NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 24, ISSUE 4: MAY 2023

ENFORCING PERSISTENT "SMART CONTRACTS": ADMIN KEYS AND THE MYTH OF DECENTRALIZED FINANCE?

Max Parasol*

"The only way that you can truly feel secure while using these DeFi products currently is to trust in the competency of the team and their ability to secure their admin key."–DeFi Watch[1]

This Article discusses the possible practical legal enforcement of disputes on an Ethereum blockchain. It contains two key ideas that may help courts to enforce smart contract dispute determinations. First, it begins by discussing how smart contracts work on the Ethereum network, noting they are less like legal contracts and more like lines of self-executing computer code known as "persistent scripts." They are designed to be "alegal." This is the important starting distinction for understanding the possible enforcement of so-called "smart contracts." As persistent scripts have self-executory capabilities, this idea is important to understanding how a court may actually resolve a dispute that is likely more transactional than contractual. Crucially, this concept of persistent scripts explains why admin keys exist.

Secondly, and relatedly, the private keys, known as "admin keys," held by blockchain platform administrators could potentially be used for legal enforcement. Admin keys are connected to the persistent script conception, as they are often created for blockchain

* Dr. Max Parasol is a Research Fellow at the RMIT Blockchain Innovation Hub. Email: max.parasol@rmit.edu.au. He was previously a Research Fellow at UNSW Sydney, researching FinTech. The Author would like to thank research assistant Maria Lai for her help in preparing this manuscript. This research was supported by the Australian Government through the Australian Research Council's (ARC) Laureate Fellowship (project no. FL200100007). The views expressed are those of the Author and not the Australian Government or the ARC.

[1] Chris Blec, *What Is Admin Key Risk?*, GITHUB (Feb. 24, 2020), https://github.com/chrisblec/defiwatch/blob/master/admin-key-config-and-opsec/what-is-admin-key-risk.md [https://perma.cc/SZE5-88PL].

platforms to modify the rules of a transaction. For example, they can be utilized if a hack or coding error occurs. While, in a decentralized world, no "admin" may ever want to hand over their private keys, a multi-signature arrangement could lead to some admins turning over keys to remove another admin with whom conflict exists. This is a plausible—but still problematic—scenario. Critically, the challenges of legal enforcement through admin keys and other options such as governance tokens are explained in this Article. This Article is purely theoretical as of early 2023.

TABLE OF CONTENTS

I. INTRODUCTION

Traditionally, to pursue enforcement of any contractual dispute, a lawyer might start by asking where the assets are located. In private international law, a party must sue a debtor where the debtor resides, and the party must also enforce a judgment there.[2] Where the debtor resides is a complex factual matrix to answer for "smart contracts." Blockchain-based smart contracts, specifically, the immutability and pseudo-anonymity offered by blockchains make this a wicked problem. Immutability is important because smart contracts are not like other apps. If, for example, there is a bug in Microsoft Word, then Microsoft could produce a patch update to fix the glitch. Yet blockchains are immutable and persistent and will continue to code.[3] It might be possible to fork the blockchain to before the smart contract was executed, and re-design future outcomes, but bugs in a persistent smart contract cannot be patched.[4]

However, "admin keys," which are the private keys held by the blockchain platform administrators, are another way to resolve this issue of immutability. As described in this Article, admin keys are canvassed as a complex but plausible way to fix a glitch or potentially right a legal wrong. In fact, this issue of immutability

---

[2] Australian law, for example, generally recognizes the autonomy of the parties to choose the system of law that will apply to their contract. That choice is to be found by an express choice of law clause that will make the parties' intention clear (e.g., the phrase "Governing Law" or interpreting the contract to ascertain whether the parties intended to choose a particular system of law) or, if no intention is ascertainable, by identifying the proper law of the contract.

"The contract choice of law rule has remained unchanged since the 1930s when the High Court accepted the principle of party autonomy. The choice of law rule requires enforcement of the parties' actual choices of law, whether expressed or not. If there is no effective choice, then the law of the legal system with the closest and most real connection to the contract—the objective proper law—is applied." Mary Keyes, *Improving Australian Private International Law*, *in* AUSTRALIAN PRIVATE INTERNATIONAL LAW FOR THE 21ST CENTURY: FACING OUTWARDS 15, 32 (Andrew Dickinson et al. eds., 2017).

[3] *See* discussion *infra* Section I.C.

[4] Forking is when source code from an open-source software program is used to develop an entirely new program.

currently presents an unprecedented level of enforcement difficulty.[5] There is a broad spectrum of possibilities for where the assets reside—such as the possibility of a multi-jurisdictional location of assets.[6]

The next key issue (intertwined with the problem of where the assets may be located) is ascertaining the identity of the contracting parties and how a creditor could enforce their rights and the right of the promise. Numerous related questions will apply; for example, how could the board of a company fulfill its duties if it cannot guarantee the identity of the contracting parties?[7] Further, identifying the actors connected to the wallet addresses on the blockchain is complex. There is a lot of forensic analysis required to identify people.[8] Importantly, what if the actor in the contract is not a person (i.e., another algorithm or a bot)?[9] Thus, the problem this Article addresses is how to balance enforcement practicalities and contractual legal principles with the reality of how blockchain technology is deployed in smart contracts. Admin keys are one complex but plausible option.

In many ways, it is a wicked problem. There is a continuing risk that the law does not engage with issues early enough as technology advances.[10] Further, the law tends to look to the solutions of the past.

---

[5] Rodrigo Coelho et al., *Supervising Cryptoassets for Anti-Money Laundering*, FSI INSIGHTS ON POL'Y IMPLEMENTATION 19 (Apr. 2021), https://www.bis.org/fsi/publ/insights31.pdf [https://perma.cc/DEY4-5DTK].

[6] *See* discussion *infra* Section I.E.

[7] *See* Richard Mitchell et al., *Shareholder Protection in Australia: Institutional Configurations and Regulatory Evolution*, 68 MELB. UNIV. L. REV. 15, 32 (2014). Directors of corporations are subject to legal duties and the common law duty to act with care, skill, and diligence. *See, e.g.*, Corporations Act, 2001 (Cth.) § 180 (Austl.)

[8] Coelho et al., *supra* note 5.

[9] *See* Morit Zwang et al., *Detecting Bot Activity in the Ethereum Blockchain Network* (2018), https://arxiv.org/pdf/1810.01591.pdf [https://perma.cc/8JJ5-DRFP].

[10] "There is something about law and technological development that seems vaguely incompatible. One is reminded of references to the inability of law to 'keep up' with changes in technology. Such claims are usually made in the absence of any meaningful definition of what it means for law to 'keep up' with change. Most technological developments do not even generate a need to 'catch up.' All conduct, including conduct aided by technology, is subject to law. It is

But which comes first, the chicken or the egg (the tech or the law; the blockchain or the law)?[11] That determines how this problem could be solved. However, we know which came first: blockchain (whose supporters, such as Ethereum Founder Vitalik Buterin, see the technology as a law itself, discussed below). Then, the legal system adapted to address these novel issues. Thus, this Article considers, (1) the limitations of and (2) the applicable mechanisms of blockchain technology in resolving the issue of contractual disputes, while noting the relevant existing legal solutions as relevant reference points.

This Article focuses on Ethereum smart contracts, as the release of Ethereum and its Solidity programming language have been the drivers behind the growth in smart contracts since 2015.[12] Since then, numerous other blockchains have emerged and seek to compete with Ethereum in smart contract applications.[13]

---

murder to kill whether one uses bare hands or a newly-designed high technology device. The latest model of Holden is still subject to ordinary rules of the road. In most instances, there is little 'catching up' to do." Lyria Bennett Moses, *Adapting the Law to Technological Change: A Comparison of Common Law and Legislation*, 26 UNIV. N.S.W. L.J. 394, 394 (2003).

[11] *See generally* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE (1999). An updated version of the book was published in 2006. *See* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2006).

[12] *See Why Are Most dApps Built on Ethereum?*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/dapps-ethereum-decentralized-application [https://perma.cc/UT46-N88K] (last updated Mar. 23, 2021). *See also* GAVIN ZHENG ET AL., ETHEREUM SMART CONTRACT DEVELOPMENT IN SOLIDITY 10 (2021) ("Solidity is an advance programming language based on smart contract. It has similar syntax as JavaScript. It supports static types, integration, library, and composite user-defined type. It can be compiled into EVM assembly and therefore can be executed on all Ethereum nodes. There are other smart contract programming languages: Serpent, Vyper, and LLL. Undoubtably, Solidity is the hottest, most popular programming language for smart contract. EVM is a runtime sandbox. So all smart contracts rested on Ethereum is segregated from surrounded environment. As a result, smart contract on EVM cannot access network, file system, or other processes on Ethereum.").

[13] For example, Polkadot, Solana, and Binance Smart Chain ("BSC") are other blockchains are arguably catching up with a faster rate of growth. *See* Maria Shen, *Electric Capital Developer Report*, ELEC. CAP.: MEDIUM (Jan. 5, 2022), https://medium.com/electric-capital/electric-capital-developer-report-2021-f37874efea6d [https://perma.cc/52YS-T4SS].

This Article is divided into two parts. Part II introduces Ethereum smart contracts and explains that smart contracts were not conceived as legal contracts by Vitalik Buterin—Ethereum's most well-known founder—but as "persistent scripts" of self-executing computer code within an ecosystem. That ecosystem is crucial to any off-(block)chain enforcement. This persistent code notion within a multi-faceted ecosystem leads to the practical problem of smart contract enforcement by a court. Part III discusses the possibility of legal enforcement through admin keys attached to a blockchain product or protocol. An admin key is typically held by a project's founders or core team to provide special access to make changes to a blockchain project's protocol or smart contract. Protocols and products that are capable of accepting deposits are protected by an admin key. This key is typically an Ethereum smart contract that is capable of upgrading the protocol or product. This means that a court could, in theory, identify someone as the party responsible for parts of the contracts for the purposes of a breach or voided contract. Courts could then freeze the assets for the purposes of adverse judgments.

The persistent script idea is crucial to understanding how a court may *actually* resolve a dispute that is likely more transactional than contractual. The concept of a persistent script explains why admin keys exist in the first place. Thus, this whole discussion is not about taxonomies or semantics, but the necessary mechanical understanding required for possible legal dispute resolution and enforcement.

Supporters of the promise of decentralized finance ("DeFi") may unquestionably deify the high levels of trust derived from the Ethereum blockchain, including its immutability. In reality, for many DeFi platforms, one major and less often mentioned risk is linked to the private keys held by the platform administrators. They have the ability to modify the rules of the contract in an arbitrary manner. Yet admin keys can also provide a possible but still largely undiscussed resolution to this wicked problem of legal enforcement for smart contracts or persistent scripts. This a pathway fraught with obstacles, but it still offers some scope for further research and potential deployment. First, Ethereum smart contracts must be introduced.

II. BACKGROUND: AN "ALEGAL" ETHEREUM ECOSYSTEM

The Ethereum technology ecosystem[14] has evolved exponentially since 2015, and it seeks to create a parallel financial ecosystem without legal intervention. Ethereum is known for serving as a platform that uses smart contracts for building distributed applications ("DApps") on a blockchain.[15] However, Ethereum smart contracts[16] are not aptly named, and this phrase has created hype, mismanagement of expectations, and much misconception about how smart contracts operate.[17] Smart contracts are not, as it is often noted, that smart,[18] and they were not conceived as contracts by Ethereum's most well-known founder Vitalik Buterin.[19] This has been made clear by Buterin.[20] Accordingly, this Article argues that Buterin's original conception should inform the way smart contracts are viewed by legal courts with regards to contractual legal disputes.

The concept of a smart contract remains too complex for the law to account for satisfactorily. In simple terms, smart contracts are

---

[14] Ethereum is the cryptocurrency with the second largest market capitalization behind the first cryptocurrency Bitcoin. Nathan Reiff, *Bitcoin vs. Ethereum: What's the Difference?*, INVESTOPEDIA (Oct. 4, 2022), https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp [https://perma.cc/QY3P-TPR9].

[15] However, there are problems associated with the blockchain, such as high transactions costs known as gas prices (discussed in section D below). *See What is Ethereum and How Does it Work?*, COINTELEGRAPH, https://cointelegraph.com/ethereum-for-beginners/what-is-ethereum-a-beginners-guide-to-eth-cryptocurrency [https://perma.cc/CRX4-7Y49] (last visited Jan. 26, 2023).

[16] Most smart contracts run on the Ethereum platform, though competitors are gaining ground. *See Top Smart Contracts Tokens by Market Capitalization*, COINMARKETCAP, https://coinmarketcap.com/view/smart-contracts/ [https://perma.cc/E7HQ-BTV7] (last visited Mar. 27, 2023).

[17] *See* Kelvin F.K. Low & Eliza Mik, *Pause the Blockchain Legal Revolution*, 69 INT. COMPAR. L.Q. 135, 166 (2020).

