Nebraska Law Review

Volume 99 | Issue 2 Article 3

2020

Smart Contracts and the Limits of Computerized Commerce

Eric D. Chason
William & Mary Law School

Eric D. Chason*

Smart Contracts and the Limits of Computerized Commerce

TABLE OF CONTENTS

* Professor of Law, William & Mary Law School.

I. INTRODUCTION

Having recently celebrated its ten-year anniversary, Bitcoin should be considered a qualified success. In October 2020, each unit[1] was worth about $10,700, and the entire market capitalization was approximately $200 billion.[2] Bitcoin is a significant economic force with sizable market value. Despite this success, however, Bitcoin has not been widely adopted as a method of payment, which was its intended use.[3]

By providing a template for a durable cryptocurrency, Bitcoin also blazed a path for other cryptocurrency projects. In terms of market capitalization and current importance, Ethereum is comfortably in second place.[4] In October 2020, it had a market capitalization of approximately $40 billion.[5] Unlike Bitcoin, however, Ethereum was not designed primarily to serve as a method of payment. Ethereum supports a system of sophisticated "smart contracts" that would not work on the Bitcoin system.

Smart contracts and cryptocurrencies have sparked considerable interest among legal scholars in recent years, and a growing body of scholarship focuses on whether smart contracts and cryptocurrencies

1. In this Article, Bitcoin (capitalized) will refer to the overall system for this particular cryptocurrency. In contrast, bitcoin (lowercase) will refer to units of the cryptocurrency. This Article will also use the abbreviation BTC to refer to bitcoin units. A parallel example using United States currency might illuminate this distinction. The dollar can refer to the entire system of currency, or it can refer to the individual units. Also, the abbreviation USD (or $) refers to dollar units. Other currencies separately name the system and the units. For example, the renminbi is the Chinese currency, while the yuan is the unit of the currency. Similarly, Ethereum is a cryptocurrency system with units called ether.
2. *See Bitcoin (BTC)*, CoinMarketCap, https://coinmarketcap.com/currencies/bitcoin [https://perma.unl.edu/PU6X-9H76] (last visited Oct. 5, 2020).
3. *See* David W. Perkins, Cong. Research Serv., The Potential Decline of Cash Usage and Related Implications 15 (2019), https://crsreports.congress.gov/product/pdf/R/R45716 [https://perma.unl.edu/PK4X-EYWX] ("Certain analyses appear to show that digital currencies are not being widely used and accepted as payment for goods and services, but rather as investment vehicles.").
4. *See Top 100 Cryptocurrencies by Market Capitalization*, CoinMarketCap, https://coinmarketcap.com [https://perma.unl.edu/4WHX-WMAE] (last visited Jan. 30, 2020).
5. *See Ethereum (ETH)*, CoinMarketCap, https://coinmarketcap.com/currencies/ethereum[https://perma.unl.edu/274A-WH9A] (last visited Oct. 5, 2020).

can sidestep law and regulation altogether.[6] Bitcoin is famously decentralized, without any central actor controlling the system. Its users remain largely anonymous, using alphanumeric addresses instead of legal names. Ethereum shares these traits and also supports smart contracts that can automate the transfer of the Ethereum cryptocurrency (known as ether). Ethereum also supports specialized "tokens" that can be tied to the ownership of assets, goods, and services that exist completely outside of the Ethereum blockchain.

The goal of this Article is to evaluate the degree to which cryptocurrencies and smart contracts can operate outside the reach of law and regulation. By some accounts, cryptocurrencies and smart contracts will revolutionize private law.[7] Some argue they have the potential to displace contract and property law. For example, in a previous article, I argued that Bitcoin represents a system of private property that exists wholly outside of traditional legal structures.[8] In this Article, I will argue that a complete revolution is not inexorable.[9] Facing the technical and complicated nature of this subject, we should keep in mind a simple fact: cryptocurrencies and smart contracts are computer data and computer programs. To a large extent, they will have legal force only if given force by judges, regulators, and legislators.

Part II describes Bitcoin and how it creates a system of property that exists outside of legal structures. Bitcoin is special because it controls no external assets (like securities, dollars, or gold). It is purely "notional" property that exists only on a computer file.

Part III describes Ethereum and how it builds upon the principles of Bitcoin. The primary innovation of Ethereum is smart contracts, which allow for variable and conditional transfers of cryptocurrency.

---

6. *See, e.g.*, Hilary J. Allen, *$=€=Bitcoin?*, 76 MD. L. REV. 877 (2017) (describing the relationship between cryptocurrencies and payment systems); Eric D. Chason, *A Tax on the Clones: The Strange Case of Bitcoin Cash*, 39 VA. TAX REV. 1 (2019) (describing the challenges that cryptocurrency innovation poses to the income tax); Eric D. Chason, *Cryptocurrency Hard Forks and Revenue Ruling 2019-24*, 39 VA. TAX REV. 279 (2019) (same); Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805 (2015) (describing the relationship between cryptocurrencies and property law).
7. *See, e.g.*, PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW 5 (2018) ("With blockchains, people can construct their own systems of rules or smart contracts, enforced by the underlying protocol of a blockchain-based network. These systems create order without law and implement what can be thought of as private regulatory frameworks . . . .").
8. *See* Eric D. Chason, *How Bitcoin Functions as Property Law*, 49 SETON HALL L. REV. 129 (2018).
9. Prior scholarship has noted convergence between "smart contracts" and traditional contract law. *See, e.g.*, Kevin Werbach & Nicolas Cornell, *Contracts* Ex Machina, 67 DUKE L.J. 313, 382 (2017) ("Contract law is nothing if not resilient. We have little doubt it will survive the onslaught from smart contracts, if indeed that is what is happening.").

To be of commercial value, however, smart contracts must incorporate economic or financial information (e.g., interest rates or exchange rates). Ethereum allows users to incorporate this information using third party "oracles." While oracles allow for sophisticated transactions, their presence illustrates some of the limits of smart contracts.

Part IV extends the discussion of Ethereum and explains how many developers use it as a way to effectuate property transactions. Tokens are specialized smart contracts used to represent ownership of assets or certain privileges. Conceivably, ownership in any asset—homes, cars, etc.—could be represented by Ethereum tokens. Rather than using a deed of transfer, owners could simply transfer the representative tokens.

Part V develops what this Article calls a "remote-computer model" of Bitcoin and Ethereum. Because Bitcoin and Ethereum are computer programs and computer data, we can view each as constituting a single *computer*. This hypothetical computer is *remote* in the sense that judges, regulators, and legislators can exercise little control over it directly. The remote computer controls ownership of cryptocurrency units, leaving direct cryptocurrency transactions outside the scope of traditional legal institutions. That being said, smart contracts often purport to control external resources and rights. For example, a smart contract might purport to control the transfer of land or stock in a corporation. These transactions have effects outside the hypothetical remote computer and can potentially be subject to control by legal institutions.

II. BITCOIN AND SIMPLE TRANSFERS

A. Digital Currency as Computer Data

Cryptocurrency units are essentially computer data. In Bitcoin, the total units of circulating bitcoin are collectively referred to as unspent transaction output (or UTXO).[10] In rough terms, UTXO associates bitcoin units with owners. Ownership of bitcoin is not, however, personal to individuals, corporations, or the other legal actors. Instead, ownership is determined cryptographically, typically by controlling a "private key" that "function[s] like a password."[11] If Alice owns one unit of bitcoin, it is because she controls the private key associated with that unit.

10. *See* Andrew M. Hinkes, *Throw Away the Key, or the Key Holder? Coercive Contempt for Lost or Forgotten Cryptocurrency Private Keys, or Obstinate Holders*, 16 NW. J. TECH. & INTELL. PROP. 225, 258 n.183 (2019).

11. *See* Chason, *supra* note 8, at 141–42.

In most Bitcoin transactions, the transferor sends the units of bitcoin to the "address" of the recipient.[12] We can imagine this address as being like an account number. Each address, in turn, has an associated private key, which we can imagine as being like a password. Anyone who knows the private key can, within the Bitcoin system, transfer the associated bitcoin units to another address. So, in more precise terms, UTXO associates bitcoin units with addresses, which users control with private keys.

For purposes of this Article, the cryptographic details have lesser importance. What is important, however, is that bitcoin ownership is reflected in computer data and cryptographic control. Bitcoin is not backed up by external securities, cash, or other investments. And, by design, bitcoin ownership is not enforced by courts or other legal actors. For reasons discussed below,[13] courts and other legal actors find it difficult or impossible to deal directly with Bitcoin, Ethereum, and many other cryptocurrencies.

To explain this difficulty, this Article will develop a legal model of cryptocurrencies based on a single hypothetical computer.[14] This hypothetical computer holds the history of all prior transactions (known as the blockchain) from which one can readily derive current ownership (or UTXO). Importantly, this hypothetical computer is legally "remote," meaning that judges, regulators, and legislators cannot alter the data and programs held on the computer. The remote-computer model will give us (as legal observers) a way to understand how the law can and cannot interact with cryptocurrencies.

B. Problems with Centralized Digital Currency

1. Introduction

The remote-computer model is useful when dealing with legal questions. But, as a technical matter, it does not fully describe Bitcoin or Ethereum. These cryptocurrencies do not exist on a single computer (remote or otherwise). Instead, they exist in practically identical form on a multitude of different computers around the world.[15] Because each cryptocurrency exists in identical form on these computers, we can imagine that it exists on a single computer. If Bitcoin or Ethereum actually existed on a single, physical computer, however, it would not

12. *See* ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN 136 (Tim McGovern et al. eds., 2d ed. 2017) ("The vast majority of transactions processed on the bitcoin network spend outputs locked with a Pay-to-Public-Key-Hash . . . . These outputs contain a locking script that locks the output to a public key hash, more commonly known as a bitcoin address.").
13. *See infra* section V.C.
14. *See infra* section II.D and Part V.
15. *See* DE FILIPPI & WRIGHT, *supra* note 7, at 24 (describing process by which "the network reaches *consensus* as to who owns what amount of bitcoin").

be remote as described in our model. The computer would physically exist somewhere, need power, etc. Moreover, some person would have control over the physical computer. This section discusses the problems that would plague a centralized (or non-remote) digital currency.

2. Regulatory Oversight

When creating Bitcoin, Satoshi Nakamoto expressly wanted to avoid centralized control.[16] A centralized actor (e.g., a bank) could be subject to laws, regulations, and politics that run contrary to the interests of the Bitcoin community. Nakamoto offered the somewhat idiosyncratic and surprising example of reversible payments.[17] A consumer who pays for an item using a bank-issued credit card has the right, by statute, to reverse the payment in certain circumstances. Even if the community of users wants non-reversible transactions, a central administrator would have to follow the law and allow for reversible payments.

Bitcoin would, by design, offer non-reversible payments.[18] The goal of non-reversible payments may seem like a relatively minor reason to create an entirely new and private currency. And, making payments non-reversible introduces an array of risks into the system. Victims of credit card fraud, for example, have a wide array of remedies and protections. Victims of Bitcoin fraud or theft, in contrast, have none. The best the victim could hope for is for the thief to be arrested and forced to return the stolen bitcoin as part of the judicial process.

For better or for worse, decentralization allows Bitcoin to operate in a way that makes it nearly impervious to law and regulation. No central administrator exists. Indeed, the system does not even differentiate between different types of users. Everyone (including you and me) has the same technical privileges within the system. Users interact with the system through user addresses, which we can think of as alphanumeric pseudonyms.[19] Users can (and should) generate distinct addresses for separate transactions. Because of this level of decentralization, law and regulation have no easily identifiable person or entity to control.

Since it operates outside the law, Bitcoin has often been used for illegal purposes. The "Silk Road" market for illegal drugs was con-

16. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 1, 2, https://bitcoin.org/bitcoin.pdf [https://perma.unl.edu/S8TW-6ZCG] (last visited Jan. 30, 2020).

17. *See id.* at 1.

18. *See id.*

19. *See supra* note 12 and accompanying text.

ducted almost entirely in Bitcoin before it was shut down in 2014.[20] Additionally, computer malware often directs victims to pay bitcoin to a certain address in exchange for returning control of the victims' computers.[21]

We should not, however, dismiss Bitcoin as simply money for criminals. Bitcoin (and Ethereum) are structures for conducting economic transactions. And, as business lawyers know, some transactional structures are subject to less regulation than others. For example, anyone creating a business entity can choose from a wide range of state laws (e.g., Delaware versus Virginia), entity types (e.g., corporation versus LLC), and tax treatments (e.g., taxable entities versus pass-through entities).[22] Would-be owners can look outside the United States for even more options.[23] Some of these non-U.S. options are routinely abused.

