William & Mary Business Law Review

Volume 15 (2023-2024)
Issue 3

Article 3

4-2024

Crypto-Counterfeiting

Joshua Fairfield

CRYPTO-COUNTERFEITING

JOSHUA FAIRFIELD*

ABSTRACT

The current crypto winter has given rise to a range of legal challenges. One of the most important sets of legal challenges goes to the heart of cryptocurrency. Cryptocurrency was intended to be non-duplicatable at will, that is, not to be counterfeitable. Blockchain technology is supposed to prevent token counterfeiting through a combination of game theory and cryptography that prevents normal users from simply ordering the system to generate more tokens for their benefit.

The difficulty is that blockchain software is still software. People in charge can order and program the software to generate many more tokens for those individuals' benefit. Hackers can find ways to exploit the software to generate counterfeit tokens. Software will never be free from bugs and exploits, and humans with discretion within a system will always be susceptible to the temptations of power and greed.

Given the strong technological restraints on digital duplication of cryptocurrency and other crypto assets, many organizational structures and cultures surrounding cryptocurrency are set up particularly poorly to handle the problem of crypto-counterfeiting. Often in an attempt to avoid legal sanction, blockchain projects are set up in such a way that no legal entity controls the software. This is because there is a widely perceived vulnerability in having any single entity control a blockchain. Such a legal entity may be targeted for enforcement purposes in a murky regulatory climate.

When someone duplicates cryptocurrency, the harm is easily articulated: the duper has decreased the value of the cryptocurrency, and everyone else's holdings, by virtue of having generated for themselves many more of the tokens. Similarly, the solution is fairly straightforward. The duped currency must be deleted in

* Joshua Fairfield, William D. Bain Family Professor of Law, Washington and Lee University School of Law.

order to restore the value of the entire system. The difficulty is that legal rules must evolve in the face of the narratives crypto communities share and hold. In a fully decentralized system, who should be the plaintiff? If a token has been improperly generated, whose property has been stolen or converted?

Blockchain was supposed to solve the problem of asset duplication, referred to in blockchain circles as the double-spending problem, or in more recent incidents, an "infinite mint" attack. Ironically, it did not. Rather, blockchain created a difficult set of legal problems that this Article attempts to address. The future of the law in this space is clear. Wrongful generation of tokens will be sanctioned by courts with the remedy of deletion of those tokens. But the legal problems presented will benefit from clarification, and the precommitments of the communities that make those arguments do nothing to reduce the difficulty of the legal fit.

TABLE OF CONTENTS

INTRODUCTION

Blockchain technology was supposed to stop the double-spending problem.[1] The double-spending problem is best described as a way for a user to counterfeit currency by exploiting vulnerabilities in the settlement network.[2] For example, if one has money in a bank account, one might double spend that money illegally, by writing a bad check for it. In the period of time it takes to settle the bad check, one may already have received goods and services in exchange for the check's promised value. Blockchain solves the double-spending problem by creating a public ledger and leveraging a combination of cryptography and game theory to make it vastly difficult and prohibitively expensive to counterfeit tokens.[3]

As blockchain technology has matured, however, enterprising fraudsters have discovered new ways to exploit the blockchain ecosystem. For example, the creator of a blockchain who still retains control over the blockchain software might simply instruct it to issue a large number of tokens to the blockchain founder themselves, so that the blockchain founder may dump those assets prior to pulling the rug on the project.[4] Or, a bug in the blockchain software (or, equally often, in software that bridges between blockchains or operates distributed apps riding on blockchains) may permit a user to wrongfully take tokens for himself or herself that the system was not intended to generate.[5] Or, a

---

[1] *What is Double Spending in Blockchain?*, GEEKSFORGEEKS.ORG [hereinafter GEEKSFORGEEKS, *Double Spending*], https://www.geeksforgeeks.org/what-is-double-spending-in-blockchain/ [https://perma.cc/2X4X-A5V3].

[2] CFI Team, *Double-Spending—definition, causes, how to prevent*, CORP. FIN. INST., https://corporatefinanceinstitute.com/resources/cryptocurrency/double-spending/ [https://perma.cc/PA9U-AJVL].

[3] *Id.*

[4] *NFT, Token & Crypto Scams: What Your Lawyer Should Know*, TRAVERSE LEGAL, https://www.traverselegal.com/blockchain-attorneys/crypto-nft-fraud/ [https://perma.cc/PS5N-JZFR].

[5] *Yes, Blockchain Can Be Hacked: 3 Ways It Can Be Done*, EPIQ, https://www.epiqglobal.com/en-us/resource-center/articles/blockchain-can-be-hacked [https://perma.cc/AJ5H-RYGA]; *see also* Mike Orcutt, *Once Hailed as Unhackable, Blockchains are Now Getting Hacked*, MIT TECH. REV. (Feb. 19, 2019), https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ [https://perma.cc/PV9A-9ACZ].

hacker might simply compromise the software overall, and instruct it to issue tokens that the software was never intended to generate.[6] These and other methods of attack raise again the specter of crypto-counterfeiting.[7] The elaborate systems that prevent double spending turn out to only have blocked one common method of duplication.[8] There are many others—for each flaw in the software, there are as many ways to circumvent the blockchain's prevention of counterfeiting.[9] For other attacks more central to the software itself, blockchain systems remain as vulnerable as any other software system.[10]

Moreover, the politics and precommitments of many blockchain communities make certain basic legal precautions that might help to ameliorate the problem of crypto-counterfeiting rarer than one might expect.[11] Crypto-communities like to view themselves as decentralized and operating on a flat, non-hierarchical basis.[12] Thus, even though a common way of structuring a blockchain project is to form a foundation or other entity that promotes the blockchain or currency, which I term throughout this Article as a "blockchain curating entity," these foundations often do not have technical control over the code, nor do they have legal control over members of the community.[13] This means that such entities are not able to establish basic community rules by contract, license, or other standards to stop crypto-counterfeiting.[14]

---

[6] *Id.*

[7] *See* Shin v. ICON Found., No. 20-cv-07363-WHO, 2021 WL 1893117 (N.D. Cal. May 11, 2021);

[8] *See* GEEKSFORGEEKS, *Double Spending*, *supra* note 1.

[9] *Id.*

[10] *See* EPIQ, *supra* note 5.

[11] *See* KEVIN WERBACH, THE BLOCKCHAIN AND THE NEW ARCHITECTURE OF TRUST 133–48 (MIT Press 2018) [hereinafter WERBACH, ARCHITECTURE OF TRUST] (discussing the paradoxical need for governance in blockchain communities, and the complexities that the political precommitments of such communities bring to the table).

[12] *See* Mally Anderson, *Exploring Decentralization: Blockchain Technology and Complex Coordination*, J. DESIGN & SCI. (Feb. 6, 2019), https://jods.mitpress.mit.edu/pub/7vxemtm3/release/2 [https://perma.cc/76FL-CXLR].

[13] *See* Griffin McShane, *What Is a Crypto Foundation?*, COINDESK (June 2, 2023), https://www.coindesk.com/learn/what-is-a-crypto-foundation/ [https://perma.cc/MX4Z-WQZ8].

[14] *See id.*

This Article discusses and then demonstrates solutions to fill that gap. The wrongful generation of tokens must be prohibited and punished under law, or the very technological integrity that is the hallmark of blockchain communities will be so fundamentally undermined as to render valueless the digital assets they facilitate and produce. There is also no question as to the final legal sanction. Wrongfully generated tokens must simply be deleted, rather than transferred to any entity. But the legal frameworks for reaching this result are still developing, and must be significantly strengthened by analysis, careful scholarship, and good judging. That is the project of this piece.

I. THE SETUP

Blockchain technology is supposed to prevent counterfeiting.[15] In fact, what blockchain does is prevent counterfeiting by individual users through a very specific method. The much-vaunted combination of game theory and cryptography that lies at the center of the blockchain prevents a user from giving cryptocurrency to person B and person C at roughly the same time, and receiving goods or services from each, before reconciliation of the accounts with the network reveals the fraud.[16] That is, blockchain has a pretty strong set of technological safeguards against the equivalent of writing bad checks.[17]

But all the discussion around double spending and how to stop it has stunted consideration of another inevitable set of problems.[18] Blockchain software remains software. It is written by someone, it has bugs, and it can be exploited or hacked.[19] The author of blockchain software can write it in such a way as to award themselves a large number of tokens. The entities that maintain control over the network can order it to generate tokens to permit them to dump tokens on the market before pulling the

---

[15] *See* Vassilis Zikas, *Research Vignette: Cryptography and Game Theory for Blockchains*, SIMONS INST. FOR THE THEORY OF COMPUTING (Sept. 30, 2020), https://simons.berkeley.edu/news/research-vignette-cryptography-game-theory-blockchains [https://perma.cc/KT4R-U33E].

[16] *Id.*

[17] *Id.*

[18] *See* EPIQ, *supra* note 5.

[19] *Id.*

rug on the project. A hacker can find, create, or exploit a bug in the code to generate for themselves a large number of tokens. In these circumstances, the promised protection of blockchain networks against crypto-counterfeiting does not help at all.[20] And, as the next section demonstrates, the social and legal protections of cryptocurrency projects are often less robust than they should be because of blockchain communities' organizational precommitments.[21]

A. Blockchain Organization

The organization of blockchain communities often reflects community precommitments toward decentralization and flattened hierarchy.[22] These aspirations are, in practice, rarely met, because blockchain ecosystems often deeply recentralize despite their organizational commitment to decentralization.[23] For example, consider the recentralization of the famed Bitcoin blockchain through mining consortia, or recentralization through the control of the software developers themselves.[24] That said, however, community political precommitments to decentralization often leave legal actors in the penumbra of a blockchain ecosystem without clear recourse to rectify certain community problems.[25]

Consider the usual case. When a blockchain is spun up, often some or several entities are incorporated to promote the

---

[20] Loi Luu et al., *Making Smart Contracts Smarter*, *in* PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 254–69 (2016).

[21] WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 133–48 (discussing the lack of and need for blockchain governance); PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 74–75 (Harv. Univ. Press 2018).

[22] *See* Primavera De Filippi & Samer Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, 21 FIRST MONDAY no. 12, Dec. 2016, https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657 [https://perma.cc/3H84-NLQ2].

[23] *See* Arthur Gervais et al., *Is Bitcoin a Decentralized Currency?*, 12 IEEE SEC. & PRIVACY, May/June 2014, at 54–60.

[24] Adem Efe Gencer et al., *Decentralization in Bitcoin and Ethereum Networks*, *in* FINANCIAL CRYPTOGRAPHY & DATA SECURITY 439, 447–48 (Sarah Meiklejohn & Kazue Sake eds., Springer 2018).

[25] Kevin Werbach & Nicolas Cornell, *Contracts* Ex Machina, 67 DUKE L.J. 313, 318 (2017).

project.[26] That corporation may control things like copyright interests in the blockchain software or it simply may act to coordinate the community and support the project.[27] Frequently, these organizations are intentionally constructed to be as distant from the reins of power as possible.[28] This is for two reasons. First, these blockchain project curation entities do not want to appear to have the power to make direct changes to the blockchain because they have promised their users a decentralized and nonhierarchical experience.[29] One of the major talking points of blockchain community organizations is that there is no centralized authority who can step in and devalue an asset, or force a transfer from one member to another.[30] This precommitment speaks to the cypherpunk, cyberanarchist, and libertarian bent of many blockchain projects.[31] Even when a project takes a democratic turn, the entity in charge of promoting the product or project does not want to appear to be directly in control of the community.[32] Thus, for political and community reasons, these organizations often do not avail themselves of all of the tools that they otherwise might have—like intellectual property licenses, terms of use, or terms of service—in order to restrain participants from wrongfully generating tokens.[33]

Second, blockchain entities organize themselves with significant legal distance from the projects they promote in order to leverage the international, decentralized nature of blockchain technologies.[34] Their purpose in doing so is to avoid legal regulations and sanctions. This approach has only been partially successful.[35] Any organization with a significant degree of proximity to

---

[26] Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 869 (2015).

[27] *See id.* at 872.

[28] Primavera De Filippi & Benjamin Loveluck, *The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure*, 5 INTERNET POL'Y REV. 3, 5 (2016).

[29] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 139.

[30] *See id.* at 139–40.

[31] *See id.* at 67–68, 143.

[32] *See id.* at 141–43.

[33] *See id.* at 140–41.

[34] *See* DE FILIPPI & WRIGHT, *supra* note 21, at 66–67.

[35] *See id.* at 61, 66.

a blockchain project has in fact been subject to sanctions and regulations.[36] Consider the history of legal regulation of blockchain exchanges.[37] These exchanges themselves did not spin up the blockchain projects, but merely facilitated the cryptographic transfer of tokens.[38] Regardless, they were almost effortlessly incorporated into the legal regulation of financial systems in the United States through application of the Bank Secrecy Act.[39]

Regardless of the actual efficacy of blockchain curation entities' attempts to distance themselves from legal responsibility for their projects, the hands-off and arms-length nature of the relationship between blockchain curation organizations and their projects again means that these legal entities have little ability to immediately sanction bad actors within the community.[40] Sometimes an attack is so profound that the community must react, and then these organizations serve as a focal point for the resulting debate. Consider here the role of the Ethereum foundation in the hack of The Decentralized Autonomous Organization (DAO), whereby the community came together and decided not to recognize the hackers' ill-gotten gains through the functional equivalent of the issuance of an entirely new currency, in effect forking the Ethereum blockchain.[41] One of the first insights of this Article, therefore, is that this legal distance is rarely worth

---

[36] Andres Guadamuz & Chris Marsden, *Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies*, 20 FIRST MONDAY no. 12, Dec. 2015, https://firstmonday.org/ojs/index.php/fm/article/view/6198/5163 [https://perma.cc/3H84-NLQ2].