[18] Georgios Dimitropoulos, *The Law of Blockchain*, 95 WASH. L. REV. 1117, 1135–36 (2020) ("But, 'the name smart contracts is a misnomer: They are neither smart (there is no cognitive component, simply automatic execution once a precondition is fulfilled), nor a contract in a legal sense.'"); *see also* Low & Mik, *supra* note 17.

[19] *See* discussion about Buterin *infra* Section I.A.

[20] *See infra* Section I.B.

simply computer code stored on a blockchain that execute when predetermined conditions in the code are met. "Fuzzy legal predicates" have trouble subsuming smart contracts, including how they are used, and how the virtual asset aspect of Ethereum fits in with their usage.[21] Notably, incentivized "tokenomics" (and its risks)[22] are part of the bargain.[23] Often, scholarly legal discussions of smart contracts tend to use the supply chain smart contract example (i.e., payment will be automated when the goods arrive, streamlining logistics) to describe how smart contracts operate and interact with an existing legal system. Today, this is an over-simplification of smart contracts. Enterprise blockchains such as supply chain management tools are, in practice, a management tool for companies.[24] The Ethereum technology ecosystem, today, is far more complex.

Twenty-five years after Nick Szabo—the first to envisage smart contracts in 1994[25]—began this smart contract discussion, there remains a lack of consensus as to what constitutes a smart contract. Others have continued to construe smart contracts more broadly than Buterin's ideas. Specifically, opinions diverge as to whether they need to be entirely self-executing, self-enforcing, or reduced to code.[26] Buterin's idea was that these self-executing lines of code would be "alegal."[27]

---

[21] Jeffrey M. Lipshaw, *The Persistence of "Dumb" Contracts*, 2 STAN. J. BLOCKCHAIN L. & POL'Y 1, 1 (2019).

[22] "Tokenomics" refers to the factors that impact the demand and supply of tokens.

[23] *See infra* Section I.E.

[24] *See* Alyssa Hertig, *What Is an Enterprise Blockchain?*, COINDESK (Sept. 14, 2021, 8:14 AM), https://www.coindesk.com/tech/2021/02/19/what-is-an-enterprise-blockchain/ [https://perma.cc/S8PS-CHWU].

[25] Szabo was the first to coin the phrase "smart contracts" in 1994. *See* Nick Szabo, *Smart Contracts* (1994), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html [https://perma.cc/KP8B-926C].

[26] Riccardo de Caria, *Definitions of Smart Contracts: Between Law and Code, in* THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORM (Larry A. DiMattero et al. eds., 2020) 19, 21–23.

[27] Buterin's idea that a legal system would not be needed for Ethereum transactions is explained further below. *See* Allen Scott, *Vitalik Buterin: I Quite*

The implications of this alegality are important[28] because changes to smart contracts, as envisaged by Buterin (and Szabo), are made as building blocks on previous code and should (at least, in decentralized technology theory),[29] (see below) only occur for the purposes of technical maintenance. While a legal wrong may seek to be corrected by a complainant, there must be a viable mechanism to address that wrong. Of course, contracting parties drafting bespoke contracts can always invoke off-chain remedial mechanisms such as a court to address what they perceive as an on-chain injustice, but the question this Article answers is how a court can actually redress and enforce a judgment for a legal wrong on an Ethereum smart contract. Therefore, this Article re-imagines how courts visualize Ethereum smart contracts operate.

Furthermore, the Ethereum ecosystem and DeFi have evolved rapidly since 2015 and seek to create a parallel financial ecosystem for persistent scripts without legal intervention.[30] The ecosystem has expanded rapidly from 2020 to 2022, spurring the rise of DeFi, widespread adoption of nonfungible tokens ("NFTs"),[31] and the

---

Regret Adopting the Term 'Smart Contracts' for Ethereum, BITCOINIST, https://bitcoinist.com/vitalik-buterin-ethereum-regret-smart-contracts/ [https://perma.cc/5L77-WDRF] (last visited Mar. 4. 2023).

[28] *See infra* Section I.E regarding existing dispute resolution mechanisms within the Ethereum ecosystem.

[29] The blockchain protocol, a peer-to-peer transaction system without an intermediary, was developed to avoid regulation and create transactions without a legacy financial institution. *See* Don Tapscott & Alex Tapscott, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD 4–5 (Portfolio, 2016). Part of this community also decries the greed of recent financial crises. *See* Syed Omer Husain, Alex Franklin & Dirk Roep, *The Political Imaginaries of Blockchain Projects: Discerning the Expressions of an Emerging Ecosystem*, 15 SUSTAINABILITY SCI. 379, 380 (2020).

[30] "DeFi" refers to the provision of financial services without an institutional middleman, for example via a public blockchain rather than through a bank. *See Decentralized Finance (DeFi) Policy-Maker Toolkit*, WORLD ECON. F. 6–7 (June 2021), https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/06/DeFi-Policy-Maker-Toolkit-Final.pdf [https://perma.cc/DP96-A59H] [hereinafter *DeFi Policymaker Toolkit*].

[31] *See, e.g.*, Robyn Conti & John Schmidt, *What Is an NFT? Non-Fungible Tokens Explained*, FORBES ADVISOR, https://www.forbes.com/advisor/investing/nft-non-fungible-token/ [https://perma.cc/RZ88-C35D] (last updated Mar. 17, 2023, 12:57 AM).

Metaverse.[32] New business models such as play-to-earn online gaming now exist, where gamers can earn tokens playing computer games enabled by smart contracts.[33] In general, persistent scripts are not isolated contracts between two clearly identified parties, for example, but transactions between parties within a wider technology ecosystem. Ethereum is known for its smart contract capabilities that currently power DeFi (or DeFi DApps) and NFTs, making this discussion more critical and timely.

A. Not Smart Legal "Contracts" but "Persistent Scripts"

Broad literature, including technical computer science, legal, and economic scholarship, describes both strong and weak smart contracts.[34] This Article focuses on auto-executing, real-time transactions—*persistent scripts*—on the Ethereum platform. This Article also focuses upon decentralized smart contracts that utilize distributed ledger technology to facilitate the automated execution of an agreement. Contracts can be entirely or partially expressed in code.[35] Self-enforcing over-collateralized smart contracts[36] means the court will often not be required to enforce them by ordering damages or specific performance.

Ethereum smart contracts were never created to rely on third-party enforcement, but rather they were created as automated transactions that exist in a complex ecosystem with set

[32] The Metaverse is an emerging interoperable network of real-time rendered 3D virtual worlds.

[33] Play-to-earn emerged in 2020–2021 in blockchain gaming and refers to where players can monetize the time they spend playing video games, such as Axie Infinity and the Sandbox.

[34] Raskin notes, "For legal purposes, I will further differentiate between strong and weak smart contracts. Strong smart contracts have prohibitive costs of revocation and modification, while weak smart contracts do not. This means that if a court is able to alter a contract after it has been executed with relative ease, then it will be defined as a weak smart contract. If there is some large cost to altering the contract in a way that it would not make sense for a court to do so, then the contract will be defined as strong." *See* Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305, 310 (2017).

[35] de Caria, *supra* note 26, at 24. *See also* Buwaneka Arachchi, *Chains, Coins and Contract Law: The Validity and Enforceability of Smart Contracts*, 47 AUSTL. BUS. L. REV. 40, 42 (2019).

[36] *See infra* Section I.E.

predetermined rules and pre-existing building blocks. Vitalik Buterin tweeted in October 2018 that he regretted using the name smart contracts. He wrote, "To be clear, at this point I quite regret adopting the term 'smart contracts'. I should have called them something more boring and technical, perhaps something like 'persistent scripts.'"[37] The problem is that lines of code programmed as automated transactions are neither contracts nor particularly smart.[38] The name "smart contracts," while a good marketing ploy, has disrupted analysis and construction of the Ethereum ecosystem.[39] Smart contracts sounded better in 2015, and perhaps, Ethereum may not have achieved the same success with a technical name. In that October 2018 Twitter thread, Buterin further noted, "I do think that persistent scripts controlling assets compete with the legal system on some margins, but so do locks on doors. So [in my opinion] it's wrong to equate them with a specific philosophy of law privatization."[40]

Further, Buterin never envisaged a contract on Ethereum in its initial Whitepaper: "Note that 'contracts' in Ethereum should not be seen as something that should be 'fulfilled' or 'complied with';

---

[37] Vitalik Buterin (@VitalikButerin), TWITTER (Oct. 13, 2018, 1:21 PM), https://twitter.com/vitalikbuterin/status/1051160932699770882?lang=en [https://perma.cc/6BDA-GUF4].

[38] Angela Walch, *Deconstructing "Decentralization": Exploring the Core Claim of Crypto Systems*, CRYPTOASSETS: LEGAL, REGULATORY, AND MONETARY PERSPECTIVES 39 (Chris Brummer ed., 2019); Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains, in* REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 58 (Philipp Hacker et al. eds., 2019); Sarwar Sayeed et al., *Smart Contract: Attacks and Protections*, 8 I.E.E.E. ACCESS 24416 (2020), https://ieeexplore.ieee.org/abstract/document/8976179 [https://perma.cc/J8FH-TUHQ]. *See also* LESSIG, *supra* note 11.

[39] David G.W. Birch, *They're Not Smart and They're Not Contracts*, FORBES (Sept. 4, 2021), https://www.forbes.com/sites/davidbirch/2021/09/04/theyre-not-smart-and-theyre-not-contacts/?sh=6240fbc4397e [https://perma.cc/UFR2-TF5Q].

[40] Vitalik Buterin (@VitalikButerin), TWITTER (Oct. 13, 2018, 1:22 PM), https://twitter.com/VitalikButerin/status/1051161357104635906 [https://perma.cc/SY6H-F8VH].

rather, they are more like 'autonomous agents' that live inside of the Ethereum execution environment."[41]

In addition, an earlier version of the Ethereum Whitepaper described a "contract" as:

> [E]ssentially an automated agent that lives on the Ethereum network, has an Ethereum address and balance, and can send and receive transactions. A contract is "activated" every time someone sends a transaction to it, at which point it runs its code, perhaps modifying its internal state or even sending some transactions, and then shuts down.[42]

The most profound characteristics of a smart contract are its self-enforcing and self-executory capabilities.[43] In practice, every Bitcoin or cryptocurrency transaction is technically a simplified

---

[41] VITALIK BUTERIN, A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM, ETHEREUM (White Paper, Dec. 2014), https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf [https://perma.cc/AF34-53LR] [hereinafter ETHEREUM WHITEPAPER]. The Ethereum Whitepaper that was published in 2013 has undergone internal revisions since. The Whitepaper has also been complemented by a series of subsequent technical papers, including Gavin Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger*, ETHEREUM (Yellow Paper, 2014), https://web.archive.org/web/20140410013339/http://gavwood.com/Paper.pdf [https://perma.cc/Q8Q3-RFET]; Vitalik Buterin, *Ethereum 2.0*, ETHEREUM (Mauve Paper, 2016), https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf [https://perma.cc/ACX2-8XCW]; Gavin Wood, *Polkadot: Vision for a Heterogeneous Multi-Chain Framework*, ETHEREUM (Polkadot Paper, 2016), https://polkadot.network/PolkaDotPaper.pdf [https://perma.cc/6GR6-PKU4]. Each of these papers pushes "smart contract" usage in new directions, including Gavin Wood's Polkadot Paper suggestion to move towards the development of a "contract language." These narrower uses are somewhat outside of the scope of the present analysis, but certainly demand much closer scrutiny.

[42] Vitalik Buterin, *Created Old Ethereum Whitepaper (Markdown)*, ETHEREUM (White Paper, Apr. 9, 2014), https://github.com/ethereum/wiki/commit/b6f357b32f6cf90b588fb2717572664e315c1cd3#diff-ef6c54cac698aab0469a6ba11b8a72dd [https://perma.cc/GD77-VXDK] [hereinafter *Old Ethereum Whitepaper*].

[43] Alexander Savelyev, *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classical Contract Law* 15 (Nat'l Rsch. Univ. Higher Sch. Econ. Working Paper No. WP BRP 71/LAW/2016 2016), https://wp.hse.ru/data/2016/12/14/1111743800/71LAW2016.pdf [https://perma.cc/Y4J7-RT4S]; Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 320, 335, 353 (2017); Arachchi, *supra* note 35, at 45.

version of a smart contract—automated lines of code.[44] This is why the persistent script idea is very useful to understanding how a court may resolve a dispute that is most likely *more transactional than contractual*. Based on this idea, legal enforcement would be a problem from the outset: "Buterin was clearly conscious about contract enforcement needs—and Ethereum's potential inability to satisfy those needs."[45] Buterin clarified that he did not anticipate this system of smart contracts would rely on any third-party enforcement mechanisms: "Note that financial contracts of any form do need to be fully collateralized; the Ethereum network controls no enforcement agency and cannot collect debt."[46]

In other words, Buterin designed fully collateralized, self-automated lines of code, not a legal agreement to contract. This created a difference in how he foresaw the smart contracts being used, in comparison to legal contracts. Each node has the rules predetermined in the code, and all smart contracts exist within guiding parameters, as explained below:

> Unlike most blockchain networks which are described as a distributed ledger, Ethereum is what's considered a distributed state machine, containing what's known as the Ethereum Virtual Machine (EVM). This machine state, which all Ethereum nodes agree to keep a copy of, stores smart contract code and the rules by which these contracts must abide. Since every node has the rules baked in via code, all Ethereum smart contracts have the same limitations.[47]

This is important. "Because of Ethereum's EVM (Ethereum Virtual Machine, the part of Ethereum that allows it to run software), the full spectrum of possible applications are able to be built and added

---

[44] Layer-two solutions are in development to expand the Ethereum network's functionality (i.e., handling transactions off the Ethereum Mainnet (layer 1)) for speed and efficiency. *See Scaling*, ETHEREUM, https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/ [https://perma.cc/6NLL-SRAT] (last updated Feb. 27, 2023).