More philosophically, Bitcoin achieves certain libertarian ideals.[24] Governments routinely regulate markets by regulating central actors. For example, the United States imposes extensive anti-money-laundering regulations on financial institutions. The rationale behind these regulations may be, in part, to address the possibility that the institutions themselves are engaging in money laundering. However, a more significant rationale is that customers may use financial institutions to engage in money laundering. Customer-level activity may be hard for the government to detect directly, so the government commands the assistance of the financial institution to monitor its customers. Financial institutions are subject to "know your customer" (KYC) rules and must also report certain transactions.[25]

A libertarian would likely object to such rules on the grounds that they are overinclusive and invasive of financial privacy. Financial institutions must "know" and monitor all of their customers, not just the small fraction that might be engaged in criminal activity.[26] Also, anti-money-laundering regulations commandeer the resources of all finan-

20. *See generally* CAROL GOFORTH, REGULATION OF CRYPTOTRANSACTIONS 117–58 (2020) (describing the Silk Road and resulting legal actions).
21. *See generally Bitcoin Network*, WIKIPEDIA, https://en.wikipedia.org/wiki/Bitcoin_network#Alleged_criminal_?activity [https://perma.unl.edu/QZ7E-LU4G] (last visited Jan. 30, 2020) (describing criminal activity surrounding Bitcoin).
22. *See generally* James M. Kehl, *Choice of Entity: Organizational Issues*, 700-4th U.S. Income Portfolios (BNA) (2020) (describing relative advantages of different organizational forms).
23. *See id.* at 62–70.
24. *See* SAIFEDEAN AMMOUS, THE BITCOIN STANDARD: THE DECENTRALIZED ALTERNATIVE TO CENTRAL BANKING 200–05 (2018) (describing the individual sovereignty offered by Bitcoin).
25. *See* Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271, 325–26 (2015) (discussing KYC requirements applicable to Bitcoin).
26. *See id.*

cial institutions, not because of their own activities but because of the activities of customers. In the hands of sophisticated users, Bitcoin can avoid such regulation.[27] It has no central actor who acts as a gatekeeper for users. No financial institution maintains Bitcoin accounts for anyone. As a result, the government cannot deputize financial institutions to keep watch over Bitcoin users. Thus, Bitcoin offers far more privacy and secrecy than traditional bank accounts.

As a monetary system, Bitcoin has no use for central banks, the ultimate financial institution. Proponents claim that Bitcoin is "sound money," unlike the U.S. dollar and other sovereign currency.[28] The supply of bitcoin is algorithmically fixed, and no central institution has any power to alter the algorithm. In contrast, the supply of U.S. dollars is determined largely at the discretion of the Federal Reserve.[29] Whether this discretion is a good or bad thing is well beyond the scope of this Article. This distinction between the U.S. dollar and bitcoin is, nevertheless, illuminating. The U.S. dollar fluctuates in supply because a central actor determines its supply. Bitcoin is fixed in supply because no central actor can alter its supply.

3. Trust

The prior subsection noted that Bitcoin removes itself from the control of politics and the regulatory state. Even if we thought such forces were neutral or even beneficial, centralized control still has disadvantages. Suppose that Satoshi Nakamoto maintained Bitcoin on a single computer. When creating Bitcoin, he developed a system that automated many aspects of the transfer process and removed those aspects from the discretion of a central administrator. For example, a central administrator could not readily steal bitcoin units held by other people.[30] But, the central administrator could still harm the functioning of the system in the following ways:

Denial of service. Suppose that Alice executes a computer file that transfers 1 BTC to Bob. For the transfer to be effective, it must be recorded on the central computer. The central administrator might simply ignore Alice's transfer to Bob rendering Alice's 1 BTC worthless to her.[31]

---

27. *See, e.g.*, *supra* note 20 and accompanying text (discussing Silk Road case).

28. *See* AMMOUS, *supra* note 24, at 135–36 (describing principles of "sound money").

29. *See id.*

30. *See* ARVIND NARAYANAN, JOSEPH BONNEAU, EDWARD FELTEN, ANDREW MILLER & STEVEN GOLDFEDER, BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 34 (2016) (describing how technology can prevent theft by a central administrator).

31. A leading introduction to Bitcoin discusses a hypothetical and centralized "Scroogecoin" administered by "Scrooge." *See id.* at 22–25 (discussing Scrooge's refusal to approve transactions).

Assistance with fraud. Suppose that Alice executes a computer file that transfers 1 BTC to Bob in exchange for $9,000. Hoping to keep Bob's $9,000 and her 1 BTC, Alice executes another file that transfers the very same 1 BTC to her spouse, Charlie. Alice also enlists the assistance of the central administrator, who records the transfer to Charlie (and rejects the transfer to Bob).

Abandoning the project. The central administrator might tire of the project and simply shut down the computer on which it exists.[32]

When considering these examples, we can note similarities between the central administrator and the recorder of deeds to real property.[33] The recorder is a central party who records the deeds. That system works because the parties believe they can trust the recorder of deeds. Fraud or other malfeasance in that system is fairly easy to discover and would be punishable under criminal law. Perhaps because it operates within the government, we also trust that the system will exist for the foreseeable future.

Returning to Bitcoin, this trust does not obviously exist. Suppose that the creator (Satoshi Nakamoto) gave himself authority to act as the recorder of all Bitcoin transactions. If he engaged in a fraud, we might not discover it, and the authorities might not be able to prosecute him. Participants might worry that Nakamoto (acting as recorder) would become disinterested at some point, pull the plug (literally and figuratively), and let the whole system collapse. Moreover, the police might not even treat Nakamoto as a criminal if he manipulated the hypothetical record of Bitcoin deeds. In short, parties to real estate transactions can trust their central registry; parties to a Bitcoin transaction cannot.

C. Bitcoin and Decentralization

This section focuses on Bitcoin and how it achieves decentralization.[34] Remarkably, Bitcoin achieves consensus about ownership of bitcoin units even though no central party administers it. As we will see, the main innovation of Bitcoin is organizational rather than technical.

We saw that UTXO is computer data that associates bitcoin units with owners (or their alphanumeric addresses).[35] For Bitcoin to function as a currency, owners must be able to transfer their units to new

32. *See id.*
33. *See* Chason, *supra* note 8, *passim*.
34. Ethereum has similar mechanics in dealing with transfers of its underlying cryptocurrency. *See generally* ANDREAS M. ANTONOPOULOS & GAVIN WOOD, MASTERING ETHEREUM 99–125 (Rachel Roumeliotis et al. eds., 2018) (discussing technical aspects of Ethereum transactions).
35. *See supra* note 12 and accompanying text (discussing "pay-to-public-key-hash" transactions).

owners. Mechanically, Bitcoin uses a system of transfer that resembles real estate transfers.[36] When transferring ownership, users execute computer files that resemble deeds. They identify themselves with alphanumeric addresses rather than legal names. And, they execute digital signatures rather than signing with pen and paper.

Bitcoin replicates the functions of a centralized recorder of deeds but does so without any centralized party. In the world of real property transfers, transferees record their deeds with a central registry. Doing so alerts other would-be transferees of the transfer. For example, Bob would check with the recorder of deeds before accepting a deed from Alice conveying Blackacre to him. If Bob found a prior deed (e.g., by which Alice conveyed Blackacre to Charlie), then Bob would know that Alice is trying to defraud him.

Conversely, transactional data is recorded on the Bitcoin blockchain in a form that most readers cannot decipher directly. That being said, the essential transactional data can be formatted in a way that people can readily interpret once they have some knowledge of how Bitcoin operates. Consider an actual transaction from the very early days of Bitcoin. In May 2010, a man wanted to conduct the first commercial transaction denominated in bitcoin.[37] In an internet forum, he offered to pay 10,000 BTC for two pizzas.[38] At the time, this amount of bitcoin was worth about $25.[39] In October 2020, this same amount was worth $107 million.[40]

In computer-readable form, the transaction would look like the following:

> 01000000018dd4f5fbd5e980fc02f35c6ce145935b11e284605bf599
> a13c6d415db55d07a1000000008b483045022100990814ca6539e
> 09512b9295c8a27050d478fbb96f8addbc3d075544dc41328702201
> aa528be2b907d316d2da068dd9eb1e23243d97e444d59290d2fddf
> 25269ee0e0141042e930f39ba62c6534ee98ed20ca98959d34aa9e
> 057cda01cfd422c6bab3667b76426529382c23f42b9b08d7832d4
> fee1d6b437a8526e59667ce9c4e9dcebcabbffffffff0200719a
> 81860000001976a914df1bd49a6c9e34dfa8631f2c54cf39986027501
> b88ac009f0a5362000000434104cd5e9726e6afeae357b1806be25a4c3
> d3811775835d235417ea746b7db9eeab33cf01674b944c64561ce3388
> fa1abd0fa88b06c44ce81e2234aa70fe578d455dac00000000[41]

---

36. *See* Chason, *supra* note 8, *passim*.
37. *See* Molly Jane Zuckerman, *Bitcoin Pizza Guy: Laszlo Hanyecz on Why Bitcoin Is Still the Only Flavor of Crypto for Him*, COINTELEGRAPH (May 27, 2018), https://cointelegraph.com/news/bitcoin-pizza-guy-laszlo-hanyecz-on-why-bitcoin-is-still-the-only-flavor-of-crypto-for-him [https://perma.unl.edu/638X-J92S].
38. *Id.*
39. *See Bitcoin History* BITCOIN WIKI, https://en.bitcoinwiki.org/wiki/Bitcoin_history#Bitcoin_in_2010 [https://perma.unl.edu/YRW9-WSFG] (last visited June 15, 2020).
40. *See Bitcoin (BTC)*, *supra* note 2 (describing October 2020 exchange rate).
41. *See* BLOCKCHAIN, https://blockchain.info/tx/cca7507897abc89628f450e8b1e0c6fca4ec3f7b34cccf55f3f531c659ff4d79?format=hex[https://perma.unl.edu/N9AB-

This collection of numbers and letters is meaningless to the human reader. However, a computer can easily interpret it,[42] and the interpreted rendering bears many similarities to a formal deed. It identifies the transferor and the transferee by their Bitcoin addresses.[43] It also identifies the 10,000 BTC which were the subject of the transfer.[44]

The life cycle of Bitcoin transactions follows a pattern. First, the participants (transferor and transferee) form the transaction privately. The result of that formation is something like the "hex data" shown above, which is a convenient and compact form for transmission. They would not manually create the data but would rely upon "wallet software" to create the hex data for them.[45] As just noted, this hex data can be decoded into a form that resembles a deed, and we can think of the formation of the hex data as the preparation and execution of a deed.[46]

Next, the parties broadcast the transaction (using hex data) to other users on the Bitcoin network. They do not transmit the transaction to a central party (like a bank) because no central Bitcoin authority exists. The Bitcoin users who receive the transaction will then share the hex data with other users. Because the hex data contains a digital signature, it is resistant to tampering. We can think of this step as presenting a deed to the recorder's office.

Finally, a Bitcoin "miner" will include the hex data in a block that will become part of the Bitcoin blockchain. The mining process will check the validity of the transaction. In particular, the transaction cannot be included on the blockchain if doing so would result in a "double spend." For example, if Alice transfers 1.5 BTC to Bob, the mining process would prevent any later attempt by Alice to transfer the same 1.5 BTC to Charlie. In the case of the hex data above (i.e., from the pizza deal), it was included on block 57044 on May 22, 2010.[47] We can think of this step as when the recorder of deeds accepts a deed, stamps it, and records it. Like the county's collection of

---

WGV9] (last visited Jan. 30, 2020). The linked webpage is a "blockchain explorer" that allows anyone with an internet connection to examine Bitcoin transactions. *See* CLIFFORD CHANCE, BUSTING BITCOIN'S ANONYMITY—THE IMPLICATIONS FOR FINANCIAL INSTITUTIONS 2 (2019), https://www.cliffordchance.com/content/dam//briefings/2019/09/busting-bitcoins-anonymity-the-implications-for-financial-institutions.pdf [https://perma.unl.edu/3AVT-VNUU].

42. *See Summary*, BLOCKCHAIN, https://blockchain.info/tx/cca7507897abc89628f450e8b1e0c6fca4ec3f7b34cccf55f3f531c659ff4d79 [https://perma.unl.edu/R2DS-4DWB] (last visited Jan. 30, 2020).
43. *See id.*
44. *See id.*
45. *See* Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 180 (2012) (discussing Bitcoin wallets).
46. *See* Chason, *supra* note 8, at 146–50.
47. *Summary*, *supra* note 42.

deeds, the entire history of Bitcoin transactions is accessible by anyone. Blockchain explorers allow users to inspect any Bitcoin transaction they like (e.g., the pizza-deal transaction described above).[48] The explorer will present important information like the addresses of the transferor and the transferee and the amount of bitcoin transferred.

In sum, the hex data functions like a legal document, and the blockchain functions like a recorder of deeds. We cannot read the hex data directly, but converting it to a human-readable form is a trivial computing task. Once the transaction (represented by the hex data) is included in the blockchain, the transferor may no longer spend the transferred bitcoin. Recordation of deeds serves a similar function, preventing the transferor from fraudulently selling the same real property twice. Moreover, the blockchain, like the record of deeds, is open to the public for inspection.

