Washington Journal of Law, Technology & Arts

Volume 18
Issue 1 *BLOCKCHAIN, ARTS, & LAW*

Article 3

1-16-2023

REGULATORY SANDBOXES ENABLE PRAGMATIC BLOCKCHAIN REGULATION

Joshua Durham

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 18, ISSUE 1 WINTER 2023

REGULATORY SANDBOXES ENABLE PRAGMATIC BLOCKCHAIN REGULATION

Joshua Durham

ABSTRACT

Since blockchain technology supports digitally-native money, the centralized chokepoints that governments have traditionally targeted to regulate commerce no longer apply to our (digital) property. However, competent regulation furthers basic public policy goals and should enable responsible innovation of this promising technology. This Article discusses pragmatic policies that enable responsible innovation by cultivating regulatory expertise required to write enforceable rules. Responsible innovation is necessary because unlike the early internet, where programmers could manipulate simple colors and text on webpages, these same individuals can now create financial services applications that manipulate actual money—we are faced with an inescapable reality that more is at stake.

Keywords: *blockchain, crypto, cryptocurrency, DeFi, technology, sandbox, sand-box, innovation, responsible innovation, rule-making, Bitcoin, Ethereum, regulation, financial services, securities, commodities, money transmission*

TABLE OF CONTENTS

INTRODUCTION

> *Regulation in cyberspace is, or can be, different. If the regulator wants to induce a certain behavior, she need not threaten, or cajole, to inspire the change. She need only change the code–the software that defines the terms upon which the individual gains access to the system or uses assets on the system.*[1]

The internet fundamentally transformed society by providing an abundance of information and greater efficiency in communication. As countries moved online, people could then instantly send millions of files and messages to anyone else in the world at unprecedentedly low cost — this made the internet truly exceptional.[2] Chat rooms and email proliferated as paper-based communication systems declined.[3] However, the early internet brought only abundant content and data, thus creating a cyberspace that was not yet whole—innately scarce property could not be completely digitized.[4] Property like money, commodities, or stocks could not yet wholly exist as digital assets because they relied on centralized entities.[5]

In John Perry Barlow's famous declaration of independence of cyberspace, he confidently claimed that governments, the "weary giants of flesh and steel . . . possess [no] methods of enforcement" in cyberspace.[6] However, that declaration proved untrue. Governments largely engaged in business as usual, regulating known, centralized entities that happened to carry out

---

[1] Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan. L. REV. 1403, 1408 (1996).

[2] David G. Post, *Against Cyberanarchy*, 17 BERKELEY TECH. L.J. 1365, 1374 (2002).

[3] *See generally*, Barry M. Leiner, *Brief History of the Internet*, INTERNET SOCIETY (1997), https://www.internetsociety.org/internet/history-internet/brief-history-internet ("Roberts expanded its utility by writing the first email utility program to list, selectively read, file, forward, and respond to messages. From there email took off as the largest network application for over a decade. This was a harbinger of the kind of activity we see on the World Wide Web today, namely, the enormous growth of all kinds of 'people-to-people' traffic.").

[4] Der Gigi, *Bitcoin as an Idea*, https://dergigi.com/2021/06/13/bitcoin-is-an-idea/ (last visited Oct. 18, 2021) ("Various digital cash systems have been developed before Bitcoin. All of them failed eventually, and all for similar reasons. The following are particularly interesting in the context of Bitcoin:

> Ecash by David Chaum (1982)
> E-gold by Douglas Jackson and Barry Downey (1996)
> hashcash by Adam Back (1997)
> bit gold by Nick Szabo (1998)
> b-money by Wei Dai (1998)
> RPOW - Reusable Proofs of Work by Hal Finney (2004)

… 'I hope it's obvious it was only the centrally controlled nature of those systems that doomed them.'")

[5] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf (last visited Oct. 18, 2021) (explaining that digital property required trusted third parties to resolve the double spend problem because "[t]he problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.").

[6] John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/cyberspace-independence.

business online.[7] The early internet was not yet whole since its commerce still relied on physical financial infrastructure which served as traditional points of control by regulators.[8]

Now, however, blockchain technology provides a means to bring such property online, "extra-institutionally," bypassing the regulatory controls in place on centralized physical infrastructure.[9] By enabling digital scarcity, blockchain brings the once ethereal and abundant internet closer to reality. Critically, since assets are now digitally native, they are also programmable, meaning anyone can program financial services or even entire organizations onto a blockchain.[10] Consequently, the centralized chokepoints that governments have traditionally targeted to regulate the internet, no longer apply to our (digital) property.[11]

Since regulators can no longer control this digital property, including money, they will struggle to enforce their laws in cyberspace.[12] However, as Lawrence Lessig presciently wrote, regulators "need only change the [computer] code."[13] Blockchain as an internet innovation requires regulators to change their methods of enforcement, notably, by changing blockchain's actual

---

[7] *See generally* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1229-30 (1998).

[8] JOHANNES KÖPPEL, THE SWIFT AFFAIR: SWISS BANKING SECRECY AND THE FIGHT AGAINST TERRORIST FINANCING Annex 1 (2011), https://books.openedition.org/iheid/323 ("Before SWIFT came into existence, international interbank telecommunication was handled through Telex-Messages. They were not very secure and not automated. Telex Networks were developed from the 1930s onwards and they have been on the decline since the 1980s. The financial industry was one of the first industries to replace the Telex network through a proprietary system.1 In 1973, 239 banks from 15 countries founded SWIFT in order to create a shared worldwide data processing and communication link. . . General market transactions can be classified into three broad categories. (Geiger 2000) First, there are commercial transactions such as "business to business" or "business to consumer" transactions. Secondly, there are financial transactions such as "bank to business" or "bank to bank' transactions. "Bank to business" transaction involve a financial product or service, such as securities. Like "bank to bank" transactions, they are often of high value and electronically transmittable. The third category is "street side" transactions between banks and the banking system. All payments involving a seller and a buyer who do not have their respective accounts in the same bank, trigger secondary "street side" transactions, such as clearing and settlement. SWIFT plays the intermediary for transactions in the second and third categories of market transactions, where banks are involved.")

[9] Raina S. Haque et al., *Blockchain Development and Fiduciary Duty*, 2 Stan. J. BLOCKCHAIN L. & POL'y 139, 140 (2019).

[10] *Decentralized finance (DeFi)*, ETHEREUM.ORG (last accessed Oct. 30, 2021), https://ethereum.org/en/defi/; *Decentralized autonomous organizations (DAOs)*, ETHEREUM.ORG (last accessed Oct. 30, 2021), https://ethereum.org/en/dao/.

[11] There are no place-based physical intermediaries to regulate, financial services exist as mere lines of code.

[12] Iwa Salami, *Decentralised finance calls into question whether the crypto industry can ever be regulated,* THE CON
VERSATION (Dec. 11, 2021),https://theconversation.com/decentralised-finance-calls-into-question-whether-the-crypto-industry-can-ever-be-regulated-151222.

[13] Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 (1996).

computer code or the "law" by which blockchain operates.[14] Enforcing regulations through blockchain-native code is a new idea, but it already has been provably explored in research by Professor Carla Reyes.[15] Apart from changing the core rules of blockchain protocols, this Article suggests merely targeting the computer code that is deployed and executed on blockchains, particularly pertaining to decentralized finance (DeFi).

This Article is not about empowering regulators to arbitrarily throw their weight around a highly promising industry, nor is it about allowing innovators to deploy highly consequential code at their whims. Rather, this Article advocates responsible innovation by giving regulators the expertise required to write rules that make compliance possible, and then ensuring that compliance actually occurs.

Responsible innovation is necessary because unlike the early internet, where programmers could manipulate simple colors and text on webpages, these same individuals can now create financial services applications that manipulate actual money. More is at stake. Flawed computer code without safeguards can now result in billions of dollars lost or stolen from innocent consumers. Indeed, the budding blockchain industry has already suffered $2.99 billion worth of attacks in 2021 alone.[16] If this technology is the disruptive force that its proponents claim it to be, it must adopt robust consumer protections. Otherwise, adoption will be paltry, and hiccups severe. Promoting responsible innovation is an elementary and banal goal; however, since crypto policy is pursued so poorly, this Article resolves crypto policy's most glaring deficiencies that bar such responsible innovation.[17]

The practical steps required to implement compliant and responsible code in the present regulatory environment have been largely unexplored. Currently, instead of collaborative approaches, many regulators focus on antagonistic skirmishing that attempts to force unworkable rules onto this new technology.[18] Regulators must fight their "reflex to force age-old legal concepts from prior techno-economic paradigms onto new economic models."[19] At the same time,

---

[14] Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 Vill. L. Rev. 191 (2016) ("This Article lays the foundation for adopting an endogenous theory of decentralized technology regulation. Drawing on theories of endogenous economic regulation, endogenous development, and functional financial regulation, this Article proposes that decentralized technologies, including the blockchain technology underlying decentralized payment systems such as bitcoin, are robust enough to support a theory of endogenous, technology-assisted regulation. Specifically, when this Article proposes an endogenous theory of regulation, it suggests that regulators undertake the dual task of enacting a law or regulation via statute and then implementing that statute through code by engaging in an iterative and cooperative process with the technologies' core developers and with consensus from the network, so that regulation is endogenously incorporated into the decentralized ledger technology and the applications running on top of the technology.").

[15] Creating Cryptolaw for the Uniform Commercial Code, 78 WASH. & LEE L. REV. (forthcoming 2021) (developing smart contract based back-end software for the Article 9 filing system).

[16] Carla Mosée, *Cryptocurrency hacks and fraud are on track for a record number of incidents in 2021, data shows*, MARKETS INSIDER (Aug. 31, 2021), https://markets.businessinsider.com/news/currencies/cryptocurrency-hacks-fraud-cases-record-bitcoin-ethereum-wallets-breaches-defi-2021-8.

[17] Infra Section III.

[18] *See* discussion *infra* Section III.C.ii.

[19] Raina S. Haque, *Blockchain Development and Fiduciary Duty*, 2 STANFORD J. BLOCKCHAIN L. & POL'Y 139 (2019).

innovators must also communicate what rules and regulations would prove more practicable than current ones.[20] Regulators must then draft such workable regulations and incentivize industry participants to implement them in their code.

