2019

How Bitcoin Functions As Property Law

Eric D. Chason
William & Mary Law School, edchas@wm.edu

How Bitcoin Functions As Property Law

*Eric D. Chason**

Bitcoin replicates many of the formal aspects of real estate transactions. Bitcoin transactions have features that closely resemble grantor names, grantee names, legal descriptions, and signatures found in real property deeds. While these "Bitcoin deeds" may be interesting, they are not profound. Bitcoin goes beyond creating simple digital deeds, however, and replicates important institutional aspects of real estate transactions, in particular recordation and title assurance. Deeds to real property are recorded in a central repository (e.g., the public records office), which the parties (and the public) can search to determine title. When one grantor executes more than one deed covering the same property, recordation acts (race, notice, and race-notice) determine which grantee wins.

The Bitcoin blockchain replicates the public records office, giving anyone with a computer the ability to see any Bitcoin transaction. Bitcoin mining replicates the recording of deeds, a process by which formally valid transactions between two parties become essentially a public record. When one grantor executes more than one transaction covering the same Bitcoin, a miner determines which grantee wins simply by moving one transaction to the blockchain before the others.

Remarkably, Bitcoin replicates these aspects of real estate transfers without any governing authority to coordinate or supervise activities. It has no central database for the blockchain. Instead, users across the globe maintain the blockchain in identical form. Bitcoin has no recorder of deeds to time-stamp and process transactions. Instead, it relies on dispersed and competitive miners to, in effect, time-stamp transactions and add them to the blockchain. Ultimately, this Article will show that Bitcoin succeeds because it leads its community of users to a consensus about the blockchain.

Thus, this Article will conclude that Bitcoin replicates elemental pieces of property law, but it does so wholly outside of traditional legal structures. Ownership is based on computer protocols, computer records, community expectations, and nothing more. Bitcoin functions as law, even though it operates outside of the law.

* Associate Professor of Law, William & Mary Law School.

I. INTRODUCTION

The history of Bitcoin sounds like it was pulled from a science fiction novel. In the fall of 2008, the world was suffering its worst financial crisis since the Great Depression. Financial institutions collapsed, and governments struggled to keep the entire financial system from failing.[1] On Halloween Day in 2008, a writer, using the pseudonym Satoshi Nakamoto, published a whitepaper titled Bitcoin: A Peer-to-Peer Electronic Cash System. In the whitepaper, Satoshi Nakamoto proposed a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[2] Satoshi Nakamoto's stated rationale was to create "[t]ransactions that are computationally impractical to reverse."[3] When parties transact via financial institutions, "financial institutions cannot avoid mediating disputes."[4] Chargebacks and stopped checks are two examples that American consumers and institutions may be familiar with.

Barely two months later, in early January 2009, Bitcoin "went live" with the creation of the first units of Bitcoin.[5] These initial units, known as the "genesis block,"[6] belong to their creator, Satoshi Nakamoto. Embedded in the computer code creating the genesis block was the text "The Times 03/ Jan/2009 Chancellor on brink of second bailout for banks."[7] Drawn from

---

[1] *See generally* Robert K. Rasmussen & David A. Skeel, Jr., *Governmental Intervention in an Economic Crisis*, 19 U. PA. J. BUS. L. 7, 13–21 (2016) (detailing governmental intervention during financial crisis).

[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.ORG 1, https://bitcoin.org/bitcoin.pdf. (last visited Oct. 13, 2018).

[3] *Id.*

[4] *Id.*

[5] Jake Goldenfein & Dan Hunter, *Blockchains, Orphan Works, and the Public Domain*, 41 COLUM. J.L. & ARTS 1, 7 (2017) ("Nakomoto mined the first 'genesis block' of bitcoins in January 2009, as well as a substantial number of early bitcoins.")

[6] *See* Larissa Lee, *New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market,* 12 HASTINGS BUS. L.J. 81, 100 (2016) (referring to the genesis block as "the very first block on the Blockchain").

[7] *See* Seth Litwack, Comment, *Bitcoin: Currency or Fool's Gold?: A Comparative Analysis of the Legal Classification of Bitcoin*, 29 TEMP. INT'L & COMP. L.J. 309, 313 n.42 (2015); Eric P. Pacy, Comment, *Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes*, 49 NEW ENG. L. REV. 121, 124 (2014).

the front page of the Times (of London), the text of the computer code references attempts by the United Kingdom to bolster its banking system in the middle of the financial crisis. The text may have been a simple attempt at establishing a date for the genesis block. Satoshi Nakamoto may have, however, been subtly arguing that the U.K. government was abusing its monetary power by propping up rich and connected banks.[8] If financial systems ultimately did collapse, people might stop using state-sponsored currency (dollars, pounds, etc.) and turn to alternative stores of value that operate outside of state control.

Nearly a decade after these events, newspaper headlines speak not of crisis but of Bitcoin, which has grown from an obscure whitepaper to a significant investment vehicle. The success of Bitcoin has spawned new but related technologies, generally known as cryptocurrencies. Everyone, it seems, has an opinion about Bitcoin and cryptocurrency, ranging from the euphoric[9] to the apocalyptic.[10]

Rather than voice another opinion, this Article will attempt to describe Bitcoin in a way that is thorough and meaningful for lawyers, law students, and law professors. As will be discussed, Bitcoin replicates many of the formal aspects of simple real estate transactions. Bitcoin "deeds" have features that closely resemble grantor names, grantee names, legal descriptions, and signatures. These "Bitcoin deeds" may be interesting, but they are not profound. Bitcoin goes beyond creating simple digital deeds and replicates important institutional aspects of real estate transactions. Bitcoin uses a concept that is similar to real estate's "chain of title" concept. Deeds to real property are recorded in a central repository (e.g., the public records office), which the parties can search to establish title. When one grantor executes more than one deed covering the same property, recordation acts (race, notice, and race-notice) determine which grantee takes the property.

---

[8] *Cf.* Goldenfein & Hunter, *supra* note 5, at 7 (describing Satoshi Nakamoto as "a kind of crypto-libertarian mashup of Spartacus, Keyser Söze, and Jay Gatsby").

[9] *See* Tunku Varadarajan, *The Blockchain Is the Internet of Money*, WALL ST. J.: THE WEEKEND INTERVIEW (Sept. 22, 2017), https://www.wsj.com/articles/the-blockchain-is-the-internet-of-money-1506119424.

[10] *See* Paul Krugman, *Bitcoin Is Evil*, N.Y. TIMES: OPINION (Dec. 28, 2013), https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil.

When Satoshi Nakamoto created Bitcoin, he[11] faced similar issues. Suppose Alice wants to buy a car for three bitcoin (BTC) from Bob. How can Bob know that Alice really owns 3 BTC? Moreover, suppose that Alice executes a Bitcoin "deed" conveying 3 BTC to Bob, but executes another deed conveying the same 3 BTC to Chelsea a few minutes later. Does Bob own the 3 BTC? Does Chelsea? Do they both own 3 BTC? Does Alice still own 3 BTC? If Bitcoin is to function rationally, it must allow Bob to confirm that Alice owns 3 BTC. Following the transfer, it must grant recognition upon transferees (Bob as the owner of 3 BTC) and also strip recognition from transferors (Alice as the prior owner of 3 BTC).

Dealing with these issues would have been easy (at least conceptually) if Satoshi Nakamoto kept all Bitcoin records on his laptop. Alice would own 3 BTC if the laptop says she does. As between Bob and Chelsea, Satoshi Nakamoto would presumably choose the transferee he learned about first (essentially favoring the first to file or record).[12] This solution—using Satoshi Nakamoto's laptop as the central hall of records—was unacceptable and is not what Bitcoin does. Satoshi Nakamoto wanted to allow for direct payments without any central institution, not even Satoshi Nakamoto himself. According to this specification, Bitcoin cannot be administered by Satoshi Nakamoto himself. As a leading book says, "Bitcoin . . . is decentralized and has no single entity in charge. Satoshi's not in charge."[13]

The challenge for Bitcoin, then, can be stated in terms that are familiar to readers who have taken a class on property law. Bitcoin needs a system of title assurance and a system for recording the relevant instruments of transfer,[14] which this Article refers to as "Bitcoin deeds." These systems, however, cannot rely upon any central authority or institution. The solution comes from two innovations: Bitcoin mining and the blockchain. We can think of the blockchain as "the public records office, where all instruments affecting land titles . . . are recorded."[15] We can think of mining as the

[11] We do not know the true identity, much less gender, of Satoshi Nakamoto. Satoshi Nakamoto may have been several individuals. However, the Japanese name is masculine (like, for example, David Smith), and Satoshi Nakamoto registered as a male on internet sites where he first proposed Bitcoin. *See generally Satoshi Nakamoto*, WIKIPEDIA, https://en.wikipedia.org/wiki/Satoshi_Nakamoto#Characteristics_and_identity (last visited Oct. 13, 2018).

