CV-80614, 2022 WL 2805315, at *2 (S.D. Fla. Apr. 22, 2022) (“Plaintiff’s stolen assets have been traced to . . . cryptocurrency wallet addresses at cryptocurrency exchanges . . . — wallet addresses which are believed to be owned or controlled by Defendant or an unknown third-party to whom he has transferred those stolen assets, and which have been used to launder the assets stolen from Plaintiff.”); *id.* at *3 (“[C]onsidering the speed with which cryptocurrency transactions are made as well as the anonymous nature of those transactions, it is imperative to freeze the Destination Addresses to maintain the *status quo* to avoid dissipation of the money illegally taken from Plaintiff.”).

⁸⁰ See *Larkin*, *supra* note 72, at 39 (“[S]hould the crypto market move dramatically in reverse and the assets depreciate greatly, the plaintiff’s opportunity for recovery would be devastated.”). Of course, the value of digital assets also may increase exponentially over time. See *id.* at 38-39 (“Considering that bitcoin rose nearly 70% in value within a month in early 2024 for an all-time high value of \$72,000 per coin, the volatility of cryptocurrency can be profitable.”).

2. Deficient Efficacy of Equitable Remedies

Equitable remedies for blockchain fraud, by definition, fail to adequately serve desirable retributivist and utilitarian goals that may also be important to the sustainability of permissionless public blockchains. Punitive damage awards in civil enforcement actions and criminal enforcement may be better designed to serve these goals. Ultimately, a more consistent punishment of fraudulent actors and the imposition of remedies that provide effective specific and general deterrence against fraud may not only discourage fraudsters but also encourage the adoption of fraud reduction norms that would help to create a fairer and more sustainable blockchain industry. Thus, in blockchain fraud actions, as in certain other actions relating to a breach of trust, multiple remedies may best provide recompense to victims and incentivize market actors to change their positions and behaviors.⁸¹

Yet, equitable remedies are designed to serve aims of justice in the individual case rather than punishment or deterrence that may be more likely to have broader positive market and societal impacts.⁸² In the rapidly growing, relatively unregulated digital asset markets in which blockchain businesses operate, retribution and deterrence may serve important functions by nudging these anchor blockchain players toward policies and practices that better protect blockchain participants against fraud. Although perhaps a lesser concern for individual victims of blockchain fraud, ineffective retribution against primary blockchain fraudsters and ineffectual deterrence of blockchain fraud may contribute to making blockchain usage and participation unattractive.

Unfortunately, even remedies applicable to individual frauds that provide appropriately significant levels of punishment or

⁸¹ See, e.g., George P. Roach, *Compensation Forfeiture: Stacking Remedies Against Disloyal Agents and Employees*, 47 ST. MARY'S L.J. 249, 287 (2015) ("The dual goals for breach of fiduciary duty are (1) to compensate the principal for loss or damages, and (2) to deter further disloyalty by disgorging any profit related to the breach. To satisfy both goals, a remedy in equity and a remedy at law will generally be required." (footnotes omitted)).

⁸² See, e.g., *id.* at 301 ("The goal of remedies in equity is to deny unjust enrichment to the defendant; thus, the principal's damages are irrelevant.").

otherwise offer effective specific or general deterrence may largely be futile because the pseudonymity of blockchain users presents potentially insurmountable challenges in identifying and locating primary fraud perpetrators. Blockchain fraudsters who cannot easily or reliably be identified will not suffer negative consequences that prevent or deter them from continuing their fraudulent activity. Accordingly, purveyors of blockchain fraud are likely to be recidivists. Moreover, general market knowledge of a failure to adequately punish fraudulent conduct is likely to encourage more fraudulent actors and activities. The presence of recidivist and additional blockchain fraudsters creates disincentives to continued and new blockchain market participants.

Moreover, recoveries against intermediaries may fail to create sufficient financial or reputational harm or incentives for enhanced protections for blockchain fraud victims. Although fraud conducted on or through blockchain platforms and exchanges may, in certain cases, result in the imposition of legal remedies on those blockchain businesses, the location, size, and number of these organizations may limit the overall retributive and deterrent value of those remedies. Obtaining and enforcing remedies against platforms and exchanges across borders may present jurisdictional and other challenges. Platforms and exchanges that are well resourced financially and operationally may not be significantly affected by damage awards, although injunctive relief and reputational harms associated with repeated fraud may be effective incentives. And the continuing entry of new blockchain platforms and exchanges into the market makes it hard to establish healthy market norms across the board.