This Article argues that the above approach to responsible innovation implemented through computer code should be accomplished through the expansion of regulatory sandboxes. The regulatory sandbox proves to be an adaptable and efficient policy tool for any regulator first grappling with blockchain. Generally, a sandbox is a "safe space' in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question."[21]

Collaboration through these sandboxes would: (1) culminate in regulators the technical expertise required to draft practicable regulations, and (2) incentivize sandbox participants to incorporate such regulations in their code. In effect, this will produce "law as code," which will constitute the nascent stages of a secure blockchain infrastructure, or a "compliance layer" to the blockchain stack.

This analysis will consist of four parts. Part I explains blockchain technology and its implications. Part II summarizes the current ineffective methods of regulating blockchain. Part III explores sandboxes as the pragmatic solution to blockchain regulation.

I. BLOCKCHAIN PRIMER

Discussing the complex legal implications of blockchain is uniquely difficult because of its steep learning curve. As a result, inconsequential generalizations are necessary for coherence of analysis, please review the footnotes for more technical details.

A. Basic Terminology

This Article will use the following helpful definitions and terminology. Just as there are many different connected networks and internets that form "the internet," there are also many different blockchains that are (or will be) connected to form "the blockchain." Different blockchains are optimized for different purposes like security, decentralization, or efficiency.[22] Blockchain as a concept and technology is referred to as either "blockchain" or "blockchain technology." Specific networks or chains on the blockchain are referred to by their specific names, such as the "Ethereum blockchain" or "Bitcoin blockchain."

---

[20] Heather Hughes, *Designing Effective Regulation for Blockchain-Based Markets*, 46 J. CORP. L. 899 (2021) ("Effective regulation . . . requires platform developers and coders to communicate what they can automate and what they cannot, working with lawmakers and lawyers to yield the best possible confluence of automation, decentralization, and legal clarity.").

[21] FINANCIAL CONDUCT AUTHORITY, REGULATORY SANDBOX, 2015, at 1 (UK).

[22] *See* Nathaniel Popper, *The Rush to Coin Virtual Money with Real Value*, The New York Times (Nov. 11, 2013), https://dealbook.nytimes.com/2013/11/11/the-rush-to-coin-virtual-money-with-real-value [https://perma.cc/5LMD-QNXC].

As a data type, blockchain networks maintain separate blocks of data (e.g., transactions), that are chronologically linked to each other, forming a digital chain of blocks.[23] This chain, consisting of the "ledger," is the complete, global economic history of ownership on the blockchain.[24] While technologists may debate the precise nature and definition of a blockchain, for the purposes of this Article, blockchains are best understood as being: (1) physical networks that maintain virtual computers,[25] computing economic functions,[26] that (2) maintain a distributed ledger[27] in an append-only[28] manner, and (3) secured through various cryptographic consensus mechanisms.[29]

---

[23] *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (Nov. 8, 2008),
[24] Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (Jan. 2017), https://hbr.org/2017/01/the-truth-about-blockchain.
[25] ANDREAS M. ANTONOPOULOS & GAVIN WOOD, MASTERING ETHEREUM: BUILDING SMART CONTRACTS AND DAPPS ch. 1 (2018).
[26] *Id.*
[27] Blockchains maintain a single, shared ledger of all economic activity. A ledger is a record of accounts and transactions. Ledger, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A book or series of books used for recording financial transactions in the form of debits and credits; esp., a book in which a business or bank records how much money it receives and spends. — Also termed general ledger."). In its simplest form, ledgers can be used to record transactions as a credit from one account and an equal debit to another account. This method of accounting (i.e., double-entry bookkeeping) is the foundation of modern capitalism. *See* MAX WEBER, GENERAL ECONOMIC HISTORY 208 (Frank H. Knight Trans., First Collier Books ed., 1961) ("[T]he most general presupposition for the existence of . . . present-day capitalism is that of rational capital accounting . . . .").Blockchain is a form of Distributed Ledger Technology (DLT). Harish Natarajan et at., *Distributed Ledger Technology (DLT) and Blockchain*, WORLD BANK GROUP VII (2017), https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf ("A 'blockchain' is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called 'blocks' that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner."). Instead of one centralized server and ledger, DLT takes one ledger and duplicates it across different computers (nodes), *Id.* at 2 ("A shared ledger can be a . . . distributed ledger which consists of multiple ledgers maintained by a distributed network of nodes . . .") with a validation and consensus scheme explained below. *Id.* at 1-2. All changes to the ledger are publicly available, and processed simultaneously and in parallel on every node. In other words, every transaction is redundantly computed by every single node, thus ensuring accuracy. This architecture of redundancy and cryptographically-based validation is a hallmark of modern cybersecurity. Bev Littlewood and Lorenzo Strigini, *Redundancy and Diversity in Security*, *in* COMPUTER SECURITY – ESORICS 2004 423, 423 (2004) ("Redundancy as a general approach is clearly understood to be a valid defense against physical faults. There is a rich set of understood design "tricks" that use redundancy against various forms of faults and failures, and knowledge about how to optimize them for different purposes . . .").
[28] *Blockchain & Distributed Ledger Technology (DLT)*, WORLD BANK, https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt (Apr. 12, 2018).
[29] To process new blockchain transactions and other economic activity (i.e., add new blocks), blockchain networks levy cryptographic and algorithmic methods to maintain consensus on the correct and updated state of their ledger by making it prohibitively expensive to add fraudulent blocks. To add such fraudulent blocks, one must control more than half of the network (i.e., a 51% attack). Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Comprehensive Survey*, 22 IEEE COMMC'NS SURVS. AND TUTORIALS 1977, 1981 (2020) ("Conceptually, Blockchain can be viewed as a repository of data that is tamper-evident due to its replication over all nodes in a peer-to-peer system. Transactions represent the events that drive the Blockchain application. Blockchain applications use various consensus algorithms for trust among peers over the state of the ledger. Moreover, the consensus algorithms ensure a consistent and transparent view of the Blockchain, thereby resolving conflicts and forks. This is, no block is added to the Blockchain, until it fulfills the conditions outlined by the consensus algorithm. Moreover, each algorithm has unique functional and operational properties that drive the consensus over the Blockchain."). Two major consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS), PoW secures a blockchain by requiring "miners"

With such core functionality, blockchains enable new forms of scarce data to be transmitted over the internet, including money (i.e., cryptocurrency).[30] The validity of this scarcity is "based on cryptographic proof instead of trust" in third parties, like banks.[31] Transactions processed on blockchains can be publicly viewable and prohibitively expensive to reverse, thus ensuring finality of payments and ensuring that payors cannot fraudulently spend the same cryptocurrency twice.[32]

The first globalized blockchain and accompanying cryptocurrency was described in the Bitcoin whitepaper in 2008.[33] Its anonymous creator(s) combined more than 40 years' worth of cryptographic research[34] in a novel way to create the world's first decentralized and internet-native digital currency.[35] While there have been different blockchains developed since 2008, this Article addresses the blockchains that contain similar elements as Ethereum[36]: (1) distributed ledgers and (2) consensus mechanisms, that (3) enable blockchain-based smart contracts.[37]

(i.e., nodes that validate transactions and blocks) to use immense computing power and electricity to validate transactions and new blocks. *Id. But see* Jon Truby et al., *Blockchain, Climate Damage, and Death: Policy Interventions to Reduce the Carbon Emissions, Mortality, and Net-Zero Implications of Non-Fungible Tokens and Bitcoin*, 88 ENERGY RSCH. & SOC. SCI. 1, 11 (2022) (discussing the perverse climate consequences of the use of NFTs in energy-intensive PoW mining). The more computing power a miner has, the higher the likelihood of mining a new block, which rewards that miner with cryptocurrency. If someone wanted to take over the network to add faulty transactions, they would have to control more than half of the entirety of the computing power of the network, which is economically unfeasible with large and mature blockchains. Saad, *supra* note 49, at 1982. Conversely, PoS secures a blockchain by requiring "validators" (i.e., nodes that validate transactions and blocks) to "stake" (i.e., lock up) a portion of their tokens to validate transactions and new blocks. *Id.* The higher the amount staked, the higher the likelihood of validating a new block, which rewards that validator with cryptocurrency. With some PoS schemes, if an entity unsuccessfully attempted to push a faulty transaction or block, they would lose their staked cryptocurrency which raises the costs of an attack. *Id.* Like PoW, in PoS, someone would have to control more than half of a blockchain's staked value to successfully take over the network which is prohibitively expensive with large and mature blockchains. *Id.*

[30] *See generally* Satoshi Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System (Oct. 31, 2008) (unpublished manuscript), https://bitcoin.org/bitcoin.pdf [https://perma.cc/QGW4-W934] (last visited Oct. 26 2021). Nakamoto's identity has never been conclusively identified.

[31] *Id.* at 1.

[32] Emmanuelle Anceaume et al., *On finality in blockchains*, HAL 2 (revised Sept. 9, 2021), https://hal-cea.archives-ouvertes.fr/cea-03080029v3/document.

[33] *See generally* Nakamoto, supra note 31.

[34] David Andreesson, *Why Bitcoin Matters,* N.Y. TIMES (Jan. 21, 2014, 11:54 AM), https://archive.nytimes.com/dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/.

[35] The most fundamental innovations are digital signatures and public-key cryptography. *See generally,* Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IEEE TRANSACTIONS ON INFORMATION THEORY VOL. IT-22, NO. 6, 644 (Nov. 1976); R.L. Rivest, A. Shamir & L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMMUNICATIONS OF THE ACM, 120 (Feb. 1978).

[36] For example, some of the most widely used blockchain networks that enable smart contract functionality are: Ethereum, Solana, Stellar, Polkadot, Tezos, Cardano, and Algorand. These blockchains are not wholly private and incorporate complex smart contracting. *Infra* note 31.

[37] Kevin Werbach*, Trust, but Verify: Why the Blockchain Needs the Law*, 33 BERKELEY TECH. L.J. 489 (2018).