[37] *See id.*

[38] *See id.*

[39] *See* Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813, 815 (2014).

[40] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 133–35.

[41] *See id.* at 138–41 (discussing the governance paradox surrounding The DAO); *see also* Quinn DuPont, *Experiments in Algorithmic Governance: A history and ethnography of "The DAO," a failed decentralized autonomous organization*, *in* BITCOIN AND BEYOND: CRYPTOCURRENCIES, BLOCKCHAINS, AND GLOBAL GOVERNANCE, 157–58, 164 (Malcolm Campbell-Verduyn ed., Routledge 2017); *see also* Bitcoin Magazine, *A Legal Analysis of the DAO Exploit and Possible Investor Rights*, NASDAQ (June 21, 2016, 12:52 PM), https://www.nasdaq.com/articles/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-2016-06-21 [https://perma.cc/9VLL-NCBF].

the candle. Blockchain curation organizations do not usually escape the enforcement efforts of agencies bent on enforcing the law, and simultaneously these organizations are giving up both substantial power and potential avenues for legal recourse to stop bad actors from wrecking the integrity of the chain.[42]

B. Duping and Infinite Mint Attacks

Thus, for political and legal reasons, blockchain entities themselves often lack the same direct power over blockchain projects that game companies and other corporations that have overseen the creation of digital value traditionally possess.[43] Consider an example from the early 2000s of what was called "duping," short for duplicating a currency.[44] Within the game Star Wars Galaxies, a credit exploit was discovered, which permitted exploiters to generate video game currency within the game.[45] The duping exploit devalued the game's virtual economy, requiring the company that created the game, Sony Online Entertainment, to take steps to identify dupers, ban their accounts, and delete huge amounts of in-game currency that functionally inflated the value of assets to near-zero worth.[46]

Duping in massively multiplayer online games was a common phenomenon for two reasons. First, players of course wanted to seek an advantage in the game by finding an exploit that would permit them to generate in-game currency.[47] But second, the generation of in-game currency interacted with the real-world economy through the medium of player exchange.[48] An entire gray-market business developed in which players would purchase in-game currency from so-called gold farmers.[49] Players

---

[42] *See* Middlebrook & Hughes, *supra* note 39, at 816, 834.

[43] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 135, 138–42.

[44] GREG LASTOWKA, VIRTUAL JUSTICE: THE NEW LAWS OF ONLINE WORLDS 159–60 (Yale Univ. Press 2010).

[45] *See* golem, *SWG Credit Duping Scandal*, NEOGAF (Aug. 26, 2004), https://www.neogaf.com/threads/swg-credit-duping-scandal.11919/ [https://perma.cc/86BE-24HB].

[46] *Id.*

[47] *See* LASTOWKA, *supra* note 44, at 159.

[48] *Id.*

[49] *Id.*

could purchase in-game currency for real-world dollars.[50] As a result, gaming companies in the early 2000s became extremely adept at detecting and deleting currency exploits, even employing virtual economists to track and monitor the development of online value creation.[51] The wrongful generation of in-game currency inflated the entire in-game economy, decreased the value of playing the game in order to receive in-game currency, and of course deflated the value of the currency for anyone who held it.[52]

Duping was, therefore, a prominent and well-understood phenomenon in the digital communities and digital property systems of the 1990s and early 2000s.[53] The solution to the problem was correctly deduced and enforced by gaming companies intent on preserving the value of the game experience for their players: they deleted the duplicated currency when and where they could.[54]

Such centralized management of virtual economies by game companies (literally at the time called "game gods") came at a significant and quite literal price.[55] As will be discussed below, game companies leveraged their intellectual property licenses over game code and game graphics to control virtual economies. The same End User License Agreements stated that players did not own anything, thus the game companies were free to delete counterfeit assets at will.

Players and community members in those early games owned only attenuated rights in their virtual assets (and the game companies argued that players owned nothing at all).[56] Players thus did not cleanly own the significant and valuable virtual assets they generated and in which they had invested real-world

---

[50] *See* Richard Heeks, *Understanding 'Gold Farming' and Real-Money Trading as the Intersection of Real and Virtual Economies*, 2 J. VIRTUAL WORLDS RSCH. no. 4, Feb. 2010, at 3, 8.

[51] *See* VILI LEHDONVIRTA & EDWARD CASTRONOVA, VIRTUAL ECONOMIES: DESIGN AND ANALYSIS 181–82 (MIT Press 2014); EDWARD CASTRONOVA, SYNTHETIC WORLDS: THE BUSINESS AND CULTURE OF ONLINE GAMES 2 (Univ. of Chi. Press 2005).

[52] *See* LEHDONVIRTA & CASTRONOVA, *supra* note 51, at 181–82; CASTRONOVA, *supra* note 51, at 2.

[53] *See* LASTOWKA, *supra* note 44, at 160.

[54] *Id.* at 24.

[55] *See id.* at 153.

[56] *See id.* at 125–32.

currency.[57] As a result, the entire system of value became rife with fraud and undergirded with uncertainty.[58] Ownership must be the foundation of investment; without the certainty of ownership, investment in an asset must fundamentally be speculation.[59]

Web3 and blockchain projects strongly addressed this key issue by unequivocally deeming legitimate token holders to be true owners of digital assets. But even as blockchain projects granted project participants clear personal property interests in tokens, the problem of counterfeiting (which subverted and diluted those ownership interests) remained. It is not without some irony that the problem of exploitation, duping, or crypto-counterfeiting arose most strongly after the Web 3.0 revolution, which was centered on and represented the ideals of decentralization and distributed control.[60] The digital asset counterfeiting that was called duping in virtual worlds and games is now called an "infinite mint" attack in Web3.[61] In an infinite mint attack, malfeasors exploit some vulnerability in the distributed ledger of the blockchain, or exploit an exchange between blockchains, in order to generate functionally infinite counterfeit cryptocurrency tokens.[62] Infinite mint attacks are a regular and increasing event among cryptocurrency projects, particularly as layers of Web3 applications permit exploitation of gaps in the code managing the relationship between an underlying blockchain and an app riding on that blockchain, or exploiting incompatibilities in code bridging between blockchains, or simply exploiting bugs in the blockchain validation code itself such that a bad actor can create or receive counterfeit tokens.[63]

Against this rising tide of infinite mint attacks, blockchain projects lack long-standing and time-tested methods of addressing crypto-counterfeiting. Although Web3 decentralization opened the door to new kinds of community and recognized the essential

---

[57] *Id.*

[58] *Id.*

[59] *Id.* at 27.

[60] *Id.* at 125–32.

[61] *See Infinite Mint Attack*, BLOCKCHAIN REPORTER, https://blockchainreporter.net/glossary/infinite-mint-attack/ [https://perma.cc/T8DR-WSLR].

[62] *Id.*

[63] *See Top Crypto Infinite Mint Attacks*, PONTEM BLOG, https://pontem.network/posts/top-crypto-infinite-mint-hacks [https://perma.cc/GT7V-NFZ9].

value proposition by online investors seeking to own digital property, it also removed a central form of protection for the digital economy.

The following sections attempt to bring the old and, without question, correct enforcement solutions for wrongful generation of digital assets (that is, detection and deletion) forward in time to engage with a fully fledged legal framework that recognizes ownership interests of community members in their digital property, which is of course essential to the entire blockchain, cryptocurrency, and digital value project.

II. THE APPROACHES

The fundamental problem is that the traditional setup of legal rights within the private law arena is (roughly) between two entities: A must have harmed B, and also, B must have some recognized right to sanction A. That turns out to be an issue where blockchain organizations do not have or do not exercise the traditional rights of contract and intellectual property licenses to keep members in line.[64] Crypto-counterfeiting harms everyone who legitimately holds non-counterfeit digital assets. This section therefore lays out several approaches for how to sanction the wrongful generation or misappropriation of tokens—the perpetrators of infinite mint attacks—given the strange context in which these claims arise.

A. Criminal Law

A first stop would be to turn to criminal law. Criminal law would vindicate the sense that crypto-counterfeiting is wrong, but the question is, against whom has the wrong been done? Again, there is no real question in the economic sense: everyone who holds legitimate tokens feels the harm, as the value of their assets is diluted as a function of the counterfeiting; the question is how to prosecute the violation within traditional criminal law frameworks.

---

[64] *See* Joshua A.T. Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, 97 IND. L.J. 1261, 1294–99 (2022) [hereinafter Fairfield, *Tokenized*].

1. Theft

Under criminal law, there are two distinct approaches. The first would be to recognize a traditional crime of theft.[65] The argument there is straightforward: a person who wrongfully misappropriates tokens intended for other members of the community clearly engages in theft; they have wrongfully taken something that does not belong to them.[66]

Thus, for example, Jimmy Zhong, who stole three billion dollars' worth of cryptocurrency in 2012, was investigated, caught, and eventually prosecuted.[67] The law had no particular difficulty determining that he had stolen assets, that the assets did not belong to him, that the assets ought to be returned, and that those facts gave state and federal investigators adequate legal ground to pursue and prosecute the case.[68]

The difficulty in certain kinds of crypto cases is that criminal prosecution of this sort is more complex—although still entirely appropriate—when the theft is from the entire community rather than from specific accounts.[69] This is related to the questions of duplication, infinite minting, and double-spending discussed earlier: the law has found it simpler to prosecute under the law of theft when cryptocurrency has been issued to a given member of the community, rather than when the theft is from the project or community as a whole.[70] Because the project or community may not have a legally defined and distinct organizational form—such as a company—courts may struggle to conceptualize the theft as

---

[65] *See* Henry Zaytoun, *Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft*, 97 N.C. L. REV. 395, 431 (2019) ("Prosecution of this theft will merely recognize an interest in Bitcoin that society already acknowledges—Bitcoin is a thing that can be owned and taking it is an action that the law must punish.").

[66] *Id.*

[67] *See* Press Release, U.S. Att'y's Off. S.D.N.Y., U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure and Conviction in Connection with Silk Road Dark Web Fraud (Nov. 7, 2022) [hereinafter Silk Road Dark Web Fraud], https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction [https://perma.cc/TNV4-747P].

[68] *Id.*

[69] *See* Colleen Flynn, *$9M Cryptocurrency Theft Case Dropped*, KDVR.COM (Aug. 4, 2023, 4:17 PM), https://kdvr.com/news/local/mark-shin-cryptocurrency-theft-case-dropped/ [https://perma.cc/76XB-DW2V].

[70] *See* Silk Road Dark Web Fraud, *supra* note 67.

being from everyone in the community, even though that is exactly where the wrong and how the harm are quite clearly felt.[71]

This problem—although prosecutors can punish theft, they face difficulties determining theft from *whom*—causes this form of criminal law sanction to be under-used, even where a clear, coherent, and supported claim could be brought. For example, where a single entity controls an entire project, the taking of wrongly generated tokens may well be deemed theft of company assets. The difficulty is that the organizing or curating entity may be loath to claim those new tokens either for purposes of tax or control. Thus the disconnect between the real damage caused by crypto-counterfeiting and traditional claims of theft is complicated by the political and community commitments of actors like blockchain-promoting groups, organizations, or incorporated bodies. These entities do not want to appear to be acting on behalf of the community, taking the reins of power from the community, or claiming ownership of the assets themselves. Thus, unlike in the game company context, there is no easy proxy for the community in terms of who is able to claim harm for the theft engendered by crypto-counterfeiting.[72]

2. Computer Fraud and Abuse Act

The second low-hanging fruit is prosecution under the Computer Fraud and Abuse Act (CFAA).[73] This act provides both civil and criminal penalties for unauthorized access of, or exceeding authorized access to, a protected computer system.

The CFAA serves as the primary federal anti-hacking statute in the United States.[74] Enacted in 1986 as an amendment to the first federal computer fraud law, the CFAA criminalizes unauthorized access or exceeding authorized access to protected computers, resulting in various forms of damage or fraud.[75] A "protected computer" under the CFAA definition includes not only computers used by the federal government or financial institutions,

---

[71] *See* Flynn, *supra* note 69.

[72] *See* Zaytoun, *supra* note 65, at 428–31.

[73] 18 U.S.C. § 1030; *see* LASTOWKA, *supra* note 44, at 161, 163–64.

[74] 18 U.S.C. § 1030.

[75] *See* Orin Kerr, *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1615–16 (2003) [hereinafter Kerr, *Cybercrime's Scope*]; LASTOWKA, *supra* note 44, at 161.

but also any computer "used in or affecting interstate or foreign commerce or communication."[76] This broad definition effectively brings almost all computers under the ambit of the CFAA. The Act addresses a spectrum of behaviors, from accessing a computer without authorization to the transmission of harmful code, and it has both criminal and civil components.[77]

The relevant question for this analysis is whether accessing a blockchain-adjacent system, such as a computer used to run a mining node or verify transactions, a wallet program used to maintain cryptocurrency, programs run in a distributed manner on the blockchain itself, *or the blockchain itself*, constitutes a "protected computer" under the CFAA.[78] Because of the broad ambit discussed above, including all computers used in or affecting interstate or foreign commerce or communication, there is no question that not only are standard computers—ASIC miners used to mine nodes, or wallet programs on smartphones—properly deemed "protected computers" under the CFAA, but so are blockchains and distributed apps running on them.[79] Consider the Ethereum blockchain, which provides a Turing-complete computer language to run programs that run directly on the Ethereum blockchain itself, creating the possibility of decentralized and distributed computing. Blockchains store state just like a regular piece of physical memory does. There is no reason that accessing or causing a blockchain program to issue tokens does not constitute access to a "protected computer" system.