In sum, equitable remedies are, and will continue to be, important in creating a fair and just environment for blockchain business. Yet, these remedies are inadequate because they are difficult to obtain and effectively enforce in the blockchain business environment and because they fail to effectually punish or deter fraudulent conduct—an additional significant component of a sustainable environment for blockchain commerce. However, remedies at law and other penalties are similarly inadequate. Increased individual and market harms seem certain unless meaningful change is implemented. That meaningful change is

most likely to be successful in the blockchain environment if it comes from outside the court system.⁸³ Indeed, stemming the tide of fraud itself—in addition to clarifying and improving access to remedies—emerges as a propitious option for successful reform efforts.

III. POTENTIAL INNOVATIONS IN BLOCKCHAIN FRAUD PREVENTION

Both legal and market forces may be brought to bear to offer a more protective environment for blockchain participants. This part identifies and offers commentary on several nonexclusive options that may help curtail fraud in blockchain environments. These options are not intended as substitutes for, but rather as adjuncts to, traditional remedies that may be used to address blockchain fraud.

At the outset, however, it is important to recognize that legal (including regulatory) solutions may face uphill challenges. The blockchain industry resists traditional governmental regulation. Blockchain technology was originated and developed as an alternative to centralized legal modes of transacting that utilize human or other external regulation or intermediation.⁸⁴ Its decentralized nature is valued for creating a system of self-governance, obviating the need for formal government regulation.

“Decentralization” and “trustlessness” are presented as ultimate values that must be strived toward—even if their implementation leads to commercially undesirable results and may hinder the widespread adoption of blockchain technologies. . . . Purportedly, decentralization leads to equality, individual empowerment[,] and a dispersal of power

⁸³ See, e.g., Schmitz, *supra* note 77, at 171 (“[S]mart contract and NFT disputes demand non-judicial remedy systems that are cross-jurisdictional, extralegal, and efficient.”).

⁸⁴ See MAGNUSON, *supra* note 19, at 11 (“The roots of the blockchain lie in a long-standing debate in political philosophy about power and where it should lie.”); Eliza Mik, *Blockchains: A Technology for Decentralized Marketplaces*, in THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORMS 160, 160 (Larry A. DiMatteo et al. eds., 2023) (“[T]he decentralized character of blockchain technologies is meant to disintermediate commercial exchanges, lower transaction costs and empower sellers and buyers alike.”).

deriving from a detachment from traditional institutions such as banks, courts, etc.⁸⁵

Accordingly, market, rather than legal, solutions are more likely to be accepted by the blockchain industry.⁸⁶

Having noted this, suggestions for external regulation abound. The potential for federal legislative and regulatory action has been noted by others and is one obvious route for reforms—assuming there can be agreement around the substantive focus of that action and the construction of effective enforcement mechanisms. One commentator asserts that “[j]ust as the American Wild West eventually abandoned its lawless roots, the crypto market must abandon its principles against regulation and allow the market to properly develop under needed regulatory oversight.”⁸⁷

Some urge the U.S. Congress to expressly provide for comprehensive regulation of the industry with the goal of more effective fraud prevention and enforcement.

Congress must act as urgently as possible to create and enact a comprehensive regulatory scheme for the market to institute much-needed protections for consumers. This regulatory framework should utilize the two agencies, the SEC and CFTC, who are already providing the majority of enforcement oversight in the market and expand their registration authority over all crypto entities. This regulatory framework should be informed by current issues plaguing consumers in the market, include protections that help prevent crypto frauds from occurring, and put crypto consumers in a better place when fraud or other market

⁸⁵ Mik, *supra* note 84, at 161; see also Omri Marian, *Blockchain Havens and the Need for Their Internationally-Coordinated Regulation*, 20 N.C. J.L. & TECH. 529, 568 (2019) (“The unique characteristics of blockchain technology—in particular, decentralization, temper resistance—make it almost impossible to regulate after the fact. It is therefore an inviting environment for illicit users, as recourse is next to impossible.”).

⁸⁶ See, e.g., Marian, *supra* note 85, at 565 (“The very birth of the blockchain technology is in libertarian principles. One might argue it is sensible to let the market run its course. Unsuccessful blockchain technologies will disappear, and good ones will prevail.”).