[45] CleanApp, *Crypto's Founding Fallacy: How Mistakes in the "Smart Contract" Genesis Block Weaken the Whole Chain*, MEDIUM (Jan. 31, 2019), https://medium.com/cryptolawreview/cryptos-founding-fallacy-aaa151b795ff [https://perma.cc/Y8BZ-KB8A].

[46] *Old Ethereum Whitepaper*, *supra* note 42.

[47] *What is a Smart Contract, and How Does it Work?*, COINTELEGRAPH, https://cointelegraph.com/ethereum-for-beginners/what-are-smart-contracts-guide-for-beginners [https://perma.cc/T5WY-ZULJ] (last visited Apr. 1, 2023).

to the ecosystem."[48] So, Ethereum operates as an ecosystem: "This is what turns Ethereum from a single use-case like Bitcoin, to an infinite set of use-cases, only limited by the imagination and engineering skills of the builders who are building on it."[49]

Ethereum-based smart contracts empower parties to engage in peer-to-peer transactions without an intermediary. Rather, validator nodes or "miners" automatically process transactions in accordance with cryptographically-based consensus algorithms.[50] These smart contracts seek to increase the efficiency of doing business whilst eliminating the costs of engaging third parties.[51] This means that so-called smart contracts are not only *more transactional than contractual* self-executing persistent scripts of code, but they also exist in a complex ecosystem with predetermined rules and pre-existing building blocks. "The more apps that are on the computer-side of the spectrum the more self-perpetuating structures there are inside Ethereum, and the more Ethereum is itself a self-perpetuating system-of-systems."[52]

This alegal ecosystem is important. For example, a key factor which hinders the adaptability of smart contracts is the immutability of the blockchain. A party cannot discretionarily suspend a smart contract's automated enforcement unless a mechanism allowing for this to occur was originally programmed into the contract.[53] This contrasts a transaction governed by an ordinary contract, where a vendor is able to make a decision to excuse a customer's late payment in the interests of "preserving [a] long-term commercial

---

[48] David Hoffman, *Ether Is Equity*, BANKLESS (Jan. 29, 2020), https://newsletter.banklesshq.com/p/ether-is-equity [https://perma.cc/C8MQ-D5FX].

[49] *Id*.

[50] Miners are those who solve complex cryptographic hash puzzles (via computers) to verify blocks of transactions that are updated on a decentralized blockchain ledger. It is a mechanism to verify blockchains so no one single person controls the ledger.

[51] Mark Giancaspro, *Is a 'Smart Contract' Really a Smart Idea? Insights From a Legal Perspective*, 33 COMPUT. L. & SEC. REV. 825, 825 (2017).

[52] Hoffman, *supra* note 48.

[53] Jeffrey D. Neuburger et al., *Smart Contracts: Best Practices* (2019), https://prfirmpwwwcdn0001.azureedge.net/prfirmstgacctpwwwcdncont0001/uploads/dc2c188a1be58c8c9bb8c8babc91bbac.pdf [https://perma.cc/N49V-D7E8].

relationship."[54] Thus, this complex ecosystem with predetermined rules and pre-existing building blocks was designed to be alegal but has security mechanisms built in, which are discussed further below. Moreover, solutions can be provided by contracting parties through the design of their smart contracts (such as over-collateralization, allocation of liability, and specification of the governing law and dispute resolution mechanisms, if so desired for bespoke smart contracts).[55] Collateral assets are now commonly used in DeFi applications. These DApps use Ethereum, for example, as a collateral asset.

Yet, where no provisions for self-enforcement are made, possible outside enforcement remains the key gateway issue. How a court could enforce such a decision is still *the* outstanding key issue. Thus, this Article explores how that might be done by a court by explaining the role of admin keys for blockchain and crypto products. While no admin may ever want to hand over their private keys, a multi-signature ("multi-sig") arrangement could lead to some admins turning over keys to remove another admin with whom conflict exists. Admin keys are like the keys that drive a car, so it may have to involve legal pressure to make the admin hand over the private key. Thus, a court may enforce admins handing over their unique password logins in legal disputes.

Certainly, legal enforcement is still a worthwhile discussion, despite persistent scripts being considered more transactional than contractual, as "applications built on blockchains are [decentralized] ecosystems that are nonetheless [often] built by [centralized] firms."[56] This dilemma, where a centralized firm builds a decentralized product, and the concept of persistent scripts are key reasons why admin keys exist and impact possible legal

---

[54] Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/ [https://perma.cc/QW3V-2DGJ].

[55] *See infra* Section I.E.

[56] Chris Berg, *Rent Seeking in Blockchain Governance: The Awkward Transition from Market Decision Making to Non-market Decision Making* 1 (Mar. 8, 2021), https://ssrn.com/abstract=3801103 [https://perma.cc/8PR9-UN8W].

enforcement. The decentralized movement itself has not yet figured how these protocols and products could be completely automated.

B. Bespoke Smart Contracts Could be Common Law Contracts; Persistent Scripts are more Complex

To be considered a contractual dispute, first, a contract must exist in law. Bespoke smart contracts *could* amount to common law contracts,[57] yet persistent scripts present a more complex problem (to be expanded upon in the next section). Persistent automation will limit intervention by a court until after the execution of the transaction and transfer of the funds, shifting the litigation or dispute resolution burden to the innocent party. Yet, this Section argues that both a legally enforceable bespoke smart contract and a persistent script smart contract can still meet all the traditional elements of a binding contract.[58]

---

[57] Common law contracts are defined as "an agreement between two or more persons as to something that is done in the future by or both of them," while having "legal effect." CHARLES L. KNAPP ET AL., PROBLEMS IN CONTRACT LAW: CASES AND MATERIALS 2 (9th ed. 2019).

[58] "When a digital agreement to enter into a legally binding contract is made between two willing and capable individuals, and the contract is hosted in Australia, Australian Law recognizes the contract as legally binding given that sufficient conditions are met for the contract to be legally permissible. A distributed ledger system can be configured to enable transactional smart contracts to contain the expression to participate in the value transaction along with the necessary contractual terms for the contract to be considered consistent with Australian Contract Law. The necessary terms within Australian Contract Law for a value exchange to be legally enforceable include an offer made by one party, the acceptance of the offer by a second party and a consideration, which is often money, is required to be paid between the parties. Additionally, both parties involved within the contract are required to have a mutual intent and capacity to enter into a legally binding agreement. The smart contracts are executed through permissioned user interaction within the system, as an automated feature of the value exchange for derivatives between system users. Interactions are triggered through a client program hosted on same server as the blockchain and operating through a separate server port to enable communications between the separate system modules." Julian Adam Wise et al., *Legal Smart Contracts for Derivative Trading in Mining,* 35 KNOWLEDGE ENG'G REV. 1, 2 (2020) (citations omitted). *See* Brian Coote, *The Essence of Contract: Part I*, 1 J. CONT. L. 91, 99–107 (1988). *See generally* P.S. Atiyah, *Contracts, Promises and the Law of Obligations*, 94 L.Q. REV. 193 (1978).

In common law contract law, to form a binding contract, there must be (a) an offer and acceptance of that offer; (b) consideration, or some value exchange for that offer; (c) an intention to form a contract; and (d) a certainty of the terms of the contract.[59] Each stage offers problems for Ethereum smart contracts. For example, (a) when does offer and acceptance occur on the smart contract? If it is an instantaneous offer and acceptance, is that a transactional persistent script that continues to the next instantaneous transaction or is it a contractual agreement? Also, as these transactions occur in real-time, there can be little opportunity for enforcement of an award of damages. Further, (b) what qualifies as consideration for the offer, and how is this numerical value captured? The order of events on the chain is crucial for Ethereum based-smart contracts. In addition, (c) for transactions conducted on a blockchain, the parties might be in a "decentralized" relationship that the law has yet to define precisely.[60] Also, smart contracts facilitate the execution of pseudonymous transactions. Although this may be attractive for some seeking anonymity, it may make it more difficult for a plaintiff to identify who legal proceedings should be initiated against, due to the pseudonymity provided to the parties.[61] And, finally, (d) how

---

[59] "It is of the essence of contract, regarded as a class of obligations, that there is a voluntary assumption of a legally enforceable duty." *See* Ermogenous v. Greek Orthodox Community of SA Inc, (2002) 209 C.L.R. 95, 105 [24] (Austl.) (citations omitted). To be a legally enforceable duty there must, of course, be identifiable parties to the arrangement, the terms of the arrangement must be certain, and, unless recorded as a deed, there must generally be real consideration for the agreement. *Id.* Yet "[t]he circumstances may show that [the parties] did not intend, or cannot be regarded as having intended, to subject their agreement to the adjudication of the courts." *Id.*

[60] With crypto asset exchange-traded products attracting significant attention globally, the Australian Securities and Investments Commission ("ASIC") released *Consultation Paper 343 Crypto-Assets as Underlying Assets for Exchange-Traded Products and other Investment Products* in July 2021 to consider how to regulate exchange-traded products. *See 21-153MR ASIC Consults on Crypto-asset Based ETPs and Other Investment Products,* AUSTL. SEC. & INVS. COMM'N (June 30, 2021), https://asic.gov.au/about-asic/news-centre/find-a-media-release/2021-releases/21-153mr-asic-consults-on-crypto-asset-based-etps-and-other-investment-products/ [permanent link unavailable].

[61] Giancaspro, *supra* note 51, at 837; Arachchi, *supra* note 35, at 56; Mateja Durovic & Andrew Janseen, *Formation of Smart Contracts under Contract Law*,

certain are the terms? This is especially pronounced for on-and-off-chain transactions (see below in section D), where the recording of time is contained outside the blockchain smart contract.[62] However, while the transparency of transactions on a permissionless blockchain may instill confidence for users, a possible downside is that the substance of a smart contract will not remain confidential. Yet, this also means a court could find certainty in the terms of the agreement as per the code.[63]

These issues are more easily addressed by bespoke contracts, meaning contracts that are created as an agreement, say between two parties. A wholistic front-end legal approach would consider bespoke contractual drafting issues in the first place, that is, as per its drafting. The immutable nature of smart contracts makes it impossible to include changes in the operation of the contract. For bespoke smart contracts, a possible solution would be to leave certain terms of the contracts modifiable, while restricting others from modification.

For example, the fact that payment is necessary would be an immutable term, while the length of time a debtor has before she is in default could be modifiable.[64] Another possible, yet very theoretical, solution could be a system in which the relevant jurisdiction creates a publicly available database and application programming interface ("API") of relevant legal provisions. These would be provisions related to the terms of the contract. The smart contract could theoretically draw upon these terms and would be able to update the relevant provisions in accordance with the jurisdiction's update of the database.[65] The usual rules relating to contract formation will first need to apply to determine the legal status/existence of a smart contract. Thus, whether a particular smart

---

in THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORM 72 (Larry A. DiMattero et al. eds., 2020).

[62] *See* Low & Mik, *supra* note 17.

[63] Cristina Poncibo & Larry A. Dimattero, *Smart Contracts: Contractual and Noncontractual Remedies*, *in* THE CAMBRIDGE HANDBOOK OF SMART CONTRACTS, BLOCKCHAIN TECHNOLOGY AND DIGITAL PLATFORM 133 (Larry A. DiMattero et al. eds., 2020).

[64] Raskin, *supra* note 34, at 327.

[65] *Id*.

contract amounts to a legally binding contract will likely depend on the type of smart contract at issue and the factual matrix within which it operates.[66]

The legal issues are addressable by contract law, which leaves the freedom to innovate with smart contracts, while providing underlying security of potential recourse when things go wrong. In code-is-law[67] type arguments (where the code is the law rather than statute or case law), smart contracts have been characterized as "entire agreement[s]."[68] When using smart contracts, the computer code of the contract constitutes its terms, and any written documents serve as *just an explanation*.[69] Yet, even in the absence of explicit contractual provisions, courts could possibly resolve contractual disputes using existing laws.