Running such a system on a decentralized blockchain in no way removes it from the protection of the CFAA. In fact, a decentralized computing system running on a blockchain hosted across hundreds of thousands of computers worldwide is *a fortiori* a protected computer system because it without question impacts interstate or foreign commerce and communication.[80] Interfering

---

[76] 18 U.S.C. § 1030(e)(2).

[77] 18 U.S.C. § 1030(a)(5), (c), (g).

[78] *See generally* Kerr, *Cybercrime's Scope*, *supra* note 75 (discussing interpretations on what constitutes unauthorized access).

[79] *See* 18 U.S.C. § 1030(e)(2); Zaytoun, *supra* note 65, at 419–22.

[80] 18 U.S.C. § 1030. Several cases of CFAA claims have been brought with crypto currency claims, but were unsuccessful for reasons other than the merits of the claims. *See*, *e.g.*, Fraser v. Mint Mobile, LLC, No. C 22-00138 WHA,

with such a protected computer system by causing it to wrongfully issue counterfeit cryptocurrency provides ample grounds to argue that the CFAA applies and can be used to protect blockchain systems and the hardware, firmware, and software that run such systems or constitute such systems.[81]

Consider, for example, the hack of The DAO in 2016.[82] The DAO was supposed to be a distributed autonomous organization, like a corporation, but written in blockchain code. The DAO was supposed to gather investments in the form of cryptocurrency, and then fund projects that would return a profit on to The DAO's investors. However, due to code vulnerabilities in The DAO's smart contracts, The DAO was promptly hacked, draining the entity of more than $50 million of investor funds.[83]

The DAO was a computer system running on a distributed and decentralized blockchain.[84] But there is no question that it is a protected computer system for purposes of the CFAA. Tens of millions of dollars in investor funds stolen of course impacts interstate and international commerce, not to mention the fact that The DAO's code ran on a decentralized database hosted on nodes across the United States and around the world—elements making the hack of The DAO a clearcut case for application of the CFAA.[85]

2022 WL 2391000 (N.D. Cal. July 1, 2022); Schober v. Thompson, No. 21-cv-01382-NYW, 2022 WL 136907 (D. Colo. Jan. 14, 2022).

[81] *See* Andrew Hinkes, *US Supreme Court's Computer Fraud Ruling has Big Implications for Crypto*, COINDESK (June 15, 2020 5:19 PM), https://www.coindesk.com/policy/2020/06/15/us-supreme-courts-computer-fraud-ruling-has-big-implications-for-crypto/ [https://perma.cc/7ZDP-GG43].

[82] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 67–69; *see also* Cryptopedia Staff, *What Was the DAO?*, CRYPTOPEDIA (Oct. 5, 2024), https://www.gemini.com/cryptopedia/the-dao-hack-makerdao [https://perma.cc/9P7Q-YQX5].

[83] *See* Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016), https://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html [https://perma.cc/AT22-CA5N]; *see also* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 67–69.

[84] *See* Cryptopedia Staff, *supra* note 82.

[85] *See* 18 U.S.C. § 1030(a)(4)–(5); Cryptopedia Staff, *supra* note 82.

As a separate point, the CFAA has been a subject of debate, especially concerning the interpretation of "unauthorized access" and what constitutes "exceeding authorized access."[86] Under the statute, "'exceed[ing] authorized access' means to access a computer with authorization, [but] to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter."[87] This language has generated significant litigation over its scope, particularly around the issue of whether violating terms of service or corporate policies can be grounds for a CFAA violation.[88]

Recent case law has sought to clarify the extent of "exceeding authorized access" under the CFAA. In *Van Buren v. United States*, the Supreme Court narrowed the scope of the CFAA, holding that "an individual 'exceeds authorized access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to him."[89] The Court clarified that the CFAA does not cover those who have improper motives for obtaining information that is otherwise accessible to them.[90] *Van Buren* thus resolved a circuit split by adopting a narrower interpretation of "exceeding authorized access," focusing on whether the individual had the right to access the information in the manner they did, rather than their use or motive behind accessing the data.[91]

In the blockchain context, this debate around exceeding authorized access is likely to be the subject of significant discussion. At a base level, a blockchain system necessarily allows many people to have the right to write to the blockchain itself, by engaging in legitimate transfers or activities.[92] However, the entire point of such a system is to prevent the creation or transfer of

---

[86] *See* 18 U.S.C. § 1030(e)(10); Orin Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1163–65 (2016) [hereinafter Kerr, *Norms*].

[87] 18 U.S.C. § 1030(e)(6); *see* Kerr, *Norms*, *supra* note 86, at 1163–65.

[88] *See* Jeremy T. Merkel, *Coming to Terms with Computer Misuse: When Violating Terms of Service Becomes a Crime Under the Computer Fraud and Abuse Act*, 42 LINCOLN L. REV. 60, 66–72 (2017).

[89] 141 S. Ct. 1648, 1662 (2021).

[90] *Id.* at 1652.

[91] *Id.* at 1653–54.

[92] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 140.

false tokens.[93] The point of a ledger is to stop people from falsifying who owns what by stopping exploits that permit false ledger entries. The wrongful inflation of the number of tokens destroys the entire purpose of having a distributed ledger that keeps track of a limited supply of tokens. The point of the ledger is to create scarcity of tokens. That is the source of their value. Wrongfully causing a blockchain protocol to issue tokens by hacking, exploiting, or building hidden back doors into the code devalues the holdings of other token holders, and compromises the value of any given blockchain project. No project that does not address crypto-counterfeiting can survive, because its assets cannot hold value.

A simpler method of applying the CFAA to blockchain hacks is simple "unauthorized access." While token holders may be permitted to submit transactions to validation nodes for the purposes of effecting legitimate transfers, they most certainly are *not* permitted to execute exploits of the mining or validation software and cause it to issue or generate illegitimate tokens. This is hacking pure and simple. Thus, there is no need for a *Van Buren* analysis. Infinite-mint exploits are a clean fit with the portions of the statute prohibiting unauthorized access of or damage to a protected computer.[94]

B. Contracts

It is somewhat ironic that the primary method of community control of the distributed and decentralized communities that participate in blockchain projects is by means of centralized End User License Agreements (EULAs), codes of conduct, and terms of use (TOUs).[95] These terms are imposed on a decentralized and

---

[93] *See* Joshua A.T. Fairfield, *Making Virtual Things*, 64 WM. & MARY L. REV. 1057, 1069–71 (2023) [hereinafter Fairfield, *Making Virtual Things*] ("Blockchain is a solution to the Byzantine Generals Problem, which essentially asks how to form a community of trust when one knows that bad actors will be part of the mix. If you know that some signals you receive are good ones, and some bad, how can you trust anyone? (Hence the name of the problem—Byzantine generals, historically corrupt, must coordinate to attack a city. Some of them are known to be traitors, but nobody knows which.)").

[94] 18 U.S.C. § 1030(a).

[95] For consideration of how the law has adapted to ubiquitous terms of use outside of the blockchain context, see generally Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459 (2006).

non-hierarchical group of participants by leveraging strict intellectual property laws. Although a full read of the reach and role of EULAs and TOUs in governing blockchain communities is beyond the scope of this Article, a brief sense of the strength of the intellectual property laws which permit private regulation of a population that views itself as essentially ungovernable is important for practical purposes.[96] EULAs and TOUs are the simplest and most powerful means for constraining crypto-counterfeiting. They do so by leveraging powerful intellectual property protections combined with some degree of centralization of code or application.

1. EULAs and Intellectual Property

The imposition of centralized control on a decentralized population through intellectual property licenses functions as follows. Generally, there is some element of copyrightable code that serves as a central component of a blockchain ecosystem.[97] Even the most decentralized blockchain projects—ones that spin up a unique blockchain and provide a mechanism for the validation of transactions in tokens—require some software for doing so.[98] The software generally runs on mining nodes or, in proof-of-stake systems, on validation nodes run either by those staking currency or more commonly those to whom significant numbers of tokens have been staked.[99] These actors—miners, staking representatives, or validation node operators—run software to validate transactions, open new blocks on the chain, and generally ensure

---

[96] *See* Joshua A.T. Fairfield, *Anti-Social Contracts: The Contractual Governance of Virtual Worlds*, 53 MCGILL L.J. 428, 451 (2009).

[97] *See, e.g.,* John Biggs, *Craig Wright Attempts to Copyright the Satoshi White Paper and Bitcoin Code*, COINDESK (Sept. 13, 2021), https://www.coindesk.com/markets/2019/05/21/craig-wright-attempts-to-copyright-the-satoshi-white-paper-and-bitcoin-code/ [https://perma.cc/EA46-UXFC].

[98] *See* Paul Kiernan, *The Five People Keeping Bitcoin Alive*, WALL ST. J. (Feb. 23, 2023), https://www.wsj.com/podcasts/the-journal/the-five-people-keeping-bitcoin-alive/5d156987-2868-4308-bc1d-adcb55d22468 [https://perma.cc/XPG8-AQN9].

[99] *See* David Yaffe-Bellany, *Crypto's Long-Awaited 'Merge' Reaches the Finish Line*, N.Y. TIMES (Sept. 15, 2022), https://www.nytimes.com/2022/09/15/technology/ethereum-merge-crypto.html [https://perma.cc/K6NM-2U8W].

transactions cannot be falsified or unwound.[100] Performing this task together requires that mining nodes or staked-currency representatives run the same software.[101]

For example, the Bitcoin blockchain software runs on both mining and validation nodes.[102] That software includes the methods used by the proof-of-work algorithm to determine who is rewarded with new bitcoins as new blocks are mined, and adjusts the difficulty of the algorithmic hash required to open a new block, such that a new block opens roughly every ten minutes.[103] Nodes achieve this coordination by running the same software. It is a remarkable degree of centralization for a supposedly decentralized system, and one that the law of intellectual property can use to impose rules governing the entire community.[104] If an entity controls the copyright for the coordination algorithm itself, that entity can impose contractual protections grounded in powerful copyright protections.[105]

The central mining, voting, staking, or verification software of a blockchain is not the only opportunity a caretaker entity might have to impose contractual duties that constrain community members to refrain from hacking or exploiting the blockchain itself or smart contracts built on the blockchain. Many blockchain ecosystems rely on centrally located proprietary pieces of software. Consider, for example, a blockchain project that uses a specific wallet software for most members.[106] Or, for example, consider a project that is generally grouped around a specific exchange or marketplace that permits transfers of tokens or tokenized assets.[107] Such communities can publish, as

---

[100] *See* ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION 104–05 (Princeton Univ. Press 2016).

[101] *Id.*

[102] *See* SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 3 (2008).

[103] *See id.* at 3–4.

[104] *See* Siobhan Roberts, *How 'Trustless' is Bitcoin, Really?*, N.Y. TIMES (June 22, 2023), https://www.nytimes.com/2022/06/06/science/bitcoin-nakamoto-blackburn-crypto.html [https://perma.cc/BC78-JNMP].

[105] *See* Sebastian Pech, *Who Owns the Blockchain? How Copyright Law Allows Rights Holders to Control Blockchains*, 16 J. BUS. & TECH. L. 59, 63–65 (2021).

[106] *See Terms of Use*, METAMASK (Apr. 2023), https://metamask.io/terms-of-use/ [https://perma.cc/2HP2-PLPG].

[107] *See Terms of Service*, OPENSEA (Apr. 4, 2023), https://opensea.io/tos [https://perma.cc/3VNA-K8HC].

part of their site or service's terms of use, requirements that the users not engage in crypto-counterfeiting or other exploits or malicious acts. When those terms are violated, the offending user can be denied access to the community, and by extension its resources.[108] Finally, consider the example of smart contracts themselves, such as the smart contracts used to build a supply of non-fungible tokens on top of a more traditional blockchain. Smart contracts are code; that code can be copyrighted, and the use of the copyrighted code can be conditioned on compliance with an intellectual property license.[109]

End User License Agreements serve a pivotal role in governing the relationship between blockchain project creators and their community of users.[110] Given that blockchain projects often involve the creation and distribution of software, EULAs become crucial in setting the legal parameters for how that software can be used, replicated, modified, and shared. They help establish the framework within which the community operates, delineating rights, responsibilities, and limitations. This is particularly important for blockchain projects, which are by nature decentralized and rely on the collective action of a dispersed user base to maintain the integrity and security of the blockchain. By clearly defining what is permissible within the project's ecosystem, EULAs can help prevent misuse of the software, contribute to the project's sustainability, and protect intellectual property rights, while at the same time fostering an environment that encourages innovation, participation, and compliance with regulatory standards.[111] They can, for instance, prohibit activities that

---

[108] *See, e.g., Terms of Use*, BINANCE (Aug. 12, 2023), https://www.binance.com/en/terms [https://perma.cc/AGA2-S6EF] ("[Users may be banned if they] use the Binance Services for anything which, in Binance's sole opinion, is conduct designed to control or artificially affect the price of any Digital Asset (market manipulation) including, without limitation, pump and dump schemes, wash trading, self-trading, front running, quote stuffing, and spoofing or layering) [sic] regardless of whether prohibited by Applicable Law.")

[109] *See* Gregory Klass, *How to Interpret a Vending Machine: Smart Contracts and Contract Law*, 7 GEO. L. TECH. REV. 69, 77–79 nn.20–21 (2023).