[12] *Cf.* 66 AM. JUR. 2d *Records and Recording Laws* § 71 (2018) ("The purpose of a statute requiring the recording of all conveyances of real property is to protect subsequent judgment creditors, bona fide purchasers, and bona fide mortgagees against the assertion of prior claims to land based upon any recordable but unrecorded instrument.").

[13] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 176 (2016).

[14] *Cf.* JESSE DUKEMINIER ET AL., PROPERTY 693–776 (8th ed. 2014) (describing issues of title assurance).

[15] *Id*. at 693.

process by which some official (like the county recorder) takes executed deeds and records them. Bitcoin replicates the functions of the public records office and the county recorder but without any central authority.

This is a remarkable achievement. Bitcoin is a system of property that replicates the functions of legal instruments (deeds) and institutions (public records offices) without relying on legal institutions or even the law itself to coordinate the transfer or enforcement of property interests. This fact may explain some of the excitement and dread that surrounds Bitcoin.[16] Those who prefer a limited role for law and government may see Bitcoin as a means to their end. Those who prefer a more robust role for law and government may see Bitcoin as a serious threat. This Article does not take a position on whether Bitcoin is good or bad. Bitcoin exists, and we should attempt to understand it on its own terms.

Scholars have already done important theoretical work concerning Bitcoin. Professor Joshua Fairfield has used the advent of Bitcoin "to reflect on property theory"[17] to develop "a theory of property as information"[18]—namely, "who owns what."[19] Professor Michael Abramowicz views Bitcoin and cryptocurrencies as creating "protocols [that] can be used to aggregate human judgment and make legal decisions."[20] Several other scholars have made similarly important contributions to the nascent legal literature on Bitcoin.[21]

---

[16] *Compare* Tunku Varadarajan, *The Blockchain Is the Internet of Money*, WALL ST. J.: THE WEEKEND INTERVIEW (Sept. 22, 2017), https://www.wsj.com/articles/the-blockchain-is-the-internet-of-money-1506119424, *with* Paul Krugman, *Bitcoin Is Evil*, N.Y. TIMES: OPINION (Dec. 28, 2013), https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil. *See* Varadarajan, *supra* note 9; *see also* Krugman, *supra* note 10 and accompanying text (noting the polarized responses to Bitcoin).

[17] Joshua A.T. Fairfield, *Bitproperty*, 88 S. CAL. L. REV. 805, 810 (2015).

[18] *Id.* at 811–12.

[19] *Id.* at 812.

[20] Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 363 (2016).

[21] *See, e.g.*, Benjamin W. Akins et al., *A Whole New World: Income Tax Considerations of the Bitcoin Economy*, 12 PITT. TAX REV. 25 (2014) (analyzing the tax aspects of Bitcoin transactions); Benjamin Akins et al., *The Case for the Regulation of Bitcoin Mining as a Security*, 19 VA. J.L. & TECH. 669 (2015) (arguing for securities law to apply to Bitcoin mining); Hilary J. Allen, *$=€=Bitcoin?*, 76 MD. L. REV. 877 (2017) (identifying systemic risks of widespread adoption of Bitcoin); Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE L. REV. ONLINE 22 (2014) (analyzing the legal classification of Bitcoin); Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U. L. REV. 1485 (2014) (raising the possibility of autonomous legal entities); Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144 (2014) (identifying areas for regulatory attention); Jeanne L. Schroeder, *Bitcoin and the Uniform Commercial Code*, 24 U. MIAMI BUS. L. REV. 1 (2016) (analyzing U.C.C. aspects and implications of Bitcoin); Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271, 272 (2015) (urging coordinated regulatory response to challenges of cryptocurrencies); Angela Walch, *The*

This Article approaches Bitcoin from a different perspective. It seeks to develop our understanding of Bitcoin as a new type of legal phenomenon, one that exists outside of the normal legal environment of laws, governments, and institutions. Perhaps unwittingly, Satoshi Nakamoto identified and replicated two key elements of real estate transactions: deeds and title assurance. Rather than using laws and institutions to coordinate and regulate his new form of property, Nakamoto relied on technology and incentive engineering to bring a community (Bitcoin users) into consensus about ownership.

II. COMPARING BITCOIN TO REAL PROPERTY

A. *Deeds to Avalon and Notional Property*

The initial goal is to understand Bitcoin by comparing it to transfers of real property. As will be shown, Bitcoin replicates many formal aspects of deeds (signatures, chain of title, and title assurance). Substantively, however, the comparison is weaker. Title to Blackacre lets me use and occupy Blackacre.[22] "Title" to 50 BTC does not let me use or occupy anything because Bitcoin is not backed by any assets or enterprise.[23]

To develop the comparison between Bitcoin and real property deeds, imagine an eccentric or insane monarch who grants deeds to fictitious land. Perhaps our monarch has a thing for King Arthur and grants deeds in Avalon (an island in Arthurean legend)[24] to several of his trusted subjects. Since our monarch has not yet surveyed Avalon, all grants are of undivided interests in the whole (e.g., 1%, 2.5%, etc.). To keep things simple (and similar to Bitcoin), we will suppose that the monarch simply grants quitclaim deeds[25] of undivided interests.

We might assume that Avalon deeds are completely worthless, but we will continue our little fiction for a moment and assume that, in this realm, paper money is unavailable. We will also assume that our monarch invests considerable resources in a public records office for Avalon. Avalon deeds

Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837 (2015) (analyzing Bitcoin in the context of the larger financial system).

[22] When speaking of real property, I will assume that all interests are fee simple, "the broadest property interest allowed by law." *Fee Simple*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[23] *See* Nicolas Wenker, Note, *Online Currencies, Real-World Chaos: The Struggle to Regulate the Rise of Bitcoin*, 19 TEX. REV. L. & POL. 145, 174 (2014) ("Bitcoin is not backed up by any entity or assets and its value is entirely virtual and subjective.").

[24] *See Avalon*, WIKIPEDIA, https://en.wikipedia.org/wiki/Avalon (last visited Oct. 13, 2018).

[25] In other words, the grantor makes no covenants to the grantee. *See Deed*, BLACK'S LAW DICTIONARY (10th ed. 2014).

are recorded quickly and, once recorded, are available for public inspection. Officials at the registry are also adept at spotting forgeries and other frauds. Parties can transfer and record Avalon deeds without paying any fees or taxes.

Operating under these new details, citizens of the realm might plausibly use Avalon deeds as a form of currency, something our realm does not otherwise have. Rather than lugging gold or silver around to pay for goods and services, citizens could simply execute a deed for an interest in Avalon if citizens view it as a store of value. The Avalon public records office might well function like a central bank, keeping track of everyone's interests in Avalon. Citizens of the realm could carry preprinted deed forms with themselves and use them the way that we use check books in the real world.

If interests in Avalon are property, then they are "notional," meaning they exist only as a matter of recordkeeping.[26] Owners have the right to transfer their interests, but have no rights to enjoy Avalon (because it either does not exist or it cannot be identified). In contrast, owners of existing real property have rights beyond the right to transfer their property (e.g., the right to use or rent the property).[27] As described, the Avalon deeds seem useful as stores of value or as currency: the interests are transferable; the public records office tracks everyone's interests in Avalon and clamps down on fraud; and, because the sovereign expressed the initial grant as percentage interests in the whole, owners can readily aggregate and disaggregate their holdings. For example, a 2.5% interest plus a 1.25% interest would be worth 3.75%.

Bitcoin shares many similarities with these hypothetical Avalon deeds. Neither is backed by real assets. Unlike legal tender, neither has any set value in the eyes of the sovereign.[28] Both are valuable only to the extent that other people are willing to buy them, and both are easily transferable.

The Avalon deeds, however, depend upon a central institution and sovereign. The sovereign established the Avalon public records office, which is the central repository for deeds. Officials there examine the deeds and police them for fraud. In the event of competing deeds from the same grantor, the officials might honor the first deed recorded or might follow one

---

[26] Derivatives contracts, for example, are often written using a "notional principal amount" that determines the payout to a party. *See* Henry T.C. Hu, *Misunderstood Derivatives: The Causes of Informational Failure and the Promise of Regulatory Incrementalism*, 102 YALE L.J. 1457, 1513 n.6 (1993).

[27] *See* J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. REV. 711, 732 (1996) (describing incidents of ownership).

[28] "'Legal tender' refers to the coin, paper money, or circulating medium that the law compels a creditor to accept in payment of a debt when tendered by the debtor. A medium of exchange need not be legal tender to be classified as money." 53A AM. JUR. 2D *Money* § 11 (2018).

of the more nuanced rules (race, notice, or race-notice) found in American recording acts.[29] In short, the law and a legal institution seem to be an essential component of Avalon's deed system, even though the interests in property are notional. As we will see, Bitcoin resembles the hypothetical Avalon deeds, but does not rely upon any central institution or laws.