Any unravelling of an auto-executing smart contract, say for example induced by fraud, will likely require restitution using fiat money substitutes and a court to consider equitable principles. There are two ways to consider smart contracts: Either smart contracts should be seen as the master agreement which determines the content of the legal contract or "[courts] will construe the underlying code according to long-standing principles of contract law interpretation and, if necessary, the help of experts."[70]

Enforcement, however, is still complex. As this entire Article notes, the first step will be for a court to determine whether it has

---

[66] For further analysis of whether smart contracts have a legally binding effect in the US, the UK, Australia, Canada, Germany, France, China, and South Africa, *see* R3 & Norton Rose Fulbright, *Can Smart Contracts Be Legally Binding Contracts?* (Nov. 2016), NORTON ROSE FULBRIGHT https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/norton-rose-fulbright--r3-smart-contracts-white-paper-key-findings-nov-2016.pdf [https://perma.cc/ZQP4-4AXR] [hereinafter *R3 and Norton Rose Fulbright White Paper*].

[67] LESSIG, *supra* note 11. *See also* Marco Rizzi & Natalie Skead, *Algorithmic Contracts and the Equitable Doctrine of Undue Influence: Adapting Old Rules to a New Legal Landscape*, 14 J. EQUITY 301, 302 (2020).

[68] Werbach & Cornell, *supra* note 43, at 348.

[69] *Id*. at 351.

[70] PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 78 (2018).

any mechanism to enforce a judgment.[71] Then, it may consider if the smart contract is unenforceable, void, or voidable.[72] Yet, despite the legitimacy of these concerns, many commentators have contended that smart contracts can be legally binding under common law contract law if they satisfy the requisite doctrinal requirements for contract formation.[73] But for persistent scripts, as outlined in this Article, contractual enforcement is more complex. Contracts also require off-chain certainty for enforcement.

So even if "smart contracts" are viewed as "legal contracts" by a court (based on contract law principles), because they are autonomous and self-enforcing agreements, the term "smart contracts" remains an inappropriate ill-description. First, a contract is a legally binding agreement.[74] On the other hand, smart contracts, or persistent scripts *must* be coded to be legally enforceable against the parties in a jurisdiction with dispute resolution mechanisms.[75] As noted, contracting parties can always invoke off-chain remedial mechanisms, such as a court, to address what they perceive as an on-chain injustice. Even smart contracts explicitly stating those terms cannot be easily enforced by a court, due to the following constraints:

---

[71] *See supra* Part I.A.

[72] In this case, the courts will have to undo the transaction after it has been executed using the tools of rescission and restitution, perhaps via fiat currency substitutes and other options discussed below in Part II.

[73] *See R3 and Norton Rose Fulbright White Paper, supra* note 66, at 19; Arachchi, *supra* note 35, at 48–58; UK JURISDICTION TASKFORCE, LAWTECH DELIVERY PANEL, *Legal Statement on Cryptoassets and Smart Contracts* 31-4 (Nov. 2019). *See, e.g.,* Electronic Transactions Act, 1999 (Cth.) § 8, 15C; Electronic Transactions Act, 2000 (N.S.W.) § 7, 14C. Subsequently, once there is precedent confirming that smart contracts can be legally binding agreements, it is likely that businesses will be more inclined to innovatively experiment with their deployment.

[74] In general, in Australia, unless there are statutory requirements, a contract does not necessarily have to be wholly written. It may be partly written and partly oral, wholly oral, or inferred from conduct. *See* J.W. CARTER, CARTER ON CONTRACT [01-010] (2021), LexisNexis.

[75] Like a standard contract, the terms must be certain to be self-enforcing.

- The difficulty of coding third party *enforcement* (this would require off-chain[76] commitments by the parties);[77]
- The "usage of legal forms to create alegal processes" (resulting in legal relations that are "more complex than traditional contracts, while offering a fraction of traditional contract protections and benefits");[78] and,
- Incorrect usage of legal terms to "write your own law" could result "in more, not less, legal scrutiny" and increasing transaction costs.[79]

In theory, bespoke smart contracts create significant doctrinal and practical issues to contractual relief by a court. Returning to the idea of legal enforcement of a dispute on a transactional persistent script in practice is even more problematic.

C. Persistent Scripts are Coded in a Sequence on Ethereum

This Article previously introduced the concept of persistent scripts, and discussed how bespoke smart contracts could be considered common law contracts. Revisiting the concept of persistent scripts, this Section explains that in Ethereum's programming language, Solidity, the ordering of the transactions in the code is critical to a transaction.[80] This has further implications for legal enforcement such as in contractual disputes and any proposed legal liability.

As noted above, for Buterin, smart contracts are embodied by the concept of persistent scripts, and this layered, automated coding system holds significance for contractual disputes and any proposed legal liability. Smart contracts—or persistent scripts, as outlined in this Article—are auto-executing and auto-enforcing and cannot be

---

[76] Off-chain refers to parts of the agreement outside the blockchain.

[77] João Pedro Quintais et al., *Blockchain and the Law: A Critical Evaluation*, 2 STAN. J. BLOCKCHAIN L. & POL'Y. 86, 88 (2019).

[78] CleanApp, *supra* note 45.

[79] *Id.*

[80] Solidity is a programming language created in 2014 by co-founder Gavin Wood as a Turing-complete computer language to interact with the Ethereum Virtual Machine. *See Learn Solidity: What is Solidity?*, ALCHEMY, https://www.alchemy.com/overviews/solidity [https://perma.cc/M6T2-QDSW] (last updated Oct. 4, 2022).

subsequently modified by coders. They are persistent scripts of computer code that create enforceable obligations which can be regarded as binding agreements with the impossibility of breach or tampering.[81]A major difference between a "traditional contract and a so-called smart contract, is that [traditional] contracts create enforceable obligations, whereas smart contract[s] automatically enforce obligations."[82] Smart contracts use automation on a blockchain to compel the performance of obligations. Once parties create a smart contract, payment obligations are automated and there is no reversing them. Szabo's often-cited analogy is that a smart contract is like a vending machine that will automatically complete the transaction, akin to dispensing a Coke can.[83]

Yet, it is more complex than that. The persistence and verifiability of smart contracts allowing third parties to trust the programming and automated results is not part of the vending machine example. Persistence and verifiability are the key characteristics of smart contracts. For example, if someone issues a bond on the blockchain and the bondholder is programmed to get a quarterly interest payment, this interest payment program can be confirmed and verified by anyone with a smart contract on Ethereum, and even the developers cannot alter it after it is finished. In short, no one can alter the system if the program is created properly. Admin keys (explained below) may still offer a back door. In fact, admin keys exist solely because of this issue of persistent scripts and the risk of coding errors or other hazards (described in the next section).

---

[81] Savelyev, *supra* note 43, at 130.

[82] Andrew Luesley, *Unravelling Smart Contracts: Smart Contracts and the Law of Rescission in Canada*, 19 ASPER REV. INT'L BUS. & TRADE L. 155, 156 (2019).

[83] *See* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, FIRST MONDAY (Sept. 1, 1997), https://firstmonday.org/ojs/index.php/fm/article/view/548/469 [https://perma.cc/5DLL-DTHW] ("The vending machine is a contract with bearer: anybody with coins can participate in an exchange with the vendor. The lockbox and other security mechanisms protect the stored coins and contents from attackers, sufficiently to allow profitable deployment of vending machines in a wide variety of areas.").

Szabo's original definition of smart contracts from his 1996 conception is still helpful.[84] From a legal perspective, a smart contract as first defined by Szabo, is "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[85] The offer being made by the vending machine is the entirety of the contractual environment for its transactions—"its performance of the contract is effectively final."[86] Even in Szabo's earliest smart contract definition, there is a clear certainty of a bargain. However, a self-contained ecosystem defined by agreed upon protocols is envisaged without recourse to the courts.[87] That was Szabo's theoretical underpinning of smart contracts born in his 1994 edition of *Smart Contracts*.[88] The founders of Ethereum sought to build this ecosystem with greater functionality for making self-contained agreements on blockchains.[89]

From a technical perspective, the founders of Ethereum utilized persistent scripts or rules that needed to be coded in a certain sequence within the ecosystem, meaning that A must happen before

---

[84] *See* Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996), https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2 [https://perma.cc/8RZ7-T28A] [hereinafter *Smart Contracts 1996 Rewrite*]. The Ethereum Yellowpaper (authored by Gavin Wood, one of Ethereum's co-founders) gives a more formal introduction to "smart contracts:" "Early work on smart contracts has been done by Szabo [1997] and Miller [1997]. Around the 1990s it became clear that algorithmic enforcement of agreements could become a significant force in human cooperation. Though no specific system was proposed to implement such a system, it was proposed that the future of law would be heavily affected by such systems. In this light, Ethereum may be seen as a general implementation of such a crypto-law system." *See Ethereum: A Secure Decentralised Generalised Transaction Ledger Berlin Version*, ETHEREUM 2 (Yellow Paper Berlin Version beacfbd, Oct. 24, 2022), https://ethereum.github.io/yellowpaper/paper.pdf [https://perma.cc/RR7J-SD8R]. *See also* Szabo, *supra* note 83; Mark S. Miller, *Computer Security as the Future of Law*, YOUTUBE (Aug. 11, 1997), https://www.youtube.com/watch?v=kOFzisF7aNw [https://perma.cc/9WVL-LDMZ].

[85] *See Smart Contracts 1996 Rewrite*, *supra* note 84.

[86] Werbach & Cornell, *supra* note 43, at 324.

[87] Szabo, *supra* note 25.

[88] *Id.*

[89] *See* ETHEREUM WHITEPAPER, *supra* note 41, at 18.

B can occur. This is a very important point because it means every transaction is part of a wider ecosystem rather than a self-contained, bespoke legal contract. Therefore, Ethereum's programming language Solidity renders the ordering of the transactions in the code as critical to the outcomes:

> DeFi uses a multi-layered architecture. Every layer has a distinct purpose. The layers build on each other and create an open and highly composable infrastructure that allows everyone to build on, rehash, or use other parts of the stack. It is also crucial to understand that these layers are hierarchical: They are only as secure as the layers below.[90]

As noted, the release of Ethereum and the architecture of its Solidity programming language are the drivers behind the growth in smart contracts since 2015,[91] and this layered coding system holds great significance for contractual disputes and any proposed legal liability.

First, the order of these transactions prevents a double spending problem for the network.[92] Proof-of-work ("PoW") means that groupings of tractions (blocks) are established in a certain order for a set price for that block.[93] The so-called "London Fork" of August 2021, which updates the Ethereum protocol, would automate that

---

[90] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, 103(2) FED. RSRV. BANK OF ST. LOUIS REV. 153, 155 (2021), https://files.stlouisfed.org/files/htdocs/publications/review/2021/04/15/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.pdf [https://perma.cc/ETU7-NNNQ].

[91] Stegos, *Smart Contracts Are Useless*, MEDIUM (Feb. 22, 2019), https://medium.com/hackernoon/smart-contracts-are-useless-f710293ec15f [https://perma.cc/R4Q3-DX9L].

[92] Huru Hasanova et al., *A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures*, 29 INT'L J. NETWORK MGMT. e2060 at 3 (2019), https://nmlab.korea.ac.kr/publication/published.papers/2019/2019.01-Survey_on_Blockchain_Vulnerabilities-IJNM.Journal.pdf [https://perma.cc/4ACN-36BK].

[93] Ethereum was launched using the proof-of-work ("PoW") consensus protocol, similar to Bitcoin. The PoW data essentially does two things: allows computer nodes, which secure and guard the platform, to agree on the validity of the information published on the Ethereum network, and thwarts economic attacks on the network.

bidding process for miners to validate transactions on the network.[94] This was designed to increase the certainty of the bargains being made.[95] In 2022, the so-called "Merge" was intended to shift the Ethereum blockchain from PoW consensus mechanism to a proof-of-stake ("PoS") model, intended to be faster and more energy efficient. This would eventually take place in September 2022.[96] The outcome is similar, but the mechanism is different. In PoS systems, a validator is chosen randomly, based in part on how many coins they have locked up, or "staked", in a blockchain network.[97]

Further, "[t]he core philosophy of the DeFi space" is to "build for interoperability."[98] "In DeFi, projects are designed to not only be used as a stand-alone product but also easily integrated into products that can benefit from their functionality."[99] Specifically, the parties' obligations are immutably enshrined as "if-then" rules on the blockchain to be automatically executed.[100] This intentionally reduces the monitoring and enforcement costs which are normally incurred by contractual parties in the course of business.[101]

Thus, Ethereum could be aptly described as a distributed log file with stored procedures. Each node on the network downloads the log file and executes each script.[102] This idea is important as it better

---

[94] EFT Trends, *Ethereum Completes Its 'London' Hard Fork*, NASDAQ (Aug. 6, 2021), https://www.nasdaq.com/articles/ethereum-completes-its-london-hard-fork-2021-08-06 [permanent link unavailable].

[95] *Id.*

[96] *Id.*

[97] *The Merge*, ETHEREUM (Oct. 22, 2022), https://ethereum.org/en/upgrades/merge/ [https://perma.cc/6LCK-C2NR]. Mining refers to a global network of computers running code work to ensure that transactions are legitimate and added correctly to a cryptocurrency's blockchain. Staking serves a similar function to mining, whereby network participants add the latest batch of transactions to the blockchain and earn cryptocurrency in exchange.