[110] *See, e.g., Blockchain.com User Agreement*, BLOCKCHAIN.COM (Dec. 7, 2023), https://www.blockchain.com/legal/terms [https://perma.cc/73Y6-6WDR].

[111] *See What is an end user license agreement (EULA)?*, SERVICENOW, https://www.servicenow.com/products/it-asset-management/what-is-eula.html [https://perma.cc/QP8P-DB9R].

would threaten the security of the network, threaten the privacy of its users, or otherwise disrupt the project's intended functionality. In the dynamic and often legally uncharted waters of blockchain technology, a well-crafted EULA is indispensable for setting expectations, mitigating legal risks, and providing a stable foundation for community governance and project development.

EULAs benefit from a powerful battery of protections and sanctions. Under the legacy of *MAI v. Peak Computer* and its successors, any loading or use of software constitutes the making of a copy.[112] Making a copy of the computer program, including even the making of a copy to run the program, constitutes copyright infringement by a user if the user is not following the terms of a license agreement; so, functionally speaking, running code requires a license.[113] This is true even if that code is fully bought-and-paid-for.[114] Moreover, EULAs have been deemed a technological anti-copying measure under the Digital Millennium Copyright Act, as has been described at great length in other scholarship.[115] And the contents of these EULAs can have powerful tools to help constrain bad actors from undermining the integrity of the blockchain by wrongly appropriating tokens to themselves that they did not earn, or by wrongfully causing the system to issue tokens by means of a hack, exploit, or intentionally programmed back door.

In the case of bad actors who exploit a blockchain system in order to hack, exploit, back-door, or dupe currency, a EULA can provide powerful community protection. The first opportunity and problem is contractual remedies. Remedies for breach of contract can in the normal case be quite anemic. If a person is paying for a site or service, then contract expectation damages might be something like the license fees lost as a result of the

---

[112] *See* MAI Sys. Corp. v. Peak Comput., Inc., 991 F.2d 511, 515 (9th Cir. 1993).

[113] *Id.* at 518 ("Peak's loading of copyrighted software into RAM creates a 'copy' of that software in violation of the Copyright Act.").

[114] *See* AARON PERZANOWSKI & JASON SCHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY, 125 (MIT Press 2016).

[115] 17 U.S.C. § 1201(a)(3)(A); *see generally* David Fry, *Circumventing Access Controls Under the Digital Millennium Copyright Act: Analyzing the SecuROM Debate*, 8 DUKE L. & TECH. REV. 1 (2009).

breach.[116] And because almost all software in this space is given away because of the bolstering effect broad participation has on the community, recovery of the price or cost of software is a rare and small remedy.[117] However, backing community-protecting prohibitions on exploiting or back-dooring a blockchain project with intellectual property law can leverage powerful sanctions, including the Copyright Act's $150,000 per-infraction penalty for willful infringement.[118]

Contracts also provide a powerful backstop to technological protections because they are written in natural language. The code that makes up the mining, staking, or voting algorithms of a blockchain community or project, or the code that makes up smart contracts using the blockchain as a foundation and database, is written in formal computing languages.[119] Bugs are inevitable.[120] And given the complexity of interactions between layers of code (say, the interactions between a blockchain with smart contracts that ride on top of it) or between different smart contracts themselves, there is no chance that the code will always act the way the drafters of that code intended, no matter how competent they may have been.[121] Code is certain to sometimes act against the clear intentions of the parties who drafted the code.[122] No matter how carefully programmers vet for bugs, their code will occasionally and inevitably produce catastrophic errors. In the context of the present discussion, bad actors will

---

[116] *See* MDY Indus., LLC v. Blizzard Ent., Inc., 629 F.3d 928, 941 (9th Cir. 2010) (discussing the difference between contractual promises and license conditions).

[117] *See id.*

[118] *See id.*; 17 U.S.C. § 504(c)(2).

[119] *See* Sudhani Verma et al., *Introduction of Formal Methods in Blockchain Consensus Mechanism and Its Associated Protocols*, 10 IEEE ACCESS, June 2022, at 66611.

[120] *See* Adrian Bridgwater, *A (Software) Bug's Life*, FORBES (Nov. 22, 2022), https://www.forbes.com/sites/adrianbridgwater/2022/11/22/a-software-bugs-life/?sh=27c2a1e25c0d [https://perma.cc/AXE5-SU2K].

[121] Werbach & Cornell, *supra* note 25, at 365.

[122] *See generally* Nicola Atzei et al., *A Survey of Attacks on Ethereum Smart Contracts*, *in* PRINCIPLES OF SECURITY AND TRUST 164–86 (Springer 2017) (discussing how there is a "misalignment" between programming languages, software platforms, and a programmer's goal).

always be able to exploit these errors, interactions, loopholes, and other lacunae in the code.[123]

This is where the natural language of a community-supporting contract can come to the forefront. By expressing the intentions of the parties in natural language, the parties can make clear what it is that they expect their blockchain community or project to do. Such a statement of the parties' intent can be invaluable. For one, it puts paid to the oft-repeated (and clearly erroneous) argument that the parties have agreed to transact in whatever way the code permits them to transact.[124] This is of course nonsense. The nature of code means that sometimes the automatic execution will do something entirely outside the contemplation of any human. Say, for example, the code crashes entirely; that is obviously not what a community or project intended to accomplish. In the context of blockchain tokens and transactions, this argument surfaces occasionally when a bad actor can steal, duplicate, or counterfeit tokens. That party then argues that the outcome of the exploit must have been what the parties intended because this is how the system in fact functions. That argument must facially fail. No one would enter into a blockchain project with the understanding that destroying the value of their holdings through an exploit is permitted.

Contracts, again usually in the form of a EULA, tied to mining software, wallet software, or central community site or marketplace, can provide a guiding narrative for a blockchain community. Natural language can be interpreted to avoid the kind of inevitable and catastrophic failures of formal languages. And a contractual narrative can set out the expectations of the community when it comes to interacting with the distributed database, exercising smart contracts built on top of that distributed database, or even transacting in tokens themselves.[125] Of course there will be problems of ambiguity in natural language—if natural language's strength is that it is complete (that is, one can express all truths in it), then it is not consistent (legal language often and notoriously contradicts itself). But this is where the automatic execution of smart contracts comes to the forefront: here,

---

[123] *Id.* at 165, 173.

[124] *See* Werbach & Cornell, *supra* note 25, at 369.

[125] *See id.* at 365.

the formal language is consistent but not complete, and its rigorous consistency can often give a court or other interpreting body a reasonable sense for which way to lean in case of ambiguity when the code was clearly and intentionally structured to operate in a given way.[126]

In this sense the formal language of smart contract and the natural language of legal contract complement each other.[127] Or, to ground this discussion in concrete examples, it would be very hard for a hacker or exploiter to argue that the exploit they found or the vulnerability they utilized in a hack followed from the system working as intended when there is a contract, a EULA, a community code of conduct, or a TOU that clearly delineates a standards-based set of expectations around not exploiting bugs, not hacking to dupe, misappropriate, or wrongfully generate illegitimate tokens, not undermining the integrity of the blockchain, reporting bugs, and so on.

2. Dispute Resolution and Remedies

One final note is appropriate regarding the use of contractual means to constrain crypto-counterfeiting, as well as other forms of theft, hacking, exploitation, or the like. The remedy for wrongful misappropriation of tokens should be to return or burn the exploited tokens. 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.[128] Appropriately drafted contracts can also contain arbitration clauses, which have plagued consumer attempts to seek redress for small-dollar-value and high-volume harms (the arbitration revolution has largely been a concerted attempt to undermine class actions), but which can

---

[126] Joshua Fairfield & Niloufer Selvadurai, *Governing the Interface Between Natural and Formal Language in Smart Contracts*, 27 UCLA J.L. & TECH. 79, 101–06 (2022).

[127] *See id.* at 361.

[128] *See* Melvin A. Eisenberg, *The Disgorgement Interest in Contract Law*, 105 MICH. L. REV. 559, 580, 601 (2006).

work better in the present context.[129] The number of exploiters of a blockchain system is likely to be quite small in comparison to the overall number of users whose holdings are diluted by a currency hack, making the one-to-one nature of arbitration more appropriate for a blockchain caretaker entity to bring one or a few bad actors to account. Thus, contracts can establish the ground facts of the damage crypto-counterfeiting can cause to a project, can set agreed-upon remedies appropriate to that context, and can establish a forum for the resolution of such conflicts that can draw on institutional competence regarding the nature of blockchain projects.

There are a few other reasons that contractually established arbitration is well-suited for the blockchain project context. Arbitral panels can follow procedures and be drawn from panels of experts that reflect the particular technological knowledge base necessary to make wise decisions around token rights.[130] For example, it is possible courts may become confused around ownership rights in intangibles (most states do not recognize a right of replevin in fully intangible digital assets, for instance), whereas experts with knowledge in the field of blockchain projects will understand that the creation of digital scarcity through a distributed and decentralized list is the entire point of using a blockchain.[131] Relatedly, costs of arbitration are supposedly lower, meaning that a blockchain caretaker entity could realistically afford to enforce its prohibitions.[132] And, of course, there are advantages in being able to set the form of arbitration: parties might agree on means of submitting evidence, rely on common

---

[129] *See, e.g.,* Amy Schmitz, *Arbitration in the Age of Covid: Examining Arbitration's Move Online*, 22 CARDOZO J. CONFLICT RESOL. 245, 273 (2021) (discussing potential advantages of online arbitration); Sam Brown, *Arbitration of Cryptoasset and Smart Contract Disputes: Arbitration Unchained?*, CLIFFORD CHANCE (Jul. 19, 2023), https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/08/arbitration-of-cryptoasset-and-smart-contract.pdf [https://perma.cc/3SUZ-3PRA].

[130] *See* Amy Schmitz, *Resolving NFT and Blockchain Disputes*, 62 STAN. J. BLOCKCHAIN L. & POL'Y 156, 175–76 (2023).

[131] *Id.* at 184; *see* further discussion *infra* Section III.C.2.

[132] *See* Coinbase v. Bielski, 599 U.S. 736, 740–41, 741 n.2 (2023) (demonstrating the potential for arbitration in the blockchain context to resolve disputes).

oracles, or engage in other practices that render proof and adjudication costs significantly lower than even the traditional arbitration context.[133]

As a final caveat, there are two elements that make applying arbitration agreements—which after all are largely the point of IP-backed EULAs—truly stick and serve as a method for constraining crypto-counterfeiting or similar illicit acts that undermine the entire structure of a blockchain project. The first is that arbitration agreements must be included in a contract, in contractual language.[134] This may seem to be a minor hurdle, but it is one well worth pointing out. The golden standard for convincing a court that online parties have entered into contractual arrangements is the use of a mandatory, non-leaky, drag-down, click-through "I Agree" contract, of the sort that each of us has agreed to regularly, if not daily.[135] But where arrangements are decentralized, a blockchain-curating entity may not be certain to require each token holder to agree to contractual terms.[136]

Consider, for example, an entity incorporated in order to shepherd and protect a blockchain project. Assume it owns the copyright and thus can effectively license node-verification and mining software that forms the core of the blockchain. Moreover, it offers a proprietary wallet solution (which it again licenses to the community), and that wallet is integrated with a marketplace on which the tokens are bought and sold. The wallet has an EULA that contains the above provisions and binds users who download the wallet to their smartphones or use a browser-based version of the wallet. And of course, everyone who purchases tokens through the website or the market may well be bound by browsewrap terms of service that purport to bind anyone who makes use of the site or service.

---

[133] *See* Schmitz, *supra* note 129, at 171–72.

[134] *See* Tamar Meshel & Moin A. Yahya, *Crypto Dispute Resolution: An Empirical Study*, 2021 U. ILL. J.L., TECH. & POL'Y 187, 198–201 (2021).

[135] *See* Werbach & Cornell, *supra* note 25, at 321.

[136] *See* Rensel v. Centra Tech, Inc., No. 17-24500-CIV-KING/SIMONTON, 2018 WL 4410110, at *10, *14 (S.D. Fla. June 14, 2018) (purchaser of crypto tokens not bound by arbitration agreement where the purchaser bought directly from a smart contract and not through the website where the arbitration agreement and terms of service appeared).

Nevertheless, the decentralized nature of a blockchain project and the fundamental nature of hacks and exploits may make contractual control of blockchain projects difficult. First, a user who obtains tokens without using the proprietary wallet, or without going to the website or marketplace may not be deemed to have agreed to the contract terms.[137] The point of tokens is often that they can be resold, and resale conditions and context are often nowhere near as easily controllable as an initial distribution.[138] Second, an exploit or hack, by definition, means that some technological loophole has either been created or simply used to wrongfully misappropriate tokens, wrongfully duplicate existing currency, double spend existing currency (which amounts to the same thing), wrongfully exploit the system into either transferring tokens to which the bad actor was not entitled, or cause the creation of new tokens that should never have been created.[139] To put it bluntly, an exploiter, hacker, or currency duper may not have clicked through an "I Agree" agreement or even interacted with the caretaker entity's site, service, or marketplace. Here, intellectual property licenses help. If the hacker is running code without a license, by executing that code in violation of the terms of a posted license, there is a strong argument that the bad actor would at the least be a copyright infringer. But given the decentralized nature of these projects, and the intentional design by which tokens are meant to be transferred forward in a more-or-less unlimited fashion, the specter of an exploiter who has not clicked "I Agree" must certainly be considered a real possibility.[140]

---

[137] *Id*. at 10.