Of course, differences do exist between the Bitcoin system and the system of real property transfers. Formally, the parties identify themselves using alphanumeric addresses rather than using their legal names. Thus, Bitcoin users can operate with some degree of anonymity.[49] The most extreme example is that "Satoshi Nakamoto" is the founder of Bitcoin and owns bitcoin worth a fortune. We do not, however, have reliable evidence to say who Satoshi Nakamoto is.[50]

More substantively, real property deeds control the transfer of land, which has inherent value recognized across centuries. If you own land, you have the right not only to transfer it but also to occupy it, rent it, and extract its natural resources. Bitcoin, in contrast, is a ten-year-old creation that is backed by no external assets. If you own bitcoin, you have the right to transfer it but nothing more.

D. Bitcoin as a Remote Computer

As discussed more below, observers often compare Ethereum to a "world computer."[51] It is a *computer* because users can execute programs using a general-purpose programming language. It is a *world* computer because the programs are executed in identical fashion across the entire network of users. Your laptop computer is surely different from mine in the types of programs it runs, the data it stores, etc. Ethereum, in contrast, is identical regardless of who runs it. This

48. *See id.*
49. *See* Omri Marian, *Are Cryptocurrencies* Super *Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 42 (2013) ("[C]ryptocurrency accounts are anonymous. Users can start as many online 'wallets' as they want to buy or mine Bitcoins and trade them without ever providing any identifying information.").
50. Heather Hughes, *Blockchain and the Future of Secured Transactions Law*, 3 STAN. J. BLOCKCHAIN L. & POL'Y 21, 30 n.30 (2020) ("The conclusive identity of Satoshi Nakamoto remains elusive.").
51. *See infra* section V.A.

Article uses a similar concept—calling Ethereum a "remote computer"—to emphasize its ability to operate outside of traditional legal structures.[52]

Bitcoin is certainly remote in this way. Because it is decentralized, legal authorities cannot directly exercise control over it. Bitcoin also has some characteristics of a computer. It holds data, which links all previously issued bitcoin units (UTXO) with current owners (or their addresses). Bitcoin also includes a protocol by which owners can transfer these units and by which new units are produced. Thus, someone owns bitcoin units because they have the ability to make a transfer of units and change the UTXO.

This computer model also reinforces the point that Bitcoin does not have any underlying assets like securities, precious metals, or sovereign currency.[53] Ownership is only UTXO (which is computer data) and the ability to change that data by making a transfer (which is accomplished using cryptography and a computer protocol). Policymakers routinely regulate investment assets like securities, but they cannot indirectly regulate Bitcoin by regulating any underlying assets.

III. ETHEREUM AND SMART CONTRACTS

A. Bitcoin Smart Contracts as Locks

Bitcoin offers a weak version of what are commonly called smart contracts. At this point in the Article, we must not assume that such smart contracts resemble legal contracts at all. This section will describe Bitcoin smart contracts as cryptographic locks. The lock can be more sophisticated than simply knowing a password (or private key), and the most common forms of Bitcoin smart contracts resemble joint-ownership arrangements rather than traditional legal contracts. Some Bitcoin smart contracts do have limited contractual characteristics (e.g., offering rewards for solving cryptographic puzzles).[54]

Recall that ownership of bitcoin units means the ability to transfer those units.[55] If Alice owns 1.5 BTC, it is because she has the ability to transfer 1.5 BTC to another user. Moreover, no one else has this abil-

52. *Cf.* Shaanan Cohney, David Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591, 603 (2019) (referring to Ethereum as a "world computer").

53. *See* Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24 U. MIAMI BUS. L. REV. 1, 4 n.3 (2016) ("[B]itcoin can be considered a fiat currency in that it also has no underlying asset.").

54. *See* David Canellis, *There's $70,000 Worth of Bitcoin Hidden Inside This Image*, TNW (June 25, 2019, 11:21 UTC), https://thenextweb.com/hardfork/2019/06/25/satoshi-treasure-bitcoin-cryptocurrency-prize-puzzle [https://perma.unl.edu/L7TN-FSGT].

55. *See supra* section II.A.

ity. In a standard transaction, Bitcoin transfers occur between Bitcoin addresses.[56] Continuing with Alice and a standard transaction, assume someone previously transferred 1.5 BTC to the Bitcoin address that Alice controls. Alice controls this address (and thus the 1.5 BTC) by knowing a private key associated with the address. Alice's 1.5 BTC are locked cryptographically. If she (and only she) knows the appropriate private key, then she alone can unlock the 1.5 BTC by transferring it to another user.[57] As a result, we can say that Alice owns the 1.5 BTC.

This standard pay-to-public-key-hash transaction dominates Bitcoin, but other transactions are possible. Parties can also transfer bitcoin to "scripts," which are a set of conditions expressed in a simple programming language. Anyone who can satisfy the conditions can spend the bitcoin. For example, a Bitcoin transaction might be transferred to the control of multiple transferees. Alice might transfer her 1.5 BTC to the control of three transferees—Bob, Charlie, and Darlene. Two of the three transferees could agree to spend the 1.5 BTC.[58] Bitcoin commentators would call this structure a smart contract. A lawyer, however, would simply consider it a form of joint ownership between Bob, Charlie, and Darlene.

Another common condition is to restrict the transferee from spending the bitcoin until a certain amount of time has elapsed. For example, Alice might transfer 1.5 BTC to Bob subject to the restriction that Bob cannot spend the 1.5 BTC until three months have passed.[59] Again, lawyers would likely not consider this structure contractual. Instead, Bob appears to own the 1.5 BTC subject to some restriction rather than being subject to some obligation to provide goods or services to Alice.

A handful of "puzzle transactions" do offer the glimmer of a contractual offer.[60] Suppose that I wanted to offer a 1 BTC reward to anyone who could guess what I am thinking about. Secretly, I am thinking about the Preamble to the United States Constitution, but publicly I cannot reveal this fact. To implement the puzzle, I announce that the winner is the first person to identify data that, when

56. *See supra* note 12 and accompanying text (discussing pay-to-public-key-hash transactions).

57. *See* Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111, 117 (2012) ("[Bitcoin] can only be accessed through the use of the associated private key.").

58. *See* ANTONOPOULOS, *supra* note 12, at 149 (describing multisignature transactions).

59. *See id.* at 157 (describing timelock transactions).

60. *See Script: Transaction Puzzle*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Script#Transaction_puzzle [https://perma.unl.edu/9SSA-NGV3] (last visited Jan. 30, 2020).

processed with a cryptographic hash function, will produce the following output:

bdec063f229e703e19570569fc552f44a936b528764620fa1 bf7f3fa93202f62[61]

The hash function finds many uses in cryptocurrencies. In this case, it allows me to make a commitment without revealing information. I know what I am thinking about (the Preamble to the United States Constitution), and I want to commit to paying a 1 BTC reward to the first person who guesses this fact. I do not, however, want to reveal what I am thinking about. More generally, a cryptographic hash function takes some textual input (e.g., the Preamble) and returns a seemingly random textual output (e.g., bdec063f22 . . .).[62] The permissible input is text (or a "string") of any size, but the output must be fixed in length.[63]

It is possible to implement this "guess what I am thinking" game using the Bitcoin script. In fact, a Bitcoin user created a very similar challenge in 2012 (using the first Bitcoin transaction rather than the Preamble to the United States Constitution as the subject).[64] This puzzle transaction does seem like a contractual offer, making bitcoin payable to anyone who can perform some task. In my Preamble puzzle, I knew that I was thinking about the Preamble, and I simply wanted someone to guess what I was thinking. The Preamble puzzle might offer some recreational value to the participants. Beyond that, it is difficult to identify any economic potential.

An important feature of cryptographic hashes is that they are "collision resistant."[65] "A collision occurs when two distinct inputs produce the same output."[66] My Preamble puzzle, for example, would not work well if some other input text (like the Declaration of Independence) produced the same hash output. To win the puzzle, the player would either need to identify the Preamble or stumble upon some other solution simply with blind luck. In 2013, a Bitcoin enthusiast created a puzzle transaction that would pay almost 2.5 BTC to anyone

61. *See* U.S. CONST. pmbl.; *SHA-256 Hash Calculator*, XORBIN, https://xorbin.com/tools/sha256-hash-calculator [https://perma.unl.edu/48KT-XJ7S] (last visited Jan. 30, 2020). People will get this output when the Preamble is put into the hash function. You can try this by inputting "WE THE PEOPLE of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this CONSTITUTION for the United States of America." into the hash calculator linked to in this note.
62. NARAYANAN ET AL., *supra* note 30, at 2.
63. *Id.*
64. *See Script: Transaction Puzzle*, *supra* note 60 ("The required data happened to be the Genesis block, and the given hash in the script was the genesis block header hashed twice with SHA-256.").
65. NARAYANAN ET AL., *supra* note 30, at 2–5.
66. *Id.* at 2.

who could identify a specific cryptographic collision.[67] This "collision puzzle" is one puzzle transaction that may have economic substance beyond recreation because many cryptographic projects rely on hash functions.

In broader terms, the collision puzzle offered a bounty to the first person who could identify a particular cryptographic weakness. The collision puzzle, like the Preamble puzzle, does have contractual elements resembling an offer. Despite their contractual nature, however, these puzzle contracts do not seem to point toward a fuller use of Bitcoin as a commercial platform. In both cases, performance was measured cryptographically (because the task to be performed was cryptographic) based on a hash function. Other Bitcoin smart contracts are possible, but performance must be such that it can be proven cryptographically.[68]

B. Limits of Bitcoin Smart Contracts

1. Variable-Payment Contracts

Consider a relatively simple option contract based on the relative value of gold (i.e., the precious metal) and bitcoin units. In October 2020, 1 BTC was worth about 6 ounces of gold.[69] Alice and Bob agree that if gold becomes more valuable six months from now, Bob will pay Alice the excess value measured in bitcoin. For example, if after six months 6 ounces of gold is worth 1.2 BTC, then Bob must pay Alice an additional 0.2 BTC; if 6 ounces of gold is worth 1.7 BTC at that point, then Bob must pay Alice an additional 0.7 BTC, etc. In contrast, if gold does not become more valuable over this time period, no further payment occurs.[70] Because the contract can benefit only Alice, she makes an upfront payment to Bob.

Continuing with the example, let us assume that the contract has a maximum payment of 1 BTC. Alice and Bob want to deploy their con-

67. *Script: Incentivized Finding of Hash Collisions*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Script#Incentivized_finding_of_hash_collisions [https://perma.unl.edu/L9ED-2LUH] (last visited Jan. 30, 2020).

68. The Ethereum White Paper gives a more sophisticated example of a potential Bitcoin smart contract: "[O]ne can even construct a script that says something like 'this Bitcoin UTXO is yours if you can provide [cryptographic] proof that you sent [another cryptocurrency] transaction of this denomination to me', essentially allowing decentralized cross-cryptocurrency exchange." VITALIK BUTERIN, ETHEREUM WHITE PAPER 12 (2013), https://cryptorating.eu/whitepapers/Ethereum/_white_paper.pdf [https://perma.unl.edu/4CBQ-992R].

69. In rough terms, the October 2020 prices were $10,700 per 1 BTC and $1,880 per ounce of gold. *Bitcoin (BTC)*, *supra* note 2; *Daily Gold Price History*, USAGOLD, https://www.usagold.com/reference/prices/goldhistory.php?ddYears=2020 [https://perma.unl.edu/BMC3-NYYA] (last visited Oct. 8, 2020).

70. This arrangement is a cash-or-nothing option. JOHN C. HULL, OPTIONS, FUTURES, AND OTHER DERIVATIVES 606–07 (Donna Battista et al. eds., 9th ed. 2015).

tract on the Bitcoin blockchain using a smart contract. Because the transaction is more complex than transferring bitcoin to an address, Bob would pay 1 BTC to a Bitcoin "script."[71] The transfer of 1 BTC essentially secures Bob's performance, whereas the script determines the future payout.[72] The script should measure the price of 6 ounces of gold relative to bitcoin six months from today and pay Alice the excess of the six-month price (1.2 BTC or 1.7 BTC in our examples) over the current price of gold (1 BTC in this contract). Any amounts not paid to Alice would return to Bob.

The contract is seemingly mechanical and involves little discretion on anyone's part. Nevertheless, Alice and Bob could not deploy this contract on the Bitcoin blockchain. First (and more obviously), the Bitcoin blockchain does not incorporate the relative values of gold and bitcoin. Of course, markets exist for both gold and bitcoin. Contract law allows Alice and Bob to specify, with precision, which markets they wish to use for their contract. But, they would have no way to express that agreement on the Bitcoin blockchain.