[98] Totle, *Building with Money Legos*, MEDIUM (Aug. 17, 2019), https://medium.com/totle/building-with-money-legos-ab63a58ae764 [https://perma.cc/8N66-PDRR].

[99] *Id.*

[100] Werbach & Cornell, *supra* note 43, at 353; Arachchi, *supra* note 35, at 45.

[101] Werbach & Cornell, *supra* note 43, at 335.

[102] "Ether is meant to be used to pay for running *smart contracts*, which are computer programs that run on an emulated computer called the *Ethereum Virtual Machine* (EVM). The EVM is a global singleton, meaning that it operates as if it

explains the "contracting" parties' intent. That is, A must occur before B can occur. This is *not a self-contained contract, but a series of continuing procedures—lines of code that continue to self-execute*.[103] A persistent script grants rights to the participants, where the terms of the contract are enforced by the program's continuing execution. Yet, there are exceptions (such as admin keys and the technical maintenance of hard and soft forking of the code, as explained further below) that provide a window for the law to interact with this process of persistent scripts. This is an important distinction, as, for example, institutional blockchain platforms[104] (typically permissioned[105]) usually (and expectedly) have stated hierarchical structures or a multi-sig arrangement to reverse a transaction, a governing node can be empowered to correct an erroneous entry into the database.[106]

---

were a global, single-instance computer, running everywhere. Each node on the Ethereum network runs a local copy of the EVM to validate contract execution, while the Ethereum blockchain records the changing *state* of this world computer as it processes transactions and smart contracts." *See* ANDREAS M. ANTONOPOULOS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS 26 (2018).

[103] "Miners execute the bytecode inside the Ethereum Virtual Machine (EVM). At present, each miner must execute all transactions of all contracts and hold the current value of all the memory associated with all of the contracts." *See* Peter Robinson, *The Merits of Using Ethereum MainNet as a Coordination Blockchain for Ethereum Private Sidechains*, 35(e30) KNOWLEDGE ENG'G REV. 1, 2 (2020). "Ethereum contracts are programs that control money, which run inside a virtual machine called the EVM. They are created by a special transaction that submits their bytecode to be recorded on the blockchain. Once they are created on the blockchain, they have an Ethereum address, just like wallets. Anytime someone sends a transaction to a contract address it causes the contract to run in the EVM, with the transaction as its input." ANTONOPOULOS & WOOD, *supra* note 102, at 33.

[104] Such as the Australian Stock Exchange's replacement for its CHESS settlement system.

[105] A permissioned blockchain is one where "only authorized members can participate." *See* Tatsuo Mitani & Akira Otsuka, *Traceability in Permissioned Blockchain*, 8 I.E.E.E. ACCESS 21573, 21573 (2020).

[106] Savelyev suggests two solutions to this, both of which he views as sub-optimal: (1) creating government super-users who can override the blockchain; and (2) giving courts and states the power to pursue specific users and force them to make the changes in the blockchain themselves in combination with

In the Ethereum-charged DeFi ecosystem, also known as financial Lego,[107] it is usually impossible to remove the foundational building blocks.[108] The persistent scripts will continue to self-execute because the entire code is pre-programmed.[109] As noted above, they are not isolated contracts between two parties, but instead are transactions between two parties within a wider technological ecosystem. Yet, as discussed below in Part II, admin keys often—but not always— exist (and sometimes unexpectedly for "decentralized" products), even in DeFi products.

Yet again, even in the vending machine example, there are situations where the vending machine malfunctions (i.e., money is inserted but the product is not dispensed). The customer is then directed by a notice on the vending machine to call a customer service number for assistance for a refund, thereby reinstating the customer to the position they were in before they performed their part of the contract. Arguably, this is when intervention from outside the self-contained ecosystem is required. Does a similar concept apply to other smart contracts? For example, does a similar concept apply if there is a malfunction in the code and third-party intervention is required to either ensure the transaction occurs as intended (enforce performance of contract) or restore parties to their original positions (restitution)?

This Article suggests below that the idea of admin keys and possibly Decentralized Autonomous Organization ("DAO") governance protocols reflect that assistance phone number on the side of the vending machine. Next, the hazards of smart contract drafting are noted below. In some examples, admin keys could possibly be used.

D. The Hazards of Smart Contracts

One key point in resolving any dispute is that resolution first depends on how a smart contract is structured and what caused the

---

using traditional tort, unjust enrichment, and specific performance claims. Savelyev, *supra* note 43, at 133.

[107] *See generally* Andrei-Dragoş Popesecu, *Decentralized Finance (DeFi)—The Lego of Finance*, 7 SOC. SCI. & EDUC. RSCH. REV. 321 (2020).

[108] *See* Schär, *supra* note 90, at 155–56.

[109] *See* Levi & Lipton, *supra* note 54.

contract to fall apart. This is then followed by identifying the parties, and then finally locating enforcement mechanisms. What is the smart contract "failure mechanism" that caused the smart contract to fail? Was it the enabling protocol?[110] Or a fault of the parties? As discussed above, can the admin keys solve this enforcement problem? The potential hazards of smart contracts can include:

1. *Misidentified parties.* If the parties to the smart contract are pseudonymous or anonymous, there will be difficulties in ascertaining their identity.[111] Ideally, bespoke commercial smart contracts would clearly identify the parties in the code. In Ethereum transactions, private keys could still be used as an identifier, and parties could possibly opt-in to a legal suit.[112]

2. *Coding error.* Incorrect structuring of the contract due to poor or inaccurate coding and/or contractual requirements has several externalities. A preliminary concern for the courts is who bears liability if a mistake is made in the code, which could nullify a contract.[113] Traditional legal doctrines could cover such situations, which include negligent coding and mistake/unjust enrichment by the coder(s) who may not be parties to the contract. Human error is always possible, and that coding error could lead to exploits. This happened with the attack on Ethereum's DAO in 2016. Hackers exploited a vulnerability in the DAO's fundraising smart contract and used it to secrete funds from the project.[114] This is an example of where admin keys could have been used to correct a wrong.

3. *Hacking.* Insufficient cybersecurity protections prevent hacking of smart contracts in novel ways. In theory, for example, a

---

[110] Smart contracts are formed when computer protocols with the transaction instructions are recorded onto a blockchain containing the contracting parties' private keys. One party unilaterally records the smart contract protocol on the blockchain.

[111] *See supra* Section I.C.

[112] "All types of transactions must be signed by a private key corresponding to an account and include a nonce value that prevents replay attacks." Robinson, *supra* note 103, at 2.

[113] *See* KNAPP ET AL., *supra* note 57, at 720.

[114] Osman Gazi Güçlütürk, *The DAO Hack Explained: Unfortunate Take-off of Smart Contracts*, MEDIUM (Aug. 1, 2018), https://ogucluturk.medium.com/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562 [https://perma.cc/2PUF-7B8D].

miner could reorganize the chain, thereby affecting the order required for contractual events to occur.[115] Though this has not been done, this is an example of where admin keys could also be used.[116]

4. *Changes in legislation.* Many governments are still drafting or amending legislation to manage the crypto market. Changes to, for example, a class of crypto asset, or a tax consideration, could affect a contract's operation.[117] Admin keys might be useful in this instance.

5. *Technology fault or forking.* For example, Ethereum smart contracts use "gas" akin to a transactional cost due each time a contract executes.[118] High gas fees could make smart contracts uneconomical to the contractual parties, particularly those coded prior to the London Fork.[119] Inefficient use of smart contracts can create unnecessary (or unforeseen) costs. Ethereum's so-called "London fork" is again relevant here.[120] The changes which occurred between August and December of 2021 introduced a new fee structure to make Ethereum less inflationary. This protocol change

---

[115] For technical analysis, *see* Jude Nelson, *Bringing Clarity to 8 Dangerous Smart Contract Vulnerabilities*, STACKS (Mar. 11, 2020), https://blog.blockstack.org/bringing-clarity-to-8-dangerous-smart-contract-vulnerabilities/ [https://perma.cc/YW9J-EEH].

[116] *See* Tellor example, *infra* Section II.B.

[117] AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION, *Crypto-assets as Underlying Assets for ETPs and Other Investment Products* (Consultation Paper 343, June 2021), https://asic.gov.au/media/yhbgvq02/cp343-published-30-june-2021.pdf [permanent link unavailable] [hereinafter *CP 343*].

[118] "Gas" is a network fee. *See* Kristin N. Johnson, *Decentralized Finance: Regulating Cryptocurrency Exchanges*, 62(6) WILLIAM & MARY L. REV. 1911, 1956 (2021). *See also What Is Gas?*, ETH GAS STATION (July 31, 2019), https://ethgasstation.info/blog/what-is-gas/ [https://perma.cc/C8FH-W5WD].

[119] *Gas and Fees*, ETHEREUM (Sept. 12, 2021), https://ethereum.org/en/developers/docs/gas/ [https://perma.cc/RC93-N6PT]. Again, the London Fork was designed to offset this.

[120] Ethereum is not the only platform to offer DeFi smart contracts, but it does have 80% of the market. "EIP 1559," also known as "the London Fork," introduces a new fee structure to make Ethereum less inflationary. This protocol change is highly controversial because it aims to burn part of the fees, hence decreasing miner revenue. *See* Myles Sherman, *Ethereum's London Hard Fork Expected to Launch on Aug. 4*, COINDESK (July 7, 2021), https://www.coindesk.com/ethereum-london-fork-launch-date-august [https://perma.cc/X3K3-TE5V].

is controversial because it aims to burn part of the gas fees, decreasing miner revenue. Miners are needed to verify the contracts.[121] A smart contract coded before the London Fork was discussed and implemented may not have foreseen that this hard fork would alter the terms of the contract. This is an example of where admin keys might not be used as the fork reflects the change itself.

6. *External data*. Smart contracts may rely on external data that is not natively available on-chain and must be provided by external data sources. These "oracles" introduce dependencies and may, in some cases, lead to heavily centralized contract execution.[122] This is an example of where admin keys would not be used, as off-chain changes cannot be made on-chain.

Crucially, the power of the courts to sever defective terms will likely be impeded by the immutability of smart contracts unless a mechanism to effect these changes was coded into the contract at the time of formation. Nevertheless, for those transactional disputes that could be commercially viable to pursue through the legal system, there may be other enforcement options.

E. Enforcement via Crypto Law in the Ethereum Ecosystem

Seeking legal solutions is highly complicated by the architecture of the Ethereum blockchain, as described above in Part I, because of its immutability and pseudo-anonymity. Accordingly, few legal cases exist globally testing the recovery of crypto assets on an Ethereum blockchain.[123] The problem is that enforcement options such as an injunction or a freezing of assets could arguably be

---

[121] *Id.*

[122] Oracles are off-chain nodes that pull information from outside a blockchain and make it compatible with blockchain networks. Sheldon argues that reliance from information outside the blockchain should affect how participants view the nature of the contractual bargain. Mark D. Sheldon, *Auditing the Blockchain Oracle Problem*, 35 J. INFO. SYS. 121, 121–33 (2021).

[123] *See* Michael Ng, *Choice of Law for Property Issues Regarding Bitcoin under English Law*, 15 J. PRIV. INT'L L. 315 (2019). That article cited *B2C2 Ltd v Quoine Pte Ltd*, [2018] S.G.H.C.(I.) 04, a Singaporean case that concerned the alleged wrongful reversal of a trade of Ethereum for Bitcoin. In that case, and on appeal in 2020 (Quoine Pte Ltd v B2C2 Ltd, [2020] S.G.C.A.(I.) 2), the court held that contracts formed through deterministic algorithms are valid.

ordered by a court if they have jurisdiction where the assets are located. If a contract is a legally enforceable agreement between two or more parties,[124] then third parties are the ones who make an agreement "legally enforceable."

Also, enforcement actions of any sort of contract can also ignore the way people contract in the business world: signing a contract (even a large commercial deal) is not necessarily pre-determinative to executing the work.[125] Work often begins as lawyers and in-house counsels finalize the terms.[126] Taking a modest financial loss is often more economically efficient than seeking relief from the legal system. Compelling the performance of void or voidable obligations of a part of a contract (whether on a smart contract or not) is often economically prohibitive.

While law is just one normative tool for contractual enforcement, the third party to the blockchain (i.e., the applicable legal system) will outline the basic operational notions of contract law. The stated legal jurisdiction in any common law contract will affect: (1) who decides whether a contract exists, and/or what it means, and/or whether it was breached; and (2) what standard should be used according to a particular jurisdiction to determine contractual formation, interpretation, and a possible breach in a particular context.[127] This third-party problem is *the* legal problem itself. If a persistent script on Ethereum cannot be enforced by a third party (i.e., the applicable legal system), then it is not a "legal" contract.