[138] *Id.*

[139] Dikla Barda et al., *Scammers are Creating New Fraudulent Crypto Tokens and Misconfiguring Smart Contracts to Steal Funds,* CHECK POINT RSCH. (Jan. 24, 2022), https://research.checkpoint.com/2022/scammers-are-creating-new-fraudulent-crypto-tokens-and-misconfiguring-smart-contracts-to-steal-funds/ [https://perma.cc/555B-S87Q]; Sam Cooling, *Double Spending*, TECHOPEDIA (Dec. 29, 2023), https://www.techopedia.com/definition/double-spending [https://perma.cc/83PB-GJ57].

[140] *See* EPIQ, *supra* note 5; Gareth Jenkinson, *DeFi Exploits and Access Control Hacks Cost Crypto Investors Billions in 2022: Report*, COINTELEGRAPH (Feb. 13, 2023), https://cointelegraph.com/news/defi-exploits-and-access-control-hacks-cost-crypto-investors-billions-in-2022-report [https://perma.cc/B797-VJT4].

Several considerations within the law of arbitration itself complicate contractual control of blockchain projects to constrain crypto-counterfeiting and other bad acts by token holders or community members. Mandatory arbitration is both favored and disfavored. The Supreme Court's jurisprudence, from *Concepcion* to *Italian Colors* and beyond, has forwarded a clear policy of favoring arbitration even (perhaps especially) when its effect is to reduce costs by rendering the ability to vindicate a legal right impossible.[141] On the other hand, there has been significant push-back against arbitration clauses, both as a matter of legislation (see, for example, recent legislation limiting the use of forced arbitration in the workplace) and as a matter of court determinations, even given pro-arbitration Supreme Court precedent.[142]

One major concern is courts' consideration of mutuality of recourse as part of the unconscionability analysis. One of the few means of challenging EULA or clickwrap-based arbitration agreements is on unconscionability grounds.[143] A full treatment of the law of unconscionability in online arbitration agreements is beyond the scope of this Article, but the basics are as follows. Arbitrated cases do not become legal precedent.[144] Given the widespread use of online arbitration agreements, the only cases that make it to courts are ones in which the arbitration clause has been invalidated (except for a very few in which the site or service provider has not included such a clause).[145] The law of unconscionability has mutated rapidly in response.

---

[141] AT&T Mobility LLC v. Concepcion, 563 U.S. 333, 344 (2011); Am. Express Co. v. Italian Colors Rest., 570 U.S. 228, 235–36 (2013); *see generally* Viking River Cruises, Inc. v. Moriana, 596 U.S. 639 (2022).

[142] *See*, *e.g.*, Ending Forced Arbitration of Sexual Assault and Sexual Harassment Act of 2021, Pub. L. 117-90 (Mar. 3, 2022) (codified as 9 U.S.C. §§ 401–02) ("[N]o predispute arbitration agreement or predispute joint-action waiver shall be valid or enforceable with respect to a case which is filed under Federal, Tribal, or State law and relates to the sexual assault dispute or the sexual harassment dispute.").

[143] Kevin Dong, *Developing a Digital Property Regime*, 105 CORNELL L. REV. 1745, 1767 (2020); Daniel D. Huan & Eric P. Robinson, *Do You Agree?: The Psychology and Legalities of Assent to Clickwrap Agreements*, 28 RICH. J.L. & TECH. 625, 651 (2022).

[144] *See* W. Mark C. Weidemaier, *Toward a Theory of Precedent in Arbitration,* 51 WM. & MARY L. REV. 1895, 1903–06 (2010).

[145] David Horton & Andrea Cann Chandrasekher, *After the Revolution: An Empirical Study of Consumer Arbitration*, 104 GEO. L.J. 57, 72–73 (2015).

The law of mutuality is an example of this rapid mutation. Courts generally hold that unconscionability contains two components: procedural and substantive.[146] Procedural unconscionability reflects concerns that the bargaining process itself was unfair.[147] Substantive unconscionability reflects concerns that the unfair bargaining process has led to an unfair result.[148] For online contracting, many courts are willing to accept that "take-it-or-leave-it" contracts reflect a certain degree of procedural unconscionability.[149] Thus, the emphasis is on substantive unconscionability. While the traditional notion of unconscionability focuses on the overall degree to which the bargain "shock[s] the conscience," newer doctrine focused on the unconscionability of arbitration clauses drills down on the degree to which the party with less power is forced to bear costs that they would not have to bear were the case to go to litigation, and whether one party has power during the dispute resolution process that the other party does not have.[150] It was born of the intuition that corporations were drafting clauses that permitted cases corporations cared about to go to court, while locking cases that consumers cared about out of court.[151] Thus, for example, a common clause that stands on questionable grounds because of mutuality is one that allows a corporation to bring intellectual property claims in court, but requires labor claims to go to arbitration.[152]

This jurisprudence has fuzzy edges, however, and those edges may bear on the complex question of how blockchain caretaker entities can police hacking, duping, counterfeiting, or misappropriation of tokens. For example, powers reserved by a caretaker

---

[146] *See Concepcion*, 563 U.S. at 340.

[147] *Id.* at 340.

[148] *Id.*

[149] Huan & Robinson, *supra* note 143, at 651–52.

[150] *See* Ferguson v. Countrywide Credit Indus., Inc., 298 F.3d 778, 783, 785 (9th Cir. 2002); Gentry v. Superior Ct., 42 Cal. 4th 443, 468–69 (2007) (substantive unconscionability focuses on the one-sided nature of the contract term); Sonic-Calabasas A, Inc. v. Moreno, 311 P.3d 184, 212–13 (Cal. 2013).

[151] Meredith R. Miller, *Contracting Out of Process, Contracting Out of Corporate Accountability: An Argument Against Enforcement of Pre-Dispute Limits on Process*, 75 TENN. L. REV. 365, 367 (2008).

[152] *See* Susan Randall, *Judicial Attitudes Toward Arbitration and the Resurgence of Unconscionability,* 52 BUFF. L. REV. 185, 186–87 (2004).

entity through its control of the blockchain software, or control of a site, marketplace, or other service, may raise questions of mutuality. Regarding the current discussion, an electronic contract or EULA may reference misappropriation of tokens, or list narrative standards under which a user's actions may be deemed to undermine the security and integrity of the blockchain or project. The remedy is usually straightforward: currency duping or counterfeiting is best resolved by deletion of the misappropriated, counterfeited, double spent, or otherwise duped currency. The difficulty is that this clear problem (say, a ban on hacking outlined in the contract) and solution (deletion of wrongfully generated tokens) might, at first blush, appear to a court to trigger consideration of whether the remedy was mutually available to both sides.

An example of how this might happen is the old case of *Bragg v. Linden Research, Inc.*[153] In that case, the defendant operated a virtual world, *Second Life*. Linden Labs sold plots of virtual land through an online auction system.[154] Plaintiff Marc Bragg discovered an exploit whereby he could access land auctions listed online before the auctions were publicly available. He was therefore, the only bidder on the land and could purchase virtual land before auction at vastly lower prices.[155] Upon discovering his exploit, Linden Labs banned Bragg from *Second Life* and cut off his access to the wrongfully acquired land.[156] Bragg sued, and Linden Labs moved to compel arbitration.[157] The *Bragg* court determined that the arbitration clause was unenforceable because Linden Labs had the power to ban Bragg and cut off his access to the misappropriated virtual land during the dispute-resolution process.[158] This determination used analysis bearing on mutuality; the idea that one party could dispose of what was ostensibly the other party's digital property during the dispute resolution process constituted a non-mutual power.[159]

---

[153] 487 F. Supp. 2d 593, 607 (E.D. Pa. 2007).

[154] *Id.* at 595; *see also* LASTOWKA, *supra* note 44, at 16–19.

[155] *See* LASTOWKA, *supra* note 44, at 16.

[156] *Id.* at 17.

[157] *Id.* at 19.

[158] *Id.*

[159] *See* Bragg v. Linden Rsch., Inc., 487 F. Supp. 2d 593, 607–08 (E.D. Pa. 2007); *see also* LASTOWKA, *supra* note 44, at 19.

The solution for the mutuality problem is for the parties to agree in an EULA or electronic contract that the wrongful generation or misappropriation of tokens contravenes the intentions of the party making use of the blockchain site or service, and that—assuming the blockchain curating entity chooses to do so—the matter is best determined by arbitration. As part of the EULA, deletion of duped currency would be expressly contemplated as a remedy, but any deletion of the currency would rest on a determination by the arbitrator rather than serving as a de facto remedy.

This solution creates its own problems. The entire point of a deletion solution is to move quickly, in many cases, before the duped currency is traded to innocent recipients or good faith purchasers for value. In the worst case, tokens might be laundered through exchanges intended to wash currency clean of prior transaction history, which would also serve to dissociate the wrongful origins of illegitimate tokens.[160] There is significant tension, therefore, between the effectiveness of a deletion solution and its speed. In no event, though, should the agreed-upon nature of the remedy damage its use. The overarching goal is to make it clear that crypto-counterfeiting is banned by agreement of the parties, and deletion is the agreed-upon remedy.

Finally, it is again worth mentioning why this common online mix of EULAs and arbitration agreements is less commonly used to control the blockchain community.[161] This model assumes that there is some legal entity—in the blockchain development space, the norm is a caretaker entity that holds some intellectual property licenses and has been tasked with overseeing the healthy growth of the project—that can serve as a counterparty for these contractual promises and enforce them. But often, there is no such entity. The Blockchain Foundation, for example, has no special relationship, legal authority, or intellectual

---

[160] *See, e.g.*, Ed Caesar, *How a Young Couple Failed to Launder Billions of Dollars in Stolen Bitcoin*, NEW YORKER (Feb. 14, 2022), https://www.newyorker.com/business/currency/how-a-young-couple-failed-to-launder-billions-of-dollars-in-stolen-bitcoin [https://perma.cc/LN3H-PVAH].

[161] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 133–35 (discussing the governance paradox: the more a blockchain entity forswears effective governance, the less protected the project it purports to be guiding becomes).

property license, and is not responsible in any way for blockchain projects, as it often has to explain to authorities.[162] Even when a guiding or caretaker entity exists for the blockchain product, it may be reluctant to exercise such authority.[163] This reluctance springs from the cyberlibertarian commitments of many blockchain projects, which seek to disintermediate some functions (usually financial) and free transactions or communities from the control of intermediaries.[164] Contractual and intellectual property control directly conflict with this political and social tenet. And, of course, if an entity does have some control over the community via EULAs or electronic contracts, it may become subject to state regulation and attempted law enforcement, or be the target of a private lawsuit, because of its asserted control over a blockchain project or community. It is hard for a blockchain caretaker entity to assert both that it holds the ability to control the community to enforce standards against theft or counterfeiting, for example, and that the blockchain is so decentralized and disintermediated that the caretaker entity cannot be held responsible for contravening public or private law.

3. CFAA and Contracts

The relationship between breaching an online contractual license, such as Terms of Use, and incurring liability under the Computer Fraud and Abuse Act has been a complex and evolving area of law.[165] As stated above, the CFAA criminalizes, among other things, accessing a computer without authorization or exceeding authorized access, thereby obtaining information from any protected computer.[166] However, the subject of legal debate is whether a mere violation of the Terms of Use constitutes "unauthorized access" or "exceeding authorized access" under the CFAA.[167]

---

[162] *See* McShane, *supra* note 13.

[163] *Id.* at 141.

[164] WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 136–37 (discussing the historical origins of consensus and decentralization as technologist values).

[165] *See* Kerr, *Norms*, *supra* note 86, at 1146–47.

[166] *See* LASTOWKA, *supra* note 44, at 161.

[167] *See* United States v. Van Buren, 141 S. Ct. 1648, 1662 (2021) (resolving dispute about "exceeding authorized access" in favor of requiring that the

Initially, some courts took a broad view of the CFAA, holding that violations of Terms of Use or website terms and conditions could constitute unauthorized access. This perspective was exemplified in cases such as *United States v. Drew*, where the defendant was charged under the CFAA for creating a fake profile on a social network in violation of the site's terms of service.[168] However, the *Drew* court ultimately dismissed the CFAA charges, highlighting concerns about the statute's potential for broad application.[169]

In contrast, a more recent and narrower interpretation of the CFAA can be seen in the Supreme Court's decision in *Van Buren v. United States*.[170] In *Van Buren*, the Court held that "exceeding authorized access" occurs when a person accesses a computer with authorization but then obtains information located in particular areas of the computer that are off-limits to them.[171] The Supreme Court emphasized that the CFAA does not cover situations where individuals misuse access to information they are otherwise entitled to obtain.[172] This decision suggests that mere violations of contractual terms like Terms of Use or a Code of Conduct, without more, would not typically constitute a CFAA violation. Thus, for a violation of Terms of Use or a Code of Conduct to constitute a violation of the CFAA post–*Van Buren*, the user would likely need to circumvent distinct technological barriers or restrictions intentionally set up by the owner of the online system that clearly delineates authorized from unauthorized access.[173] Merely using the system in a manner contrary to the owner's expectations or desires, without bypassing any technological access barriers, would not be enough.[174]

The current legal landscape suggests that a user who simply breaches the terms of an online agreement without engaging in

---

defendant have accessed off-limits files, not merely accessed files in contravention of policy).

[168] *See* United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

[169] *Id.* at 467.

[170] *See supra* notes 89–91 and accompanying text.

[171] *Van Buren*, 141 S. Ct. at 1649.

[172] *Id.* at 1652.

[173] *Id.* at 1654.