B. *Bitcoin Scarcity*

Another comparison may be drawn between Bitcoin and the fictitious Avalon deeds. Both are scarce. I suggested that the sovereign granted undivided interests in the entirety of Avalon. Altogether, these interests must equal 100%. Similarly, the supply of Bitcoin is fixed by the computer protocol that all users follow. The current Bitcoin supply is roughly 16.5 million BTC.[30] The mining process[31] continues to add to this supply, which will grow to twenty-one million BTC.[32] Even though the supply of Bitcoin is currently growing, it has a fixed growth rate that will eventually end with a limited supply.

Decentralization buttresses the scarcity of Bitcoin. If some central authority administered Bitcoin on a database that it controlled, the authority would likely have the technical means to issue new Bitcoin at will.[33] Newly issued Bitcoin dilute the claims of current owners, much in the way that the issuance of new currency results in inflation. Bitcoin owners, in such a world, would need to rely on legal recourse against the central authority to prevent dilution by the issuance of additional Bitcoin.

Since Bitcoin relies upon decentralized authority and consensus, all users run the same (or very similar) computer code that enacts the Bitcoin protocol. According to this protocol, successful Bitcoin miners receive a mining prize (called the coinbase transaction),[34] and these coinbase transactions are the only way to issue new Bitcoin. After the total supply has reached 21 million BTC, the coinbase transactions will terminate.

C. *A Lawyerly Definition of Bitcoin*

Before turning to what Bitcoin is, let us understand some things that it is not. Bitcoin is certainly not legal tender or fiat currency issued by a

---

[29] *See, e.g.*, ROBIN PAUL MALLOY & JAMES CHARLES SMITH, REAL ESTATE TRANSACTIONS: PROBLEMS, CASES, & MATERIALS 266–68 (5th ed. 2017) (describing the three types of recording acts).

[30] *Controlled Supply*, BITCOINWIKI, https://en.bitcoin.it/wiki/Controlled_supply (last visited Oct. 13, 2018).

[31] *See infra* Part V.C.

[32] *See supra* note 30.

[33] *See* NARAYANAN ET AL., *supra* note 13, at 25 (stating that the sponsor of a centralized cryptocurrency could "create as many new coins for himself as he wants").

[34] *See infra* Part V.D.4.

sovereign.[35] It is a purely private creation. Bitcoin is also not a business enterprise, at least not of the sort that lawyers commonly deal with. Adding to our confusion is the term "Bitcoin" itself. The "coin" part is metaphorical and aspirational, reflecting the hope that Bitcoin would become a common system for payment. Bitcoin is not backed by any identifiable assets or business activities. Owners will never receive dividends, redemptions, or similar distributions.

Thus, Bitcoin as units of transfer are "notional," existing as recordkeeping entries only.[36] If you own 12.47 BTC, you effectively have a bookkeeping entry, but nothing else. You have the right to transfer some or all of those units to another person, and the Bitcoin system makes this transfer simple and direct. You might be able to receive non-Bitcoin value (dollars, goods, services) in exchange for Bitcoin. You would not, however, be able to receive value directly from the Bitcoin system.

"Bitcoin" may refer to either the entire Bitcoin system or to individual units of transfer. Similar usage, of course, applies to "the dollar" or "the pound." A financial analyst who says "the U.S. dollar is weak" is not describing some particularly poor piece of paper in her pocket, but rather is describing the entire U.S. monetary system. A cashier who says, "that will be three dollars" just wants some currency, preferably three $1 bills.

To lessen the confusion, this Article uses "Bitcoin" to describe the entire system or the currency in the abstract, much in the way that the word "dollar" is used. It uses "BTC" to describe individual units of transfer, much in the way that the "$" symbol or the "USD" abbreviation are used. Readers should note that, unlike a dollar bill, a single Bitcoin (one BTC) is divisible. The smallest unit is 0.00000001 BTC (sometimes called a "satoshi").[37] If it is assumed that 1 BTC is worth $10,000, then 100 satoshis would be worth $0.01 (a penny).

Owners of Bitcoin establish their ownership by what lawyers would call a "chain of title," or what Satoshi Nakamoto called "a chain of digital signatures."[38] Each transfer of Bitcoin resembles a deed of real estate, as the "grantor" refers to the prior transaction under which she holds. Modern cryptography allows users to replace legal names and handwritten signatures with alphanumeric public addresses and digital signatures.[39]

---

[35] *See supra* note 28. Fiat money or currency is "[p]aper money that, in contrast to hard currency, is not backed by reserves but instead derives its value from government regulation or law declaring it legal tender." *Money*, Black's Law Dictionary (10th ed. 2014).

[36] *See supra* Part II.A.

[37] *See* NARAYANAN ET AL., *supra* note 13, at 46.

[38] Nakamoto, *supra* note 2, at 2 ("We define an electronic coin as a chain of digital signatures.").

[39] "'Cryptography means' 'secret writing in' Greek, but the science of cryptography encompasses more than just secret writing, which is referred to as encryption. Cryptography

This Article will now attempt a definition that may help illuminate what Bitcoin is. The Bitcoin system creates a notional unit of transfer called "Bitcoin," which may be further fractionated (down to a "satoshi"). Owners may transfer units (in whole or in part) by following a protocol established by the Bitcoin system. Ownership of the units is established by a set of records called the "blockchain." The blockchain serves to record—and link—all transactions going back to the initial creation of Bitcoin in early 2009. Bitcoin has no central authority or super-user[40] with enhanced authority. It is administered by all users, collectively, and the consensus of all users determines ownership of bitcoin (and settles any disputes about ownership).

In brief, the Bitcoin system comprises both a protocol for transferring ownership and a set of records of all transactions. Bitcoin is usually called a "cryptocurrency" because both the transfer protocol and the set of records depend on cryptography. Bitcoin is the first successful cryptocurrency, but others exist.[41] We can distinguish Bitcoin from the other cryptocurrencies using the brief definition given above. The Bitcoin set of records would contain all transactions going back to Bitcoin's initial creation in early 2009. Other cryptocurrencies might have similar transfer protocols, but they would have different starting points and a different set of transactions.[42]

This Article will attempt to describe both elements of Bitcoin, the transfer protocol and the set of transaction records. We will see that both can be compared to elements of real estate transactions. Bitcoin units are transferred using computer files that look and function like deeds to real property. These files, which are referred to in this Article as "Bitcoin

can also be used to prove knowledge of a secret without revealing that secret (digital signature), or prove the authenticity of data (digital fingerprint)." ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: PROGRAMMING THE OPEN BLOCKCHAIN 55 (2d ed. 2017).

[40] "In various versions of UNIX and UNIX-like Operating Systems, 'superuser' . . . is the name given to the user account that a system administrator can use to make almost any change to the system. This is also known as the 'root' account." Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1333 n.9 (2008) (citation omitted).

[41] *See generally* NARAYANAN ET AL., *supra* note 13, at 242–71 (describing "Altcoins and the Cryptocurrency Ecosystem").

[42] Bitcoin has, however, experienced intentional "forks" in the blockchain. The Bitcoin community relies on using a common protocol. Some users might want to introduce new features to the existing protocol that were previously invalid (a "hard fork") or eliminate features that were previously valid (a "soft fork"). *See* NARAYANAN ET AL., *supra* note 13, at 73–75; ANTONOPOULOS, *supra* note 39, at 260–61. Bitcoin has experienced several forks that have produced related but distinct cryptocurrencies (notably Bitcoin Cash and Bitcoin Gold). *See List of Bitcoin Forks*, WIKIPEDIA, https://en.wikipedia.org/wiki/List_of_bitcoin_forks (last visited Oct. 13, 2018).

deeds,"[43] name the transferor and the transferee,[44] describe the interest being transferred, state how the transferor acquired the interest, and contain a (digital) signature executed by the transferor. Moreover, the set of Bitcoin transaction records (i.e., the blockchain) resembles a registry of real property deeds, enabling any user to determine who owns what within the Bitcoin system. Even though Bitcoin resembles real estate transactions, this resemblance alone does not make it particularly interesting. What makes it interesting (and possibly revolutionary) is how Bitcoin replicates the functions of deeds and deed registries.

D. *The Double Spend Problem*

The chief problem facing Satoshi Nakamoto—preventing owners from "double spending" their Bitcoin holdings—has a clear counterpart in the law of real estate transfers. If Alice transfers Blackacre to Bob, we expect Bob to record the deed (e.g., at the public records office). Under various title assurance statutes (race, notice, and race-notice statutes), Alice could not convey title to Chelsea by executing a deed after Bob records his. The law of real estate transfers relies on central authority—the public records office—to assure Bob of his title.

Now suppose that Alice owns 1.5 BTC, and she transfers it to Bob. How can we prevent Alice from transferring the same 1.5 BTC to Chelsea?[45] Bitcoin could solve this "double spend" problem with a central registry, much the way that the law of real estate transfers offers a central registry for the recordation of deeds. But Satoshi Nakamoto's stated goal in creating Bitcoin was to create a decentralized currency.[46] His creation would have no central authority or user with special privileges.