So, again, is legal ambivalence an agreed part of the transactional bargain on Ethereum? The contract does not exist in

---

[124] CARTER, *supra* note 74 (citing *Cornish & Co v. Kanematsu*, (1913) 13 SR (NSW) 83, 87 (Austl.); *Foster v. Wheeler*, (1887) 36 Ch. D. 695, 698 (Kekewich J) (Austl.); *Dunlop Pneumatic Tyre Co Ltd v. Selfridge & Co.*, [1915] AC 847, 855 (Lord Dunedin) (Austl.); *Ermogenous v. Greek Orthodox Cmty. of SA Inc.*, (2002) 209 CLR 95, 105 (Gaudron, McHugh, Hayne & Callinan, JJ.) (Austl.)); Brian Coote, *The Essence of Contract: Part II*, 1 J. CONT. L. 183, 201 (1989).

[125] *See* Catherine Mitchell, *Contracts and Contract Law: Challenging the Distinction Between the "Real" and "Paper" Deal*, 29 OXFORD J. L. STUD. 675, 682 (2009).

[126] *Id*.

[127] *See, e.g.*, KNAPP ET AL., *supra* note 57, at 32.

the ether; it exists within the Ethereum ecosystem. If a contract is an agreement, then surely in the context of the Ethereum universe those minds meet in a jurisdiction where they understand the difficulties in enforcing those bargains. Just as venture capital is a risky investment, so, too, is staking tokens to build a new protocol.[128]

Furthermore, "Crypto Law is responsible for managing disputes in blockchain governance, and making sure that they are resolved via legal processes that don't break the protocol."[129] "Szabo's law is simple: Do not implement changes to the blockchain protocol unless the changes are required for the purpose of technical maintenance."[130] Changes to a smart contract should only occur for the purposes of technical maintenance.[131] This is because a variety of built-in tech solutions already exist for dispute resolution within Ethereum smart contracting practice. They are cited in depth below.

1. Excess Collateral Built into Smart Contracts

There are crypto systems that deal with contractual disputes by coding for peer-to-peer enforcement. Enforceability is achieved by over-collateralization of the contract accounting for errors that can occur. For example, with the DAI ERC20 stablecoin, contracting parties must stake $1.50 in Ethereum for every dollar pledged.[132] This is how Buterin conceived smart contracts to operate without the law in persistent scripts where over-collateralization is part of the bargain. The vast majority of tokens are issued on the Ethereum blockchain through a smart contract template referred to as the

---

[128] A token is "staked" if it is "locked into the token holder's or a third-party's account." *See* Alexis Collomb et al., *Blockchain Technology and Financial Regulation: A Risk-Based Approach to the Regulation of ICOs*, 10 EUR. J. RISK REGUL. 263, 279 (2019).

[129] Vlad Zamfir, *Against Szabo's Law, For a New Crypto Legal System*, MEDIUM (Jan. 26, 2019), https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827 [https://perma.cc/YC3W-8FKR].

[130] *Id*.

[131] CleanApp, *Crypto Legal Theory*, MEDIUM (Oct. 23, 2018), https://medium.com/cryptolawreview/crypto-legal-theory-299fa35be21f [https://perma.cc/39GF-P429].

[132] *See* Adriana Hamacher & Ki Chong Tran, *How to Use DAIStablecoin: Beginner's Guide (2021)*, DECRYPT (Jan. 18, 2021), https://decrypt.co/resources/dai-explained-guide-ethereum-stablecoin [https://perma.cc/EC85-FMK8].

ERC-20 token standard.[133] These tokens are interoperable and can be used in almost all DeFi applications. As of January 2021, there were already over 350,000 ERC-20 token contracts deployed on Ethereum.[134]

Fluctuating transactional "gas" fees are why over-collateralization began as a practice, "Are you a smart contract owner? Did you pay enough to deploy the smart contract? No? Then your contract will just stop mid-execution."[135] "Even if you're careful, the gas price fluctuates all the time, so it's impossible to properly budget the costs of running contracts."[136] This is why over-collateralization became a popular option to offset contractual disputes and another reason for the London hard fork and "The Merge," as noted above.[137]

2. Third-party Firms Audit the Code

Smart contract and blockchain architecture can already be designed to prevent unenforceable smart contracts from being executed.[138] Transactions can be automated using smart contracts hosted and executed on a blockchain. Smart contract audits can mitigate these potential risks. Specialized smart contract auditors help optimize smart contracts and identify threats and anomalies in the smart contract code. This is a growing industry that will help to avoid disputes over smart contracts.[139]

---

[133] Fabian Vogelsteller & Vitalik Buterin, *EIP-20: Token Standard*, ETHEREUM IMPROVEMENT PROPOSALS (Nov. 19, 2015), https://eips.ethereum.org/EIPS/eip-20 [https://perma.cc/GWF3-SSSJ].

[134] *See Token Tracker*, ETHERSCAN, etherscan.io/tokens [https://perma.cc/6VZV-H4DN] (last visited Mar. 30, 2023).

[135] Stegos, *supra* note 91.

[136] *Id*.

[137] *See* ETHEREUM, *supra* note 97.

[138] Bill Marino & Ari Juels, *Setting Standards for Altering and Undoing Smart Contracts,* RULE TECHNOLOGIES: RESEARCH, TOOLS, AND APPLICATIONS 151 (Jose Julio Alferes et al. eds., 2016); Joshua Ellul et al., *Regulating Blockchain, DLT and Smart Contracts: A Technology Regulator's Perspective*, 21 E.R.A. FORUM 209 (2020).

[139] Ellul et al., *supra* note 138.

3. Escrow

Escrow—the holding of funds on trust until a condition has been met—is the simplest in-built technology solution for dispute resolution within smart contracting practice. One simple example of a smart contract would be, "parties place Bitcoins or other digital currency [like Ether] into a suspended state on the blockchain, and once certain terms are met, those Bitcoins [or Ether] are transferred to the appropriate account."[140] In so far as they can be used to suspend digital currency pending the satisfaction of certain conditions, smart contracts resemble escrow-like mechanisms. Escrow mechanisms are used to "suspends [the] execution of a valid contract, and empowers a trusted third party to complete the process."[141]

Yet the key legal question of this Article remains: How can existing legal dispute resolution mechanisms interface with autonomous, truly immutable[142] blockchains that continue to strive for an autonomous and "alegal posture?"[143] One solution is by utilizing a platform's admin keys. Admin keys are one rarely mentioned backdoor for many DeFi products that could lead to the enforcement of any legal case by freezing the assets.

---

[140] Werbach & Cornell, *supra* note 43, at 334.

[141] *Id*. at 344.

[142] There is research about some experimental attempts dealing with the unstoppable nature of smart contracts, such as a programmatic function that listens to "external input[s] from oracles" and carries out the instructions which it receives. *See* Durovic & Janseen, *supra* note 61, at 73. For example, pursuant to a court order, a command could be dispatched which directs the function to toggle a pre-coded "kill switch" to disable the operation of an unfair term or alternatively, the entire contract. *See* Marino & Juels, *supra* note 138, at 161–63. *See generally* Olaf Meyer, *Stopping the Unstoppable: Termination and Unwinding of Smart Contracts*, 9 J. EUR. CONSUMER & MKT. L. 17 (2020); Robert Herian, *Smart Contracts: A Remedial Analysis*, 30 INFO. & COMMC'N TECH. L. 17 (2021). An immutable smart contract cannot be wholly or partially erased, but perhaps some or all of its terms could be "deactivated" by storing new points of data on the blockchain—such as an "on" state for the Boolean variable of a "kill switch" toggle. Marino & Juels, *supra* note 138, 162–63.

[143] CleanApp, *supra* note 131.

III. LEGAL ENFORCEMENT THROUGH ADMIN KEYS?

Many DeFi protocols and products that can accept deposits are protected by an admin key. This key is typically an Ethereum smart contract capable of upgrading the protocol or product.[144] This means a court could, in theory, identify someone as the party responsible for parts of the contracts for the purposes of a breach or voided contract. Courts could then freeze the assets for the purposes of an adverse judgment. Further, an administrator account or key can take several possible forms, including a single address, a multi-sig wallet, or even a DAO[145] controlled by a voting process.[146] For multi-sig structures, multiple people could hold the admin keys to the account, so an admin key is not necessarily tied to a single accountable person. This provides a plausible opportunity for legal enforcement, which has never been done before.[147]

---

[144] Admin keys are a form of centralized control in a crypto or DeFi project which allows the developers or founders to change the rules of their smart contract or blockchain. Connor, *What are Admin Keys? (Ultimate DeFi Risk),* LIQUID LOANS.IO, https://learn.liquidloans.io/security/admin-keys/ [https://perma.cc/U2GK-JXL2] (last visited Mar. 30, 2023).

[145] *Decentralised Autonomous Organisation (DAO)*, DYOR CRYPTO WIKI, https://dyor-crypto.fandom.com/wiki/DAO [https://perma.cc/YJF6-CW4X] (last visited Jan. 26, 2022).

[146] 1. Administrators could:

- Pause the system?
- Modify balances?
- Whitelist/blacklist of tokens and/or users?
- Upgrade a subset of the system.
- Upgrade all of the systems (which is equivalent to omnipotence).

2. Which of these actions do and do not have a time delay on them?
3. If there is a time delay, how long is that time delay?
4. Modify how many people have administrator privileges?
5. How many admins must approve before an action is taken?
6. Any administrative actions controlled by on-chain governance (i.e., a DAO)?

See John Mardlin, *Questions DeFi Users Should Be Asking DeFi Developers*, CONSENSYS DILIGENCE (Mar. 2, 2020), https://consensys.net/diligence/blog/2020/03/questions-defi-users-should-be-asking-defi-developers/ [https://perma.cc/26AP-MVP2].

[147] *See supra* Section I.A.

Admin keys are a risk,[148] in "that the original deployers of a contract hold the admin keys to the contract,"[149] and because the "majority of popular defi protocols have some form of centralized control that enables specific 'administrator' addresses to intervene in powerful ways."[150] Yet, they are also a possible party identifier and liability chain creator for an administrator holding an admin key and accused of wrongdoing or mistake.[151]

A. Admin Keys: Both a Form of Security and a Form of Control

The next question is how admin keys could be used for legal enforcement of a decision. This is a challenging problem because these products are designed to be alegal. Indeed, internet memes today refer to some of these protocol administrators as so-called "shadowy super coders."[152] This term, while an internet meme, is grounded in fact. That is because these super coders or crypto protocol architects often do not reveal their identity and avoid being exposed to their jurisdiction's legal reach. The vast majority of DeFi projects still could enter "God Mode" and unilaterally make changes

---

[148] Blec, *supra* note 1.

[149] David Hoffman, *Are We Trustless Yet?—Market Monday LITE (10/26)*, BANKLESS (Oct. 27, 2020), https://newsletter.banklesshq.com/p/are-we-trustless-yet-market-Monday [https://perma.cc/J4UT-NJ9M].

[150] Mardlin, *supra* note 146.

[151] Is the administrator a party to the contract or are they a third-party to the contract who makes an unauthorized change to the contract without the knowledge of the actual parties to the contract? The possible legal remedies would differ accordingly—as per the doctrine of privity of contract, contracts can only be enforced against those who are parties to the contract (and not third parties)—so if the administrators are third parties to the contract, then any remedy against them would not be a contractual remedy but a different type of legal remedy. "The doctrine of privity of contract states that only the parties to a contract are entitled to enforce and be legally bound by a contract." CARTER, *supra* note 74.

[152] This phrase emanates from a Senator Elizabeth Warren quote: "Instead of leaving our financial system at the whims of giant banks, crypto puts the system at the whims of some shadowy, faceless group of super-coders and miners, which doesn't sound better to me." Will Gottsegen, *Senator Warren: Crypto Puts Financial System in the Hands of "Shadowy Super-Coders,"* DECRYPT (July 28, 2021), https://decrypt.co/76997/elizabeth-warren-crypto-big-banks-shadowy-super-coders [https://perma.cc/9FT8-V5BQ].

to many aspects of the platform or protocol.[153] Twelve out of fifteen of the most popular DeFi protocols still have access to a "God Mode" admin key, according to data on crypto product review platform DeFi Watch.[154] "God Mode" admin keys mean certain parties with that key can control the protocol.

On the one hand, admin keys offer some security benefits because admin keys can amend a glitch or change a protocol, but they also mean that users have to trust the administrator(s) not to abuse their privileges to steal funds or conduct a "rug-pull." A rug-pull is where developers abandon a project and run away with investors' funds. It also adds the risk of an attacker gaining access to an administrator's private keys and all the associated privileges of those admin keys. Full-access controls can allow developers to modify or replace the smart contracts underpinning their projects and possibly adjust users' balances.[155] Admin keys have been justified as a way to protect users' funds and are often used with security features, such as timelocks and multi-sig keys.[156] Timelocks

---

[153] Joshua Mapperson, *How Many DeFi Projects Still Have "God Mode" Admin Keys? More than You Think*, COINTELEGRAPH (Sept. 25, 2020), https://cointelegraph.com/news/how-many-defi-projects-still-have-god-mode-admin-keys-more-than-you-think [https://perma.cc/G782-EQJ7].