Second (and less obviously), the Bitcoin scripting language does not offer a way to have variable payments from a single transaction. Alice and Bob have agreed that Bob's payments should vary along with the relative prices of gold and bitcoin. Contract law easily accommodates this deal. The Bitcoin script does not because payments are "all-or-nothing."[73] Like a lock, the Bitcoin script is either opened or closed. There is no ability to allow for a variable, contingent transfer.[74]

As noted earlier, Bitcoin smart contracts rely on cryptographic locks. As the *Ethereum White Paper* notes, "[T]here is no way for a [Bitcoin] script to provide fine-grained control over the amount that can be withdrawn."[75] Many significant contracts are, of course, either all or nothing. Life insurance policies are one obvious example. The insured is either dead or not, and death triggers payment of a set amount. Gambling contracts are another example. Typically, gamblers win a pot (collected from a group of gamblers) or a fixed amount. Nevertheless, many contracts are inherently variable in nature. De-

71. *See* ANTONOPOULOS, *supra* note 12, at 151–55 (describing pay-to-script-hash transactions).

72. *See* HULL, *supra* note 70 (describing price calculations for binary options).

73. *See* BUTERIN, *supra* note 68 (discussing "value-blindness" of Bitcoin smart contracts). Alice and Bob could create several mini-contracts, each of which is all or nothing. For example, they could break their deal into 100 separate contracts each involving 0.01 BTC. If the six-month price of 6 ounces of gold was 1.2 BTC, then the first 20 of these mini-contracts would pay Alice while the remaining 80 would pay Bob. Computationally, this approach works, but it is cumbersome and expensive. *See id.*

74. *See id.*

75. *Id.*

rivatives contracts, like the one described above, typically involve variable payments.[76]

2. Malicious "Looping" Contracts

Unlike the puzzle transactions, the failed gold-option contract does not rely on cryptography. And, because payments are variable, it cannot be readily expressed as an opened or closed lock. Such limits exist by design because they protect the Bitcoin system from a malicious attack. Broadly speaking, sophisticated smart contracts with variable or contingent payments could undermine the entire Bitcoin system. Consider the following example. If Alice wants to destabilize the Bitcoin system, she might place some computationally intensive condition on a small transfer to Charlie. For example, Alice might create the following malicious contract:

Step 1. Set the variable x to equal the number 1.
Step 2. Check to see if x equals the number 0.
  a. If x does equal 0, give 0.001 BTC to Charlie.
  b. If x does not equal 0, repeat step 2.

After analyzing this process, we quickly discover that it never terminates. We set x to equal 1. Because x does not equal 0, we repeat the process. After checking the value of x, x still does not equal 0, so we repeat the process again. The halting condition (x equals 0) never occurs.

Analyzing the language as lawyers, we would conclude that it fails for impossibility (or impracticability).[77] A computer, however, might simply continue checking the condition *ad infinitum*. Indeed, such was Alice's intent in our example. If she could deploy a contract like the one above, miners could not evaluate it. Moreover, Bitcoin miners would see all of their computational resources being diverted into a futile attempt to evaluate the language.[78]

3. Economically Useful "Looping" Contracts

Bitcoin solves this problem by limiting the types of conditions that users can insert into transactions. The type of condition given above would simply be invalid in Bitcoin because the Bitcoin script cannot

76. Discrete payment options are considered "exotic" or nonstandard options. *See* HULL, *supra* note 70. One can, however, approximate a single variable-payment contract with several discrete-payment contracts. *See* BUTERIN, *supra* note 68 (describing several discrete-payment contracts as a "very inefficient hack").

77. *See* RESTATEMENT (SECOND) OF CONTRACTS § 266 (AM. LAW INST. 1981) (discussing impracticability under traditional contract law principles).

78. *See* ANTONOPOULOS, *supra* note 12, at 131 (warning against "an infinite loop or other form of 'logic bomb' that could be embedded in a transaction in a way that causes a denial-of-service attack against the bitcoin network").

contain complex "looping" structures.[79] The loop occurs because of the direction to repeat step 2. A looping structure could, however, be contractually important. Alice and Charlie might be derivatives traders who agree to the following contract. Up front, Charlie pays Alice 1 BTC. In exchange, Alice agrees to pay Charlie 1.5 BTC if the price of gold ever exceeds some threshold (e.g., $2,000 per ounce). Alice might have to pay Charlie tomorrow, but she might not ever have to pay Charlie at all. Alice and Charlie might like to automate their contract using language similar to the example above:

> Step 1. Charlie pays Alice 1 BTC.
>
> Step 2. Check to see if the price of gold is greater than $2,000 per ounce.
>
> a. If it is, Alice pays Charlie 1.5 BTC, and the contract terminates.
>
> b. If it is not, repeat step 2 tomorrow.

As before, the contract has a looping structure (because of the direction to repeat step 2). But, unlike before, the contract has economic meaning.

Nevertheless, because of the limits inherent in the Bitcoin system, Alice and Charlie could not deploy this contract directly on the Bitcoin blockchain.[80] The reality is that the derivative contract may not ever terminate. There is no guarantee that gold will ever reach $2,000 in the future. The fact that a contract does not have an ascertainable or guaranteed end does not mean it should be disabled as a smart contract. In our example, Alice and Charlie have an open-ended deal that requires a daily check of the price of gold. A smart-contract platform would need to allow a looping structure to facilitate their contract. Since Bitcoin currently disables looping structures to prevent malicious attacks,[81] however, as stated above, Alice and Charlie could not deploy their contract on the Bitcoin blockchain.

As described in the next section, the Ethereum cryptocurrency was designed expressly to accommodate contracts like the gold-derivative example above. It allows looping structures but suppresses malicious contracts by imposing a charge (known as "gas") on the computational resources consumed by smart contracts. Later, this Article will discuss another complex aspect of the gold-derivative contract.[82] Because financial data (like the price of gold) does not appear directly on the blockchain, the contract would need an outside source (known as an oracle) to provide it.

---

79. *See id.* ("The bitcoin transaction script . . . is deliberately limited in one important way—there are no loops or complex flow control capabilities . . . ."). Thus, Bitcoin's scripting language is not "*Turing Complete*." *Id.*

80. *See id.* at 131–32.

81. *Id.*

82. *See infra* subsection IV.A.3.

C. Ethereum Smart Contracts

1. Introduction

In rough terms, we can think of Bitcoin as implementing a form of property transfer law. That law is self-executing and does not rely on courts or officials. Bitcoin also supports a very limited class of transactions, known as smart contracts, that have traits of traditional contracts. Bitcoin smart contracts are limited, however, to cryptographic locks. They do not support variable payments or a full spectrum of conditional payments.

Before proceeding, we should consider how to define the term "smart contract." Many definitions refer to self-executing agreements between parties.[83] The term predates Bitcoin by more than a decade and is generally credited to Nick Szabo, a legal scholar and computer scientist. Szabo called a smart contract "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[84] This Article adopts a more focused and less intuitive definition of a smart contract. On the Ethereum platform, a smart contract is a computer program.[85] Because Ethereum is decentralized, the program must run deterministically; your execution must be identical to my execution. Because smart contracts are Ethereum transactions, they can result in the transfer of value (ether) or the transfer of data.[86]

In order to expand Bitcoin's limited system of smart contracts, Vitalik Buterin created Ethereum.[87] With a few differences outside the scope of this Article, Ethereum implements its currency (known as ether) in a manner similar to Bitcoin. In terms of cryptocurrency market capitalization, Bitcoin is the clear leader with a market capitalization of roughly $200 billion in October 2020.[88] Ethereum occupies second place with a market capitalization of roughly $40 billion.[89] What distinguishes Ethereum is that it supports a much richer array of smart contracts than Bitcoin. In particular, Ethereum supports "Turing complete" smart contracts that allow for looping structures.

Ethereum supports its smart contracts with general-purpose programming structures. In the prior section, we discussed two different

83. *See, e.g.*, DE FILIPPI & WRIGHT, *supra* note 7, at 75 ("Once the wheels of a smart contract are put into motion, the terms embodied in the code will be executed . . . .").
84. Werbach & Cornell, *supra* note 9, at 319.
85. ANTONOPOULOS & WOOD, *supra* note 34, at 127 ("[W]e use the term 'smart contracts' to refer to immutable computer programs that run deterministically . . . on the decentralized Ethereum world computer.").
86. *Id.* at 108.
87. BUTERIN, *supra* note 68, at 13.
88. *See supra* note 2 and accompanying text.
89. *See supra* notes 4–5 and accompanying text.

smart contracts with similar looping structures. One was malicious and was designed simply to tie up computational resources of Bitcoin miners.[90] The other, however, reflected an economic deal between two parties who created a derivatives contract.[91] The challenge for Ethereum is how to allow the beneficial contract while disallowing the malicious one. Computationally, the two contracts seem similar, and there may not be a feasible way to distinguish between legitimate and illegitimate smart contracts algorithmically.

Ethereum's solution is largely economic. Ethereum users must pay for the resources consumed by smart contracts. Recall that the malicious contract[92] created an endless loop; the value of x was always 1, but the program does not terminate unless x equals 0. Bitcoin limits its smart-contract system so that all looping contracts are impossible. Ethereum, in contrast, broadens its system of smart contracts to make the malicious contract possible but with a significant catch. On the Ethereum platform, smart contracts do not execute automatically. Instead, they must be supported with the purchase of gas, which we can think of as a user fee for the computational resources required by the smart contract.[93] Thus, the malicious contract is possible in Ethereum, but it is not economical.

As a single computer, Ethereum presents a problem of shared resources. If I install a smart contract, every full user of Ethereum must execute it in order to determine the appropriate ether balances. Out of sloppiness or even malice, I might write a smart contract that is very difficult and time-consuming for Ethereum users to execute. Bitcoin avoids this problem altogether with a simple system of smart contracts that I compared to a cryptographic lock. Bitcoin's simplicity is incompatible with the more robust system of smart contracts that Ethereum envisions. As a result, Ethereum deals with sloppy and malicious contracts by imposing the gas fee on smart contracts. A malicious, resource-intensive smart contract would generate a very high gas fee. Unless the creator paid this fee, the smart contract would not be able to execute. In contrast, simple and efficient smart contracts generate lower gas fees.[94]

We also examined a more economically significant looping contract that paid one party a fixed amount once the price of gold passed a certain threshold.[95] This arrangement can be expressed as an Ethereum smart contract as well. Depending on the economic significance of the contract, the parties might find it useful to administer it on the

90. *See supra* subsection III.B.2.
91. *See supra* subsection III.B.3.
92. *See supra* subsection III.B.2.
93. ANTONOPOULOS & WOOD, *supra* note 34, at 105–06.
94. *See id.*
95. *See supra* subsection III.B.3.

Ethereum platform and pay the gas charge. This particular contract, however, is not an ideal place for us to begin our consideration of Ethereum smart contracts. It has an added layer of complexity from its use of external financial data. Before turning to such contracts,[96] we will explore Ethereum smart contracts that do not require external information.

2. A Smart Ponzi Contract

A Ponzi scheme may seem to be a dubious place to begin an examination of smart contracts. After all, they are a classic fraud and scam.[97] For a moment, however, let us suspend our disbelief and assume that a Ponzi promoter is completely open and honest. We will assume that the promoter will create the scheme using Ethereum smart contracts. All transactions will be denominated in ether (abbreviated ETH), the Ethereum cryptocurrency.[98]

The promoter wants to offer the following Ponzi scheme. Participants enter the scheme by paying 100 ETH. Contributions by early-stage participants go directly to the promoter because the scheme has no pre-existing participants to pay. In later stages (e.g., after the first month of the scheme), new contributions go directly to pre-existing participants. Let us assume that participants automatically exit the scheme after receiving 200 ETH (representing their initial 100 ETH contribution plus profit of 100 ETH).

We can conceptualize this scheme as a physical box for collecting money with rules for dividing cash as it comes in. The money is ether. The box and the rules, together, constitute an Ethereum smart contract.[99] Most importantly, the Ponzi contract is deterministic and public. Smart contracts exist on the Ethereum blockchain. Anyone can read the computer code that creates the smart contract and observe transactions related to the contract.[100] Also, the Ponzi contract is deterministic. Anyone who observes both the Ponzi contract code and the

96. *See generally infra* section IV.A (discussing Ethereum oracles).

97. Ponzi schemes are, however, a common occurrence on Ethereum. *See* Massimo Bartoletti, Salvatore Carta, Tiziana Cimoli & Roberto Saia, *Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact*, 102 FUTURE GENERATION COMPUTER SYS. 259 (2020).

98. *Ethereum (ETH)*, *supra* note 5.

99. *See* BUTERIN, *supra* note 68, at 13 (describing smart contracts as "cryptographic 'boxes' that contain value and only unlock it if certain conditions are met").

100. Even though smart-contract code is public and readable, it may not be understandable, even to sophisticated users. Typically, Ethereum developers *write* smart contracts in a high-level programming language like Solidity. The resulting programming is compiled into a more compact machine code called EVM bytecode. ANTONOPOULOS & WOOD, *supra* note 34, at 129. EVM stands for "Ethereum Virtual Machine." *Id.* at xxviii.

ether contributions will be able to determine who receives the contributed ether.