"Public" blockchains, like Bitcoin and Ethereum, are "permissionless" since any member of the public may interact with them.[38] "Private" blockchains, like Hyperledger, are "permissioned" since users and participants must seek approval by a centralized authority before interacting with these blockchain.[39] Because private blockchains are maintained by known, centralized entities, they do not readily pose the same legal implications as public blockchains. As such, this Article will only consider public blockchains, with case studies and examples particularly relating to the Ethereum blockchain.

B. Distributed Ledgers

A ledger is a record of accounts and transactions.[40] In short, ledgers can be used to record transactions as a credit from one account and an equal debit to another account. This method of accounting (i.e., double-entry bookkeeping) is the foundation of modern capitalism.[41]

Blockchain is a form of Distributed Ledger Technology (DLT).[42] Instead of one centralized server and ledger, DLT takes one ledger and distributes it across different computers (e.g., nodes)[43] to simultaneously, and in parallel, process transactions by implementing a game theoretic[44] validation and consensus scheme.[45] This architecture of redundancy and cryptographically-based validation is a hallmark of modern cybersecurity.[46]

---

[38] Fran Casino et al., *A systematic literature review of blockchain-based applications: Current status, classification and* 36TELEMATICSANDINFORMATICS55,57(2019), https://www.sciencedirect.com/science/article/pii/S0736585318306324.

[39] *Id.*

[40] Ledger, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A book or series of books used for recording financial transactions in the form of debits and credits; esp., a book in which a business or bank records how much money it receives and spends. — Also termed general ledger.").

[41] *See* Max Weber, GENERAL ECONOMIC HISTORY 276 (Frank H. Knight trans., 1927) ("[T]he most general presupposition for the existence of . . . present-day capitalism is that of rational capital accounting . . . .").

[42] *Distributed Ledger Technology (DLT) and Blockchain*, WORLD BANK GROUP, at VII (2017) ("A 'blockchain' is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called 'blocks' that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic method storecord and synchronize data across a network in an immutable manner."), https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=5&isAllowed=y.

[43] *Id.* at 2 ("A shared ledger can be a . . . distributed ledger which consists of multiple ledgers maintained by a distributed network of nodes . . .").

[44] *See generally* Z. Liu, *A Survey on Blockchain: A Game Theoretical Perspective*, 7 IEEE ACCESS 47615 (2019).

[45] WORLD BANK GROUP, *supra* note 43, at 2.

[46] Bev Littlewood & Lorenzo Strigini, *Redundancy and Diversity in Security*, CENTER OF SOFTWARE RELIABILITY (2004) ("Redundancy as a general approach is clearly understood to be a valid defense against physical faults. There is a rich set of understood design "tricks" that use redundancy against various forms of faults and failures, and knowledge about how to optimize them for different purposes . . .").

All changes to the ledger are publicly available, but users' personal financial data remains protected since their identities are at least pseudonymous, and at most wholly anonymous.[47] For example, on the Ethereum blockchain, user account addresses only exist as semi-random sets of 42 characters.[48] These addresses are "pseudonymous" because all users' financial activity is traced to their addresses, but their addresses do not inherently link to the users' actual identities. Conversely, on the Zcash blockchain, transactions can be fully anonymous because they are not traceable to any one address.[49]

C. Consensus

To process cryptocurrency transactions (i.e., add them to the new block), blockchains levy cryptographic methods that record and synchronize data across the blockchain network.[50] These methods maintain consensus on the correct and updated state of their ledger. To make it prohibitively expensive to take over a network (i.e., controlling more than half of the nodes), blockchains maintain consensus through various consensus mechanisms such as Proof of Work and Proof of Stake.[51]

"Proof of Work" (PoW) secures a blockchain by requiring "miners" (i.e., nodes that validate transactions and blocks) to use immense computing power and electricity to validate transactions and new blocks.[52] The more computing power a miner has, the higher the likelihood

---

[47] *Distributed Ledger Technology (DLT) and Blockchain*, WORLD BANK GROUP, at 4 ("The anonymity offered for transacting rapidly online attracted the attention of criminals and Bitcoin has been used for financing illicit activities. However, even though the identities of transacting partners can be anonymous, all Bitcoin transactions are recorded in a distributed ledger that is visible to the public and it is possible to associate Bitcoin transactions with specific anonymous entities. (This is why the term 'pseudonymous' is often used in the context of Bitcoin.) The anonymity provided by Bitcoin can be compared to the anonymity provided by an email address. All Bitcoin transactions contain a wallet address of the sender and the receiver, which can be thought of as pseudonyms, similar to email addresses.") https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=5&isAllowed=y.

[48] *See* Dr.. Gavin Wood, *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER BERLIN VERSION 888949c*, at 18 (Dec. 15, 2021), https://ethereum.github.io/yellowpaper/paper.pdf ("Address: A 160-bit code used for identifying Accounts.").

[49] Symposium, *Empirical Analysis of Anonymity in Zcash*, 27TH USENIX CONFERENCE ON SECURITY (Aug. 2018) ("To receive funds, users can provide either a transparent address (t-address) or a shielded address (z-address). Coins that are held in z-addresses are said to be in the shielded pool."). https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf.

[50] *Supra* note 33.

[51] Muhammad Saad et al., *Exploring the Attack Surface of Blockchain: A Comprehensive Survey*, 22 IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, 1977, 1981 (2020). ("Conceptually, Blockchain can be viewed as a repository of data that is tamper-evident due to its replication over all nodes in a peer-to-peer system. Transactions represent the events that drive the Blockchain application. Blockchain applications use various consensus algorithms for trust among peers over the state of the ledger. Moreover, the consensus algorithms ensure a consistent and transparent view of the Blockchain, thereby resolving conflicts and forks. This is, no block is added to the Blockchain, until it fulfills the conditions outlined by the consensus algorithm. Moreover, each algorithm has unique functional and operational properties that drive the consensus over the Blockchain."). https://ieeexplore.ieee.org/abstract/document/9019870?casa_token=VN4beCawl2QAAAAA:1iin50UDm12ZKqrEfOWN7-zKpS8VvdtGkOMH44A7l-moJr9CPxXCz-nUcNQySNWuY44sGbTCMg.

[52] *Id*.

of mining a new block, which rewards that miner with cryptocurrency.[53] If someone wished to take over the network to add inaccurate transactions, they would have to control more than half of the entirety of the computing power of the blockchain's miners, which is economically unfeasible with large and mature blockchains.[54]

"Proof of Stake" (PoS) secures a blockchain by requiring "validators" (i.e., nodes that validate transactions and blocks) to "stake" (i.e., lock up) a portion of their tokens to validate transactions and new blocks.[55] The higher the amount staked, the higher the likelihood of validating a new block, which rewards that validator with cryptocurrency. With some PoS schemes, if an entity unsuccessfully attempted to push a faulty transaction or block, they would lose their staked cryptocurrency which raises the costs of an attack.[56] Like PoW, in PoS, someone would have to control more than half of a blockchain's staked value to successfully take over the network which is prohibitively expensive with large and mature blockchains.[57]

D. Blockchain Enables Programmable Money

The unprecedented levels of security in some blockchains, from fully transparent and auditable operational code to crypto-economic consensus mechanisms, enable currencies, unique assets, and other sensitive or scarce data to exist solely on the internet, without relying on centralized physical infrastructure or entities. Unlike fiat money, where currencies issued by countries are backed by the mercurial "full faith and credit" of governments, blockchain-based cryptocurrencies are backed by hard cryptographic proof. Importantly, since money is now digitally native, it is also programmable by code called smart contracts.[58]

---

[53] *Id*.
[54] *Id*. at 1982.
[55] *Id*.
[56] *Id*.
[57] *Id*.
[58] Alexander Lee, *What is programmable money?*, Board of Governors of the Federal Reserve System (Jun. 23, 2021), https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.htm ("One facet of successful public blockchain systems that may provide some clarity is how they closely link digital value and programmability in a single system that only functions properly when both are present. In traditional financial technology systems, digital money is typically defined by database entries. Any "programmability" offered for this money, whether internally to the entity maintaining the database or exposed to its customers via an application programming interface (API), involves another technology system built separately from that database and then connected in some fashion. While newer cryptocurrency systems also use a database (often in the form of a blockchain data structure), a key difference is that the records in such blockchains either directly incorporate some programmable script (as Bitcoin records do, for example), or sit alongside a general programming functionality within the system that allows for direct manipulation of those records (the model used by Ethereum, among others). In both designs, the value represented in those systems and the programmability of that value are tightly integrated. There is no notion, for example, of "bitcoins" without an associated script governing their spending conditions, whereas a traditional ledger could certainly hold digital records of money without offering a programming interface to those records.").

Developers can now write smart contracts that execute simple or complex tasks with cryptocurrencies on the Ethereum blockchain.[59] Termed decentralized finance ("DeFi"), financial services can exist as mere smart contracts on a blockchain.[60] Like a financial Rube Goldberg machine, users of the Ethereum blockchain who seek the financial services of DeFi applications merely have to send their cryptocurrency to them, then their smart contracts will automatically execute their predetermined functions using that cryptocurrency. Moreover, smart contracts are deployed and run on a distributed blockchain network, not in centralized servers. Thus, smart contracts are as immutable as transactions. The fact that mere lines of code can provide the same services as brick-and-mortar businesses proves how potent blockchain is as an innovation.

II. CURRENT INEFFECTIVE BLOCKCHAIN REGULATORY APPROACHES

This section explores impracticable approaches to blockchain regulation that led to impossible compliance and impossible enforcement. Instead of evaluating the justifications of such regulations, this section will expose the technical realities that are pain points for legislators and regulators. Lastly, this section will explain why the enforcement of any regulation—even if practicable—requires changing the actual code of smart contracts.