⁸⁷ Shawn Stevenson, Note, *Taming the Digital Wild West: The Need to Fully Regulate the Crypto Market*, 27 LEWIS & CLARK L. REV. 1349, 1387 (2024).

failures occur. While cryptocurrencies may prove to be a highly beneficial innovation with practical, real-world value in the future, this goal will never be achieved without an adequate regulatory system to allow the market to grow and develop. If crypto is going to survive, proponents must embrace regulation and Congress must act.⁸⁸

Congress has, in fact, considered blockchain consumer protection legislation.⁸⁹ Those legislative proposals provided for, among other things, the registration of cryptocurrency businesses (effectively treating them like financial institutions) and trading prohibitions on digital assets likely to be part of fraudulent activity.⁹⁰

Congressional action establishing statutory or punitive damages for cryptocurrency fraud also has been recommended as a means of expanding fraud deterrence.⁹¹ A leading U.S. securities law expert advises the adoption of regulatory tools employed in federal securities offerings.⁹² Other suggested federal interventions include requiring cryptocurrency trading platforms holding customer accounts to have minimum reserves to help ensure full coverage of potential liabilities, improve accounting transparency, and disclaim ownership rights to customer accounts, although these measures do not directly address blockchain fraud.⁹³

However, a more promising avenue, at least in the short term, for supplementing judicial remedies for, and the government

⁸⁸ *Id.*

⁸⁹ *See id.* at 1379-80 (describing 2022 legislative proposals).

⁹⁰ State regulation has already begun to do some of this work. *See id.* at 1380-81. New York State requires the licensure of cryptocurrency businesses. N.Y. COMP. CODES R. & REGS. tit. 23, § 200.3 (2026) (“No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity.”).

⁹¹ *See* Stevenson, *supra* note 87, at 1386 (“Congress should take this heightened threat of fraud seriously and add additional statutory or punitive damages provisions into the regulatory framework to strengthen deterrence in the system.”).

⁹² *See* Joel Seligman, *The Rise and Fall of Cryptocurrency: The Three Paths Forward*, 19 N.Y.U. J.L. & BUS. 93, 130 (2022) (“Regulation should not be limited to an initial registration statement and the provision of fraud remedies. Rather, crypto products should be subject to continuous periodic disclosure requirements, employing the same basic framework for textual and financial disclosure as would be used in the initial disclosure requirements similar to those in the federal securities laws, recordkeeping, voting and confidentiality provisions.” (footnote omitted)).

⁹³ *See* Stevenson, *supra* note 87, at 1386.

regulation of, blockchain fraud is the adoption of industry policies and practices designed to limit fraud or better ensure the enforcement of remedies awarded to blockchain fraud victims.⁹⁴ Market-based innovations of this kind may naturally happen over time on certain platforms and exchanges as the weight of fraud affects individual blockchain businesses financially or reputationally.⁹⁵ Indeed, there are reports that blockchain industry participants are reforming their operations in response to fraudulent conduct.⁹⁶ A student commentator expressed hope that “[b]y implementing strategies to address hacks and fraudulent activities on their platforms and actively collaborating with law enforcement agencies, blockchain and Web3 entities can enhance the likelihood of recovering stolen funds.”⁹⁷

Industry changes might include, for example, external platform or exchange quality certifications based on the blockchain’s coding, “know your customer” policies (built off the concept as it is used in financial service firms), disclosure regimes that provide more transparency, and required insurance or other financial underwriting of fraud risks.⁹⁸ In June 2025, Blockworks (an Internet research and information platform) announced a disclosure framework for tokens that it characterizes as “an opportunity to improve capital allocation in the industry by helping projects signal credibility, allow investors to better underwrite risk with standardized disclosure of information, and prevent bad actors from profiting off ambiguity.”⁹⁹ Industry-led

⁹⁴ See Marian, *supra* note 85, at 566 (“[S]hortcomings do not mean the ex-ante regulation should be abandoned altogether. There is still room to try to punish criminals or to recover from their illicit gains. But this must be supplanted by preventative medicine . . .”).

⁹⁵ See Scott, *supra* note 46, at 542 (“As different cryptoassets vie for popularity, more on-chain tracing and enforcement methods (such as orders to write code or software) may develop.”).

⁹⁶ See, e.g., Dudgeon, *supra* note 71, at 501 (“With additional regulatory measures looming, crypto exchanges are continuing to provide increased security measures.” (footnote omitted)).