[174] *See* George F. Leahy, *Keeping Gates Down: Further Narrowing the Computer Fraud and Abuse Act in the Wake of Van Buren*, 14 WM. & MARY BUS. L. REV. 215, 236–38 (2023).

activities such as exploiting bugs in code, hacking, cracking passwords, or bypassing technological access controls, would not be liable under the CFAA.[175] The interpretation of "authorization" has thus shifted away from a purely contractual framework toward an approach more tied to access control's technical and mechanical aspects.[176] This, however, is entirely consistent with attempts to constrain crypto-counterfeiting. After all, the basic setup for crypto-counterfeiting is the discovery of a hack, loophole, exploit, or incompatibility in the code that creates an opportunity for duping currency. Exploiters may assert that exploitative transactions must be the system working as intended, and that the bad actor has done nothing wrong by taking advantage of a glitch in the system. Clear contractual language puts paid to the argument that exploiting the system is all part of the expected process, and then the fact of technological exploitation, hacking, and so on puts the behavior cleanly under the CFAA. Thus, while in a post–*Van Buren* world, contravention of the terms of an End User License Agreement or Terms of Service is not enough, alone, to constitute grounds for a CFAA claim, an EULA or TOS can clarify the terms of engagement and clarify what should need no clarification—that exploiting or hacking the system is beyond any potential authorized access.

4. Third-Party Beneficiary

There is another dimension to the potential of using electronic contracting and EULAs to constrain crypto-counterfeiting.[177] Legitimate token holders are often the ones who wish to establish a process to constrain someone who has diluted legitimate holdings by engaging in crypto duping. The difficulty is that the contracts that govern most online communities do not permit third-party beneficiaries to bring suit. Take, for example, the gaming company cases of the early 2000s. A player of the online game

---

[175] *Van Buren*, 141 S. Ct. at 1661.

[176] *Id.* at 1658–59.

[177] *See generally* MARGARET JANE RADIN, BOILERPLATE: THE FINE PRINT, VANISHING RIGHTS, AND THE RULE OF LAW (Princeton Univ. Press 2012) (discussing the use of electronic contract and end user license agreements to control rights in online environments).

World of Warcraft sought to sue gold farmers under the End User License Agreement and Terms of Service.[178] Gold farming is a practice whereby players engage in automated or repetitive behavior, intending to generate in-game currency with a view toward selling that in-game currency to other players for real-world fiat currency.[179] This practice inflates the economy and is a violation of the contractual terms that govern conduct within the game.[180] The difficulty is that although gold farming damages the play experience of third parties and dilutes the value of legitimate players' efforts to secure in-game currency from actually playing, there is no direct contractual privity between players.[181] Players promised Blizzard Entertainment, the creator of World of Warcraft, that they would play according to specific rules. They did not promise each other.

Again, this led to a degree of centralization in the management of virtual worlds.[182] The "god" of the virtual world made sure to hedge out all property claims except its own, creating the gray market for virtual gold and items in the first place (the concern was that without hedging out all property claims by players for virtual currency and items, the game god would not be able to delete duped currency, ban cheating players, or even turn off the servers).[183]

Adapting these frameworks to provide legal recourse against crypto-counterfeiting requires attention to two details. First, crypto-projects often wish to create a narrative of user/purchaser ownership, and to ground that interest in law. For example, a project that creates a collectible trading card game—Gods Unchained—promotes the ownership interest that card purchasers have in

---

[178] *See* Oli Welsh, *Gamer takes gold farmers to court*: *WoW fan targets IGE with class action suit*, EUROGAMER (Apr. 8, 2008), https://www.eurogamer.net/gamer-take-gold-farmers-to-court [https://perma.cc/6U69-HERS].

[179] *See* LASTOWKA, *supra* note 44, at 22–24 (discussing the practice of gold farming and the legal challenges it presents).

[180] *See* Julian Dibbell, *Invisible Labor, Invisible Play: Online Gold Farming and the Boundary Between Jobs and Games*, 18 VAND. J. ENT. & TECH. L. 419, 430–31 (2016).

[181] *See* Welsh, *supra* note 178.

[182] *See* LASTOWKA, *supra* note 44, at 153.

[183] *See id.* at 125–27 (discussing the difficulties in recognizing property rights in virtual objects).

their digital assets, that owners can invest in and capture the rise in value of their cards because they own them, and do not merely license them.[184] Yet the major way that game companies in the 2000s cleared the way for deleting currency and restoring the economy's integrity following a currency duping exploit or hack was by denying that players had any ownership interest in the digital assets that they obtained by paying for or playing the game.[185] That narrative will not be present to clear the path for deleting duped cryptocurrency, because the narrative of property and ownership has shifted toward recognition of the personal property rights of legitimate token holders.

A second and related problem has been mentioned above: blockchain caretaker entities for crypto-projects often wish to ride a wave of unaccountability.[186] They believe, often erroneously, that no legal entity can be held responsible for actions conducted over a blockchain, and do not want to do anything to jeopardize that position.[187] They also often do not want their users or participants to have legal rights against one another, because that creates a degree of reliance on law over technology and introduces despised middlemen, professionals, and regulators back into the mix.[188]

---

[184] *See* Gods Unchained Support Team, *What Does True Ownership Mean? Don't I Own Items in Other Games?*, GODS UNCHAINED, https://support.godsunchained.com/hc/en-us/articles/1500006242742-What-does-true-ownership-mean-Don-t-I-own-items-in-other-games- [https://perma.cc/62ES-G8UJ] ("[W]e're changing this old practice to give players real ownership over the items they purchase or earn in games. This gives you the right to sell an item for ETH, use it in Gods Unchained or even take it into a different game.").

[185] *See Blizzard End User License Agreement*, BLIZZARD ENT. (May 31, 2023), https://www.blizzard.com/en-us/legal/fba4d00f-c7e4-4883-b8b9-1b4500a402ea/blizzard-end-user-license-agreement [https://perma.cc/YL9Y-YMPD] (noting that players own no legal rights, are merely licensed the game and the platform, and Blizzard maintains the ability to ban players who engage in duplication of assets).

[186] *See* Dirk A. Zetzsche et al., *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 U. ILL. L. REV. 1361, 1367 (2018).

[187] *See* Kevin Werbach, *Trust, But Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 487, 521–23 (2018).

[188] Robert A. Schwinger, *Liability Rumblings Along the Blockchain*, N.Y. L.J. (July 15, 2019), https://www.law.com/newyorklawjournal/2019/07/15/liability-rumblings-along-the-blockchain/ [https://perma.cc/A692-F8RP].

That said, third-party beneficiary clauses may serve as a means for caretaker entities to step back once they have set intellectual property or electronic contracting obligations. Violation of an EULA can be complex where the claim sounds in IP, but the plaintiff does not own the copyright (and it is usually copyright) in play. But a Code of Conduct or Terms of Use—if the obligations are stated to expressly run to other token holders bound by the same terms and conditions—could set up a system whereby community members have a mechanism to hold each other accountable for undermining the integrity of the blockchain.[189]

Consider the effect of a clause in a binding community Code of Conduct to the effect that the blockchain algorithm performs the generation and distribution of tokens to secure the integrity of token ownership, and that misappropriating tokens generated for that purpose through an exploit, hack, inconsistency, or loophole in the software violates the obligation each community member has to protect the integrity of the blockchain and thus the value of other users' tokens. Such a system has three important effects. It makes clear that the entire point of a blockchain is to secure the integrity of a record of ownership of tokens; it makes clear what should not even have to be stated, which is that attacks on that integrity damage not only the integrity of the chain itself, but also the security of the tokens on the chain, and thus the value held by legitimate token owners; and it demonstrates that the contractual structure expressly contemplates disputes between token owners on the grounds that hacking and exploiting blockchains undercut legitimate token owners' holdings.

C. Property

By way of transition, much of the above rests on a key difference between early virtual economies, which did not recognize any ownership interest in digital assets (say, by players of a massively multiplayer video game), and modern blockchain projects, where token ownership and the capture of the rise in the value of a token investment is often the entire point.[190] With this shift

---

[189] Mark Verstraete, *The Stakes of Smart Contracts*, LOY. U. CHI. L.J. 743, 745–47 (2019).

[190] *See* Fairfield, *Tokenized*, *supra* note 64, at 1263–64.

in attention comes a shift in the necessity of applying property frameworks to sanction and rectify the use of hacks, exploits, loopholes, or incompatibilities in code.[191] Put bluntly, early regimes for stopping software exploits that devalued virtual economies were supercharged by platform creators' claims that users owned nothing.[192] World of Warcraft players did not own their in-game gold or the magic swords their characters wielded, and thus, when a duping exploit was found, the company could simply delete the gold.

But with the development of blockchain projects, virtual property grew up.[193] Projects relied on promises that users owned their virtual assets in order to attract investment and engagement. Without such promises, blockchain investors would not have been drawn into the project in the first place. With that change in business model comes a change in the governing legal regime. Companies that start or manage blockchain projects no longer use intellectual property licenses to block personal property ownership interests in online assets.[194] Although claims sounding in property were viable under the old intellectual-property-based structure, they apply with even greater strength in the Web3 context.

1. Conversion

The first set of personal property-based arguments that those wrongfully damaged during a duplication or misappropriation scheme might bring, could be grounded in the growing set of cases recognizing a right to claim conversion for digital assets.[195]

---

[191] *See id.* at 1263–65 (discussing the emergence of property ownership standards for crypto-assets).

[192] *See id.*

[193] *See id.*

[194] Cam Thompson, *NFTs and Intellectual Property: What Do You Actually Own?*, COINDESK (Oct. 14, 2022), https://www.coindesk.com/learn/nfts-and-intellectual-property-what-do-you-actually-own/ [https://perma.cc/ED3A-YDEX]. Again, the scheme of licensing in-game content as IP, how World of Warcraft players were not deemed to own their in-game assets, serves as an instructive example.

[195] *See, e.g.,* Domain Prot., LLC v. Sea Wasp, LLC, 426 F. Supp. 3d 355 (E.D. Tex. 2019); E.I. Dupont de Nemours & Co. v. Kolon Indus., Inc., 688 F. Supp. 2d 443 (E.D. Va. 2009); Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272 (N.Y. Ct. App. 2007).

The basics of the claim are straightforward. If a hacker or exploiter takes tokens that do not belong to them, then they may be liable in conversion for converting the property of another to their own use.[196] There are several challenges to the theory, however.

First, if the hacker or exploiter has caused entirely new tokens to be issued, then there is an argument that the new tokens taken have not been converted. This loophole creates a gap in the law, whereby a bad actor may attempt to avoid legal sanction by arguing that their conduct, while reprehensible, does not give rise to a cause of action in any given person because the hacker did not take the property of anyone in particular. This view is too simple, however. Often, tokens are pre-mined, either by blockchain project curating organizations that spin up the blockchain and pre-mine large numbers of tokens for later issuance, or the tokens are issued through the blockchain software to an account for the purpose of awarding to project participants who, through proof-of-work contributions or proof-of-stake staking of currency are rewarded for investing in the integrity and security of the blockchain through an award of tokens.[197] By contributing processor cycles to solving an arbitrarily complex math problem, miners in a proof-of-work system are awarded new tokens; by staking currency in a proof-of-stake system, participants incentivize the network to reach consensus (because if it does not, and the system follows a different consensus, the stakers lose their stake).[198] In either case, the supply of tokens does not come from nowhere—it often comes from an account set up by the software for the creation of tokens and their transfer then to the final recipient.[199] If a hacker or exploiter robs tokens from that account, a court should find that the tokens were converted,

---

[196] *See* Robert A. Schwinger, *Ancient torts and modern assets*, N.Y. L.J. (Jan. 23, 2024), https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/nylj-ancient-torts-and-modern-assets.pdf [https://perma.cc/Q8VX-49PJ].

[197] Adam Hayes, *Premining: What It Is, How It Works, Pros and Cons*, INVESTOPEDIA (Dec. 28, 2023), https://www.investopedia.com/terms/p/premining.asp [https://perma.cc/5UPR-T6WT].

[198] E. Napoletano, *Proof of Work Explained*, FORBES (Jan 3. 2024), https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/ [https://perma.cc/9TGU-P7E3].

[199] *See generally* Hayes, *supra* note 197.

either from the blockchain project curating entity itself, or from all of the users, on behalf of whom and for whose benefit the code generated the tokens.

A second challenge is that claims in digital conversion are in a state of flux, although the trend is toward recognizing the right. Some states simply do not recognize a right of conversion in digital assets, tying the right to tangible personal property.[200] However, as other decisions note, this distinction makes little sense. If the act of breaking into a server room and setting the servers on fire would constitute conversion, there is little doubt that destroying the files by electronic means would constitute equal grounds for conversion.[201]

There has been some confusion in the cases because of the doctrine of merger. In some states, courts have begun to equate the conversion of digital assets with the conversion of personal property, where a digital right is "merged" into a physical asset.[202] Thus, for example, if a physical laptop were stolen, the intangible assets stored on the device would be properly the subject of a conversion action. At the earliest point of the doctrine of merger, it merely stands that the presence of intangible rights does not prevent a conversion claim from proceeding when the conversion of an underlying physical asset would properly meet the requirements of the claim.[203]

The doctrine has evolved, however. Courts in some states now permit digital conversion claims where the asset converted—for example, an electronic document containing a list of customers—would be the same as its physical analog (a tangible list of

---

[200] *See, e.g.*, JCorps Int'l., Inc. v. Charles & Lynn Schusterman Fam. Found., No. 20-CV-35-GKF-SH, 2021 WL 2371233, at *7 (N.D. Okla. June 9, 2021) ("In Oklahoma, the definition of conversion 'does not include intangible property.'") (quoting Am. Biomedical Grp., Inc. v. Techtrol, Inc., 374 P.3d 820, 825 (Okla. 2016)); Wells v. Chattanooga Bakery, Inc., 448 S.W.3d 381, 392 (Tenn. Ct. App. 2014) ("Conversion is the wrongful appropriation of another's tangible property; an action for the conversion of intangible personal property is not recognized in Tennessee.") (quoting Ralph v. Pipkin, 183 S.W.3d 362, 368 (Tenn. Ct. App. 2005)).