Since blockchain-based digital assets can exist in many forms and can be programmed to serve many different uses, no one regulatory agency has jurisdiction over these assets or their users and developers. Depending on its use, a blockchain-based digital asset or service "may be regulated pursuant to securities law, commodities law, money transmission law or consumer protection law."[61] None of these regulatory regimes have been tailored to the operational realities of a public blockchain network,[62] and all assume centralized, and therefore regulable entities.[63]

Although regulators can still levy place-based approaches to regulation by targeting centralized and known entities, that form of regulation is no longer sufficient because the same financial services of such entities now immutably exist as code on blockchains. Our New Deal era

---

[59] Fabian Schär, *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*, FEDERAL RESERVE BANK OF ST. LOUIS REVIEW 153 ("Decentralized finance (DeFi) is a blockchain-based financial infrastructure that has recently gained a lot of traction. The term generally refers to an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms, such as the Ethereum blockchain (see Buterin, 2013). It replicates existing financial services in a more open and transparent way. In particular, DeFi does not rely on intermediaries and centralized institutions. Instead, it is based on open protocols and decentralized applications (DApps). Agreements are enforced by code, transactions are executed in a secure and verifiable way, and legitimate state changes persist on a public blockchain. Thus, this architecture can create an immutable and highly interoperable financial system with unprecedented transparency, equal access rights, and little need for custodians, central clearing houses, or escrow services, as most of these roles can be assumed by "smart contracts."").

[60] *Id*.

[61] Lewis Cohen, *Blockchain 2021*, CHAMBERS (Jun. 17, 2021) https://practiceguides.chambers.com/practice-guides/blockchain-2021.

[62] Id.

[63] *See generally*, Cong. Research Serv., R44918, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework*, 24-5 (updated Mar. 10, 2020), https://sgp.fas.org/crs/misc/R44918.pdf. https://sgp.fas.org/crs/misc/R44918.pdf.

financial regulation regime, that assumes centralized entities,[64] is no longer fit for a world of decentralized financial services. Indeed, some regulators have even concluded that much of DeFi is entirely illegal precisely because it offers financial services without using regulable intermediaries.[65] This policy stance is unrealistic because it suggests technological regress for the sake of regulatory compliance, and it does not otherwise offer alternative approaches that better fit the technology.

Fundamentally, legislators and regulators currently lack the expertise required to adapt regulatory approaches to blockchain. Without this expertise, regulators cannot draft rules that enable technical compliance. Moreover, even if rules are promulgated that do allow for technical compliance, the highly decentralized DeFi context makes it difficult to ensure that such rules are even enforceable. Thus, even practicable rules that further responsible innovation nevertheless face futile enforcement. As such, regulators have the additional challenge of currying industry buy-in of such regulations, solutions to which are later addressed in Section IV.

A. Impossible Compliance

Several layers of government, from Congress to executive agencies, have promulgated laws and regulations without accounting for the technical and legal realities of blockchain. Consequently, such laws and regulations are impossible with which to comply. Three major mistakes by Congress, the SEC, and FinCEN are explored below.

In the fall of 2021, Congress embedded a cryptocurrency reporting provision in its $1 trillion infrastructure bill. The initial drafted definition of a "broker" was so broad that it encompassed cryptocurrency miners and developers—entities that cannot technically comply with the identity recordation requirements of brokers, and that do not otherwise act as brokers.[66] Even worse, in a proposed amendment to address this breadth, the definition of a broker would not have included anyone who "validat[es] distributed ledger transactions through proof of work (mining)."[67] This amendment wholly ignored other consensus mechanisms like PoS, which is more environmentally friendly than PoW and was effectively "a government-sanctioned safe harbor for the most climate-damaging form of crypto tech:" PoW.[68] Thus, a lack of care and expertise in drafting this bill made compliance with it impossible and created perverse and

---

[64] *See, for example*, Kimberly Amadeo, *New Deal Summary, Programs, Policies, and Its Success*, THE BALANCE (Jul. 30, 2020), https://www.thebalance.com/fdr-and-the-new-deal-programs-timeline-did-it-work-3305598 (The FDIC, for example, insures banks. Before blockchain, centralized entities, like banks, were necessary to provide financial services. This concept of centralization is so inherent in financial services, that it informs every aspect of its regulation. Now, however, financial services can be provided by decentralized, lifeless code).

[65] Comm'r Dan M. Berkovitz, *Climate Change and Decentralized Finance: New Challenges for the CFTC*, CFTC (Jun. 8, 2021), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaberkovitz7.

[66] Kalina Hannsz, *U.S. Treasury Signals that Cryptocurrency Miners & Stakers Will Not Be Subject to Broker Information Reporting Tax Requirements*, JD SUPRA (Feb. 17, 2022).

[67] 167 Cong. Rec. S140,5982 (2021).

[68] @RonWyden, Twitter (Aug. 5, 20210, 10:19 PM) https://twitter.com/RonWyden/status/1423468825610129411?s=2.

unintended policy outcomes. Such deficiencies are not unique to Congress, regulatory agencies have also made mistakes.

Regulatory agencies exist to implement the specifics of otherwise generalized laws. Regulators obtain the expertise required to adapt regulations in furtherance of a broad statutory mandate because they oversee constantly shifting industries and technologies.[69] Nevertheless, agencies like the SEC and FinCEN have struggled to apply regulations to blockchain technology, explored below.

Although cryptocurrency exchanges desire to be regulated by the SEC, compliance is nevertheless impossible because the SEC has stonewalled compliance with its own rules regarding exchanges since at least 2018. The SEC has been reluctant to allow FINRA to approve cryptocurrency custodians as securities exchanges or Alternative Trading systems (ATS).[70] Such registration is nevertheless required if an exchange wants to trade cryptocurrencies that are deemed securities,[71] which the SEC has not even sufficiently clarified.[72] Consequently, the SEC has put cryptocurrency exchanges in a "catch 22"[73] where they must register as exchanges or ATSs in order to facilitate trading of securities because they do not know which cryptocurrencies are securities, but the SEC will nevertheless not grant them such licenses. In effect, the industry has been forced to craft their own standards in attempting to divine which cryptocurrencies the SEC

---

[69] Sidney A. Shapiro, *The Failure to Understand Expertise in Administrative Law: The Problem and the Consequences*, 50 WAKE Forest L. REV. 1097, 1110–11 (2015); *see also* Cong. Research Serv., R44918, Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework, 6 (2020),

[70] Hester Peirce, In the Matter of Poloniex, LLC, (Aug. 9, 2021) U.S. SEC, https://www.sec.gov/news/public-statement/pierce-statement-poloniex-080921

[71] *See* 15 U.S.C. §§ 78e–78f; 17 CFR 240.3a1–1(a)(1)-(3).

[72] Comm'r Hester M. Peirce*, In the Matter of Poloniex, LLC* (Aug. 9, 2021) https://www.sec.gov/news/public-statement/pierce-statement-poloniex-080921 ("The Commission has been reluctant to help provide clarity, even, as evidenced by today's action, refusing to alert the market to securities determinations it has made in connection with enforcement actions like this one.").

[73] Laura Shin, *How the Greatest Decentralizing Force for Crypto Projects Is the SEC*, UNCHAINED (OCT. 5, 2021) (interviewing Collins Belton, who outlined the "catch 22.") https://unchainedpodcast.com/how-the-greatest-decentralizing-force-for-crypto-projects-is-the-sec/.

may deem as securities,[74] because the SEC has not found solutions to problems concerning registration with the SEC.[75]

Moreover, the SEC has even pursued enforcement actions against exchanges for not registering with the SEC, even though the SEC would have not accepted their application anyway. Poloniex, for example, settled with the SEC for $10,388,309.10 because it operated an exchange that made available "digital assets that were offered and sold as securities."[76] Nevertheless, the SEC did not explain which digital assets were securities.[77] Although Poloniex could have attempted to obtain a license, it would have only waited in vain.[78] Indeed, Coinbase, another cryptocurrency exchange, has been waiting since 2018.[79] The lack of clarity on which assets are securities, coupled with FINRA and the SEC not allowing cryptocurrency exchanges to register as

---

[74] Securities Law Framework, CRYPTO RATING COUNCIL (last updated May 10, 2021) https://www.cryptoratingcouncil.com/framework.

[75] Commissioner Hester M. Peirce*, In the Matter of Poloniex, LLC* (Aug. 9, 2021) https://www.sec.gov/news/public-statement/pierce-statement-poloniex-080921 ("Can the platform custody client assets, a feature typical of centralized crypto trading platforms? If so, how, given our concerns about custody of digital asset securities? If not, could a sufficient number of broker-dealers navigate the registration process to make a liquid market? Would the conditions placed on their registration permit them to function as market makers or to facilitate trading on behalf of retail investors? Can the platform trade non-securities alongside securities? If not, how can the platform, using two entities—a broker-dealer entity for digital asset securities, and an affiliated non-broker-dealer entity for non-securities, offer a seamless, or at least serviceable, trading platform to customers, who are likely, for example, to want to trade both digital assets and digital asset securities and pay for transactions in digital asset securities using non-security digital assets? How can a trading platform and its customers determine whether a particular digital asset is a security? If a token was sold in a securities offering as part of an investment contract, how long must secondary transactions in that token be deemed to be securities transactions by platforms trading the tokens? What are the mechanics of registering tokens sold as part of an investment contract as a class of "equity security" under the Exchange Act?").

[76] POLONIEX, LLC, Exchange Act Release No. 92607 (cease and desist order), https://www.sec.gov/litigation/admin/2021/34-92607.pdf.

[77] *Id.*

[78] Commissioner Hester M. Peirce*, In the Matter of Poloniex, LLC* (Aug. 9, 2021) https://www.sec.gov/news/public-statement/pierce-statement-poloniex-080921 ("Had it done so, it likely would have waited . . . and waited . . . and waited some more.").