In some respects, the Ponzi smart contract seems trivial and potentially pernicious. Given the sad history of financial scams, we should be wary about the creation of an automated Ponzi scheme.[101] Even if we can overcome these concerns, it does not look particularly beneficial. Participants are simply shuffling ether between themselves and are not creating value in the way that a business enterprise would. Nevertheless, the Ponzi smart contract has some interesting features that point toward more substantial smart contracts. The contractual terms are open for inspection,[102] and so are all of the underlying transactions. Moreover, the Ponzi smart contract is automated and, thus, self-executing. Participants do not need to trust that the promoter will actually follow the rules that it establishes.

3. Lotteries and Other Games

The Ponzi smart contract is "honest" in the sense that all participants can observe the rules and will be certain that the rules will be followed. Economically, the contract shares some traits with a lottery in the sense that participants can gauge their chances of winning and the value of the jackpot. As with the Ponzi smart contract, lotteries also just shuffle money between participants after giving the promoter or sponsor a cut.

Could promoters create a lottery using a smart contract? Not easily. Recall that our Ponzi smart contract was deterministic.[103] Money comes into the smart contract and goes out according to an algorithm. All honest observers who evaluate the money inflows in light of the rules would have to agree on the money outflows. A participant who contributes 100 ETH to the Ponzi smart contract will not know in advance what she will get in return. But, after others have contributed, rules specify precisely how much that participant will receive.

Smart contracts cannot readily create lotteries because lotteries are not deterministic.[104] A lottery might rely on transactions to determine the total payout to the winner. However, lotteries use a random number to select the winner, and random-number generation creates a thorny technical issue for smart contracts. Suppose that our lottery operates under the following rules. Participants must stake 100 ETH.

---

101. *See generally* David R. Hague, *Expanding the Ponzi Scheme Presumption*, 64 DEPAUL L. REV. 867, 871–80 (2015) (detailing history of Ponzi schemes).
102. *But see supra* note 100 (describing difficulties in reading the language of smart contracts).
103. ANTONOPOULOS & WOOD, *supra* note 34, at 253 ("In order to maintain consensus, [smart-contract] execution must be totally deterministic and based only on the shared context of the Ethereum state and signed transactions.").
104. *See id.*

Participants identify themselves numerically (through their addresses), and a randomly selected address wins the entire pot. Because the contract language and transactions are public, participants can be sure that the address identified as the "winner" does indeed receive the entire pot. Yet, selecting the winner cannot be truly random. After evaluating the smart-contract code and transactions, all users of the Ethereum system must reach a consensus about the identity of the winner.

The smart contract could, perhaps, designate an external agent who selects numbers at random in order to identify the winner and publishes this selection to the Ethereum blockchain. This solution "works" in that it allows all users to reach a consensus about the identity of the lottery winner and about the lottery transactions. Yet, it introduces a huge element of trust into the contract.[105] Users must trust that the agent selected a number at random rather than a number that she was bribed to select by a participant. For some uses (like reporting objective financial data), oracles provide an adequate solution.[106] The external agent does not offer a particularly appealing solution.

Some actual Ethereum contracts use cryptographic hash functions to create pseudorandom numbers. Recall that a cryptographic hash function takes some textual input (e.g., the Preamble to the United States Constitution) and returns a seemingly random textual output (e.g., bdec063f22 . . .). A small change to the input (e.g., changing the original spelling of "defence" to "defense") produces a very different output (e.g., a0d9fda7f4 . . .).[107] A naive way to generate a pseudorandom number would be to take the cryptographic hash of some characteristic of the transactions. For example, the naive lottery might take the alphanumeric addresses of participants and enter them all (as a single input) into the cryptographic hash function. The winner is the participant with the single address closest to the output hash.

This approach "works" in that it will produce a deterministic winner. All users could evaluate the smart-contract code and reach the necessary consensus about the identity of the winner. The problem, however, is that the random-number generator can be easily manipulated.[108] Blockchain addresses are easy to generate. A participant

105. *Cf. supra* subsection II.B.3.

106. *See* Adam J. Kolber, *Not-So-Smart Blockchain Contracts and Artificial Responsibility*, 21 STAN. TECH. L. REV. 198, 208 n.33 (2018) (discussing Ethereum oracles).

107. *See supra* notes 61–63 and accompanying text.

108. *See* Emin Gün Sirer, *How Not to Run a Blockchain Lottery*, HACKING, DISTRIBUTED (Dec. 25, 2017, 8:05 AM), https://hackingdistributed.com/2017/12/24/how-not-to-run-a-blockchain-lottery [https://perma.unl.edu/A8B5-UL6Z] ("[R]unning a lottery on a blockchain is so incredibly hard to get right.").

might generate (on her computer) several potential addresses and test for one that makes her the winner.

Any solution to the random-number problem must have the following characteristics. The winning number must be deterministic when the winner is selected. Otherwise, the Ethereum community will not reach consensus about the winner. The winning number must be seemingly random when participants are deciding to join the lottery. If not, participants will be able to influence the winning number or manipulate the lottery. In short, a task as simple as pulling a number from a hat is very difficult on the Ethereum platform. While a technical solution exists,[109] the difficulties underscore certain limits in the Ethereum platform.

In sum, Ethereum smart contracts rely on deterministic computer logic that results in the transfer of the ether cryptocurrency. Two problems follow from this observation. First, most economic relationships do not rely on deterministic computer logic. Second, the vast majority of economic deals are not denominated in the ether cryptocurrency. The next Part discusses how Ethereum addresses these two problems.

IV. HOW ETHEREUM INTERACTS WITH THE "REAL WORLD"

A. Oracles

1. Interest-Rate Swap Example

Smart-contract proponents often point to derivatives contracts as a potential use for smart contracts.[110] Consider an interest-rate swap, which is a simple but enormously important type of derivative.[111] In an interest-rate swap, the parties set a "notional amount," which is used solely for computational purposes. To continue the example, assume that the notional amount on a swap is $10,000. One party to the contract (call him Fisk) will pay to the other party a fixed rate of interest based on the notional principal amount. Suppose that the fixed rate is 2%, meaning that Fisk will pay the other party periodic interest of 2% times the notional principal amount. In our case, the notional principal amount is $10,000, and Fisk will pay $200. Let us assume that the payment occurs annually.[112]

---

109. The Niguez Randomity Engine purports to generate a pseudorandom number while avoiding the perils described in this Article. *See* The Plutocrat, *Niguez Randomity Engine*, MEDIUM (June 21, 2019), https://medium.com/niguez-randomity-engine/generating-random-numbers-on-the-ethereum-blockchain-using-solidity-random-number-generator-solidity-9f503c7e4d92 [https://perma.unl.edu/5UYJ-7QUF].

110. *See, e.g.*, Werbach & Cornell, *supra* note 9, at 334–35 n.111.

111. *See generally* HULL, *supra* note 70, at 152–63 (describing interest-rate swaps).

112. *See id.* at 153–55 (describing hypothetical interest-rate swap). Typically, payments are exchanged every six months.

The other party receives the fixed payment just described (i.e., the $200). In return, this other party pays the fixed-paying party a floating rate of interest. Let us call this floating-rate payor Variel. The parties must agree to some floating rate of interest, and the traditional choice is the London Interbank Offered Rate (LIBOR).[113] With that choice, Variel must pay Fisk LIBOR times $10,000. Again, we will assume that Variel's payment occurs annually.

The parties will usually net their obligations.[114] A couple of examples illustrate how payments would be made. Suppose that on the payment date LIBOR is 2.5%. Variel would then pay $50 to Fisk: (2.5% – 2.0%) x $10,000 = $50. In contrast, suppose that LIBOR is 1.7% on the payment date. Now, Fisk will pay Variel $30: (2.0% – 1.7%) x $10,000 = $30.

The market for interest-rate swaps is enormous. Measured in terms of contract values, the market is worth trillions of dollars. Measured in terms of notional principal amounts, the market is worth *hundreds* of trillions of dollars.[115] Interest-rate swaps are important because they allow parties, particularly financial institutions, to transform the characteristics of their assets and liabilities. Consider a simple savings-and-loan (S&L) institution that takes in deposits and makes thirty-year mortgages. Its liabilities are its deposits (which are functionally short-term debt payable to the depositors). Its assets are the thirty-year mortgages. The S&L would be in trouble if interest rates rise. Its depositors would demand higher rates of interest, or they would withdraw their deposits. So, interest expenses would go up. Its mortgage borrowers, in contrast, would pay no additional interest (because their interest payments are fixed contractually by the mortgage). So, interest income of the S&L would remain constant.[116]

113. *See id.* at 155. In the near future, U.S. financial markets will begin using the secured overnight financing rate (SOFR) in place of LIBOR. *See* Gary A. Goodman & Alice F. Yurke, *The Death of LIBOR and the Afterlife*, 34 PROB. & PROP. 8, 11 (2020); Jonathan R. Sichtermann, *The Adjusted Interest Rate Problem: How the Legal System Should Handle the LIBOR Scandal*, 82 UMKC L. REV. 757 (2014) (describing the scandal that led to LIBOR replacement). References in the text to LIBOR can be read as referring to SOFR with no difference in the analysis.

114. *See* HULL, *supra* note 70, at 154 (describing net payments between parties to the swap).

115. BANK FOR INT'L SETTLEMENTS, INTEREST RATE DERIVATIVES (2019), https://stats.bis.org/statx/srs/table/d7?f=pdf [https://perma.unl.edu/C5F3-DT9C].

116. *See* HULL, *supra* note 70, at 155–56 (describing how swaps can transform assets and liabilities). Consider what would happen if interest rates fall. Now, the S&L could lower the interest payments to its depositors without the risk that the depositors would withdraw their funds. So, interest expense would go down. The consequences for the mortgages are somewhat complicated. Rather than continuing to pay interest under the mortgage, many borrowers might refinance. As a result, the S&L could not count on receiving the prior high rate of interest.

The interest-rate swap would allow the S&L to hedge against a rise in interest rates. The S&L would want to pay fixed interest and receive floating interest (taking the role of Fisk in the prior example). Now, if interest rates rise, the S&L would (as before) pay higher interest to its depositors, but it would also receive additional income from the interest-rate swap.[117]

Automating the interest-rate swap with a smart contract could offer efficiencies. For example, the parties could avoid intermediaries and could be certain of performance by the counterparty.[118] We do not, however, need to determine whether a smart contract interest-rate swap is truly more efficient. Instead, we focus on it because it is a common and mechanical arrangement that illustrates the power and limitations of the Ethereum platform.

2. Implementing the Swap in Ethereum

As noted earlier, Bitcoin supports multi-party payments and a few other structures that commentators often call smart contracts.[119] In that discussion, however, this Article concluded that many of these structures seem more like joint ownership rather than contracts. For example, one can readily transfer bitcoin to three persons in a way that gives two of the three parties control over the transfer. Other Bitcoin smart contracts operate like cryptographic locks, allowing a party who satisfies the cryptographic challenge to take the offered bitcoin.

Bitcoin does not offer a ready way to make variable payments.[120] In our interest-rate swap example, payments are inherently variable. Variel, in particular, makes periodic payments to Fisk that vary along with the LIBOR interest rate. The Ethereum system, in contrast to Bitcoin, allows for variable payments so long as the payments can be expressed in computer code.[121]

Let us return to our interest-rate swap and sketch how one might program it in Ethereum. We will start with Fisk's obligation to pay Variel 2% of $10,000, or $200, once a year. A legal contract would need to say a bit more than this, specifying the date of payment and perhaps the method of payment. Let us assume that payment occurs at

117. If interest rates fall, the S&L would need to make a net payment under the interest-rate swap. As noted previously, the consequences to the S&L for an interest rate fall are less easily explained than for an interest rate increase. *See id.*

118. *See generally id.* at 157 (describing the role of financial intermediaries in interest-rate swaps).

119. *See supra* section III.A.

120. *See supra* subsection III.B.1.

121. *See* BUTERIN, *supra* note 68, at 13 (asserting that Ethereum contracts have "vastly more power than that offered by Bitcoin scripting because of the added powers of Turing-completeness, value-awareness, blockchain-awareness and state").

midnight on July 1 in 2021, 2022, and 2023. We can map this specification of time into the Ethereum contract.[122]

Fisk must identify the payee, Variel. Identifying Variel in Ethereum can be done easily with an address[123] that Variel controls. Variel simply needs to specify to Fisk an address that she controls. Bitcoin would work in a similar way.

Next, Fisk must specify the source of the payment. Unless enforced by a court or other legal actor, the smart contract does not create personal liability for either Fisk or Variel. As a result, Variel should reasonably demand that Fisk secure his obligation somehow. Fisk could devote a certain amount of ether to securing his obligations under the smart contract. Up front, Fisk would not know exactly how much ether to post. The contract specifies payment in U.S. dollars, but ether is the currency unit for the smart contract. Also, we are considering Fisk's gross payment of $200 per year. Variel has her own liabilities to Fisk, which we will consider in a moment. The most we can say is that Fisk and Variel should each negotiate for the other to post a certain amount of ether to secure their obligations.[124]

Finally, Fisk and Variel must deal with the problem that their economic deal is in U.S. dollars. Fisk must transfer $200 to Variel on July 1 every year for three years. An Ethereum smart contract, however, cannot deal directly with dollars. Instead, it can deal only with ether, the cryptocurrency of the Ethereum platform. In order to fit their deal into an Ethereum smart contract, they must change its specification slightly. Fisk will transfer ether worth $200 to Variel on July 1 every year for three years.