His solution was to find a way to bring about consensus among all users as to Bitcoin ownership. If all (or almost all) users could agree that Bob is the rightful owner of Alice's 1.5 BTC, then there is no need for a central authority to maintain records and mediate disputes. Bob would be the owner because other Bitcoin users recognize him as such. Moreover, the

---

[43] Unlike "mining," "blockchain," etc., "Bitcoin deed" is my own convention. *Cf.* ANTONOPOULOS, *supra* note 39, at 26–28 (describing mining and blockchain as part of standard Bitcoin description).

[44] The "Bitcoin deeds" do not use the legal names of the parties. Instead, parties operate pseudonymously, using alphanumeric "Bitcoin addresses" to identify themselves. *See infra* Part III.D.

[45] Alice and Bob are the central characters in many cryptography texts, dating back to their introduction in 1978. *See* Quinn DuPont & Alana Cattapan, *Alice and Bob: A History of the World's Most Famous Couple*, CRYPTOCOUPLE http://cryptocouple.com (last visited Oct. 13, 2018).

[46] *See* Nakamoto, *supra* note 2, at 1 ("What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.").

community of users would simply disregard any attempt by Alice to double spend her 1.5 BTC by transferring it to Chelsea after transferring it to Bob. As will be discussed later in this Article, Bitcoin uses a clever mixture of cryptography and incentive engineering to bring about this consensus.

III. CREATING A BITCOIN IDENTITY

A. *Your Generous Uncle*

Before turning to the issue of Bitcoin title assurance, this Article will first consider how Bitcoin transfers take place. Suppose you have a generous uncle who wants to make two gifts to you: Blackacre and 50 BTC. Readers who have completed a course on property law will feel comfortable with the transfer of Blackacre by deed, a written instrument that conveys land.[47] Transferring Bitcoin may initially sound daunting, but in practical terms, your uncle should not have too much difficulty transferring the 50 BTC to you. He could download a specialized "Bitcoin wallet" software that allows him to transfer Bitcoin to you without too much trouble.[48] The wallet software will generate a file of plain text that effectuates the transfer.

It would not be stretching the truth to say that the wallet software generates a "Bitcoin deed." It is a writing (a computer file of plain text)[49] that describes the property being transferred (50 BTC). It also describes the transferor (your uncle), the transferee (you), and the source of your uncle's ownership. It also contains a digital signature. This Part will walk through these elements to see how "Bitcoin deeds" function much the same way as simple real property deeds.

B. *Human Identity Versus Bitcoin Identity*

Recall that your uncle wants to make a gift of bitcoin to you. What should you do to receive it? Like your uncle, you could acquire specialized "wallet" software; in your case, it would make your acquisition seem smooth and intuitive. While important to Bitcoin users, wallet software is not a focus of this Article. Instead, this Article seeks to explain how Bitcoin works (or how the wallet works), analogizing the mechanics of the transfer to a simple real estate deed.

When your uncle made a gift of real estate, he executed a deed. He described the property, listed your legal name as grantee, and signed the paper before a notary.[50] While Bitcoin transfers rely on instruments that

---

[47] *Deed*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[48] *See generally* ANTONOPOULOS, *supra* note 39, at 93 (describing Bitcoin wallets).

[49] *See, e.g.*, UNIF. ELEC. TRANSACTIONS ACT (UNIF. LAW COMM'N 1999) (facilitating transactions through electronic, rather than paper, transactions).

[50] *See generally* 23 AM. JUR. 2d *Deeds* §§ 1, 12 (2018) (describing elements of deeds).

function like deeds, there are differences.

Bitcoin does not use legal (human) names. Instead, Bitcoin users identify themselves with alphanumeric "Bitcoin addresses."[51] In fact, Bitcoin transfers are made between addresses, and Bitcoin users will often use distinct addresses for different transfers.[52] Strictly speaking, the Bitcoin system recognizes the address (not the human being) as the principal actor.

The Bitcoin address is created using cryptographic functions largely beyond the scope of this Article. Despite this reliance on cryptography, nothing in Bitcoin is "encrypted." The details of every transaction are completely public and open for all to see. Several websites exist that describe every Bitcoin transaction.[53]

Back to the Bitcoin address that you will need to receive your uncle's gift of 50 BTC. The process of creating a Bitcoin address is as follows:

- First, the user (e.g., you) creates a "private key." This private key will function like a password.
- Second, the user derives a "public key" from the private key just created.[54] The public key has a function that we will consider later.[55]
- Third, the user derives a "Bitcoin address" from the public key.[56] The Bitcoin address functions like a user name and is controlled by the private key.

C. *Private Key*

Let us focus on the private key. Again, it is conceptually like a password, but it is also used to create the public key and Bitcoin address. Like a password, it should be something that adversaries cannot guess, ideally produced by a random process.[57] A tedious but effective way to generate a private key would be to buy a sixteen-sided die (somewhat like the large dice used in Dungeons & Dragons), roll it sixty-four times, and

---

[51] "A bitcoin address is a string of digits and characters that can be shared with anyone who wants to send you money [Bitcoin]. . . . The bitcoin address is what appears most commonly in the transaction as the 'recipient' of the funds." ANTONOPOULOS, *supra* note 39, at 64–65.

[52] *See* ANTONOPOULOS, *supra* note 39, at 94.

[53] For example, the entire blockchain is available at https://blockchain.info.

[54] *See* ANTONOPOULOS, *supra* note 39, at 60 ("The public key is calculated from the private key.").

[55] *See infra* Part IV.B.3.

[56] ANTONOPOULOS, *supra* note 39, at 65 ("The bitcoin address is derived from the public key . . . .").

[57] ANTONOPOULOS, *supra* note 39, at 58 ("A private key is simply a number, picked at random.").

record each roll on a piece of paper.[58] The result would be a series of letters (A through F) and numbers (zero through nine) that constitute a hexadecimal number. Assume that you do just that and, miraculously, you roll the following:

> ABCDEF0123456789ABCDEF0123456789ABCDEF01234567
> 89ABCDEF0123456789

This is your "private key" (though most Bitcoin applications would express it more compactly).[59] Since this particular private key is obviously not random, and it is published in this Article, it is completely worthless. To be effective, a private key needs to be known only by the intended owner (i.e., you). But, for purposes of this Article, we will pretend that it is a secret and that it will be used to receive the 50 BTC from your uncle.

This private key is not shared with anyone. It is not even shared with your uncle to receive Bitcoin. It is, however, used to create a Bitcoin address that is completely public. The mathematical details of creating the address are well beyond the scope of this Article, but the process of creating the Bitcoin address can be thought of as being a one-way street.

- If you have your private key, you can quickly create the Bitcoin address associated with it.
- If I have your Bitcoin address, I cannot reverse directions and discover the private key that created it.[60]

Private keys create public addresses, but public addresses do not reveal the associated private keys.

D. *Bitcoin Address*

Using a web application,[61] we quickly learn that your private key (ABCDEF0123 . . .) produces the following Bitcoin address: 18BjkQhqFsCy1ryFwpYjPLgZLWGZ5zTnsJ

The following printable card could even be created for safekeeping.[62] It represents your private key and Bitcoin address in a variety of formats. Note that the upper half of the printable card is safe to share; it contains your Bitcoin address and something called a public key (which will be discussed

---

[58] If you want to try it, record "10" as "0" and record eleven through sixteen as "A" through "F."

[59] The paper wallet in the text expresses a "Bitcoin Address" and a "Bitcoin Address Compressed." *See* text accompanying *supra* note 62.

[60] *See* ANTONOPOULOS, *supra* note 39, at 63 ("[T]he bitcoin address . . . can be shared with anyone and does not reveal the user's private key.").

[61] BITADDRESS.ORG, https://www.bitaddress.org (last visited Oct. 13, 2018).

[62] Visit https://www.bitaddress.org/, and select "Wallet Details." Enter the private key where specified and select "View Details."

later and is also safe to share).[63] The lower half of the card, however, must be kept private; it contains your private key in a variety of formats (including the sixteen-character format illustrated above).[64]

We now have a Bitcoin address (18BjkQ . . .), which serves as your public identity.[65] We can think of it as your username or as an entity that you control. We also have a private key (ABCDEF0123 . . .). We can think of it as a password or the mechanism of controlling your "entity." These are perfectly valid credentials that you could (but should not) use to receive Bitcoin. Note that you cannot choose your Bitcoin address directly (the way you would a username). You choose your private key (by a random process if you want it to be safe), and this private key determines your Bitcoin address.

E. *Decentralized Identity Management*

Writers routinely describe Bitcoin as "decentralized,"[66] which perfectly describes the process of creating your credentials. We did not go through any institution. We did not register these credentials, nor is there any way to do so. We simply generate credentials on our own and use them. While we

63 *See infra* Part IV.B.3.

64 It is the private key hexadecimal format. It contains sixty-four characters, drawn from zero to nine and A to F.

65 *See* NARAYANAN ET AL., *supra* note 13, at 18–20 (describing Bitcoin addresses as identities).