[79] Asiff Hirji, *Our path to listing SEC-regulated crypto securities*, THE COINBASE BLOG (Jun. 6, 2018) (announcing their applications for several licenses that will allow them to trade securities) https://blog.coinbase.com/our-path-to-listing-sec-regulated-crypto-securities-a1724e13bb5a.; Coinbase Global, Inc., Registration Statement (Form S-1) (Feb. 25, 2021) https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm ("Although we have applied to operate an ATS in the United States that would allow us to trade crypto assets that are deemed "securities" under U.S. federal securities laws, we have not yet received regulatory approval to, and do not currently, operate an ATS for trading of crypto assets deemed to be securities. Even though we have incurred substantial expenses and compliance costs, we may never receive regulatory approval to operate an ATS for the trading of crypto assets that constitute securities and, even if we were to receive such regulatory approval, the markets for trading crypto assets that constitute securities may lack the depth and liquidity of our platform. There can be no assurances that we will properly characterize any given crypto asset as a security or non-security for purposes of determining which of our platforms that crypto asset is allowed to trade on, or that the SEC, foreign regulatory authority, or a court, if the question was presented to it, would agree with our assessment. If the SEC, foreign regulatory authority, or a court were to determine that a supported crypto asset currently offered, sold, or traded on our platform is a security, we would not be able to offer such crypto asset for trading until we are able to do so in a compliant manner, such as through an ATS approved to trade crypto asset that constitute securities.")

exchanges or ATSs, has invariably stifled innovation,[80] and has moved innovation into the more decentralized and unregulable corners of the blockchain. As such, the SEC has become "the best motivator of making something truly decentralized"—and thus unregulable.[81]

Another example of impracticable agency action is illustrated by the Financial Crimes Enforcement Network (FinCEN)'s alleged "midnight rulemaking."[82] On December 23, 2020, FinCEN promulgated a notice of proposed rulemaking that afforded a mere 15 days to comment, while most regulatory agencies usually afford 50-60 days.[83] The rule would have imposed impossible recordkeeping requirements on certain "convertible virtual currency" ("CVC," e.g., cryptocurrency) payments that are not otherwise imposed on the traditional financial system. In particular, CVC transactions above $3,000 were to be subject to extraordinary requirements where "customer counterparties [must be] identified by name and physical address."[84] However, "counterparties" in cryptocurrency transactions are oftentimes just smart contracts that exist solely on the blockchain, lacking any name and physical address.[85] Even when transactions are between two individuals, it is technically impossible to accurately obtain their actual names and physical addresses since they transact using only their pseudonymous blockchain addresses.

Recall that the blockchains operate by having "addresses" (pseudorandom strings of characters) act as the identifying destinations of transactions. The base-layer code of blockchains purposefully does not include features like recording real-world identities because that is wholly undesirable from a privacy perspective.[86] Since the financial histories of all addresses are wholly public and transparent, the only way people maintain their financial privacy is through interacting

---

[80] *See generally,* Kaushal & Sheel Tyle, The Blockchain: What It Is and Why It Matters, BROOKINGS: TECHTANK (Jan. 13, 2015), https://www.brookings.edu/blog/techtank/2015/01/13/the-blockchain-what-it-is-and-why-it-matters/ ("Disruptive technologies rarely fit neatly into existing regulatory considerations, but rigid regulatory frameworks have repeatedly stifled innovation. It's likely that innovations in the Blockchain will outpace policy, let's not slow it down.").

[81] Laura Chin, *How the Greatest Decentralizing Force for Crypto Projects Is the SEC, Unchained* (Oct. 5, 2021), https://unchainedpodcast.com/how-the-greatest-decentralizing-force-for-crypto-projects-is-the-sec/.

[82] Katie Haun, *Why a16z Opposes Secretary Mnuchin's FinCEN Midnight Crypto Rulemaking*, ANDREESSEN HOROWITZ (Jan. 4, 2021).

[83] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840 (proposed Dec. 23, 2020).

[84] Jerry Brito & Peter Van Valkenburgh, *Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, ,* (Dec. 22, 2020), https://www.coincenter.org/comments-to-the-financial-crimes-enforcement-network-on-requirements-for-certain-transactions-involving-convertible-virtualcurrency-or-digital-assets/.

[85] *ETHEREUM ACCOUNTS*, ETHEREUM.ORG (last edit Sep. 5, 2021) https://ethereum.org/en/developers/docs/accounts/ (On the Ethereum blockchain, there are two types of accounts: externally owned accounts ("EOA") and contract accounts. Externally owned accounts are owned and controlled by individuals, they hold their cryptocurrency in this account and can interact with smart contracts through it. Contract accounts are smart contracts. If I want to interact with a smart contract, I identify the contract's address and then interact with it through my EOA. Both EOA and contract accounts have the same type of address format, like 0x89205A3A3b2A69De6Dbf7f01ED13B2108B2c43e7, which is all one needs to interact with any one account, like sending money to an individual or smart contract.)

[86] *See* Wood, *supra note 39* at 3, 18 (Dec. 15, 2021) ("The world state (state), is a mapping between addresses (160-bit identifiers) and account states (a data structure serialized as RLP, see Appendix B).").

with blockchains through their pseudorandom addresses, rather than through identifying information such as their name and physical address. FinCEN's proposed reporting requirements would also invoke grave Fourth Amendment concerns since they mandate the "specific collection of information about persons who are not even customers of a financial institution," which "oversteps the established constitutional bounds of acceptable warrantless searches and seizures by financial institutions.[87]

In sum, Congress and regulatory agencies have failed to promulgate practicable policies because they lack the requisite expertise for drafting laws and regulations that allow for technical compliance.

B. Impossible Enforcement

Legislators and regulators are faced with the additional challenge of enforcing laws and regulations, even if they allow for technical compliance. If centralized entities could technically comply with proposed regulations by FinCEN, they would invariably do so, but what about their decentralized counterparts? Regulation works due to a future threat of enforcement against known and therefore regulable entities. However, since blockchain developers can be anonymous—with their code immutably existing on a blockchain—there is scant an entity to target with enforcement other than individual users. Take, for example, three cryptocurrency exchanges listed by increasing levels of decentralization, and therefore unregulability: Coinbase, Uniswap, and Sushiswap.

Coinbase is a publicly traded company operating as one of the world's largest cryptocurrency exchanges by trading volume.[88] Consumers may purchase cryptocurrency with USD by linking their bank accounts or credit/debit cards, or they may purchase cryptocurrencies with other cryptocurrencies.[89] Since Coinbase is necessarily tethered to the traditional financial system by allowing USD purchases of cryptocurrency, its business model assumes regulatory compliance. Indeed, Coinbase has registered with FinCEN as a money transmitter[90] and is registered in all such states that require money transmitter licenses.[91] It has a CEO, observes all corporate formalities and SEC disclosures, and otherwise operates its business as any other

---

[87] Brito & Van Valkenburgh, supra note 72 at 26.

[88] *Top Cryptocurrency Spot Exchanges*, COINMARKETCAP (last visited Oct. 24, 2021), https://coinmarketcap.com/rankings/exchanges/.

[89] Coinbase Global, Inc., *Registration Statement* (Form S-1) (Feb. 25, 2021), https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm ("We rely on bank accounts to provide our platform and custodial services. In particular, customer cash holdings on our platform are held with one or more of our banking partners. As a registered money services business with FinCEN under the Bank Secrecy Act, as amended by the USA PATRIOT Act of 2001, and its implementing regulations enforced by FinCEN, or collectively, the BSA, a licensed money transmitter in a number of U.S. states and territories, a licensee under NYDFS's Virtual Currency Business Activity regime, commonly referred to as a BitLicense, a licensed electronic money institution under both the U.K. Financial Conduct Authority and the Central Bank of Ireland, and a limited purpose trust company chartered by the NYDFS, our banking partners view us as a higher risk customer for purposes of their anti-money laundering programs.").

[90] *Id*.

[91] *Legal*, COINBASE (last visited Oct. 24, 2021), https://www.coinbase.com/legal/licenses.

regulated corporation. Since Coinbase's cryptocurrency business model is centralized and tied to the traditional financial systems, it can be targeted with enforcement actions, and consequently remains compliant with applicable regulations.

Uniswap is Coinbase's more decentralized counterpart. Unlike Coinbase, Uniswap does not plug into the traditional financial infrastructure—it only allows cryptocurrency-to-cryptocurrency exchanges ("swaps").[92] Consequently, it can exist solely as a collection of smart contracts on the Ethereum blockchain.[93] Smart contracts are programs that can manipulate cryptocurrency according to their coded functions. Like transactions, smart contracts are immutable once they are published on blockchain, they cannot be erased. However, Uniswap is not wholly decentralized, so it can still be targeted with enforcement actions.

Uniswap Labs, the company that "developed much of the initial code for the Uniswap protocol"[94] is inconspicuously registered as Universal Navigation Inc.[95] Universal Navigation is headquartered in New York and incorporated in Delaware, has physical addresses and telephone numbers, and is managed by known entities.[96] Moreover, Universal owns Uniswap's trademarks,[97] and critically, controls the exchange's frontend (i.e., its website). Although Universal claims "it does not provide, own, or control the Uniswap protocol, which is run by smart contracts deployed on the Ethereum blockchain,"[98] it nevertheless functionally controls the protocol since it can still cut off access to Uniswap's smart contracts through Uniswap's website. In other words, since websites can still be owned and controlled by known entities, websites are still points of control which regulators can target because they are not immutable, unlike smart contracts. For example, due to regulators cracking down on other exchanges, Universal Navigation restricted access to hundreds of tokens on Uniswap—Universal bended to regulatory scrutiny.[99] Since Uniswap is controlled at least in part by centralized and known entities, it can also be influenced by the threat of regulatory enforcement.

Lastly, Sushiswap is Coinbase and Uniswap's even more decentralized counterpart. Uniswap originally operated without its own token (it only swapped existing ones), but there was

---

[92] *What is Uniswap?*, UNISWAP (last visited Oct. 24, 2021), https://docs.uniswap.org/protocol/introduction ("The Uniswap protocol is a peer-to-peer1 system designed for exchanging cryptocurrencies (ERC-20 Tokens) on the Ethereum blockchain. The protocol is implemented as a set of persistent, non-upgradable smart contracts; designed to prioritize censorship resistance, security, self-custody, and to function without any trusted intermediaries who may selectively restrict access.").

[93] *Uniswap*, GITHUB (last visited Oct. 24, 2021), https://github.com/Uniswap.

[94] *Uniswap protocol disclaime*r, UNISWAP (last visited Oct. 24, 2021), https://uniswap.org/disclaimer/.

[95] Universal Navigation Inc., *CIK Filing* (CIK #0001775180) (Apr. 29, 2019), https://sec.report/CIK/0001775180.

[96] *Id*.

[97] Uniswap, Registration No. 6183104, https://uspto.report/TM/88633022.