[201] *See* Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1274–76 (N.Y. Ct. App. 2007).

[202] *See* Near v. Crivello, 673 F. Supp. 2d 1265, 1281–82 (D. Kan. 2009) (allowing for a conversion action where stock certificates had been converted, and the ownership interest was merged with the certificates).

[203] *Id.*

customers).[204] Note that this is a change in the doctrine; equivalency is the measure, not rootedness in some physical asset, although courts sometimes provide lip service to the origins of the merger doctrine by pointing out that all computers are, at some point, physical.[205]

The reasons for not applying the doctrine of conversion to intangible assets are not likely to hold sway in cases of misappropriation or conversion of crypto-tokens. An example may demonstrate why. Consider the theft of a client list. Under the extended or evolved doctrine of merger, the electronic list might be considered equivalent to a physical one, and thus, the taking of a client list might be considered converting the owner's property to the taker's use. The response might be that the hacker or exploiter has not truly deprived the owner of the list of their beneficial use of the list, since the theft of the list was in the form of wrongful copying, rather than taking the list outright such that the original owner no longer has access to it. Under such circumstances, courts have analyzed that the owner was deprived of the beneficial use of the client list, because the original owner of the list is no longer the only one with access to it.[206] Exclusive use of the list was its value; thus, conversion is appropriate.[207]

This points to an underlying theme in digital conversion cases. Courts continue to rely on intellectual property law where

---

[204] *See, e.g.*, M.C. Multi-Fam. Dev., L.L.C. v. Crestdale Assocs. Ltd., 193 P.3d 536, 538–40 (Nev. 2008) (defendant converted plaintiff's contractor's license even though it did not prevent the plaintiff from making use of the license directly, and noting "[W]e . . . expressly reject the notion that personal property must be tangible in order to give rise to a conversion claim."); *see also* E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc., 688 F. Supp. 2d 443, 455 (E.D. Va. 2009) ("Virginia courts have, however, demonstrated a distinct willingness to expand the scope of the doctrine of conversion in light of advancing technology . . . . And, given the expansive definition of conversion employed in Virginia, i.e., 'any act of dominion wrongfully exerted over property in denial of, or inconsistent with, the owner's rights' . . . ."); Domain Prot., LLC v. Sea Wasp, LLC, 426 F. Supp. 3d 355, 392 (E.D. Tex. 2019) ("Texas courts have seemingly expanded the definition of 'document' to include electronic documents.").

[205] *Thyroff*, 864 N.E.2d at 1278.

[206] *See* Lee Nolan Jacobs, *Is What's Yours Really Mine?: Shmueli v. Corcoran Group and Penumbral Property Rights,* 14 J.L. & POL'Y 837, 870–73 (2006).

[207] Shmueli v. Corcoran Grp., 802 N.Y.S.2d 871, 876, 879 nn.3–4 (Sup. Ct. 2005).

assets are intangible because many of the most valuable intangible assets are intellectual property rights.[208] But a gap has opened with the rise of personal property interests in intangibles. There are no direct intellectual property rights in a cryptographic token. There may be IP rights in attached or hashed and embedded works, such as those associated with an NFT, or there may be IP rights in blockchain mining or staking software, or in wallet software, or even in a website that serves as a site or service intermediary for a blockchain project, but the tokens themselves are IP-free.[209] Moreover, and more importantly, taking a cryptographic token not only constructively denies the original owner of the beneficial use of an asset, but it also directly denies the owner of the actual use.[210] By converting a token, the hacker or exploiter has taken the asset away from the original owner. It has been assigned to a different cryptographic account, with a different public and private key arrangement. There is simply no way for the original owner to access the asset. Thus, the case of conversion of a crypto-asset is profoundly different from the standard argument about whether an intangible asset is properly subject to conversion. The very rivalrousness and excludability of the system that was designed to avoid duplication, counterfeiting, false spending, or other forms of wrongful use deprive the owner of all access to the asset, not merely beneficial use.

There is another challenge to the practical use of conversion as a remedy for the wrongful taking of, misdirection of, or exploitation of crypto-assets. Conversion leaves the assets in the hands of the wrongdoer. It is a forced sale. Having converted the crypto-assets to his or her use, the hacker must then pay for their fair market value.[211] Here, two points are worth noticing. First, the very exploit the hacker has used will have profoundly impacted the market's sense of the integrity of the exploited

---

[208] *See* Juliet M. Moringiello, *False Categories in Commercial Law: The (Ir)relevance of (In)tangibility*, 35 FLA. ST. U. L. REV. 119, 141, 144–45 (2007).

[209] *See* Fairfield, *Tokenized*, *supra* note 64, at 1295–96.

[210] *See* E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc., 688 F. Supp. 2d 443, 455 (E.D. Va. 2009).

[211] *See* Courtney W. Franks, Comment, *Analyzing the Urge to Merge: Conversion of Intangible Property and the Merger Doctrine in the Wake of Kremen v. Cohen*, 42 HOUS. L. REV. 489, 496, 513 n.171, 522 (2005).

blockchain.[212] Courts must exercise care in determining the value of the converted assets so as not to price them too low due to loss of value caused by the exploit. A second and perhaps more subtle point is that most crypto-assets are obtained with a view toward capturing their rise in value, their appreciation.[213] Some other remedies, such as unjust enrichment, may better capture portions of the policy problem related to the wrongdoer's capture of the rise in value related to ill-gotten assets.[214] Finally, the two problems can work in concert. An exploit, or a range of exploits, can drive the value of a crypto-asset down, and bad actors can then ride the value of their exploited currency back up as the system and legitimate token holders attempt to right the ship.

2. Replevin

Related to conversion is the remedy of replevin. Replevin represents a clear starting theory to handle some instances of the wrongful exploitation of a blockchain to cause it to issue currency.[215] The answer is simple: the assets must be given back. And in the usual case for crypto-assets, the counterfeit tokens would be destroyed in order to preserve the integrity of the blockchain project, or at least held in an account from which they are correctly awarded to legitimate users of the system who act to protect the integrity of the blockchain and are rewarded, as is the ordinary course, for their efforts.

Much more than conversion, however, there are significant hurdles. The first hurdle is that, as with conversion, replevin requires someone from whom the tokens were taken, and on behalf of whom the demand for their return can be made.[216] This

---

[212] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 139 ("The [DAO] hack itself suggested that the blockchain could not be trusted to distinguish among illegitimate transactions. A system that enforces theft, even unintentionally, is no different than one that unreliably enforces legitimate contracts.").

[213] Mallika Mitra, *Crypto Might Be the Future of Finance. But That's Not Why Most People Buy It*, MONEY.COM (Jul. 7, 2022), https://money.com/why-buy-crypto-survey/ [https://perma.cc/C9UW-XHDC].

[214] *See* discussion *infra* Section III.D; *see also* BDI Cap., LLC v. Bulbul Invs. LLC, 446 F. Supp. 3d 1127 (N.D. Ga. 2020).

[215] *See* Fairfield, *Making Virtual Things*, *supra* note 93, at 1085–87.

[216] *See* 66 Am. Jur. 2d Replevin, § 2 (Feb. 2024).

claim can be from a regular legitimate holder of tokens, if their tokens were used in the exploit or duping hack, or they could be a claim on behalf of a blockchain curating entity if that organization pre-mined the tokens or set up the blockchain system to issue tokens to a specific account from which the tokens were then to be awarded to legitimate users. Given that pre-mined or specifically issued tokens are created for the chain's security and thus secure any projects riding on a given chain, a claim for replevin can also be made on behalf of the legitimate token holders themselves. In a proof-of-work system, they are the ones who stand to benefit from the issuance of the tokens; in a proof-of-stake system, newly issued tokens are the direct financial reward for holding and staking tokens. They are generated for the present stakeholders, and then allocated to stakeholders in accordance with their staked currency. Thus, when the tokens are wrongfully taken, the community of legitimate stakeholders may demand their return.

The second and much higher hurdle is that digital replevin faces an uphill battle for recognition in the courts, largely because of flat and unreflective statements that replevin is not available for intangible rights.[217] Indeed, if one were inclined to think that intellectual property rights were the only intangible interests, then ordering the return of an intangible seems an extra step.[218] Making a copyright infringer pay for infringement, for example, or enjoining future use of copyrighted content would seem to be a sufficient remedy.

While it is true that several states outright deny rights of replevin for intangibles, it is also well worth noting that the remedy of returning what was wrongfully taken is such a natural and bedrock remedy that courts routinely make use of it without explicitly noting they are doing so.[219] Consider the entire highly

---

[217] *See*, *e.g.*, Jurisearch Holdings, LLC v. Lawriter, LLC, No. CV 08-03068 MMM, 2009 WL 10670588, at *8 n.44 (C.D. Cal. Apr. 13, 2009) ("Because replevin applies only to tangible property, the motion for summary judgment is granted to the extent this claim purports to assert rights in the intangible property represented by the information included in the database.").

[218] *See generally* Moringiello, *supra* note 208 (exploring the errors courts make when they consider intangibility to be dispositive of legal rights).

[219] *See, e.g.*, M.C. Multi-Fam. Dev., LLC v. Crestdale Assocs. Ltd., 193 P.3d 536, 538–40 (Nev. 2008); Peruto v. Roc Nation, 385 F. Supp. 3d 384, 477 (E.D.

developed field of Internet domain name disputes.[220] When person A wrongfully takes or registers a domain name that properly belongs to person B, courts have little trouble ordering the database of Internet names to be corrected so that the true owner of the domain name gets it back. The core case of *Kremen v. Cohen*, which stands for the establishment of digital property rights and exerts enormous persuasive authority across jurisdictions, essentially recognized such a right.[221] Where a bad actor fraudulently caused a domain name registrar to change the registration and, therefore, the ownership of the sex.com domain name, the court ordered the database corrected and the domain returned to the original legitimate owner.[222]

Crypto-tokens are digital ledger entries encrypted with specific accounts' private and public keys. Tokens are susceptible of unique possession under the *Kremen* standard. If the tokens are encrypted with the public key of a given account, only the private key of that account can further move the tokens. Third parties cannot move the tokens without an action by the account holder; only a court order to return the assets will effectuate their return. Replevin is not only a sound theoretical fit with the underlying nature of the asset, it is a necessary power in an era of thriving and expanding types of digital assets.

Replevin also solves the problem of capturing an increase in value by a hacker or exploiter. If the hacker is forced to return the tokens, they do not get to benefit from stealing low and selling high, as it were. Moreover, suppose the problem is that the tokens were taken from an account intended to reward miners or stakers for contributing processor cycles or staked currency to secure the integrity of blockchain transactions. In that case, the chain's integrity can only be restored and the value of the holdings of legitimate token holders returned if the wrongfully issued assets are returned to the issuing accounts—or destroyed, if wrongfully generated in the first place. Replevin takes the

---

Pa. 2019); Hydrogen Master Rts., Ltd. v. Weston, 228 F. Supp. 3d 320, 335 (D. Del. 2017).

[220] *See generally* Xuan-Thao N. Nguyen, *Cyberproperty and Judicial Dissonance: The Trouble with Domain Name Classification,* 10 GEO. MASON L. REV. 183 (2002).

[221] Kremen v. Cohen, 337 F.3d 1024, 1031–33, 1036 (9th Cir. 2003).

[222] *Id.* at 1026–27, 1031–33, 1036.

form of a court order to return the assets wrongfully taken, and such an order is very much needed as a remedy in the crypto space, because there is no other way to return assets.[223] Crypto-tokens cannot be seized or transferred forcibly without the private key of the present account in which the tokens wrongfully reside.[224] The technological solutions are to blacklist the accounts or exploited tokens, or to hard fork the blockchain (again, the very thing that blockchain projects claim they cannot do to protect the permanence of transactions), which involves coordination among miners or stakers to adopt new software that simply refuses to recognize a prior chain by fiat.[225] This kind of extreme action was how the Ethereum community survived the hack of The DAO, and it was a once-a-project kind of move.[226] After all, the permanence and integrity of transactions are the entire point of blockchain projects.[227] If the community shows that it is willing to fork the chain at the drop of a hat, the chain becomes worthless as a persistent measure of who owns what.[228]

D. Equity

Equitable remedies must also play a role in resolving the problem of double spending, counterfeiting, exploiting, or duplicating crypto-tokens. Equitable remedies are famously more flexible than legal remedies, so a full sense of the kind of injunctive relief a court could craft is beyond the scope of this piece.[229] However, at least as an exploration of the subject, it appears clear that certain kinds of injunctive relief, such as a preliminary injunction preventing duped tokens from being traded, would limit the damage of an exploit by preventing the wrongfully taken or duped or issued currency from spilling out into the token economy,

---

[223] *See* Andrew W. Balthazor, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. REV. 1207, 1214, 1226 (2019).

[224] José M. Garrido, *Digital Tokens: A Legal Perspective* 37 (Int'l Monetary Fund, Working Papers No. 151, 2023).

[225] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 139–40 (discussing the extreme nature of a blockchain fork).