66 *See generally* Allen, *supra* note 21, at 883; Tu & Meredith, *supra* note 21, at 272 (2015) ("decentralized virtual currencies").

did use a website, it was to perform mathematical calculations and format the credentials in an attractive way.

In practice, computerized processes replace the cumbersome process previously suggested for generating private keys (i.e., rolling a sixteen-sided die sixty-four times). The computer can generate several private keys (and thus Bitcoin addresses) very quickly. A single user can thus assume several different identities in the Bitcoin system. Indeed, many in the Bitcoin community strongly encourage users to generate a new Bitcoin address every time they receive a new transfer of Bitcoin.[67]

Thinking of legal analogies, a Bitcoin address (18BjkQ . . .) could be compared to a very simple corporation. Its primary activities are receiving and transferring units of Bitcoin; these activities are defined by the Bitcoin system and not by the sovereign. Control of this "corporation" goes to whomever possesses the private key (ABCDEF0123 . . .). Relatedly, the Bitcoin system does not recognize humans, corporations, or other legal actors. It only recognizes Bitcoin addresses, which legal actors control via associated private keys.

Readers familiar with several hacks of Bitcoin exchanges[68] may question the inherent security of Bitcoin. Bitcoin is only as secure as its users' private keys. As discussed earlier, private keys must be random[69] in order to be safe. Users must also store their private keys securely. If a thief guesses or steals a private key, the thief can steal any associated Bitcoin. Transactions are irreversible, and the victims of Bitcoin theft may have no way to recover their losses.

Finally, since Bitcoin is decentralized, users who lose their private keys have no way to recover or reset them. Stories abound of early Bitcoin enthusiasts who mined Bitcoin (say in 2009 or 2010), lost interest in the endeavor (say in 2011), and could not recover their discarded or forgotten private keys when the price of Bitcoin skyrocketed. Perhaps the most famous example is of James Howells, a British IT worker who mined 7,500 BTC during Bitcoin's early days.[70] In 2013, he discarded his hard drive that contained his private keys. He believes that the hard drive currently rests in a Welsh landfill, which, at current Bitcoin prices, holds a treasure worth over $75 million. Without a central authority, Mr. Howells has no way to reset

---

67 *See, e.g.*, ANTONOPOULOS, *supra* note 39, at 94.

68 *See, e.g.*, Abramowicz, *supra* note 20, at 411 n.253 (discussing failure of Mt. Gox).

69 The vast majority of users will use computerized processes to create pseudo-random passwords. Some (but not all) such processes are considered secure and appropriate for use with Bitcoin. *See* ANTONOPOULOS, *supra* note 39, at 59.

70 Aatif Sulleyman, *Man Who 'Threw Away' Bitcoin Haul Now Worth Over $80M Wants to Dig Up Landfill Site*, INDEPDENENT (Dec. 4, 2017), http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-value-james-howells-newport-landfill-hard-drive-campbell-simpson-laszlo-hanyecz-a8091371.html.

or retrieve his "password." The only way for Mr. Howells to recover his lost Bitcoin is to recover the physical hard drive from the landfill.

IV. A SIMPLE BITCOIN DEED

A. *Without Digital Signature*

The credentials we just generated are perfectly valid in the Bitcoin system, and could be used to receive Bitcoin. As we consider other aspects of the Bitcoin system, we will start simplifying our descriptions. If your uncle wants to send you Bitcoin, he certainly would send you a text file to do so. The text file would be formatted for the computer to understand, not necessarily human readers. And, it may contain information extraneous to our purposes. So, for sake of presentation, we will dramatically simplify the information that Bitcoin transactions contain.[71] When your uncle received his Bitcoin, he generated a Bitcoin address. Let us assume it is: 1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX.[72] If your uncle had a nifty card with QR codes, etc., it would look like the following:[73]

Bitcoin Address

1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX

Bitcoin Address Compressed

1M8Qk46ERsPrEtWLBRSET5NUH2Ck5wwREU

Public Key (130 characters [0-9A-F]):
044646AE5047316B4230D0086C8ACEC687F00B1CD9D1DC634F6CB358AC0A9A8FF
FFE77B4DD0A4BFB95851F3B7355C781DD60F8418FC8A65D14907AFF47C903A559

Public Key (compressed, 66 characters [0-9A-F]):
034646AE5047316B4230D0086C8ACEC687F00B1CD9D1DC634F6CB358AC0A9A8FFF

We should assume that your uncle generated his own private key, which we have no business seeing as part of the transaction.[74] Initially, we might represent our Bitcoin deed as a text file that says the following:

---

[71] Readers with some computer science background may be familiar with the concept of "pseudocode," which is a representation of a program presented for human comprehension. *See Pseudocode*, WIKIPEDIA, https://en.wikipedia.org/wiki/Pseudocode (lasted visited Mar. 1, 2018).

[72] The Bitcoin address is valid. The generating private key is similar to the one we use for our own. It is
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF.

[73] This was generated using bitaddress.org. *See supra* note 62 for details.

[74] For purposes of presentation, I will need to use your uncle's private key in order to

1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX
gives 50 BTC to
18BjkQhqFsCy1ryFwpYjPLgZLWGZ5zTnsJ

We can paraphrase that text as:

[Uncle's Bitcoin Address]
gives 50 BTC to
[Your Bitcoin Address]

But, anyone could write this statement and pass it off as your uncle's. It contains your uncle's Bitcoin address, your Bitcoin address, and the amount of the transaction. For all we know, you are simply trying to steal from your poor uncle!

B. *With Digital Signature*

1. Example of a Signed Bitcoin Deed

In order to prevent similar frauds, the law requires transferors to sign and sometimes notarize written instruments.[75] Real estate deeds are signed and acknowledged (generally before a notary public).[76] Bitcoin relies on cryptographic functions known as digital signatures that replace handwritten signatures and acknowledgments.[77] Your uncle, as grantor, is the one who needs to execute a digital signature. Let us now consider a Bitcoin deed that contains a digital signature:

1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX
gives 50 BTC to
18BjkQhqFsCy1ryFwpYjPLgZLWGZ5zTnsJ
Public Key:
044646AE5047316B4230D0086C8ACEC687F00B1CD9D1DC
634F6CB358AC0A9A8FFFFE77B4DD0A4BFB95851F3B7355
C781DD60F8418FC8A65D14907AFF47C903A559
Digital Signature:
3044022064e08626b4fb5613647e1b65ff690f015226b3b04877f9
21e0bf3e005231d1540220778ff1321d0d8c00117e61b154aec1e5
a435e8830ef3a7d3d8ec48d70bce51e9

This surely reads like gibberish. Let us paraphrase it a bit:

[Uncle's Bitcoin Address]
gives 50 BTC to
[Your Bitcoin Address]
Public Key:

generate a digital signature. You, however, will not need access to the private key in order to *confirm* the digital signature I generate.

[75] *See supra* note 50 and accompanying text.

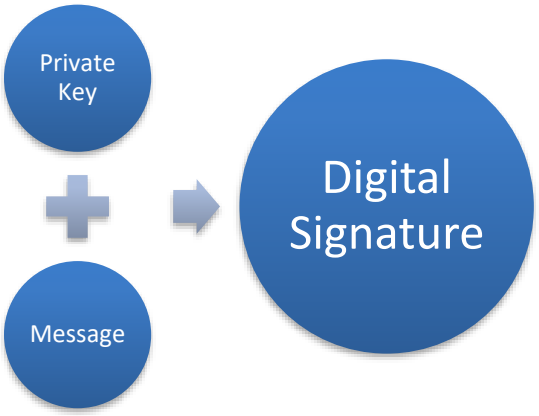
[76] *See supra* note 50 and accompanying text.

[77] *See* Lee, *supra* note 6, at 98.

> [An alphanumeric sequence associated with Uncle's Bitcoin Address that is used to verify the Digital Signature below.]
> Digital Signature:
> [A unique alphanumeric sequence that can be generated only by using the message and Uncle's private key. Even though the private key was used to generate the Digital Signature, cryptographic functions can verify the Digital Signature without accessing the private key.]

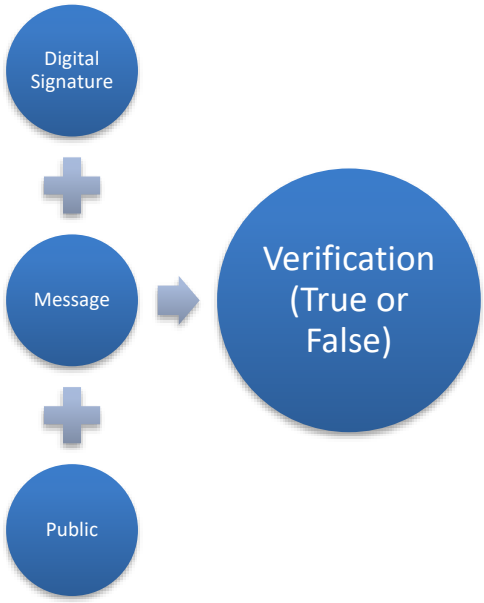
2. Generating Versus Verifying the Digital Signature

This version of the Bitcoin deed lets any observer verify that your uncle (or someone possessing your uncle's private key) executed a digital signature. We must clearly distinguish between the process by which your uncle generates the digital signature and the process by which an observer verifies the digital signature. To generate a valid digital signature, your uncle must have access to his private key.