[98] *Uniswap protocol disclaime*r, UNISWAP (last visited Oct. 24, 2021), https://uniswap.org/disclaimer/.

[99] *Token access on app.uniswap.org*, UNISWAP (last visited Oct. 24, 2021), https://uniswap.org/blog/token-access-app/; *unsupported.tokenlist.json*, GitHub (last visited Oct. 24, 2021), https://github.com/Uniswap/interface/blob/main/src/constants/tokenLists/unsupported.tokenlist.json.

a strong market demand for a token-based model.[100] An anonymous developer, "Chef Nomi," copied Uniswap's code and added a native token to the exchange's code, $SUSHI.[101] This new exchange was named "Sushiswap." Armed with its new token, Sushiswap initiated aggressive migration incentives targeting Uniswap liquidity providers to migrate from Uniswap to Sushiswap (a "vampire attack").[102] The migration caused "about $800m of liquidity to be instantly drained to SushiSwap, with Uniswap's [liquidity] plunging back to ~$400m."[103] One week later, Uniswap unsurprisingly implemented its own token, $UNI.[104]

The Sushiswap saga not only speaks to the reality of rapid blockchain innovation and the benefits of open-sourced competition, but also evidences the implications of anonymous developers and immutable code. Chef Nomi and Sushiswap are not registered money transmitters with FinCEN or any other state, nor is there an associated recorded business entity in any state. They did not need to curry investors' favor with their startup, nor did they need to consult any lawyers or businessmen in creating Sushiswap; they merely marginally modified existing smart contracts without regulatory oversight. Even if a regulator knew who all controlled Sushiswap's frontend, the blockchain industry is already actively decentralizing frontends as well, which cuts off the last point of control regulators could levy.[105] Consequently, sufficiently decentralized financial applications coded onto a blockchain functionally operate as if in a foreign country, outside of the jurisdiction of regulators due to a lack of effective methods of enforcement.

In sum, by supplanting financial services intermediaries with immutable code on a blockchain written by anonymous developers, laws and regulatory regimes have scant points of control which leads to futile enforcement. A new paradigm has emerged that compels regulators to imagine new frameworks that effectively layer traditional financial policy goals onto novel, decentralized financial services applications.

---

[100] *See Around the Block #9: The Dawn of the DeFi Protocol Wars*, Coinbase (last visited Oct. 24, 2021), https://www.coinbase.com/learn/market-updates/around-the-block-issue-9 ("Adding the $SUSHI token wasn't groundbreaking, but Sushiswap contends that their model provides better incentives for liquidity providers (LPs). If true, Sushiswap could gain more liquidity than Uniswap, leading to better trade execution for traders, and ultimately more volume for Sushiswap.").

[101] *Id.* ("Protocol Wars kicked off in late August when an anonymous group of developers suddenly announced Sushiswap, a new Decentralized Exchange (DEX) copied almost entirely from Uniswap, but with one small tweak: Sushiswap would add a $SUSHI token, acting as both a governance token (holders can vote on proposals and modifications to the platform), as well as accruing 0.05% (5bps) of all trading volume on the platform.").

[102] Infoguild, *Vampire Mining and the SushiSwap Saga*, DEFI PULSE (last visited Oct. 24, 2021), https://defipulse.com/blog/vampire-mining-and-the-sushiswap-saga/.

[103] *Id.*

[104] *Introducing UNI*, UNISWAP (Sept. 16, 2020), https://www.coindesk.com/markets/2020/09/17/uniswap-launches-governance-token-in-bid-to-keep-up-with-rival-amm-sushiswap/.

[105] *OpenFrontEnds*, GITHUB (last visited, Oct. 24, 2021), https://github.com/OpenFrontEnds; David Vorick, *Announcing Homescreen: Decentralized Frontends for Web3*, MEDIUM (Sept. 17, 2021), https://blog.sia.tech/announcing-homescreen-decentralized-frontends-for-web3-113a3564530d; getUnrekt, *Decentralization of protocol frontend*, MEDIUM (Nov. 29, 2020), https://getunrekt.medium.com/decentralization-of-protocol-frontend-9887a40f8e5.

III. TOWARD RESPONSIBLE INNOVATION

Even if agencies promulgate practicable regulations, they will nevertheless face futile enforcement if innovators do not change the code of their smart contracts to comply with such regulations; territorial regulatory regimes mean nothing to decentralized code. This comment will now explore a path toward regulatory policies that would lead to innovators implementing such regulations in their code.

The previous attempts at regulating crypto and DeFi that were described in Part III were executed as war-like skirmishes between regulators and innovators, where the threat of unworkable regulation only incentivizes innovators to innovate around regulable points of control, such as websites. These practices not only distract innovators from carefully practicing responsible innovation, but also increasingly subject consumers to weakening safeguards as developers become ever more anonymous. To further responsible innovation, regulators must think back to the very nature of the regulatory enterprise; that is, regulation must create incentives to "coax desired behavior out of market actors" either before or after the regulated activity takes place (ex-ante, ex-post).[106]

Concerning DeFi, such desired behavior, at minimum, should entail responsible innovation wherein programmers take substantial care in crafting their smart contracts and enabling robust consumer protections.[107] Ex-post regulation is impracticable at achieving this goal—if it is even possible. Since developers can be anonymous and their code immutable, ex post regulation would be ineffective as it would be difficult for regulators to identify irresponsible developers and tamper with their smart contracts. Most importantly, ex-post regulation means nothing to consumers who were already harmed by faulty smart contracts.

Whatever specific "desired behavior" regulators seek of DeFi will also necessarily be implemented through the actual code of a smart contract; it is the code, after all, that is providing the financial services and not salaried employees. Consequently, regulators should focus on ex-ante (before the fact) approaches to regulating DeFi that affect its very code. Similar conclusions have already been drawn by previous academics, like Lawrence Lessig in the 1990s:

> Regulation in cyberspace is, or can be, different. If the regulator wants to induce a certain behavior, [they] need not threaten, or cajole, to inspire the change. [They] need only change the code—the software that defines the terms upon which the individual gains access to the system or uses assets on the system.[108]

Although Lessig was speaking to the once unregulable internet of the 90's, his insight is even more pressing today as internet regulation has become even more difficult, yet necessary, through blockchain technology.[109]

---

[106] Reyes, supra note 14 at 203.

[107] Cong. Research Serv., R44918, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework*, 4 (updated Mar. 10, 2020), https://sgp.fas.org/crs/misc/R44918.pdf.

[108] Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 (1996).

[109] Reyes, supra note 14 at 203.

A. Toward Law as Code

Lessig's argument found new life in Professor Carla Reyes's work on blockchain and DeFi. She notes that there is a unique urgency in implementing blockchain-native regulation since decentralization will only increase.[110] Defining her idea as "technology-assisted regulation," Reyes rightly concluded that any regulation of blockchain must be implemented endogenously (originating from within the system, the code).[111]

Reyes outlines a generalized ex-ante path toward achieving "technology-assisted regulation."[112] She notes that regulators will be "unable to craft requisite rules" without industry cooperation since regulations must be implemented through code.[113] Moreover, only an iterative process between innovators and regulators will lead to practicable regulation.[114] Lastly, this iterative and cooperative process will inevitably lead to "discussions about translating statutory purposes into mechanisms that serve as a functional equivalent within the code."[115] Reyes does not, however, propose actual policies that could be enacted to achieve technology-assisted regulation.

To accomplish Reyes's technology-assisted regulation, instead of antagonistic skirmishes previously explained, a workable approach to regulating DeFi is the implementation of regulatory sandboxes.

B. Practical Implementations of Law as Code through Sandboxes

In financial regulatory regimes, regulatory sandboxes are safe spaces "for innovative financial institutions and activities underpinned by technology."[116] The providers of financial services that are traditionally regulated are otherwise given exemptions due to the innovative means through which they provide these services. Such means do not readily fit within current rules and regulations.[117]

At the most basic level, the sandbox creates an environment for businesses to test products with less risk of being "punished" by the regulator for non-compliance. In return, regulators require applicants to incorporate appropriate safeguards to insulate the market from risks of their innovative business.[118]

---

[110] Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 203 (2016).
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] Dirk A. Zetzsche et. al., Regulating A Revolution: From Regulatory Sandboxes to Smart Regulation, 23 FORDHAM J. CORP. & FIN. L. 31, 64 (2017).
[117] *Id.*
[118] *Id.*

Currently, there are eight U.S. states that have regulatory sandboxes with scopes encompassing blockchain and DeFi: Arizona, Florida, Hawaii, Kentucky, Nevada, Utah, West Virginia, and Wyoming.[119]

The applicability of sandboxes to DeFi regulation are incredibly apparent. Innovators can code their smart contracts without the fear of regulatory action, while incorporating consumer protection mechanisms requested by sandbox regulators.[120] They do not have to spend time innovating around points of control, instead they can focus on improving financial services for consumers and innovating toward more consumer protection. This absence of antagonism and presence of cooperation, would imbue in regulators the expertise required to craft future practicable regulations since innovators will communicate what they can and cannot do with their code.[121]

i. Developing Expertise

Sandboxes culminate in regulators the expertise required to craft practicable rules as they collaborate with innovators. Since sandbox regulators must work to understand their applicants' novel products, they necessarily take discursive approaches when working with sandbox applicants, either through phone calls, zoom meetings, emails, or the like.[122] Moreover, they also conduct their own preliminary research to develop a basic understanding of blockchain.[123]

The development of this expertise can be furthered through specific codification of discursive approaches. For example, both Wyoming and West Virginia have (or will have) the explicit codification of letting sandbox regulators meet and consult with sandbox applicants. Hawaii also engages with innovators from a purely business perspective, advising on "economic and go-to-market" aspects.[124] Nevada's sandbox regulators even "negotiate" with applicants, in part because it helps them understand what innovators are proposing.[125]

Generally, these sandbox regulators also spend a lot of time "on the front-end" learning about DeFi and blockchain, which also develops expertise. The regulator from West Virginia, for example "went on Amazon and bought every blockchain for dummies book [she] could find and

---

[119] Kentucky has a sandbox, but it is limited to only insurance applications, so it will not be examined.