This specification creates a fresh problem. How can they incorporate this information into their smart contract? A smart contract is

122. *See generally id.* at 20–21 (describing smart contracts under the heading "Financial derivatives and Stable-Value Currencies").

123. In Ethereum, individuals generally use "externally owned accounts" to send and receive ether. *Id.* at 13 ("An externally owned account has no code, and one can send messages from an externally owned account by creating and signing a transaction . . . ."). To keep the presentation manageable for a legal audience, this Article uses the Bitcoin term "address" instead of externally owned accounts.

124. More technically speaking, the smart contract is itself an actor in the Ethereum platform. It would represent itself with a "contract account." Variel and Fisk would transfer their ether to the smart contract's account, and the smart contract would then pay funds back to them according to the terms of the smart contract. *See* Vitalik Buterin, *Ethereum Whitepaper: Ethereum Accounts*, ETHEREUM, https://ethereum.org/en/whitepaper [https://perma.unl.edu/4895-6KTV] (last updated Oct. 9, 2020) (describing smart contracts as "like 'autonomous agents' that live inside of the Ethereum execution environment, always executing a specific piece of code when 'poked' by a message or transaction, and having direct control over their own ether balance and their own key/value store to keep track of persistent variables").

simply a computer program,[125] which itself is simply a series of logical statements. The relative value of ether and dollars is not a matter of logic. Instead, it is an empirical assessment of how markets operate.

The ether-dollar exchange rate is not, however, wholly subjective. Markets do exist.[126] That being said, different markets might have slightly different prices. And, the price of ether might differ based on whether we measure "bid" or "asked" prices.[127] If Fisk and Variel were negotiating a legal contract, they might be willing to allow for some ambiguity in the valuation.[128] Or, they could simply overlook the fact that valuation could occupy some range of values. Once actual payment occurs, the parties might need to negotiate within some range of values. To tie these observations to our hypothetical contract, recall that Fisk must transfer ether worth $200. Depending on the precise market observed, this dollar value might be worth between 0.999 and 1.001 ether.

For Fisk and Variel to implement their deal as a smart contract, the value could not be subject to any ambiguity. Even if the parties are willing to tolerate this small ambiguity, the Ethereum platform cannot. Their smart contract is just a computer program; a small ambiguity is just as bad as a large one. When *any* user of Ethereum runs the computer program, they must get the same output as *every* other Ethereum user. The system would not work if some parties think Fisk must pay Variel 1.0005 ether while others think he must pay 0.9995. Cryptocurrencies operate according to consensus,[129] which applies to a single set of transaction records.

Suppose that Fisk and Variel can identify in advance all the relevant information needed to specify the correct market and other metrics that lead to a precise number of ether worth $200. Precision does not solve all of their problems. Now, they must find a way to integrate this precise information into their smart contract. As noted before, a smart contract is simply a computer program, which is a series of logical statements. Even with a precise agreement, they must still under-

125. "Smart contracts are a new type of computer program that can be designed to operate autonomously from a centralized operator." Jonathan Rohr & Aaron Wright, *Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets*, 70 HASTINGS L.J. 463, 473 (2019).

126. *See* C. Daniel Lockaby, Note, *The SEC Rides into Town: Defining an ICO Securities Safe Harbor in the Cryptocurrency "Wild West,"* 53 GA. L. REV. 335, 363 n.167 (2018) (describing cryptocurrency markets); *Ethereum (ETH)*, *supra* note 5.

127. "*Bid* denotes the highest price the buyer is willing to pay, and *asked* denotes the lowest price the seller will accept." *Bid and Asked*, BLACK'S LAW DICTIONARY (11th ed. 2019).

128. *See, e.g.*, Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 93 (1989) ("If there are transaction costs of explicitly contracting on a contingency, the parties may prefer to leave the contract incomplete.").

129. *See supra* section II.C.

take some analysis of the ether and dollar markets to arrive at the precise value. Ethereum handles this problem with oracles, which allow Ethereum to incorporate data that is otherwise external to the system.

3. External Information and Oracles

In our running example, Fisk and Variel need a way to identify the ether value of $200 on July 1. Fisk will then transfer this amount to Variel. Deployed as a smart contract, this deal can rely only upon logical operations that are applied to past Ethereum transactions. What Fisk and Variel need, then, is to identify some Ethereum transaction that specifies the ether value of $200 on July 1. Their smart contract would then point to this other Ethereum transaction as containing the necessary information.

The challenges in incorporating the necessary information highlight a subtle difference between legal contracts and smart contracts. If Fisk and Variel were negotiating a legal contract, performance would be a private matter to the two parties. They could choose to be exceptionally precise or somewhat relaxed in how they identify the value, knowing that a relaxed definition might bring some interpretive difficulties later on.[130] With an Ethereum smart contract, however, performance would matter not just to Fisk and Variel but to the entire Ethereum community. Their smart contract appears on the blockchain and would need to be executed not just by them but by other users as well. All Ethereum users need to reach consensus about the execution of every smart contract.[131]

To facilitate this consensus, Fisk and Variel's smart contract needs to point to another Ethereum transaction that contains the necessary financial data. Creating such a transaction is not technically difficult because Fisk and Variel could enlist a third party to create such a transaction. Suppose they enlist Orrick, who promises to create a specialized Ethereum transaction that contains the data that Fisk and Variel need, i.e., the ether value of $200 on July 1.

Orrick's transaction highlights an important distinction between Bitcoin and Ethereum. Bitcoin transactions transfer ownership of bitcoin. Ethereum transactions can do the same, but they can also specify data output. Smart contracts, as noted earlier, are simply computer programs. Orrick's transaction would itself be a smart contract, which would allow Fisk and Variel to access the data they need.

130. *See* Ayres & Gertner, *supra* note 128.
131. *See* ANTONOPOULOS & WOOD, *supra* note 34, at 253.

Orrick and his smart contract are known as oracles[132] within the Ethereum community. More generally, oracles are necessary to incorporate data or information that is not otherwise present on the Ethereum blockchain.[133] Oracles might supply information on financial markets, the weather, sporting events, or anything else that might be relevant to a contract. More subtly, oracles can also generate random numbers, something the Ethereum platform cannot otherwise do effectively.[134]

By identifying the oracle transaction, Fisk and Variel can now specify, with complete precision, how Fisk will perform. Fisk executes a smart contract that commits, up front, a negotiated amount of ether. On July 1, 2021, 2022, and 2023, the smart contract will automatically transfer ether worth $200 to Variel. To determine the amount of ether, Fisk's smart contract will call upon a specialized oracle transaction created by Orrick.

Recall that Variel has obligations under the smart contract as well. She must transfer to Fisk an amount of ether that is worth a floating interest rate (LIBOR) times $10,000. Variel faces the same dollar-to-ether valuation problem that Fisk faced but must also determine LIBOR. The financial data she requires is different, but the solution is conceptually the same. She can ask Orrick to create another oracle transaction that specifies LIBOR on July 1, 2021, 2022, and 2023.

With the two oracle contracts, Variel can now specify the transfer to Fisk. She executes a smart contract that, up front, commits a negotiated amount of ether. On July 1 of these years, the smart contract will automatically transfer ether worth LIBOR times $10,000. To determine LIBOR and convert dollar amounts to ether, Variel's smart contract will call upon specialized oracle contracts created by Orrick.

Fisk and Variel have more details to resolve. They would execute a single smart contract that integrates the separate obligations each of them has under the deal we have explored. That smart contract would also integrate the information Orrick would provide about LIBOR and the ether–dollar exchange rate. Fisk and Variel would probably want to have the payments be made under a net basis.[135] Fisk always has a

132. Tatiana Cutts, *Smart Contracts and Consumers*, 122 W. VA. L. REV. 389, 413 (2019); Deborah Ginsberg, *The Building Blocks of the Blockchain*, 20 N.C. J.L. & TECH. 471, 488 (2019); Marcia Narine Weldon & Rachel Epstein, *Beyond Bitcoin: Leveraging Blockchain to Benefit Business and Society*, 20 TRANSACTIONS: TENN. J. BUS. L. 837, 857 (2019); Werbach & Cornell, *supra* note 9, at 336; Sarah Templin, Note, *Blocked-Chain: The Application of the Unauthorized Practice of Law to Smart Contracts*, 32 GEO. J. LEGAL ETHICS 957, 961 (2019).

133. *See* Vitalik Buterin, *Ethereum and Oracles*, ETHEREUM BLOG (July 22, 2014), https://blog.ethereum.org/2014//22/ethereum-and-oracles/ [https://perma.unl.edu/DH4J-J6NA].

134. *Cf. supra* subsection III.C.3.

135. *See* HULL, *supra* note 70, at 207 (describing netting).

$200 gross obligation. If Variel had a $140 gross obligation, they could settle the annual payment with a $60 payment (in ether) from Fisk to Variel.

4. Evaluating the Interest-Rate Swap Example

Decentralization is one of the most important ideas and structures of cryptocurrencies.[136] To some extent, the interest-rate swap is decentralized. Consider how their contract would work outside the Ethereum platform. Variel and Fisk might still need to post collateral to secure their respective obligations under their contract. The collateral would probably need to be held by a neutral third party who would need to be compensated. Variel and Fisk might even find it difficult to contract with each other directly. They might each separately contract with a trusted third party like an investment bank. The investment bank could handle collateral for each party separately and perform other administrative functions under the interest-rate swap.[137] Using traditional financial markets, the interest-rate swap may well be centralized and subject to administration by an investment bank or other intermediary.

The smart-contract variant, however, is not completely automated. Variel and Fisk must rely upon an oracle (Orrick) to supply them with necessary financial data. Orrick's presence does lead to some centralization. Yet, Orrick does not handle ether. During the life of the contract, ether is held by the smart contract itself, which automates payments. The Ethereum platform works like an automated escrow agent, holding funds for the party until the deal directs that funds be released.[138] Variel and Fisk must rely on Orrick to supply information but do not need to rely on any other intermediary, who would charge a fee to Variel and Fisk.

Variel and Fisk cannot use the Ethereum platform for free. In order to execute the smart contract, they must pay the gas fee.[139] Ethereum (like Bitcoin) is potentially inefficient because it operates under a principle of radical redundancy. One server with a backup is not sufficient to maintain a decentralized organization. The community of users can achieve consensus about ownership because many users maintain an identical set of records. Each of these users would have to execute the smart contract between Variel and Fisk. We cannot say,

136. *See supra* section II.C.

137. So long as Variel and Fisk are creditworthy, the investment bank has no net risk. The two contracts (one to Variel and one to Fisk) offset each other. *See* HULL, *supra* note 70, at 157 (describing how swap parties usually work through financial intermediaries).

138. *See* Werbach & Cornell, *supra* note 9, at 344.

139. *See* Cohney et al., *supra* note 52, at 603.

with any certainty, that the smart contract format is inherently more efficient than one administered by an investment bank.[140]

Unless assisted by courts, the smart contract cannot impose personal liability (like a contract would). To see why this is important, recall the fundamentals of the deal. Every year, Fisk must pay $200, and Variel must pay LIBOR times $10,000. Payments are netted.[141] For the moment, focus only on dollar transfers (and set aside that they pay each other in ether). They both set aside $200 to fund their separate obligations. In the first year, suppose that LIBOR surges to 5%, giving Variel a gross obligation of $500. After netting against Fisk's fixed $200 obligation, Variel's obligation is $300. Variel has set aside only $200 in the smart contract, and it all goes to Fisk. Variel still owes Fisk $100.

If we interpret their smart contract as a standard interest-rate swap, Variel has personal liability to Fisk. She owes Fisk $100 this year, and she may still owe him more in future years. If Variel refuses to pay Fisk, Fisk could sue her, obtain a judgment, etc. Had Variel entered into an interest-rate swap with an investment bank, the bank would likely monitor Variel's collateral levels on a periodic basis. As LIBOR started to surge in our example, the investment bank would almost certainly demand that Variel increase her collateral levels.[142] If Variel refused, the agreement would likely give the bank the right to terminate the swap contract.

Fisk and Variel could, conceivably, automate a process by which collateral levels increase according to market factors. Yet, they would face a now-familiar problem: the Ethereum platform does not incorporate market factors directly into its system. Fisk and Variel could turn to an oracle to set collateral levels. However, this responsibility is much more discretionary, open-ended, and continuous than simply reporting LIBOR and the ether–dollar exchange rate once a year. Orrick might also find himself subject to regulatory burdens if he intervenes too much in Fisk and Variel's deal. For now, let us assume that variable collateral levels are impracticable.