To *verify* a digital signature, an observer must have access to your uncle's "public key,"[78] a concept we have not yet discussed much.

[78] *See* ANTONOPOULOS, *supra* note 39, at 141.



3. Role of the "Public Key"

The private key, public key, and Bitcoin address are closely related. The private key produces both the public key and the Bitcoin address in what this Article has previously referred to as a "one-way" function.[79] Given the private key, we can easily produce the public key and Bitcoin address. But, given only a public key and/or Bitcoin address, we cannot reverse engineer the process to identify the private key.

Because of the vagaries of the Bitcoin system, our Bitcoin deed must list both the Bitcoin address of the transferor (which identifies the transferor) and the public key of the transferor (which allows observers to verify the digital signature).

[79] *See supra* Part III.C.

4. Verification Process

Let us return to your uncle's signed "Bitcoin deed." Our verification process would look something like this:

1. Confirm that the public key is associated with the Bitcoin address of the transferor.[80] This can be done mathematically and almost instantaneously. You can confirm my example by noting that the graphic with the QR codes for your uncle contains the Bitcoin address and public key used in the sample "Bitcoin deed."
2. Verify the digital signature using the message and the public key. This step is also done mathematically.[81]

We confirm that your uncle generated the digital signature using his private key and the message (i.e., that he is giving you 50 BTC). If he generated a different message (e.g., "sorry, no Bitcoin for you"), the digital signature would be different. So, one cannot "forge" a Bitcoin deed by copying the digital signature from one message and affixing it to another document. The digital signature is a function of both the private key and the signed message.

V. COMPETING DEEDS AND THE CHALLENGE OF DECENTRALIZED RECORDATION

A. *Introduction*

With your uncle's Bitcoin deed in hand (or on a hard drive), you can seemingly establish ownership of 50 BTC. So long as your uncle owned 50 BTC, you can claim to own them now. Suppose that your uncle was an early Bitcoin "miner"[82] and can establish that he earned 50 BTC with a successful mining effort in 2012. Perhaps he can even produce a Bitcoin deed to show that he received 50 BTC in 2012. Are you not the rightful owner now?

If Bitcoin was simply an ad hoc collection of Bitcoin deeds, you would have difficulty establishing ownership. It is true that you can prove that your uncle made a Bitcoin deed in favor of you. Perhaps you can prove that your

[80] Technically speaking, the Bitcoin address is derived from the public key. *See supra* Part IV.B.3.

[81] Readers wishing to verify the Bitcoin deed can do so at the following website: https://kjur.github.io/jsrsasign/sample/sample-ecdsa.html. For ECC curve name, select secp256k1. Bitcoin uses this for its cryptography. Do not generate an EC key pair, and leave the EC private key (hex) blank. For the EC public key (hex), input the public key from the Bitcoin deed. It is in the correct "hex" format. For the signature algorithm, leave the setting at SHA256withECDSA. To sign the message string, use "1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX gives 50 BTC to 18BjkQhqFsCy1ryFwpYjPLgZLWGZ5zTnsJ," but omit the quotation marks. For the signature value (hex), use the digital signature value from the Bitcoin deed. It is in the correct "hex" format. Click "verify it!," and you should get a message saying "valid ECDSA signature."

[82] *See generally infra* Part V.C.

uncle at one time owned those 50 BTC. If Bitcoin is just a jumble of ad hoc transfers, however, how do you prove that your uncle never made a Bitcoin deed conveying the same 50 BTC to someone else? You could not prove this negative fact unless you had a complete record of all Bitcoin transfers.

If your uncle gave you Blackacre, he would do so by written deed, which you would take to the public records office for recordation. Recording the Blackacre deed protects you in case your uncle attempts to transfer Blackacre to a subsequent grantee. Recording the deed also allows you to establish marketable title,[83] making it easier for you to sell Blackacre at some future time. Similarly, you could examine recorded deeds at the public records office to learn if your uncle ever made a deed conveying Blackacre to someone else. Recordation helps grantees prove a negative; namely, that the grantor never previously transferred the interest to someone else.

While Bitcoin has instruments that this Article has referred to as "deeds,"[84] it has no central repository for recording them. Instead, Bitcoin creates a system by which users reach a consensus about what should go into the central repository. At first, this may sound like an impossible task, but let us consider what might happen with your Bitcoin deed. After receiving it, you could simply communicate it to other users you know. The Bitcoin system actually facilitates such communications. Other users on the system might then share the news of your uncle's 50 BTC transfer with other users they know. News of the 50 BTC transfer could then propagate throughout the system until all users know that you, and not your uncle, now own the 50 BTC.

Simply allowing Bitcoin deeds to propagate throughout the community of users is a good start to reaching consensus about ownership. Suppose, however, that your uncle transferred the same 50 BTC interest to another niece or nephew twelve hours after making the transfer to you. Your cousin immediately starts propagating her competing Bitcoin deed throughout the system. Because of lags (or latency) in the network, some users might hear about your cousin's competing deed before they hear about yours, even though yours was first in time. And, without a central authority to time-stamp deeds, there may appear to be no automatic way to prove that your deed was first in time.

Satoshi Nakamoto was acutely aware of this problem. He understood that owners could not be allowed to doublespend Bitcoin.[85] If users could spend a single bitcoin several times, then Bitcoin would no longer be scarce[86] and would become worthless. Satoshi Nakamoto realized that Bitcoin

83 *See* MALLOY & SMITH, *supra* note 29, at 209–11.

84 *See supra* Part II.A.

85 *See* Nakamoto, *supra* note 2, at 2.

86 *See supra* Part II.B.

needed some party to time-stamp Bitcoin deeds, but his vision called for decentralization.

His solution was "mining" and the "blockchain." They are perhaps the least intuitive aspects of Bitcoin, but they are arguably its most important and innovative. We will return to mining and the blockchain in more detail. To preview, mining is the process by which transactions are confirmed or time-stamped, and the blockchain is the collection of all previously confirmed (time-stamped) transactions. We might compare the blockchain to the public records office, a place where you go to view the history of transactions. Similarly, we might compare mining to recordation, the process by which executed deeds are recorded in a public records office. To understand mining and the blockchain more fully, we will have to understand something called cryptographic hash functions.

B. *An Aside on Cryptographic Hash Functions*

1. Digital Fingerprint of a Document

"Cryptographic hash functions" may sound threatening and daunting. Readers may be tempted to skip this Part because of its title; however, cryptographic hash functions are an essential part of the Bitcoin consensus model, and we can understand much of their usefulness by comparison with issues that might arise in drafting a will. Suppose that Satoshi Nakamoto wants to write a will that leaves his entire estate to Alice. Satoshi goes to his lawyer, who has him execute the following document:

> I, Satoshi Nakamoto, do hereby devise my entire estate to Alice.[87]

Satoshi worries that someone will alter his will. Maybe Bob would take Satoshi's estate in intestacy (i.e., in the absence of a will), and Satoshi is worried that Bob will sneak into the lawyer's office and tamper with the will. Satoshi could post a copy of this will to an internet forum, but he wants it to remain confidential until he dies. Satoshi instead decides to post a "cryptographic hash" of his will to an internet forum. Before we describe "cryptographic hash," let us just see what it is in this case:

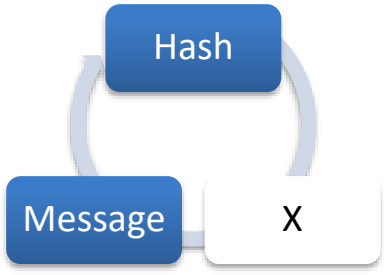
> a4dc8d1f0ccc56609158578b1def4e45f0ff9581368b70a7604ffd7 a4e2707bc.[88]

---

[87] If witnessed and executed properly, this would be a perfectly valid will. Calvin Coolidge executed a will almost as succinct: "Not unmindful of my son John, I give all my estate[,] both real and personal[,] to my wife[,] Grace Coolidge, in fee simple." Jonathan Turley, *Presidential Papers and Popular Government: The Convergence of Constitutional and Property Theory in Claims of Ownership and Control of Presidential Records*, 88 CORNELL L. REV. 651, 659 n.32 (2003).

[88] There are many cryptographic hash functions. In this example, I used the SHA 256 hash, the same function that Bitcoin actually uses. *See* NARAYANAN ET AL., *supra* note 13, at 9–10 (identifying SHA 256 as the standard Bitcoin hash function).