[120] Interview with Albert Forkner, State Banking Commissioner, WYOMING DIVISION OF BANKING (Sept. 8, 2021). (One U.S. sandbox regulator noted the need for "confronting regulations that protect both consumers and aid innovators" since current rules are otherwise bars to innovation. In other words, "regulatory sandboxes are like beta testing in financial services industry that maintain consumer protections, we promote responsible innovation by applying existing consumers protections but with technical flexibility.")

[121] Effective regulation . . . requires platform developers and coders to communicate. what they can automate and what they cannot, working with lawmakers and lawyers to yield the best possible confluence of automation, decentralization, and legal clarity; *Id.* ("[t]he main problem, honestly, is that law is always backwards looking and slow to adapt to innovation. Sandboxes allow regulators to keep rules current—to keep regulations future proof.").

[122] Interviews with Sandbox regulators from Arizona, Hawaii, Nevada, Utah, West Virginia, and Wyoming.

[123] Interview with Samuel Fox, Assistant Attorney General of Arizona (Sept. 16, 2021).

[124] Interview with Iris Ikeda, Commissioner of Financial Institutions, HAWAII DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS (Sept. 20, 2021)

[125] Interview with Chris Weiss, Management Analyst, Nevada Department of Business and Industry (Sept. 9, 2021).

shared them with [her] staff members."[126] Concerning even one applicant, the Arizona regulator started from zero knowledge about a complex DeFi concept, "liquidity pools," which required them to develop "the basic knowledge about [liquidity pools] and gather expertise on the types of risks associated with them to understand how the technology actually works."[127]

The expertise developed in these regulators is not siloed—most sandboxes either already allow information sharing agreements with the other states and countries, or plan to establish them.[128] Thus, many of the inefficiencies implicated in this "case-by-case" form of regulation is substantially lessened through information sharing. Inefficiencies are similarly reduced through reciprocity agreements. All U.S. sandboxes have or will establish reciprocity with other states and countries, which allows state regulators to rely on their peer states' assessments of sandbox applicants.[129]

Thus, regulators can develop expertise on blockchain and DeFi, but without inefficiencies of individualized regulation.

ii. Developing New Rules

As these sandbox regulators started to understand blockchain and DeFi, they began to rethink current legal paradigms and even started to imagine the wealth of new regulatory tools that blockchain provides—which, from the regulator's perspective is "one of the biggest benefits for us, it gives us a chance to figure out how we can make our laws better, that's one of the greatest tools."[130]

Wyoming, for example, realized they now have a "huge opportunity for smart contacts to automatically report data that regulators desire, this real-time reporting reduces systemic risk. It's also exciting how you can hard code many other financial requirements [in smart contracts]."[131] Concerning traditional rules that oppose anonymity, one sandbox regulator was actively coming to terms with the fact that "maybe the real question is: is the anonymity at the end of the day ok? Because you still have a public record of all the transactions."[132]

Sandbox regulators even explicitly inquire with innovators about how they can make their laws fit the technology. Oftentimes, however, when regulators asked about writing better rules, it

---

[126] Interview with Kathy Lawson, General Counsel, West Virginia Division of Financial Institutions (Sept. 16, 2021).

[127] Interview with Samuel Fox, Assistant Attorney General of Arizona (Sept. 16, 2021).

[128] A.R.S. § 41-5611(F); U.C.A. 1953 § 13-55-103(3)(c); W. Va. Code, § 31A-8G-3(b)(4); Interview with Albert Forkner, State Banking Commissioner at Wyoming Division of Banking (Sept. 8, 2021) ("Abu Dhabi").

[129] A.R.S. § 41-5611(F); FL ST § 559.952(6)(c); NRS 657A.220;); U.C.A. 1953 § 13-55-103(3)(c); W. Va. Code, § 31A-8G-3(b)(5); WY ST § 40-29-106(g);

[130] Interview with Kathy Lawson, General Counsel, West Virginia Division of Financial Institutions (Sept. 16, 2021).

[131] Interview with Albert Forkner, State Banking Commissioner at Wyoming Division of Banking (Sept. 8, 2021).

[132] Interview with Kathy Lawson, General Counsel, West Virginia Division of Financial Institutions (Sept. 16, 2021).

was "the first time [the innovators] have ever been asked about their opinions on what the regulations should be . . . although generally, they do believe there should be regulations."[133]

Three states have also codified requirements for sandboxes to provide annual reports containing "information regarding each regulatory sandbox participant and that provides recommendations regarding the effectiveness of the" sandbox program.[134] Moreover, Nevada may also "include any recommendations for legislation relating to the Program and any other information."[135] These reports allow legislators to adapt the sandbox and other rules to fit current laws to these technological developments.

Thus, given the increased expertise in regulators, they were able to start rethinking rules that better fit blockchain.

C. Current Sandbox Obstacles

Apart from enabling human progress that outdated rules otherwise hinder, regulatory sandboxes have many governmental benefits. They enhance communication between innovators and regulators since entrepreneurs can "freely discuss their concerns without fear of losing their license," while regulators learn about major risks before they materialize. That said, sandboxes are only as effective to the extent they "promote beneficial innovation based upon an in-depth knowledge exchange between innovator and regulator."[136]

This knowledge exchange increases a regulator's expertise on blockchain, which furthers rules that make compliance possible. Moreover, sandboxes also resolve impossible enforcement, or rather, perfect compliance, since the sandbox participants will implement the regulations requested by the sandbox into their smart contracts. However, there must be actual participants in a sandbox to derive any of its benefits, and such buy-in has been scant in the U.S.

Since these sandboxes weren't crafted specifically with DeFi in mind, there has been little industry buy-in due to problems with technical compliance and prohibitively burdensome restrictions. However, more engagement may arise if states adjusted their sandboxes to: (1) prohibit recording consumer information, (2) allow virtual presence in the state, (3) enable participants to serve consumers outside of the state, (4) adopt flexible standards in admitting applicants, and (5) provide other incentives to join the sandbox.

i. Issues with Technical Compliance

Technical compliance with two states' sandboxes prohibits DeFi participation. Both Nevada and Wyoming require sandbox participants to collect and maintain consumer records such

---

[133]Interview with Iris Ikeda, Commissioner of Financial Institutions in the Hawaii Department of Commerce and Consumer Affairs (Sept. 20, 2021).

[134] Nev. Rev. Stat. § 657A.530, Utah Code Ann. § 13-55-108(6); W. Va. Code, § 31A-8G-8(f).

[135] Nev. Rev. Stat. § 657A.530(3).

[136] Dirk A. Zetzsche et. al., *Regulating A Revolution: From Regulatory Sandboxes to Smart Regulation*, 23 Fordham J. Corp. & Fin. L. 31, 79 (2017).

as consumer name and contact information, correspondences between the participant and consumer, and other financial statements.[137] While recording consumer data was common practice for financial institutions before DeFi, it is undesirable in a world of public blockchains where all financial histories are public. A more practicable approach is that of Arizona, Florida, Utah, and West Virginia, which does not require such recordation. Although each state requires sandbox participants to take measures to reduce consumer risk, such measures entail *not* recording consumer data in the blockchain context.

Just as with FinCEN's proposed midnight rulemaking already explored, recording consumer information is not only a risky practice, but also technically unfeasible in the DeFi context. These protocols operate largely on public blockchains with public financial histories, and composed of only smart contracts, with no way of accurately recording identifying information. Consequently, it would be wholly radical for blockchain developers to attempt to incorporate on-chain identity standards. Off-chain identity recordation is equally radical. In the event of any hack or exploit that leaked consumer identities, the entire world would know the consumer's entire financial history on the blockchain. This novel risk is unlike that of traditional financial services intermediaries that only have consumer histories to the extent they were facilitated by these intermediaries. Thus, Nevada's and Wyoming's provisions for recording consumer data are unworkable in the DeFi context.

ii. Issues with Overly Burdensome Restrictions

Some sandboxes have restrictions that do not fit well within the blockchain and DeFi industries. Florida, West Virginia, and Wyoming require sandbox participants to be physically present within the state.[138] West Virginia goes even further, requiring participants to attempt to establish a partnership with a bank or financial institution within the state.[139] While there may be political reasons for these provisions, they are nonetheless barriers to entry as they require participants to already be in the state or otherwise require innovators to relocate. A key feature of public blockchains is that anyone in the world may build on them as long as they have an internet connection. Place-based restriction have no place on the blockchain. A better approach is that of Arizona, Nevada, and Utah that allows mere "virtual presence" in a territory, which is more in line with the industry realities of blockchain.

Similarly, Arizona, Florida, and Nevada put caps on the number of consumers a participant may serve, ranging from 10,000 to 25,000 consumers.[140] Hard-capped restrictions may weigh in favor of consumer protection, but they also severely dissuade possible industry participants since their possible consumer base is otherwise any of the billions of people with an internet connection.

---

[137] *See* R089-19 Sec. 12; WY Rules and Regulations 021.0008.1 § 4(b).

[138] FL ST § 559.952(3)(a); W. Va. Code §31A-8G-3(c)(2); WY ST § 40-29-104(b).

[139] *See* W. Va. Code, § 31A-8G-3(c)(3).

[140] A.R.S. § 41-5605(B)(2); A.R.S. § 41-5605(C)(1); FL ST § 559.952(5)(f); NRS 657A.300.

A better approach is that of Utah, West Virginia, and Wyoming that retain a flexible approach, where state regulators consider consumer maximums on a case-by-case basis.

In a similar vein, Arizona and Nevada impose restrictions on the amount of money sandbox participants can transmit to consumers, ranging from $2,500 per individual transaction to $50,000 in aggregate.[141] Such hard-capped restrictions likewise dissuade industry participants since anyone can transfer $1 billion worth of cryptocurrency just as easily as they can transfer $10 of it.[142] A more workable approach is that of Utah and West Virginia, where state regulators consider consumer maximums on a case-by-case basis.

Lastly, all states require the consumers of the sandbox participants to either be residents of the respective sandbox state, or physically located in the state.[143] However, the novelty of public blockchains is that anyone with an internet connection may access them. Having territorial restrictions on consumers is a severe limitation and turns away some of the largest possible industry participants. This limitation exists because the above limitations are not uniform—its assumed that one state sandbox should not impose their laxer standards onto other sandboxes, thus creating the current need for territorial restrictions. A uniformed approach to state sandboxes will fix this issue, which could be accomplished with flexible standards.