Even if the smart contract cannot impose personal liability, it could take an intermediate step of terminating the smart contract if Variel refuses to pay Fisk. This way, Variel would not enjoy any benefits from the smart contract if LIBOR fell in the future. Fisk would also

140. It is possible that the smart contract format allows for smaller contracts than what investment banks might allow. Variel and Fisk might be small business owners who could find it difficult to do business with large investment banks. Variel and Fisk might not present enough opportunity for profit.

141. *See supra* subsection IV.A.1.

142. Some exchange-traded derivatives require daily settlement. Each party's position is valued on a daily basis, and parties whose positions are negative must pay a margin to secure performance. *See* HULL, *supra* note 70, at 29–32.

get his money out of the smart contract immediately. Nonetheless, this early termination comes nowhere near solving the problem. If Variel and Fisk want a three-year interest-rate swap with personal liability, they cannot get it on Ethereum.[143]

Here, we may be seeing the first real cost of decentralization.[144] Courts enforce actual contracts with personal liability. Ethereum has no enforcement mechanism other than to direct the payment of ether that participants have already committed to the smart contract. Thus, the term "smart contract" is potentially misleading. For lawyers anyway, a better description is "automated escrow."[145] Parties commit value (using units of ether) to a computer program which determines whether value, expressed in the ether cryptocurrency, is transferred between parties.

B. Tokens

1. Introduction

In our smart contract examples, we saw how Ethereum allows for conditional or variable transfers of the ether cryptocurrency. As a legal construct, such smart contracts function like automated escrows. Parties commit a certain amount of value (ether) that will be transferred according to the terms of the smart contract. Smart contracts do not, however, create personal obligations (though courts might infer personal liability from the terms of the smart contract or other dealings between the parties).

So, we have considered the reach of Ethereum to personal liability and external information. We will now consider how Ethereum (and Bitcoin) can interact with external assets (that is, assets other than ether). For example, corporate managers might want their shareholders to be able to transfer shares using the Ethereum blockchain. As we will see, Ethereum *tokens* could allow for the transfer mechanically.

Ethereum tokens are, in effect, private currency issued by individual users.[146] Users create this private currency using Ethereum smart contracts, and almost all Ethereum tokens follow the form known as the ERC20 token standard.[147] In this Article, we can set aside most of the details of creating tokens. We must, however, distin-

143. They could still execute a traditional interest-rate swap (which imposes personal liability) and support that swap with an Ethereum smart contract. The point is that the smart contract does not function like the traditional contract.

144. *See generally* Werbach & Cornell, *supra* note 9, *passim* (comparing smart contract technology with contract doctrine and theory).

145. *See id.* at 344.

146. ANTONOPOULOS & WOOD, *supra* note 34, at 221; Joseph D. Moran, Note, *The Impact of Regulatory Measures Imposed on Initial Coin Offerings in the United States Market Economy*, 26 CATH. U. J.L. & TECH. 213, 246–50 (2018).

147. *See* ANTONOPOULOS & WOOD, *supra* note 34, at 227.

guish between tokens (freely created by individual users) and cryptocurrency (created by the system itself). Approaching the distinction by analogy, we can liken ether and other cryptocurrencies to dollars. In contrast, we can liken ERC20 tokens to the metal tokens one receives at a video-game arcade.

Ethereum and other blockchain tokens could conceivably represent ownership in anything (like shares in a corporation). Some adherents believe that tokens are the crucial application of Ethereum and urge us to "tokenize everything"[148] across all aspects of commerce. Skeptics argue that blockchains are important but not of such universal use. Blockchains consume a lot of computational resources because many users must maintain extensive and duplicative records. Depending upon the cryptocurrency, the "mining" process is also resource intensive. The best uses for blockchains, according to skeptics, are situations where trust is difficult or impossible to establish.[149] Shareholders in my hypothetical corporation might be inclined to trust me and my corporation to see that share ownership is transferred appropriately. Or, they might find it relatively inexpensive and easy to find a trustworthy third party to handle transfers.

This Article will not engage too deeply with this debate. Markets are almost certainly better judges about the efficiency of blockchains for commercial use. Legal observers should, however, ask whether such uses are transparent. And, we should also be wary of such uses if their efficiency lies in avoiding legal liability, regulation, and taxation. As a result, legal observers should remain neutral about whether blockchain transfers of corporate shares are efficient compared with other means of transfer.

2. Utility Tokens

As noted already, Ethereum developers commonly deploy tokens in order to give users the ability to control resources outside the Ethereum platform. Simple, non-Ethereum examples may be the best way to begin. For decades, merchants and service providers would find it convenient to sell special-purpose, physical tokens for goods and services. Laundromats, video-game arcades, and public transportation

148. Sparsh Singhal, *What Can Be Tokenized? The Tokenization of Everything*, HACKER NOON (Aug. 9, 2019), https://hackernoon.com/what-can-be-tokenized-the-tokenization-of-everything-mw1ay3bk7 [https://perma.unl.edu/ZK5T-W3M8]; *see also Tokenize All the Things*, DECRYPT, https://decrypt.co/collections/tokenized-world [https://perma.unl.edu/KX3Q-DZ27] (last updated Dec. 26, 2019) ("Blockchain technology, which eliminates the expensive middlemen (banks, brokerages, agents) in finance, coupled with tokenization, makes it cheap and efficient to create fractional shares in virtually anything.").

149. *See, e.g.*, AMMOUS, *supra* note 24, at 261 ("Trustless digital cash has so far been the only successful implementation for blockchain technology . . . .").

are prime examples.[150] Chuck E. Cheese is a chain of restaurants that serves pizza and has video games. Before the chain transitioned to "Play Pass" cards, customers would buy (or receive) brass tokens they could use to play the games on-site.[151] The tokens looked like coins and functioned like money inside a Chuck E. Cheese restaurant, allowing customers to participate in recreation. Outside Chuck E. Cheese, however, the tokens had no intrinsic value other than as collectibles.

Ethereum developers can create tokens that operate in a way similar to the Chuck E. Cheese tokens. Such "utility tokens" appear on the Ethereum platform and allow users to access consumer goods and services. For example, an Ethereum developer might create Ethereum tokens that allow users to play online video games or receive e-books. Users would pay money (ether) in exchange for the utility token.

We should carefully distinguish the token (utility or otherwise) from the currency. Inside Chuck E. Cheese, the distinction was obvious and visual. Paper and coins with dead presidents on them are currency; brass coins with a rat face on them are tokens. On the Ethereum platform, the distinction is less obvious. Ether is the currency. It has value, measured in dollars and other sovereign currencies, on fairly liquid markets. No one can create more ether because its supply is limited by algorithm. In contrast, each developer can control the number of utility tokens issued. Once issued, however, tokens can be transferred in ways similar to ether itself.

"True" utility tokens may not present many thorny legal issues. They are simply a way to sell goods and services over the internet. They do, however, represent prepaid goods and services, which can give rise to consumer-protection concerns. That being said, the consumer-protection concerns do not appear to be different from concerns that would arise when a consumer prepays for goods and services using U.S. dollars or other sovereign currency.

3. Equity Tokens

"Equity tokens" represent ownership of an asset. In concept, an equity token could represent ownership of a durable consumer good (like a car or a home) or an investment asset (like corporate stock). Recent years saw a surge in equity tokens issued in "initial coin offerings" (or "ICOs") covering decentralized organizations.[152] The ICO term is an obvious play on the traditional "initial public offering" (or "IPO") used in securities laws. Despite using the ICO name, many promoters

150. *See* ANTONOPOULOS & WOOD, *supra* note 34, at 221.
151. *See Chuck E. Cheese*, WIKIPEDIA, https://en.wikipedia.org/wiki/Chuck_E._Cheese [https://perma.unl.edu/4NY7-6482] (last updated Aug. 3, 2020, 7:59 UTC).
152. *See* Cohney et al., *supra* note 52, at 606–10.

claimed they were offering utility tokens. By incorporating some consumer goods or services into the token, the promoters believed they could avoid the reach of securities laws.[153] The SEC slowly but surely affirmed the application of securities laws to ICOs, even those that purport to be utility coins because they incorporate consumer-level goods and services.[154]

For purposes of this Article, tokens are important because they are a means to transfer non-blockchain resources using the Ethereum blockchain. Thus, they link the Ethereum blockchain to the "real" economy. Understanding this linkage helps us see limits on the ability of Ethereum or similar platforms in replacing traditional legal structures. Suppose that a blockchain enthusiast wants to make an *inter vivos* gift to you of a valuable painting. Rather than signing over the deed to you, the enthusiast transfers her unique token that represents ownership of the painting.[155] Before you take physical possession of the painting, however, the enthusiast dies. Her heirs want to keep the painting.[156]

Working solely on the blockchain, the token does not give you ownership of the painting. Suppose that the court rules against you, holding that the token transfer did not effectively transfer the painting to you. The painting would belong to the heirs. Any attempts on your part to retake the physical painting would be a theft. The problem is that this token does not directly give you anything. For the token to have value and to transfer the painting, the court must recognize it.

Consider a similar example but with a different outcome. Suppose that a Bitcoin enthusiast wants to make an *inter vivos* gift to you of 1 BTC. The enthusiast transfers her 1 BTC to you in a manner recognized on the Bitcoin blockchain. Later, however, the enthusiast dies. Her heirs want the 1 BTC back. As with the painting–token example,

153. Investing in an orange grove was famously held to be a security under *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946). Though not an aspect of the case, an added benefit of orange-juice delivery would almost certainly not have removed the contract from the reach of securities law.

154. *See* STRATEGIC HUB FOR INNOVATION & FIN. TECH., U.S. SEC. & EXCH. COMM'N, FRAMEWORK FOR "INVESTMENT CONTRACT" ANALYSIS OF DIGITAL ASSETS (2019), https://www.sec./corpfin/framework-investment-contract-analysis-digital-assets [https://perma.unl.edu/QEZ4-5AR3].

155. *Cf., e.g.*, Jerry Brito, Houman Shadab & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 205 (2014) ("For example, we could agree that a particular bitcoin (or, indeed, an infinitesimally small fraction of a bitcoin so as to allow for many tokens) represents a house, a car, a share of stock, a futures contract, or an ounce of gold.").

156. Legally, the issue is whether the enthusiast delivered the painting to you or executed "an inter vivos donative document." RESTATEMENT (THIRD) OF PROP.: WILLS AND DONATIVE TRANSFERS § 6.2 (AM. LAW INST. 2003) ("The transfer of personal property, necessary to perfect a gift, may be made (1) by delivering the property to the donee or (2) by inter vivos donative document.").

all you received was a cryptoasset. Now, it is 1 BTC. But, unlike in the painting–token example, your 1 BTC does not control any external assets. Its value derives from the fact that market participants will pay U.S. dollars for the 1 BTC. Also, and most importantly, you do not need the assistance of any court to own or transfer the 1 BTC. It is yours because the Bitcoin community and blockchain recognize it as yours. As a technological matter, no court can seize the 1 BTC because no third party (like a bank) administers Bitcoin.[157]

C. Summary

Oracles and tokens are two forms of smart contracts that allow Ethereum to interact with the real (non-Ethereum) world. Oracles are a source of outside information, allowing smart contracts to base payments on such information (e.g., interest rates or exchange rates).[158] Tokens signify ownership of some resource other than ether.[159] The resource might be anything. It could be purely digital (like an e-book), it could be land, or it could be anything in between on the spectrum of property and resources.

The existence of oracles and tokens demonstrates that many (perhaps most) Ethereum smart contracts cannot operate in a vacuum. Without tokens, Ethereum smart contracts could not control external resources. Without oracles, Ethereum smart contracts could not use financial data or other external information.

Judges, regulators, and legislators thus have more ability to regulate smart contracts than some may have assumed. Because Ethereum is largely decentralized, they may have difficulty in directly regulating the transfer of ether units between parties. But, legal authorities can more easily regulate the external interactions of oracles and tokens. Agencies might regulate parties that routinely supply financial information as oracles. Courts might choose not to give legal effect to certain types of ownership tokens. The next Part of this Article gives a more systematic account of when legal authorities can and cannot exert control over cryptocurrencies and related transactions.

157. *See generally* Andrew W. Balthazor, Comment, *The Challenges of Cryptocurrency Asset Recovery*, 13 FIU L. REV. 1207 (2019) (examining difficulties in recovering cryptocurrencies and related assets).

158. *See supra* section IV.A.

159. *See supra* section IV.B.

V. A REMOTE-COMPUTER MODEL

A. Ethereum as a Computer

The Ethereum platform could itself be considered a computer.[160] Consider what is on a typical personal computer. It has programs with which you interact. For example, if you open a web browser and type "weather tomorrow," you will be directed to a webpage that gives you a weather forecast. Somewhat more formally, you provided input ("weather tomorrow") to a program (your web browser) and obtained output (a webpage showing the forecast). Your computer also stores data. For example, you might open a list of contacts and enter the email address and phone number of a person you just met.