We can interpret the cryptographic hash as a digital fingerprint of the will (or of any message). Cryptographic hash functions are one-way streets. We can readily convert any message into its hash, but we cannot take the hash and convert it into the message.



2. Obscuring the Document Contents with a "Nonce"

Since Satoshi has such a simple will, observers might successfully guess its contents by trial and error. Someone might guess that the will leaves everything to one of three likely beneficiaries (e.g., Alice, Bob, or Chelsea), and might also guess the format of the will. The observer could then test a mere three possible wills before learning that everything goes to Alice. Satoshi could guard against this attack by adding a random number to the will. This random number, called a "nonce," has no inherent meaning; it only serves to make the trial and error attack much more difficult.[89]

Suppose that Satoshi selects a random number between 1 and 1,000,000 and appends it to his will as a nonce. Further, suppose that the observer knows that Satoshi attached a nonce of this size, but the observer does not know the actual nonce. With this nonce (which we can think of as a "tweak"), the observer's task has become much more difficult. Instead of having to do three trial-and-error tests, the observer must do up to 3,000,000[90] calculations. To keep the presentation clean, I will not include a nonce in Satoshi's will; however, it will play an important role in Bitcoin mining, as described later in this Article.[91]

Let us return to Satoshi, who has executed his will and publicized its hash. Upon Satoshi's death, his lawyer could reveal the will ("I, Satoshi Nakamoto, do hereby devise my entire estate to Alice.") and allow observers

[89] Wulf A. Kaal & Craig Calcaterra, *Crypto Transaction Dispute Resolution*, 73 BUS. LAW. 109, 123 (2018).

[90] There are three possible beneficiaries and 1,000,000 possible nonces. Still, three million calculations would be easy for a modern computer. Satoshi might more realistically select a much larger nonce with size comparable to the SHA 256 hash: 2^{256} or roughly 1.16×10^{77}.

[91] *See infra* Part V.D.3.

to confirm that it produces the hash that Satoshi himself previously publicized ("a4dc8d1f0ccc56 . . ."). If Bob tries to tamper with the will, the tampered document will produce a different hash from what Satoshi publicized.[92] Thus, the hash function allows Satoshi to make a public commitment (leaving his estate to Alice) without revealing the details of the commitment immediately.

3. Using Hashes to Specify the Order of Documents

The hash function can also be used to specify the intended order of a series of documents. Suppose that Satoshi is again working on his estate plan. He executes three documents that can be classified as wills or codicils, depending upon the order of execution. The true order is given below:

Document #0
I, Satoshi Nakamoto, do hereby devise my entire estate to Alice.
Document #1
I, Satoshi Nakamoto, do hereby devise Blackacre to Bob.
Document #2
I, Satoshi Nakamoto, do hereby devise Blackacre to Chelsea.

The standard way to interpret these documents, if executed in this order, would be to have Blackacre go to Chelsea, have nothing go to Bob, and have the remainder of Satoshi's estate go to Alice, but the order of execution matters.[93] If Document #1 was executed last, Bob (not Chelsea) would take Blackacre. If Document #0 was executed last, Alice would take Satoshi's entire estate (including Blackacre).[94]

Since the order matters, Satoshi worries that he cannot simply publish each will's hash. Satoshi, however, can use hash functions not only to prevent someone from tampering with the content, but also to prevent someone from tampering with the order of execution. Every time Satoshi executes a new document, he can assure it is the correct order by including a hash of the document that precedes the newly executed one. In the following example, Document #0 is the "genesis" will and refers to no prior document. Satoshi would then execute the following documents:

---

[92] The SHA 256 hash of "I, Satoshi Nakamoto, do hereby devise my entire estate to Bob" would be 0a07397c4946bf669547f88fad2b03e05f8fd6ddbfe0d54b4f9cd114cf8ecafe.

[93] Clearly, Chelsea takes Blackacre. The Uniform Probate Code creates a presumption that Document #1 and #2 supplement #0. *See* UNIF. PROB. CODE § 2-507(d) (amended 2010) ("The testator is presumed to have intended a subsequent will to supplement rather than replace a previous will if the subsequent will does not make a complete disposition of the testator's estate.").

[94] *See id.* § 2-507(c) ("The testator is presumed to have intended a subsequent will to replace rather than supplement a previous will if the subsequent will makes a complete disposition of the testator's estate.").

Document #0
I, Satoshi Nakamoto, do hereby devise my entire estate to Alice.

Document #1
I, Satoshi Nakamoto, do hereby devise Blackacre to Bob.
Hash of prior document:
a4dc8d1f0ccc56609158578b1def4e45f0ff9581368b70a7604ffd7
a4e2707bc[95]

Document #2
I, Satoshi Nakamoto, do hereby devise Blackacre to Chelsea.
Hash of prior document:
9782f09423b518ec2b7ee31c16faafbcff00b5878db52f291f67c7c
00d6212dd[96]

4. The Importance of the Last Message

Surprisingly, Satoshi does not need to publicize the hash of all the documents. He achieves his goal so long as he publicizes the hash of the last document. Let us see why:

- Satoshi publicizes the hash of document #2.
- Upon Satoshi's death, his lawyer reveals the contents of this document. Observers confirm that document #2's hash matches what Satoshi publicized during his lifetime. The revealed document leaves Blackacre to Chelsea, and it includes the hash of a prior document (document #1).
- The lawyer reveals document #1. Observers confirm that its hash matches what is reported in document #2. The document leaves Blackacre to Bob, and it includes a hash of a prior document (document #0).
- The lawyer reveals document #0. Observers confirm that its hash matches what is reported in document #1. The document leaves the entire estate to Alice. It does not include a hash to a prior document and so the process ends.

To summarize, cryptographic hash functions can be used to prevent tampering of both the contents and order of documents. Later, we will see how the Bitcoin system uses hash functions to create the "blockchain." The blockchain collects groups of transactions into so-called "blocks." Each block is linked to its immediately prior block using hash functions. By doing

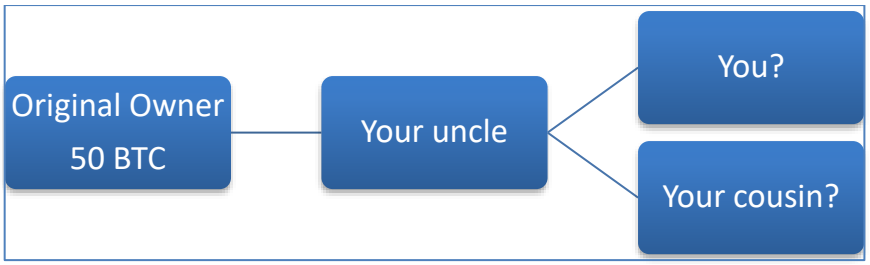
[95] *See supra* note 88 and accompanying text.

[96] hashlib.sha256 ("I, Satoshi Nakamoto, do hereby devise Blackacre to Bob. Hash of prior document: a4dc8d1f0ccc56609158578b1def4e45f0ff9581368b70a7604ffd7a4e2707 bc").hexdigest(). As a typographical convention, I do not include any returns in the message.

this, the Bitcoin system allows users to create records of all Bitcoin transactions about which the community may reach a consensus.

C. *Title Assurance and Bitcoin Mining*

This Article earlier addressed how the Bitcoin system prevents forgery of Bitcoin deeds by requiring digital signatures, but forgery is not the only type of fraud that could cause Bitcoin to collapse. The formal system described so far misses title assurance, an important element covered in first-year property.[97] Recall that earlier in this Article your uncle wanted to transfer 50 BTC to you. You (or your software) establishes that your uncle executed a formally correct Bitcoin deed. The deed bears a valid digital signature, and your uncle's Bitcoin address previously received a transfer of 50 BTC. Suppose that you learn that your uncle has another favorite niece or nephew, for which he has executed a Bitcoin deed for the same 50 BTC. They are the same 50 BTC because both they both refer back to the same original owner.



Readers may recall the problems of title assurance and competing deeds from first-year property law. Indeed, title assurance "might be considered the central issue in the transfer of real estate."[98] Under American law, states have three main systems (race, notice, and race-notice) for determining which competing deed is valid.[99] Given the computational nature of Bitcoin, we should expect a simpler system, one that does not factor in human knowledge (such as notice) or status (such as bona-fide purchaser status). A simple approach would be to give the 50 BTC to you or your cousin depending on whose interest was first in time.

Central administration would solve the problem of competing deeds. The central administrator could just honor the transfer (yours or your cousin's) that it first learns about. We cannot, however, explore that path. The whole reason Satoshi Nakamoto created Bitcoin was to have a

97 *See* DUKEMINIER ET AL., *supra* note 14, at 693–776.

98 GRANT S. NELSON ET AL., REAL ESTATE TRANSFER, FINANCE, AND DEVELOPMENT: CASES AND MATERIALS 222 (9th ed. 2015).

99 *See* MALLOY & SMITH, *supra* note 29, at 266–68.

decentralized currency. The community of Bitcoin users, as a whole, needs to determine which deed (the one to you or to your cousin) is the valid one.