[154] Of the fifteen projects reviewed on DeFi Watch, only InstaDapp, MakerDAO, and Uniswap are reported to have no admin keys associated with their product. The remaining projects—which include Aave, Compound, DDEX, Yearn Finance, Nexus Mutual, and Synthetix—all have admin keys allowing varying degrees of control. *See* Chris Blec, *Alpha Homora v2 Has a Single-signer Admin Key*, DEFI WATCH (May 31, 2021), https://defiwatch.net/alpha-homora-v2-has-a-single-signer-admin-key/ [https://perma.cc/L9HV-C62M]; Chris Blec, *Aave on Polygon Has an Admin Key*, DEFI WATCH (May 29, 2021), https://defiwatch.net/aave-on-polygon-has-an-admin-key/ [https://perma.cc/KDE9-XHXV].

[155] Mapperson, *supra* note 153.

[156] Platform and private key management:

- MakerDao, Decentralized governance;
- Instadapp, no admin key or ability to modify;
- Uniswap, no admin key or ability to modify;
- Compound2 days timelock;
- TokenSets, No timelock;
- Aave, No timelock (Dao security model Aragon coming soon);
- dYdX, days timelock;

mean that the propagation of the changes is delayed by a certain amount of hours/days for additional security.[157]

In the DeFi world, wallet multi-sig means that each time the "contract" is changed, an Ethereum wallet is accessed that allows signing transactions and changing the records in the blockchain.[158] Multi-sig systems are designed as a security solution allowing for greater distribution of power. Several private keys are distributed to founders or trustees and a minimum number of them together allows access to the contract. Yet, again, regardless of what is declared by

---

- PoolTogether, No timelock;
- Dharma, 7 days timelock;
- Ddex, 3 days timelock;
- Synthetix, info not available;
- Nuo, info not available.
- Platform Multisig key Systems:
- MakerDao, Decentralized governance;
- Instadapp, no admin key or ability to modify;
- Uniswap, no admin key or ability to modify;
- Compound, No Multisig;
- TokenSets2, keys out of 3;
- Aave, 3 keys out of 5 Dao security model Aragon;
- dYdX, 2 keys out of 3;
- PoolTogether, 2 keys out of N – Gnosis system;
- Dharma, 3 keys out of 5;
- Ddex, 2 keys out of 3;
- Synthetix, info not available;
- Nuo, info not available.

See Lorenzo Dalvit, *DeFi and Admin Keys: An Unsolved Problem*, CRYPTONOMINST (Feb. 26, 2020), https://en.cryptonomist.ch/2020/02/26/defi-admin-keys-an-unsolved-problem/ [https://perma.cc/8MF8-VJVC].

[157] How do Timelocks work in DeFi? Every relationship with the deposited tokens and those provided by DeFi platforms is governed by a smart contract. It is possible to set by code, and therefore in a verifiable way, "a fixed delay time in the application of any change to the reference smart contract. The time will be marked by the number of blocks that must elapse between the modification of the contract and its actual activation. Once set, no one can reduce the waiting time." *Id.* This "allows for a reaction time within which, in the event of an unexpected change that is not agreed upon or malicious, it is possible to unlock the funds and secure them." *See id*.

[158] *Id*.

the teams, the function of multi-sig also requires trust.[159] No one can control who the keys are distributed to and whether they are in the possession of a single person, thus increasing the risks.[160] Nevertheless, in many cases the platform's community (as in the voting token holders of a platform) has an important role to play in creating governance protocols. However, these governance protocols do not seek to engage with the legal system and instead only provide self-governance.[161]

Furthermore, while these private keys are held by the platform administrators—meaning that the platform administrators could modify the rules of the contract in an arbitrary manner—in reality, it is very difficult to achieve the goal of disintermediation (as in reducing intermediaries) without making compromises. As platforms mature, governance protocols mean that the community must make sure to continue to move towards their ultimate goal. Instead of enforcement, there exists "performance incentivization" in crypto communities where rewards are offered for performance.[162]

However, no DeFi project can prove the operational security if their admin key is strong.[163] This means that the only way that you can truly feel secure while using these DeFi products currently, is to trust in the competency of the team and their ability to secure their admin key,[164] as well as the honesty of any DAO voting protocols.[165] Any blockchain platform seeking to be truly decentralized must at some point transition from its founding team to become a

---

[159] *Id*.

[160] *Id*.

[161] *See DeFi Governance in Action*, CRYPTOPEDIA BY GEMINI (Mar. 10, 2022) https://www.gemini.com/cryptopedia/defi-solutions-decentralized-governance-meaning [https://perma.cc/SH4S-EK79].

[162] *See* Sinclair Davidson et al., *Blockchains and the Economic Institutions of Capitalism*, 14 J. INST. ECON. 639, 643 (2018).

[163] Dalvit, *supra* note 156.

[164] Blec, *supra* note 1.

[165] Decentralized Autonomous Organizations ("DAO") are organizations that function "without hierarchical management," through the interaction of users with smart contracts. *See What Is DAO?*, COINTELEGRAPH, https://cointelegraph.com/ethereum-for-beginners/what-is-dao [https://perma.cc/7R95-87BL] (last visited Jan. 26, 2022).

"decentralized" platform.[166] This creates opportunities for legal enforcement, which is rarely discussed.

B. The Challenges of Possible Legal Enforcement via Admin Keys?

The following provides some very early and speculative examples of the hazards of legal enforcement via admin keys or DAO-based governance protocols.[167] In truth, the examples also provide support for a consensus DAO-based approach to enforcing smart contracts. However, they also include a cautionary tale, in the case of Tornado Cash, where the developers ideologically burned the admin keys, so that, in theory, no legal action could be placed on the developers of Tornado Cash. As a result, Tornado Cash became self-executing code, a truly persistent script.

1. Admin Keys for Legal Enforcement: A Possible Future Example?

As DAOs become more widespread, there is a major looming issue for any proposed legal enforcement. Many projects, at some point, will face the trade-off between control (through admin keys) and complete decentralization (meaning, no longer relying on admin keys). There may only be a finite amount of time before founders transition from admin keys to a DAO. This needs to be addressed up-front. Many protocols operate with an admin key initially so the founders of the project can build the project and admin keys can upgrade the smart contracts to become persistent scripts of automated "un-stoppable" platforms. This means project founders can make changes to the base rules of the system. Again, usually admin keys work with a timelock, meaning the propagation of the changes is delayed by a certain amount of hours/days for additional security.

The current DeFi protocol models involve a lot of trust from users and investors because any DeFi product usually has a staged development phase and then transitions to less control by individuals and/or small groups. This is done via admin keys. One DeFi user noted, "[T]he end goal is trustlessness so it will have to

---

[166] Berg, *supra* note 56.

[167] DAO-based voting governance generally means voting is recorded on-chain in accordance with rules encoded via smart contracts.

evolve, especially if we start onboarding real crypto-novices en masse to DeFi."[168] "Ideally, [DeFi] protocols allow for no admin interference at all, including a front end hosted on distributed systems."[169] Yet, these new and emerging DeFi protocols and products need upgrade capabilities to progress and if anything goes wrong. It is "fine for now as most users are very involved in the scene—they often know the people working on the projects they use personally—that's my case for most DeFi services I use. If they're not involved, they are usually quite well-informed about the risk they're taking," according to Chris Blec, a well-known crypto security advocate and educator.[170]

However, the initial period is crucial for law enforcement. Much relies "on faith that the admins won't abuse their powers. Worst-case, rug pulls happen [theft of the project's crowd-sourced funding] and a team member is hacked or takes users' funds and disappears."[171] Founders of DeFi Project, for example, understand the legal implication of an admin key. They know there is a small window where law enforcement or regulatory action is possible:

> To eliminate this centralized point of risk, a small minority of projects remove the admin key by sending it to a burn address. This creates a new set of challenges. What if there's an error in how the project is built and how is it fixed? What if the community votes for a bogus change to the project? And if the project comes under attack, what are the control measures to make sure the attacker doesn't succeed when time is of the essence.

---

[168] Token_Brice, *Overview the Admin Keys Still Present in Most Common DeFi Protocols: Their Capabilities, Opsec, and Who/How Many Handles Them—Courtesy of Chris Blec*, REDDIT (Feb. 5, 2020, 6:46 AM, https://www.reddit.com/r/ethfinance/comments/ez8djp/overview [https://perma.cc/QY42-4GHZ].

[169] Nayge, *Overview the Admin Keys Still Present in Most Common DeFi Protocols: Their Capabilities, Opsec, and Who/How Many Handles Them - Courtesy of Chris Blec*, REDDIT (Feb. 5, 2020, 6:46 AM, https://www.reddit.com/r/ethfinance/comments/ez8djp/overview [https://perma.cc/QY42-4GHZ].

[170] *Id*. *See generally* Chris Blec (@ChrisBlec), TWITTER, https://twitter.com/ChrisBlec?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor [https://perma.cc/SBX8-45ZQ].

[171] Tellor Core, *Moving from Admin Key to DAO—Tellor's Parachute Smart Contract*, MEDIUM (Aug. 11, 2021), https://medium.com/tellor/moving-from-admin-key-to-dao-tellors-parachute-smart-contract-aba4cc9d71fb [https://perma.cc/26LB-AXPD].

> The risk of facing government regulation is also a wide[-]open question for "centralized" projects with an admin key. The regulators may take out projects that have a "kill switch" in the form of an admin key. DeFi projects that have centralized "custodial" control over users and their funds face heat, especially in the form of legislation. If regulators can find a centralized party or group of people, they will grab hold.[172]

Yet, as a recent example supporting this Article's central argument, one start-up—Tellor—created *new* admin keys. Their project "initially built Tellor with an admin key in place, then sen[t] it to a zero address last October [2020], and subsequently encounter[ed] a fatal error forcing [them] to fork to a new contract giving [them the] admin keys back."[173] In summary, when a "fatal error" occurred after the original admin keys were destroyed, the Tellor team simply forked new admin keys.[174] Tellor's business model uses a tokenomic system to reward users for bringing off-chain data on-chain (oracles).[175] Tellor is also an "unstoppable" or a persistent script community driven oracle network, so Tellor is a good example for this Article. This example suggests there may be a way to fork a project and create new admin keys in some cases. Courts and dispute resolution bodies should seek expert advice in the future to ascertain whether this is possible.

There is little precedent on how United States courts will handle any contractual disputes. In August 2021, the U.S. Securities and Exchange Commission Chairman, Gary Gensler, questioned *how decentralized* DeFi platforms actually may be, despite what their creators promise.[176] In another example, one case listed in New York in October 2021 is testing the premise of the "DeFi community's claim that its protocols are autonomous and self-governed."[177] The

---

[172] *Id*.
[173] *Id*.
[174] *Id*.
[175] *Id*.
[176] Dave Michaels & Paul Kiernan, *Crypto's "DeFi" Projects Aren't Immune to Regulation, SEC's Gensler Says*, WALL ST. J. (Aug. 19, 2021), https://www.wsj.com/articles/cryptos-defi-projects-arent-immune-to-regulation-secs-gensler-says-11629365401?mod=article_inline [https://perma.cc/4YY6-PG54].
[177] Dylan Tokar, *Crypto-Savings Lawsuit Puts Principles of DeFi to the Test*, WALL ST. J. (Jan. 13, 2022), https://www.wsj.com/amp/articles/crypto-savings-

claimant is suing a Delaware company, but the founders of that company argue that, as an autonomous platform, they have no control over the platform. If the claimants win and incur loses, perhaps admin keys could be utilized post-judgment.[178] It "begs the question: Who's responsible when things go wrong?"[179] The "lawsuit could be among the first to squarely address the question of who is legally accountable when a DeFi application—known as a "protocol"—is at odds with the law or causes actionable harm to a user."[180]

However, not all protocols have an admin key. Decentralized Crypto Exchange Uniswap (discussed below) operates without admin keys or upgrade capabilities.

2. Admin Keys for Legal Enforcement: Uniswap, but do Governance Tokens Hold the Key?

Uniswap is known in crypto jargon as an "automated market maker," or a code on a blockchain that makes it possible for traders to swap assets from various pools of liquidity.[181] As a truly persistent script, Uniswap does not hold any admin keys, and the code is "unstoppable" without them. Yet, Uniswap also raises the question of exactly how "decentralized" decentralized exchanges ("DEXs")[182] actually are. Truly decentralized projects are likely ones

---

lawsuit-puts-principles-of-defi-to-the-test-11642069806 [https://perma.cc/L8MQ-2A3C].

[178] The founders raised money for legal fees through the sale of NFTs to the community. *See* Brian Quarmby, *DeFi Community Rallies Behind PoolTogether to Hit $1.4M NF Defense Funding Target*, COINTELEGRAPH (June 6, 2022), https://cointelegraph.com/news/defi-community-rallies-behind-pooltogether-to-hit-1-4m-nft-defense-funding-target [https://perma.cc/PY3N-K2SM].

[179] Tokar, *supra* note 177.

[180] *Id*.

[181] Brady Dale, *PancakeSwap, Uniswap, SushiSwap and More: What to Consider When Parking Crypto in a DeFi Exchange*, COINDESK (Apr. 26, 2021), https://www.coindesk.com/markets/2021/04/26/pancakeswap-uniswap-sushiswap-and-more-what-to-consider-when-parking-crypto-in-a-defi-exchange/ [https://perma.cc/49MF-E7CD].