[226] *Id.*

[227] *Id.*

[228] *Id.*

[229] *See* Maayan Perel, *Digital Remedies*, 35 BERKELEY TECH. L.J., 1, 43–46 (2020) (discussing the need for flexible equitable remedies for digital issues).

diluting the holdings of legitimate token holders.[230] The problem is that as fast as a preliminary injunction can be, currency duping hacks can spread more quickly. 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.[231]

Assuming that some of the wrongfully taken or generated tokens escape from the community organizing to fork the chain (or otherwise immobilize the wrongfully taken tokens by instituting a trading ban with the tokens in the accounts to which the hacker wrongfully transferred them), or evade the reach of a court-ordered preliminary injunction, the remedy of unjust enrichment may serve as a useful tool for constraining wrongful issuance of tokens.[232] The strength of unjust enrichment is that the theory fits the wrongful act of duping or counterfeiting crypto-tokens precisely: the hacker or exploiter has received a benefit that is unjust for them to retain. Unjust enrichment also solves the problem of conversion, which would merely make the wrongdoer pay market value for the tokens that were wrongfully taken or issued, presumably at the market price immediately preceding the hack. As stated above, this would enable the hacker to ride the rise in the value of their illegitimate tokens during any recovery of the system from the incident that the hacker themselves directly created.

There is also a subtle component to an unjust enrichment claim that may help with the problem of finding the proper plaintiff. Unjust enrichment is a benefit that is inequitable under the circumstances for the defendant to retain.[233] An unjust enrichment

---

[230] *See, e.g.*, Astrove v. Doe, No. 22-CV-80614-RAR, 2022 WL 2805345, at *6 (S.D. Fla. June 17, 2022) (enjoining defendant from "withdrawing, transferring, or encumbering any assets held in those [cryptocurrency] wallets").

[231] Alexandra D. Comolli & Michele R. Korver, *Surfing the First Wave of Cryptocurrency Money Laundering*, 69 DEP'T OF JUST. J. FED. L. & PRAC. 183, 188–89, 191, 194–95, 220 (2021); *see also* U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 41, 44 (2020) [https://perma.cc/5BR2-JLSE].

[232] *See* Jazz Osvald, *Unjustly Enriching the Richer: A Doctrinal Analysis of Unjust Enrichment and Its Application to Cryptocurrency Hard Fork and Airdrop Events*, 1 AUSTL. NAT'L UNIV. J.L. & TECH. 1, 16 (2020).

[233] *See* 66 Am. Jur. 2d Restitution and Implied Contract § 3 (Feb. 2024).

claim does not, as a technical matter, require the plaintiff to receive the benefit.[234] This opens the door to the correct response to a duping or counterfeiting incident, which is that the wrongfully issued, generated, or received tokens should be destroyed or transferred back to the issuing account, or locked in the accounts in which it presently resides. As a technical matter, there is no difference between these solutions: the way to destroy tokens is to assign them to an account that has no key for transferring the tokens forward; they become "burned," or locked in place in a dead-end account.[235]

An unjust enrichment claim also positively conforms to the theory that a claim can and should be brought on behalf of legitimate token holders. The amount by which a currency dupe or hack extracts value from a blockchain system directly relates to the amount by which the holdings of legitimate token holders are diluted because of the inflationary effect of the counterfeiting activity. The benefit taken by the bad actor who exploits a token issuance or duplication bug exactly matches the loss to other token holders, whose holdings would have been worth more had the supply of tokens on the open market not been wrongfully increased. Disgorgement and destruction of the ill-generated and wrongfully received currency is a precisely calibrated remedy to return to the legitimate stakeholders the value of their interests had the exploit not expropriated value from the blockchain community during the hack.[236]

A cautionary note on value is appropriate. Often, it can appear as though no or less harm has been suffered by stakeholders because, despite the currency hack, the tokens continue to rise in value. This is, of course, an obvious error, and one easily corrected. Hackers rarely go after worthless tokens. The whole point of crypto-counterfeiting is to counterfeit something of value. Tokens in successful projects usually rise in value. Therefore, it

---

[234] *Id.*

[235] *See Understanding crypto token burns: A comprehensive guide*, OKX (Nov. 7, 2023), https://www.okx.com/learn/token-burns [https://perma.cc/M6K2-M32E].

[236] *See* David Zaslowsky, *The Proper Way to Compute Disgorgement Profits for Illegal Token Sale*, BAKER MCKENZIE BLOCKCHAIN (Dec. 12, 2023), https://blockchain.bakermckenzie.com/2023/12/12/the-proper-way-to-compute-disgorgement-profits-for-illegal-token-sale/ [https://perma.cc/U4QS-HK5S].

is trivial as a matter of theory to say that the inflation caused by a crypto-counterfeiter does not necessarily cause the currency to dip in value. Rather, absent the inflation, the holdings of legitimate stakeholders would be worth even more. There is even a possibility that the sense of the community that a project is well run and is guided or defended by a competent curating entity will also blunt the impact of inflationary counterfeiting, because the community may assume that the wrongful behavior will be stopped and sanctioned. For all of these reasons, the argument that counterfeiters have not harmed legitimate token holders because the price of tokens did not drastically dive as a result of the hack is a red herring.[237] Instead, courts should focus on the clean and elegant solution of elimination of the wrongfully issued or received currency, which returns the market to its natural state without distorting effects and the loss of value caused by inflation despite any gains in the project's value due to the inherent demand for the project's tokens.

E. Fiduciary Duty

A further theory that may constrain crypto-duping relies on fiduciary duty. Here, the bad actor must stand in some special relation of trust to the community or project participants, whose holdings are diluted by the dumping of illicitly generated or issued tokens onto the market.[238] Fiduciary duty claims will most likely accompany a rug-pull.[239] A rug-pull occurs when the creator or founder of a blockchain project dumps many tokens, either from a large block of pre-mined tokens (which is fairly standard practice) or by instructing the blockchain mining or staking software to issue the tokens by virtue of the power exercised by the software creator over the code itself.[240]

---

[237] *See* Megan DeMatteo, *NFT Scams: How To Avoid Failing Victim*, COIN DESK (May 11, 2023, 11:51 AM), https://www.coindesk.com/learn/nft-scams-how-to-avoid-falling-victim/ [https://perma.cc/5CZ5-G4FY].

[238] *See* Raina S. Haque et al. *Blockchain Development and Fiduciary Duty*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 139, 174–83 (2019).

[239] *See* Rosie Perper, *What is a Rug Pull? How to Protect Yourself from Getting Rugged*, COINDESK (May 2023), https://www.coindesk.com/learn/what-is-a-rug-pull-how-to-protect-yourself-from-getting-rugged/ [https://perma.cc/UQ42-6YB6].

[240] *Id.*

Fiduciary claims are perhaps an ironic outcome of the structure of blockchain projects. Although the projects are supposed to be "trustless," in fact, creators of blockchain projects must be enormously trusted by prospective project participants in order to generate demand for project tokens. As Werbach writes, there is, without doubt, a large demand for ordinary, real-world governance over blockchain projects, and the prospect that a project creator might dilute the holdings of all participants in order to exchange a large amount of tokens for real-world currency (usually in order to prepare to abandon the project and run) would kill trust in the project.[241]

Little stands in the way of a fiduciary duty claim except the self-conception of blockchain projects.[242] Certainly, blockchain curation organizations or founders would be aghast at being in any way deemed fiduciaries of their project participants,[243] and much speaks against such a theory in the normal course. Blockchain founders often do not have more control over or information about the blockchain than do normal token holders.[244]

But in some special circumstances, a claim of fiduciary duty might hold. Where a founder has not only retained exclusive control over the code but also caused it to act in a way that fundamentally contravenes the expectations of the participants or acts based on knowledge asymmetries that the founder has created and fostered, then a claim of special responsibility might stand.[245] In order for such a claim to succeed, there would have to be a special relationship between participant and founder that would run beyond the usual hands-off nature of a founder,[246] who, in the ordinary course, spins up a chain and then allows the market to unfold.

F. Self-Help

Having looked through the foregoing theories sounding in criminal law, contract, intellectual property, personal property,

---

[241] *See* WERBACH, ARCHITECTURE OF TRUST, *supra* note 11, at 133–35.

[242] *Id.*

[243] *Id.*

[244] *Id.*

[245] *Id.*

[246] *See* Carla L. Reyes, *(Un)Corporate Crypto-Governance,* 88 FORDHAM L. REV. 1875, 1907–16 (2020).

unjust enrichment, and fiduciary duty, we must come full circle. Gaming companies in the 2000s did not rely on court permission to block game currency duping: they engaged in self-help, and simply deleted currency they determined had been duped.[247]

Self-help is more complicated in the Web3 space, not least because of the personal property interests of legitimate token holders and the decentralized nature of blockchain projects—self-help by whom? Yet prompt and decisive action by the community to block and limit the damage of a crypto-counterfeiting attack is an absolute necessity. Infinite mint attacks happen quickly, and unless they are stopped in real time, a blockchain project will collapse as the counterfeit tokens swamp legitimate ones. Node operators must coordinate to patch and update the software, block an exploiter's IP address during the attack, and remain vigilant against attempts to circumvent blocks. Once the node software is updated and the bug fixed or the hack blocked, the community must find some way to rapidly come together to prevent the counterfeit tokens from flooding the economy, by forking the chain to remove the exploiter's ill-gotten gains or by blacklisting the addresses that hold identifiable counterfeit tokens, so as to lock them in place. (These are in effect the same move: the updated blockchain software simply would not recognize transfers to or from accounts stuffed with counterfeit tokens, effectively burning the tokens by making them non-transferable.)

Knowledge of the above legal framework permits node operators, blockchain curating entities, and legitimate token holders to understand what they can and cannot do in response to the emergency of an infinite mint attack, and how to minimize the risk of project collapse or lawsuits by innocent parties caught up in the efforts to stop the attack. And, of course, after an attack the community must organize in some way to pursue the causes of action and remedies discussed above.

CONCLUSION

The law must adapt to address the harms of crypto-counterfeiting. This is both ironic and inevitable. It is ironic because the prevention of crypto-counterfeiting is the entire point of a blockchain. Blockchain has been used for many ends for

---

[247] *See* LASTOWKA, *supra* note 44, at 24.

which it is not suited; the prevention of duplication of currency is the one thing that the system seemed to do well. Yet as bad acts by blockchain project organizers, hacks on blockchain projects like The DAO, or the use of exploits in infinite mint attacks proliferate, these supposedly invulnerable blockchain systems fall prey to inevitable bugs, intentional exploits, or unintended back doors in the code that permit the wrongful creation of extra tokens or the double spending of tokens. The reliance on purely technological solutions has also caused actors in the blockchain space to forgo developing legal instruments and theories that would provide governance should the worst happen. Crypto developers and communities must rediscover and develop legal constraints against bad behavior—standard in other virtual economy contexts like virtual worlds—such as EULAs and Terms of Use. They must then add the development of legal arguments around personal property and unjust enrichment to explain clearly to courts how crypto exploits steal value from individual token holders and from the entire community for whose benefit tokens are issued.

This will become increasingly important as crypto projects pass through the so-called recent crypto winter, an ongoing industry-wide downturn in value precisely caused by the lack of governance described in this Article.[248] Wild-West-style arguments, such as the argument that all transactions executed by the software, even those obviously resulting from a hack, bug, or exploit, are valid, must be soundly rejected in the courts. If such arguments hold sway, crypto projects as a whole will simply fail. Given human greed and ingenuity, the failure of technological safeguards against crypto-counterfeiting is inevitable, and the law must adapt to enable project participants and other affected entities to move quickly to prevent and fix the damage exploits cause.

At least the damage is straightforward to describe: by wrongfully causing a system to inflate the number of tokens on the market, by duping it, double spending it, counterfeiting it, or flooding the market with tokens that were supposed to be held back to reward community members for securing the integrity of

---

[248] *See* Wayne Duggan, *What Is Crypto Winter?*, FORBES (Apr. 20, 2023), https://www.forbes.com/advisor/investing/cryptocurrency/what-is-crypto-winter/ [https://perma.cc/U27M-XA68].

the blockchain, bad actors undermine the foundations of a blockchain project. First, causing a blockchain system to inflate the number of tokens wrongfully dilutes the holdings of legitimate token holders. Second, and arguably more importantly, exploiting a system to cause it to inflate the number of tokens wrongfully undermines the entire principles of artificial scarcity and digital integrity on which the blockchain's value proposition rests. The entire point of blockchain was to create virtual money and property analogs that worked because of artificial scarcity. Money simply ceases to function if it is subject to runaway inflation, whether that inflation is due to government hyperinflation or a bad actor inflating the supply of crypto-tokens. Blockchain projects can no more brook crypto-counterfeiting than a nation-state government can permit rampant counterfeiting of its fiat currency.

This basic description of the problem will necessarily generate legal solutions. The obvious disconnect between the fundamental nature of blockchain projects and attempts to justify hacking, exploiting, or back-dooring of such systems presents too clear and compelling a framework to avoid legal sanctions long-term. And indeed, the common law has already begun to work itself out clearly. It has begun to recognize legal rights of conversion in intangible digital objects, and replevin of digital assets will soon follow behind. It is simply not conceivable that valuable intangible rivalrous assets could be taken without any recourse to compel their return. Similarly, the strength of the narrative against crypto-counterfeiting is strong enough to drive legal recognition of what is obviously true: from the first days of virtual economies, digital asset counterfeiting damaged and disrupted online digital value ecosystems. The solution is straightforward. Those who wrongfully take or exploit a system to cause the generation of tokens that should never have existed must either destroy the tokens or turn them over to be destroyed. That is the remedy that fits the problem and restores both the integrity of the blockchain's scarcity of value and protects the holdings of legitimate owners of crypto-tokens.