⁹⁷ *Id.*

⁹⁸ See, e.g., Marian, *supra* note 85, at 565 (mentioning code certification); *id.* at 567 (briefly addressing “know your customer” rules, disclosure, identification, and insurance).

⁹⁹ Dan Smith, *A New Framework for Token Market Transparency*, BLOCKWORKS (June 18, 2025, at 09:00 ET), <https://blockworks.co/news/token-transparency-framework> [<https://perma.cc/TWR9-MJGA>].

reforms may incorporate collaboration with law enforcement agents.¹⁰⁰ Even industry-wide agreements on standard forms of end-user agreements or terms of use may help stem the tide of fraud or assist fraud victims in recovering their digital assets.¹⁰¹

Finally, additional consumer education should be helpful in reducing the incidence of fraud.¹⁰² As has been true for other Internet and Internet adjacent fraud, those who are intent on defrauding people interested in participating in blockchain commerce—whether to participate in cryptocurrency markets, NFT collecting, or otherwise—use identifiable strategies to find their victims and common tactics to persuade them to participate in the fraud. They take advantage of consumer curiosity, affinities of various kinds, and proven social engineering, marketing, and sales tactics; they put time pressure on acceptance of the deals they are promoting. Public campaigns to advise consumers of these strategies and tactics and generally urge caution may help decrease the number of consummated blockchain frauds, even if it does not discourage the fraudsters.

Public education initiatives alone would be unlikely to prove successful in reducing the number of fraudulent transactions on blockchains. But in combination with industry self-regulation and governmental regulation geared to both preventing fraudulent transactions from occurring and making the recovery of remedies more certain, it may serve a laudatory purpose. “[T]he reality is

¹⁰⁰ See Dudgeon, *supra* note 71, at 501 (“By implementing strategies to address hacks and fraudulent activities on their platforms and actively collaborating with law enforcement agencies, blockchain and Web3 entities can enhance the likelihood of recovering stolen funds. In the wake of digital asset fraud, there has been increased government intervention in the industry.” (footnote omitted)).

¹⁰¹ See, e.g., Joshua Fairfield, *Crypto-Counterfeiting*, 15 WM. & MARY BUS. L. REV. 497, 522 (2024) (“Appropriately drafted contracts can help set remedies and of course create a context for the enforcement of community rules, with the overarching goal of establishing that duping cryptocurrency undercuts the very fabric of the blockchain project, and that the proper remedy is the disgorgement and destruction of the ill-gotten tokens.”).

¹⁰² See Goforth, *supra* note 20, at 798 (“A better option, of course, is to take steps to avoid being defrauded in the first place. This requires consumers to be cautious any time they are dealing with someone they do not know well. If a deal sounds too good to be true, it probably is.”).

that even with being reasonably careful, it may not always be possible for consumers to protect themselves.”¹⁰³

CONCLUSION

The law is not powerless in the face of permissionless blockchains but its traditional armoury is lacking.¹⁰⁴

Blockchains provide a growing, popular form of transacting for many. Yet, with new systems of interaction, fraud always seems to follow. Blockchain transacting brings fraud that is both similar to and distinct from fraud conducted in other Internet fraud and fraud conducted in non-digital environments.¹⁰⁵ Equitable remedies would seem to serve important functions in creating a more honest and fair playing field for blockchain participants. Yet, they are difficult to obtain and enforce given the inherently unregulated and sheltered nature of blockchains and the ecosystem that has developed in and around them. In addition, equitable remedies have proven insufficient to the task of combatting fraud, either alone or taken together with other judicial remedies. As a result, more must be done to improve the environment for blockchain consumers through legal, industry, or social channels.

The principal challenge in making these improvements will be the very nature of blockchain technology as a self-regulating transactional environment. Sustainable solutions will involve significant work in and among representatives of government (ultimately, not only federal and local governments, but also foreign governments), the blockchain industry, end-users of blockchain technologies, lawyers working with all the foregoing, and potentially others (including researchers and industry beneficiaries, like the nonprofit community). If the benefits of blockchain technology are to be preserved, this work must be undertaken in the near term.

¹⁰³ *Id.* at 799. “Ideally, regulators or Congress will act to see that internet marketplaces are better regulated so that there are standards by which they operate.” *Id.*

¹⁰⁴ Kelvin F.K. Low, *Confronting Cryptomania: Can Equity Tame the Blockchain?*, 14 J. EQUITY 240, 270 (2020).

¹⁰⁵ See generally Heminway & Dethlefs, *supra* note 41 (making this precise point).