[182] DEX users execute transactions without intermediaries, as all transactions are authenticated by the network's community. DEXs are exchanges with no central location for the storage or management of the underlying technology. *See, e.g.*, Simon Taylor, *What Is a Decentralised Exchange?*, MEDIUM (Aug. 6, 2018),

that do not have custodial control over funds.[183] Thus, for DEXs, the recovery of assets by a court of law would not be an enforcement option for two reasons: (1) there are no admin keys and (2) there are no funds held in the exchange's custody.

Courts could look to DAO governance mechanisms to find an enforcement angle. While a non-custodial DEX like Uniswap does not have any admin keys, the blockchain analytics firm Glassnode argued in a September 2020 report that the famed non-custodial DeFi project has essentially created their own equivalent backdoor through the distribution of their UNI governance token.[184]

The main function of the UNI token is to grant token holders the right to make decisions about the protocol.[185] Glassnode insinuated that Uniswap's developers intentionally misled the community about how the team's allocation of UNI tokens would vest over time.[186] In short, the stated pre-programmed application of how voting governance tokens would vest does not match the code.[187] "Decentralized governance appears to present a real challenge for even the most established of DeFi projects."[188]

So, could a governance token be used for a legal challenge for even the most famed and vaunted decentralized projects? A persuasive legal argument would need to understand the technology

---

https://medium.com/@sytaylor/what-is-a-decentralised-exchange-e2b86e844fe9 [https://perma.cc/Z95W-TSAG]; *What Is a Dex: Decentralized Exchanges Explained*, LEDGER (Oct. 9, 2020), https://www.ledger.com/academy/crypto/what-is-a-dex-decentralized-exchanges-explained [https://perma.cc/JV88-KZ8N].

[183] Johnson, *supra* note 118, at 1955.

[184] Liesl Eichholz, *The UNI Token: Is Uniswap Really Decentralized?*, GLASSNODE INSIGHTS (Sept. 24, 2020), https://insights.glassnode.com/uni-token-is-uniswap-really-decentralized/ [https://perma.cc/4XSG-8NWM].

[185] *Id.*

[186] *Id*.

[187] For example, in order to submit a governance proposal, a token holder needs to possess at least 1% of the entire UNI supply. As the entire supply has not yet been released into circulation, Glassnode calculated that this threshold is actually 8% of the currently circulating supply. *Id.*

[188] Michael Kapilkov, *Glassnode: Uniswap Team May Have Misled Community over Team Token Vesting*, COINTELEGRAPH (Sept. 24, 2020), https://cointelegraph.com/news/glassnode-uniswap-team-may-have-misled-community-over-team-token-vesting [[https://perma.cc/BM7V-DHXE].

and how to unravel the technology to enforce any judgment. Perhaps a coordinated governance consensus ploy could amount to something like a class action. In truth, in any DEX or truly decentralized application currently, there is always the risk of a crypto whale (a large holder of tokens) swaying governance decisions.[189] Thus, in this example, while an admin key could not have been used, a governance token could have theoretically been used by the courts to identify the parties to the smart contract and mount a legal challenge. There is recent precedent for this premise without the courts being involved.

SushiSwap, the popular automatic market maker and decentralized cryptocurrency exchange (and major competitor to Uniswap) had an ambitious governance overhaul in January 2022, becoming a case study of DeFi governance principles.[190] "Interestingly, SushiSwap's overhaul may provide the first substantive example of activist investors swarming the virtual boardroom that is DeFi governance."[191] In this case, a management re-shuffle led by investors, not the start-up's management, passed a "signal" vote with over 88% approval.[192] This paved the way for an "overhaul of SushiSwap's leadership and [organizational] structure."[193] This all occurred after a founder "misused" funds in 2021 and was forced to return the funds. Elections were held to establish a multi-sig admin key for DeFi community members.[194] "[T]hat structure meant that the team needed approval from a majority of the multi[-]sig for any form of discretionary spending."[195] In this case, admin keys were not used for legal

---

[189] Asad Gilani, *Ethereum Founder States Token-Based Decentralized Governance Stops DeFi Sector from Growing*, COIN NEWS (Aug. 21, 2021), https://bitcoinist.com/ethereum-founder-states-token-based-decentralized-governance-stops-defi-sector-from-growing/ [https://perma.cc/U44Y-7UAJ].

[190] Andrew Thurman, *Sushi Tries to Pick Up the Pieces: A DeFi Governance Case Study*, COINDESK (Dec. 30, 2021, 5:50 PM), https://www.coindesk.com/tech/2021/12/30/sushi-tries-to-pick-up-the-pieces-a-defi-governance-case-study/ [https://perma.cc/22D6-G85F].

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] *Id*.

enforcement but for DAO governance resolutions. Misused funds were returned, and investors found a resolution through the DAO.[196] Thus, admin keys may be part of holistic dispute resolutions going forwards.

3. A Cautionary Tale: Keys for Legal Enforcement: Tornado Cash

Tornado Cash is known as a "mixer"—these are "coin anonymizers," which break the identifying links in transactions, providing anonymity for users. "Tornado Cash is a decentralized, non-custodial privacy solution built on Ethereum. It improves transaction privacy by breaking the on-chain link between source and destination addresses. Tornado Cash uses a smart contract that accepts ETH and ERC-20 deposits to do this."[197]

The use cases vary for why coin anonymizers are needed. This means that bad actors can use Tornado Cash to hide their naughty deeds.[198] Yet, this is also an issue of crypto ideology, as many supporters argue that Tornado Cash provides the "Holy Grail" of privacy infrastructure.[199] Clearly, Tornado Cash is an important and controversial product in the Ethereum ecosystem.

In 2020, Tornado Cash's developers burned their admin keys, turning the privacy tool into permissionless code. This meant that they were not responsible for the platform.[200] Nothing could be attributed to the developers. The application then operated as self-executing code.[201] This means Tornado Cash truly became a perpetual persistent script, "completely trustless and

---

[196] Thurman, *supra* note 190.

[197] *Tornado Cash (TORN)*, BINANCE RSCH. (June 11, 2021), https://research.binance.com/en/projects/tornado-cash [https://perma.cc/S8H8-T6A4].

[198] Martin Young, *Roundup of Crypto Hacks, Exploits and Heists in 2020*, COINTELEGRAPH (Dec. 26, 2020), https://cointelegraph.com/news/roundup-of-crypto-hacks-exploits-and-heists-in-2020 [https://perma.cc/NLU2-HQKD].

[199] *Tornado Cash: The Holy Grail Token Observation of Private Transactions*, INEWS, https://inf.news/en/economy/d6386831266f143fecd347a1845762a2.html [https://perma.cc/PSD7-FZGA] (last visited Mar. 29, 2023).

[200] *Id.*

[201] *See* BINANCE RSCH., *supra* note 195; Andrew Thurman, *TORN Soars 200% as Tornado Cash's Governance Token Becomes Tradable*, COINTELEGRAPH (Feb. 9, 2021), https://cointelegraph.com/news/torn-soars-200-as-tornado-cash-s-governance-token-becomes-tradable/ [https://perma.cc/L3AR-S4DX].

unstoppable."[202] Tornado Cash had first launched in August 2019 but remained an audited "experimental software"[203] because the developers retained control over user funds through a multi-sig wallet. [204] While burning the admin keys removed the issue of an admin key "rug pull" risk, where a team member could take away all the funds out of the smart contract and disappear,[205] it also shows that, in theory, many DApp platforms simply burn their admin keys to avoid any possible legal enforcement. Thus, a consensus DAO-based approach could be a more appropriate enforcement option for a court. Alternatively, could a court or a consensus DAO-based approach pursue a fork to create new admin keys, as in the case of Tellor above?

Nevertheless, in August 2022, Tornado Cash was the target of the U.S. Treasury's Office of Foreign Assets Control ("OFAC"), which sanctioned the virtual currency "mixer" for being a money-laundering tool.[206] However, "[t]his is without saying

---

[202] "The ceremony, relying on a cryptographic method known as multi-party computation (MPC), makes Tornado Cash 'completely trustless and unstoppable,' co-founder Roman Storm said in an interview with CoinDesk." *See* William Foxley, *Developers of Ethereum Privacy Tool Tornado Cash Smash Their Keys*, COINDESK (May 18, 2020), https://www.coindesk.com/tech/2020/05/18/developers-of-ethereum-privacy-tool-tornado-cash-smash-their-keys/ [https://perma.cc/WQ4T-VEQF].

[203] Tornado Cash, *Introducing Private Transactions on Ethereum NOW!*, MEDIUM (Aug. 6, 2019), https://medium.com/@tornado.cash/introducing-private-transactions-on-ethereum-now-42ee915babe0 [https://perma.cc/8ULP-BN73].

[204] Foxley, *supra* note 202.

[205] *Admin Key*, DYOR CRYPTO WIKI, https://dyor-crypto.fandom.com/wiki/Admin_Key [https://perma.cc/CZW8-3F4T] (last visited Jan. 26, 2022). Whilst blockchains are decentralized and the funds are self-controlled, DApps, created by smart contracts deployed by a developer or team, are controlled by a private key. This removes the trustlessness of blockchain technology. Consequently, some projects "give over" the keys to the community, or create a multi-sig wallet, with well-known community members holding the keys. Other projects burn the keys, resulting in smart contracts/protocols that can only be updated by deploying a new protocol to which users can choose to migrate. *Id.*

[206] *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, U.S. TREASURY OFF. OF FOREIGN ASSETS CONTROL (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916 [https://perma.cc/CZW8-3F4T].

whether or not it's practical to sanction a piece of code."[207] For the purposes of this Article, questions could arise regarding whom to sanction, however platform founder(s) are certainly at risk.[208] Open-source software including building upon the Ethereum blockchain is accessible to anyone. And the Tornado Cash code is still accessible.

IV. CONCLUSION

Innovations in blockchain and smart contracting technologies present new challenges for legal enforcement. This discussion about admin keys may somewhat lessen the euphoric promise of smart contracts—better described as persistent scripts in decentralized finance ("DeFi"), and other crypto projects. Supporters of those projects may tend to deify the high levels of trust derived from the Ethereum blockchain, its resilience, and immutability. The immutability of smart contracts means that their terms cannot be altered after formation, unless a mechanism to effect various modifications was coded into the contract at its genesis.

For many DeFi platforms, one major and ill-often mentioned risk is linked to the private keys held by the platform administrators: admin keys. The platform administrators can modify the rules of the contract in an arbitrary manner. The existence of admin keys may be an avenue for legal (or other) intervention. However, for truly decentralized projects there is an increasing expectation that eventually the project will be handed over by the founders to a DAO structure. Moving from admin keys to a DAO adds another level of complexity for legal enforcement.

Yet, as this Article shows, this kind of enforcement may still be problematic, as seen in the examples of Uniswap and Tornado Cash.

---

[207] Zac Colbert, *OFAC Backtracks but Tornado Cash Sanctions Already Set a Terrifying Precedent*, COINDESK (Sept. 15, 2022), https://www.coindesk.com/layer2/2022/09/15/ofac-backtracks-but-tornado-cash-sanctions-already-set-a-terrifying-precedent/ [https://perma.cc/TQ8R-U52U].

[208] Joel Khalili, *A New Crypto Mixer Promises to be Tornado Cash Without the Crime*, WIRED (Mar. 3, 2023, 7:20 AM), https://www.wired.com/story/new-crypto-mixer-promises-to-be-tornado-cash-crime/#:~:text=Under%20the%20sanctions%E2%80%94which%20have,allowed%20to%20use%20Tornado%20Cash [https://perma.cc/CP5V-HN6M].

The cases of Tellor and SushiSwap, however, offer some promising indicators. Thus, identifying how the barriers to the off-chain legal enforcement of smart contracts can be surmounted—including relying on admin keys, understanding DAO governance protocols, and perhaps using legislation and regulation—is an area for further research.

As further institutional investment flows into crypto, as it did from 2020 to 2022, it is anticipated that a new competitive dynamic between existing dispute resolution mechanisms, legal enforcement through admin keys, and DAO governance tokens will emerge, creating new blockchain-based dispute resolution systems. How this evolutionary process will unfold ultimately comes from choices of contracting parties, investors, and State regulatory bodies.

"[A] core thesis of blockchain and cryptocurrencies is that we can relegate financial tasks and transactions to fully autonomous code."[209] The problem for the law is that "if you allow a token to govern over a protocol, you are allowing for two separate sets of incentives to be created. These sets of incentives may or may not be aligned."[210] Crucially, the concept of persistent scripts explains why admin keys exist and how they could potentially be used for legal enforcement in select circumstances.

[209] David Hoffman, *The Two Faces of Ethereum*, BANKLESS (Dec. 19, 2019), https://newsletter.banklesshq.com/p/the-two-faces-of-ethereum [https://perma.cc/VK3B-ZPWS].

[210] *Id*.