D. The Ideal DeFi Sandbox

Although sandboxes are supposed to be "flexible" to allow for regulatory adaptability, many current implementations nevertheless adopted static requirements that have hindered industry participation. Subsequent iterations should explicitly adopt flexible standards. Flexibility affords sandbox regulators the opportunity to change regulatory practices in step with technological developments, but while still protecting consumers. Moreover, current sandboxes must: (1) prohibit recording consumer information, (2) allow virtual presence in the state, (3) enable participants to serve consumers outside of the state, (4) adopt flexible standards in admitting applicants, and (5) provide other incentives to join the sandbox.

The ideal sandbox may operate according to the following scenario. The sandbox may admit a smart contract-based lottery applicant, the code of which is provided in Appendix A. The sandbox regulators would come learn what the applicant can and cannot do with their code, for example negotiating:

(1) maximum amount of winnings

require(address(this).balance < 100 ether);

(2) maximum number of tickets sold

require(players.length <= 10,000);

---

[141] A.R.S. § 41-5605(C)(2); NRS 657A.310.

[142] *See* Timothy B. Lee, *Someone moved $1 billion in a single bitcoin transaction*, ARS TECHNICA (Sept. 10, 2019), https://arstechnica.com/tech-policy/2019/09/someone-moved-1-billion-in-a-single-bitcoin-transaction/.

[143] A.R.S. § 41-5605(B)(1); FL ST § 559.952(3)(c); NRS 657A.300; U.C.A. 1953 § 13-55-104(2)(a); W. Va. Code, § 31A-8G-4(b)(1); WY ST § 40-29-102(a)(iii).

(3) virtual presence in the state, and serving consumers outside the state by not using geo-blocking software on the frontend

The regulators could determine the above parameters based on the consumer protection mechanisms that the participant has the capability to implement, such as:

(1) having smart contract-based insurance policies

(2) having the smart contracts audited to reveal any vulnerabilities

(3) giving the regulator special permissions in the smart contracts, like a "kill switch"[144]

Such regulatory oversight would ensure responsible innovation in projects that might otherwise have gone without them. Moreover, such regulations would necessarily be implemented in the code of participants' smart contracts, which ensures actual compliance and avoids issues of impossible enforcement.

At the same time, regulators could realize that they have more regulatory tools available to them, such as automatic reporting of transactions over x amount. The adjusted parameters of the lottery smart contract and automatic reporting would be a realization of Reyes's "technology assisted regulation," the implementation of law through code. Moreover, as increasing numbers of participants used the sandbox, regulators would further their expertise on DeFi. The iterative nature of sandboxes and resulting knowledge exchange will enable these regulators to adapt current statutory purposes into practicable regulations. However, a flexible sandbox is not enough to attract industry participants, so governments and regulators need to do more to attract participants.

i. Attracting Industry Participants

The state could attract industry participants by offering protections that innovators simply cannot code into their smart contracts. For example, governments are uniquely positioned through their various privileges, such as subpoena power. The sandbox could adopt provisions that impose severe penalties on anyone who maliciously tampers with or exploits vulnerabilities in the participants' smart contracts. Although that is normally impracticable because attackers can be anonymous, the state is uniquely positioned to reveal identities through their subpoena power. There exist means that centralized crypto companies can employ at the request of governments to track transaction histories to real-world identities. Centralized companies do, after all, record consumer data as they are linked to traditional financial infrastructure. Having the state on participants' side is not only a convenient relationship to further consumer protection, but also one for incentivizing the industry to cooperate with sandbox regulators.

A more potent and direct tool governments have is taxation. States may simply offer tax incentives to consumers who use the services of sandboxed DeFi participants. Tax incentives are conveniently less costly in the DeFi context because a lot of DeFi users do not actually pay taxes on gains anyway since they know that their identities are difficult to reveal. Consequently, whatever theoretical fiscal drawback tax incentives may have on DeFi would be mitigated since

[144] Kill switches**,** CLOUDFLARE DOCS **(**Aug. 2021), available at https://developers.cloudflare.com/web3/ethereum-gateway/reference/kill-switches/.

those taxes would not have been paid anyway. Thus, tax incentives would operate more like a safe harbor for many users of sandboxed DeFi applications since they would not fear the threat of a tax audit.

Both subpoena power and taxation may prove highly effective in currying industry buy-in as they attract both developers and users. Although taxation may have a cost, consumer protection is not free. Moreover, whatever the cost of taxation imposed on the state is uniquely diminished due to the nature of the DeFi industry. Although one criticism of offering incentives to join a sandbox is that it "pick winners and losers," such an outcome should be desired in DeFi. Projects that work with governments to protect consumers and help make laws better, should invariably be the winners in the crypto ecosystem.

ii. Federal Sandboxes

This discussion focused on state regulatory sandboxes because there is just one federal sandbox. However, while speaking with sandbox regulators, it became apparent that perhaps the federal government is best positioned for DeFi regulation through sandboxes. It is more efficient to have a standardized and uniform approach to sandboxes, rather than the varied requirements by state sandboxes. However, such federal sandboxes are still nascent or only proposed, and the current sandbox has not had DeFi participants.

The Consumer Financial Protection Bureau (CFPB) has a no-action letter policy for many of the same reasons sandboxes exist. Regulatory uncertainty hinders innovation, particularly in the case where innovative products "may not have existed, or even been contemplated, at the time [their] applicable statutes and regulations were promulgated."[145] To date, there have only been six successful applicants in the CFPB's sandbox, none of which touch blockchain.[146]

One Commissioner of the SEC has proposed a similar policy, a token safe harbor. The safe harbor requires certain reports, disclosures, and other technical features to qualify for the safe harbor.[147] However, no action has been taken on the proposal.

CONCLUSION

Governments, the "weary giants of flesh and steel" have no power on the blockchain, unless they play by the rules—by changing its code. The challenges of unregulable code on the internet are not new, however they are heightened when this code can provide financial services and can be written by unknown developers. Two core challenges in this new techno-economic

---

[145] BUREAU OF CONSUMER FINANCIAL PROTECTION, Docket No. CFPB-2018-0042, POLICY ON NO-ACTION LETTERS (2019), https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-no-action-letters.pdf.
[146] *Granted applications*, CFPB (last accessed Oct. 25, 2021), https://www.consumerfinance.gov/rules-policy/innovation/granted-applications/.
[147] Commissioner Hester M. Peirce, *Token Safe Harbor Proposal 2.0*, SEC (Apr. 13, 2021), https://www.sec.gov/news/public-statement/peirce-statement-token-safe-harbor-proposal-2.0.

paradigm are reworking regulations that enable possible compliance and possible enforcement. Both of which, conveniently, can be solved through regulatory sandboxes.

Given the complex and rapidly evolving space around blockchain, legislators and regulators first need to acquire the requisite expertise in drafting laws and regulations that make compliance possible. Otherwise, the threat of impracticable regulations only incentivizes innovators to work around regulable points of control. Although the purpose behind these regulatory actions may be consumer protection, they nevertheless subject consumers to increased risks as developers increase anonymity and decentralization. Instead, a more pragmatic approach entails collaboration that furthers responsible innovation.

Regulators must reconcile the fact that their rules must fit within this new paradigm, and not the other way around. By doing so, they will realize that their rules, unlike before, must be implemented and enforced in the very code of smart contracts providing financial services. Such an approach avoids impossible enforcement, or rather, achieves perfect compliance. Moreover, since these smart contracts can be deployed by anonymous individuals and immutably exist, whatever new rules that are created must exist as ex-ante incentives that encourage responsible innovation.

Sandboxes serve as practical launching points toward this approach to regulation. First, they imbue in regulators the expertise on DeFi and blockchain that will enable them to adapt old rules to new realities. Second, they ensure that innovators incorporate into their smart contracts the rules dictated by their sandboxes. However, there must actually be participants in sandboxes for any of this to occur. Current iterations of sandboxes contain stagnant requirements that, in the DeFi context, are prohibitively restrictive and sometimes even unworkable. If there is an impetus on any state or federal regulator to regulate DeFi through sandboxes, they must, at minimum, make sandboxes more flexible; they may even provide additional incentives to participants to curry industry buy-in.

In effect, regulatory sandboxes offer a path toward responsible innovation with adequate regulatory oversight and robust consumer protections, thus resolving the issues of impossible compliance and impossible enforcement.

APPENDIX A

```
//SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.5.0 <0.9.0;

contract Lottery{

   // declaring the state variables
   address payable[] public players; //dynamic array of type address payable
   address public manager;


   // declaring the constructor
   constructor(){
      // initializing the owner to the address that deploys the contract
      manager = msg.sender;
   }


   // declaring the receive() function that is necessary to receive ETH
   receive () payable external{

      // each player sends exactly 0.1 ETH
      require(msg.value == 0.1 ether);
      require(address(this).balance < 100 ether);
      // appending the player to the players array
      players.push(payable(msg.sender));
   }

   // returning the contract's balance in wei
   function getBalance() public view returns(uint){
      // only the manager is allowed to call it
      require(msg.sender == manager);
      return address(this).balance;
   }

   // helper function that returns a big random integer
   function random() internal view returns(uint){
     return uint(keccak256(abi.encodePacked(block.difficulty, block.timestamp, players.length)));
   }
```

```
    // selecting the winner
    function pickWinner() public{
        // only the manager can pick a winner if there are at least 3 players in the lottery
        require(msg.sender == manager);
        require (players.length >= 3);

        uint r = random();
        address payable winner;

        // computing a random index of the array
        uint index = r % players.length;

        winner = players[index]; // this is the winner

        uint managerFee = (getBalance() * 10 ) / 100; // manager fee is 10%
        uint winnerPrize = (getBalance() * 90 ) / 100;      // winner prize is 90%

        // transferring 90% of contract's balance to the winner
        winner.transfer(winnerPrize);

        // transferring 10% of contract's balance to the manager
        payable(manager).transfer(managerFee);

        // resetting the lottery for the next round
        players = new address payable[](0);
    }

}
```