Returning to Ethereum, we can consider it to be a world computer because it has data and also supports programs.[161] In terms of data, it stores balances of ether (its native cryptocurrency) held by various users. Unlike your personal computer, however, Ethereum is shared by a multitude of users.[162] Moreover, for it to function properly, users must come to a consensus about its data content. For example, absolutely no one will stop me or even care if I open a spreadsheet on my personal computer, name it "balance of all the money I have," and type some really large number. Everyone else in the world is completely indifferent about what is in this computer file. In contrast, users around the world care deeply about the ether balances stored as data on the Ethereum computer.[163] To reiterate, ether units (and bitcoin units) are simply computer data; they do not represent ownership of any other assets. Unlike the data stored on your personal computer, ether and bitcoin have economic significance because they trade on markets.

Extending the computer model further, the Ethereum platform holds data (like ether balances), and it also supports computer programs known as smart contracts. As discussed above, an Ethereum smart contract can transfer ether in a way that is conditional or varia-

160. *See* Tonya M. Evans, *Cryptokitties, Cryptography, and Copyright*, 47 AIPLA Q.J. 219, 241–42 (2019) (describing Ethereum as a personal computer or world computer).

161. *See* ANTONOPOULOS & WOOD, *supra* note 34, at 26 ("Ether is meant to be used to pay for running *smart contracts*, which are computer programs that run on an emulated computer called the *Ethereum Virtual Machine* (EVM). The EVM is a global singleton, meaning that it operates as if it were a global, single-instance computer, running everywhere.").

162. *See id.*

163. We should understand ownership of ether and bitcoin as the ability to change the stored data. If you own 100 ETH, I cannot simply change ownership to myself at will. As the owner, however, you can transfer the 100 ETH to me (by following the correct protocol for making a transfer). After the transfer, I control the 100 ETH (because I can transfer it to someone else); you no longer own it.

ble.[164] For example, an Ethereum smart contract might implement an interest-rate swap, by which parties exchange payments based on fixed and variable interest rates. This smart contract implements commitments by both parties because they must contribute ether to the smart contract. Over time, the ether will be returned to the parties based on the movement of the variable interest rates.

Smart contracts do not only control the transfer of ether; they also supply information or data output. In the interest-rate swap example, the smart contract cannot make payments based solely on computer logic. It must rely on financial data (like variable interest rates). The parties can receive this information from an oracle, which itself is a smart contract that supplies information.[165] Similarly, some Ethereum smart contracts require random numbers,[166] which can be supplied by specialized smart contracts.[167]

You and I might have personal computers with identical hardware. Unless we took extraordinary measures, however, the two physical computers would have different data and software. Ethereum, in contrast, is a *single* computer.[168] No matter the user, it has the same data and the same programs. This characteristic is directly related to the consensus model of cryptocurrencies. Your personal computer and mine can coexist with different data. No one is looking to either of our computers for a record of values. Ethereum, in contrast, does store value (ether balances), and the community must agree on these balances for them to have economic value. Thus, Ethereum (like Bitcoin) is based on decentralized consensus rather than centralized control.[169]

The description of Ethereum as a single computer has importance to our understanding of it as a system of property or even contract law. Ultimately, the Ethereum platform determines ownership of the ether cryptocurrency, and ownership of ether is simply data stored on the Ethereum computer. Viewing the Ethereum platform as a single computer means that there is a single set of data and programs that determines ether ownership. An individual owns ether if and only if ownership is reflected in that data. In determining ether ownership, the Ethereum system does not rely upon any enforcement mechanisms from courts or other legal institutions. Owners protect their

164. *See supra* subsection III.C.1.
165. *See supra* subsection IV.A.3.
166. Technically speaking, computers generate pseudorandom numbers. The numbers are not truly random but behave like random numbers for a given purpose. *See Pseudorandom Number Generator*, WIKIPEDIA, https://en.wikipedia.org/wiki/Pseudorandom_number_generator [https://perma.unl.edu/G3RY-ZJBT] (last updated May 27, 2020, 20:38 UTC).
167. *See supra* note 106 and accompanying text.
168. *See supra* section II.D.
169. *See supra* section II.C.

ether cryptographically, excluding others who would take the ether for themselves. Owners also transfer ether with simple computer scripts that function like deeds.

Earlier, this Article described Bitcoin as a computer.[170] The bitcoin cryptocurrency exists as computer data, associating owners with units of cryptocurrency. As described in this section, Ethereum can also be seen as a computer. Its underlying cryptocurrency—ether—is simply computer data that associates owners with units of the cryptocurrency. The Ethereum computer, unlike Bitcoin, supports sophisticated smart contracts, which function like computer programs. This additional feature supports the computer model of Ethereum.

B. Ethereum as a Remote Computer

After describing Bitcoin as a computer, this Article characterized the Bitcoin computer as *remote* for legal purposes.[171] Bitcoin operates under principles of decentralization and consensus rather than centralized control. As a result, judges, regulators, and legislators cannot readily exercise jurisdiction over the Bitcoin computer. A judge could not easily order the transfer of bitcoin units to their lawful owner. Legislators could not mandate consumer protections for stolen or lost bitcoin units.

By describing Bitcoin as a remote computer, I mean that we can imagine it to exist on a single computer in a legally remote (or "offshore") jurisdiction. In this remote-computer model, anyone in the world can examine (or "read") the record of transactions and determine current ownership of bitcoin units. Owners still transfer units as they do in the actual Bitcoin system, submitting their transfers to miners who then submit their new blocks to the central computer. Admittedly, this remote-computer model obscures important structural issues of consensus and decentralization. For legal purposes, however, these structural issues are of secondary importance. The important points are that Bitcoin is legally remote (because it is decentralized) and purely digital (because it is backed by no external assets). These are the traits of a single offshore computer that administers a private, digital currency.

We can extend this remote-computer model to Ethereum. As with Bitcoin, we can envision Ethereum as existing on a single offshore computer. Again, anyone can see the history of ether transactions and the current state of ether ownership. What distinguishes Ethereum is its system of smart contracts, which can be used to create tokens and oracles. In fundamental terms, smart contracts are computer programs. Thus, smart contracts are entirely consistent with our remote-

170. *See supra* section II.D.
171. *See id.*

computer model. The smart contracts will execute on the Ethereum platform resulting in the output of data or the transfer of ether. Both of these effects (data output and ether transfer) appear on the Ethereum blockchain.

C. Legal Significance of the Remote-Computer Model

With the remote-computer model in mind, we can more clearly see the extent of legal authority over Bitcoin and Ethereum. Legal authorities will find it difficult or impossible to control the internal operations of Bitcoin and Ethereum because they are decentralized computers that are functionally remote. For example, suppose that a country enacts a transactions tax on all cryptocurrency transactions, naively making the tax collectible by the central administrator. Because Bitcoin and Ethereum have no central administrators, the tax would be ineffective.

Perhaps most importantly, regulators cannot force a change in the ownership of bitcoin and ether. Suppose that Alice is insolvent, owing several million dollars to Bob. Alice owns 100 ETH and transfers them to an address secretly controlled by her son, Charlie. Alice has made a fraudulent transfer, which is voidable by Bob. Although Bob might be able to prove that Alice's transfer was fraudulent, he has a limited ability to take the 100 ETH or reverse the transaction. His only avenue would be to discover Charlie's identity and try to compel Charlie to make a transfer. Only Charlie can transfer the 100 ETH because only Charlie knows the associated private key.

In the remote-computer model, individual users may still interact with the computer. Anyone can view the history of all past transactions and the current state of ownership. Existing owners may also execute new transactions that transfer cryptocurrency units to new owners. Miners collect these new transactions, form them into blocks, and add them to the blockchain. The actions of individuals interacting with the remote computer are potentially subject to regulation or legal control.

Legal authorities can thus exercise control over markets.[172] Suppose that Alice wants to create an Ethereum exchange where participants come together to trade ether for U.S. dollars. In this example, regulators can reach Alice's Ethereum activities like any other market activities. When users act publicly, regulators have much easier routes to exercise jurisdiction. Secondary markets, for example, have arisen for the buying and selling of bitcoin units. These markets function like other financial markets and can be regulated. Speaking more broadly, the remote-computer model lets us more clearly distinguish

172. *See* Tu & Meredith, *supra* note 25, at 306–07 (describing application of anti-money-laundering rules to Bitcoin).

between the internal affairs of Bitcoin and Ethereum (like ownership of cryptocurrency units) and external affairs (like markets for bitcoin units).

Based on their name, smart contracts may seem to be a way to bypass traditional legal structures. Some futurists, for example, envision a fully automated law of contracts that execute on computer platforms. Current technology, however, remains well short of full automation. The remote-computer model gives an analytical tool to approach smart contracts from a legal perspective. Smart contracts are effective at transferring units of cryptocurrency without assistance from courts.[173] For example, a smart contract could specify the conditions by which counterparties transfer ether to each other. Because the remote computer determines ownership of ether, the smart contract can be effective for this purpose without further enforcement by a court.

In contrast, a smart contract could not directly transfer other assets unless a court or other legal authority enforces the smart contract. Tokens, particularly equity tokens, may represent the clearest attempt by blockchain promoters to interact with (or even displace) traditional legal structures. The "tokenize everything" slogan supports the idea that Ethereum tokens can be used to represent ownership in a wide variety of assets, ranging from securities to automobiles. Tokens, however, are a form of smart contracts, which are computer programs that run on the Ethereum platform. By applying the remote-computer model to tokens, we see that they have limited power in displacing traditional legal structures.

For example, suppose that a car dealer "tokenizes" its inventory of automobiles. Whenever it sells a new car, it issues a token to the buyer that represents ownership of the car. Alice buys a car from the dealer and receives a unique token representing her ownership. Later, Alice purports to sell the car to two separate people, Bob and Charlie. She signs a state-issued paper document of title and gives it to Bob in exchange for $10,000.[174] Separately (and fraudulently) she transfers the dealer-issued token to Charlie in exchange for $10,000.

---

173. *See supra* Part III. As noted previously, Bitcoin does have a system of rudimentary smart contracts. *See supra* section III.A. Other cryptocurrency systems have smart contracts as well. *See What Are Smart Contracts? Guide for Beginners*, COINTELEGRAPH, https://cointelegraph.com/ethereum-for-beginners/what-are-smart-contracts-guide-for-beginners [https://perma.unl.edu/LGS6-UCM7] (last visited Jan. 30, 2020).

174. *See generally* 7A AM. JUR. 2D *Automobiles and Highway Traffic* § 36 (2020) ("In many jurisdictions where provision is made for the issuance of certificates of title to motor vehicles, the sale or transfer of a motor vehicle is consummated by the assignment of the certificate of title to the purchaser or transferee in the method prescribed by statute.").

Clearly, Alice has committed a fraudulent transfer and should be sued, prosecuted, etc.[175] Bob and Charlie, however, have a matter between themselves: Which of them has a better claim to the car? According to the Ethereum blockchain, Charlie has a token that entitles him to the car. But, this token does not give him any special access to the automobile. His ownership is perfected only on the Ethereum blockchain. Without delving too deeply into this hypothetical case, we can surmise that Bob has the superior claim based on traditional legal instruments.

VI. CONCLUSION

Cryptocurrencies, smart contracts, and tokens may well revolutionize the law. But, the revolution is not inexorable. Cryptocurrencies are, literally speaking, computer data and computer programs. Legal actors cannot readily change the contents of these files and programs. For example, a court cannot simply order that one party is the rightful owner of 1 BTC nominally held by another party. As suggested by this Article, we can view cryptocurrencies and the like as being administered on a remote computer, which determines ownership of the cryptocurrency units themselves. Because the computer is remote, courts and the like cannot control it. Thus, they cannot control the ownership of cryptocurrency, and cryptocurrency ownership is fundamentally important. Bitcoin and Ethereum, the two leading cryptocurrencies, have market capitalizations of $200 billion[176] and $40 billion respectively.[177]

Yet, some proponents envision a far more pervasive role for cryptocurrencies and their related blockchain technology. In this role, smart contracts could replace traditional contracts for a wide range of topics, and tokens could similarly replace many elements of property law. For this revolution to occur, however, cryptocurrency platforms need to interact with rights and obligations that originate outside the remote computer (or outside the blockchain). Judges, regulators, and legislators will continue to have an important role to play in recognizing this interaction. Such legal actors cannot determine the ownership of cryptocurrency directly, but they can determine the ownership of non-blockchain property. A regulator might, for example, fully embrace the use of tokens to transfer traditional securities. Or, a regulator might rule that such use is invalid.

175. *Cf. generally* 37 AM. JUR. 2D *Fraudulent Conveyances and Transfers* § 1 (2013) ("Although one can generally dispose of his or her property as one sees fit, a person cannot frustrate his or her creditor's rights and avoid obligations by changing title to his or her assets. The fraudulent transfer of assets is considered a tort . . . ." (citations omitted)).

176. *See supra* note 2.

177. *See supra* note 5.

This Article does not attempt to say which approach is better. Context matters. Regulators might have little reason to interfere with investment banks that trade derivatives between themselves using an unalterable blockchain. Consumers, on the other hand, might not even be able to understand the computer code that makes up smart contracts. Judges, regulators, and legislators will continue to play important roles as these technologies and markets evolve.