If the Bitcoin deeds were not close in time, the community might be able to recognize and honor the earlier one. But, let us assume that your uncle sends separate deeds of the same interest to you and your cousin at roughly the same time. Since there is no central administration, there is no way to time-stamp the two deeds by computer protocol.[100] Some users will hear about yours first, while others will hear about your cousin's first.

Without an effective way to choose between competing deeds, Bitcoin would collapse. It is not too far-fetched to imagine that a party would want to destroy Bitcoin. Such a party could buy some bitcoin and then attempt to make hundreds of transfers of the same interest to different parties. The "different parties" could even be different Bitcoin addresses controlled by this party. The community cannot honor all of the deeds. If it did, then the adversary could explode the supply of Bitcoin by transferring the same interest to itself via thousands or even millions of separate transactions. To work, Bitcoin must remain scarce.[101] If a user could repeatedly spend the same bitcoin, then Bitcoin would become worthless.

Two principles seem in conflict. The Bitcoin system needs some party to act like a court clerk, applying a time-stamp to validate or confirm deeds. The founding principle of Bitcoin, however, is decentralization; no user or group of users can have special administrative privileges. Possession of the time-stamp gives the user significant power. Suppose I held it. I might have enemies in the Bitcoin community and may simply refuse to time-stamp their deeds. Or I might find this role boring and unrewarding, and therefore neglect it. Or the government might take notice of my power and regulate it (via its jurisdiction over me) in a way that the community dislikes.[102]

D. *Proof of Work and the Time-stamp Function*

1. Introduction

Bitcoin solves this problem with clever social engineering. Rather than assign the time-stamp function randomly, it lets interested users compete for the right to use it. In order to use the time-stamp function, Bitcoin users must first solve a boring mathematical puzzle (essentially guessing a correct random number). By design, the puzzle has a similar difficulty for each contestant (my puzzle is just as hard as yours), but the answer for each

---

[100] Satoshi Nakamoto does speak of timestamping Bitcoin transactions. *See* Nakamoto, *supra* note 2, at 2–3. In reality, the actual time does not matter. What matters to Bitcoin is the order of transactions. *See* NARAYANAN ET AL., *supra* note 13, at xxii ("[T]imestamps aren't of much importance in Bitcoin, and the point of the system is to record the relative ordering of transactions in a tamper-resistant way.").

[101] *See supra* Part II.B.

[102] *See* Litwack *supra* note 7, at 314 (noting the appeal of Bitcoin to libertarians).

contestant is unique (my answer is different from yours). For better or worse, the Bitcoin community refers to contestants as "miners" and refers to the process of confirming (or time-stamping) transactions as "mining," because winners receive a prize of a newly issued Bitcoin.

Solving the puzzle allows the miner to create a "block" of transactions not recorded in an earlier block. Each new block contains a cryptographic link to the immediately preceding block. Thus, all blocks are linked together in a "blockchain." The blockchain thus extends backwards from the most recently mined block all the way to the first "genesis block" created by Satoshi Nakamoto in early 2009.[103]

2. The Problem of Randomly Allocating the Time-stamp Function

Recall the earlier hypothetical in which your uncle purports to convey the same 50 BTC to both you and your cousin. A miner could not confirm both transactions in the same block, as the Bitcoin system would reject such a block as invalid. Suppose a miner includes your transfer, but not your cousin's transfer, in a newly created block. Since the blockchain now has your transaction in it, a later block cannot include the transfer to your cousin. You have won and, according to the blockchain, you are the owner of the 50 BTC. In contrast, if miners systematically refuse to validate any transaction, neither you nor your cousin will ever receive any confirmation of the transaction. Or, miners might target you over some grievance and refuse to confirm any transactions involving you. In short, the miners' task is fairly simple: to time-stamp transactions for inclusion in the blockchain. As we have just seen, however, the time-stamp power can be abused.

Random, periodic assignment of the time-stamp power amongst all Bitcoin users might sound appealing. Wielding the time-stamp would require some computing resources; the user would need to collect unconfirmed transactions and organize them for confirmation. Ordinary Bitcoin users (e.g., you with your 50 BTC) might not want to maintain those resources. Users who do want the time-stamp function, however, might be motivated by a desire to destabilize the Bitcoin system (e.g., by refusing to time-stamp any transactions at all or by refusing to time-stamp the transactions of enemies).

Suppose that Bitcoin would assign the time-stamp function randomly among only those users who express some interest in having it. Users would simply put their identities in a pool of applicants and await random selection. Suppose that there are ninety honest and ten dishonest "real world" actors (human beings, corporations, etc.) that want to use the time-stamp function.

---

[103] To review Block #0, please visit BLOCKCHAIN.COM, https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (last visited Mar. 1, 2018).

The honest actors would simply confirm transactions in the order in which they learned of them (as we would expect a court clerk to do). The dishonest actors would refuse to confirm any transactions at all, or would selectively confirm transactions in the hopes of destabilizing the Bitcoin system. Based on the number of real world actors, we should expect honest users to control the time-stamp function 90% of the time. The dishonest actors could do no real harm to the system, because their refusal to confirm transactions merely delays confirmation until an honest actor has its turn.

Bitcoin relies on virtual identities (alphanumeric addresses) rather than legal names. Creating virtual Bitcoin identities is costless, and the ten dishonest actors might flood the selection pool with multiple identities (perhaps eighty-one each).[104] If the honest users do not respond, there may be 90 honest and 810 dishonest identities in the pool. Based on these numbers, we expect dishonest users to control the time-stamp 90% of the time. This level of control would probably destabilize the Bitcoin system.[105]

3. Proof of Work and the Mining Puzzle

Satoshi Nakamoto solved this problem with the "proof of work" concept.[106] The Bitcoin system establishes a task that is difficult to perform but, once performed, is easy to confirm. Proof of work may be compared to the heroic deeds of medieval knights looking to impress their ladies.[107] The knight might undertake some arduous and dangerous task merely to prove his devotion. We might imagine the following dialogue:

> Sir Everbrave: My lady, you are all that is pure and true. Would you honor me by tying one of your kerchiefs on my shield?
> Lady Pureheart: Hah! Words are cheap. Climb Mt. Dragondeath and bring me some toenail clippings from the death dragon who resides there. Only then will I let you have one of my kerchiefs.

The Bitcoin variant would be something like:

> User 1CLrr . . . : Fellow Bitcoin users, I would really like to have the power to confirm transactions over the next 10 minutes.
> Bitcoin Community: Hah! Words are cheap. Take your original message and tweak it with a nonce until the SHA-256 hash of the tweaked message has 10 leading zeros.[108] Only then will I let you

---

104 *See* Nakamoto, *supra* note 2, at 3 ("If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs.").

105 *See generally* NARAYANAN ET AL., *supra* note 13, at 48–50 (discussing attacks possible with 51% control).

106 *See* Nakamoto, *supra* note 2, at 3 (describing proof of work concept).

107 *See Knight-errant*, WIKIPEDIA, https://en.wikipedia.org/wiki/Knight-errant#Romance (last visited Mar. 1, 2018) ("A knight-errant typically performed all his deeds in the name of a lady, and invoked her name before performing an exploit.").

108 Ten leading zeros is a simplification of the puzzle. Successful hashes will indeed have several leading zeros. Strictly speaking, the successful hash must be lower than some

have the time-stamp.

The "SHA-256 hash" used in the task is a cryptographic algorithm that creates a digital fingerprint of any text. We have already seen it at work when considering Satoshi Nakamoto's last will and testament.[109] Take any text as input, and the SHA-256 algorithm produces what we might call a digital fingerprint[110] of the text.

> Text:
> Please give me the time-stamp for the next 10 minutes. 1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX 2/22/18 12:43:52 PM
> SHA-256 Hash:
> ac0bbb32396c2ffa78fefc2c7b7db242f82c8b7d21ddc776df9099754725cb25

Generating the hash is computationally simple. But, to qualify as a time-stamper, the contestant must generate a hash with a special characteristic; it must have several leading zeros. The hash of our actual message has no leading zeros (as it starts with an "a"). Fortunately, we can keep trying to generate leading zeros by "tweaking" the message with a nonce. The nonce has no informational content; it simply alters the hash of our message. We will try a tweak (nonce) of "1":

> Text:
> Please give me the time-stamp for the next 10 minutes. 1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX 2/22/18 12:43:52 PM Tweak = 1
> SHA-256 Hash:
> 664f54dcae70c896d403df99e9b0adfa969a46b057faf22f6de28732e0941d3b

Again, no luck getting even a single leading zero. The rules of the contest, however, let us use any tweak that we want. So, we can keep trying until we succeed.

What makes this task difficult is that the hash output is seemingly random. The only known way to generate a hash with a single leading zero is by trial and error. As there are sixteen possible characters, we have a one-in-sixteen chance of getting a single leading zero. After checking sixty-two possible tweaks, my computer found one that generates a single leading zero:

> Text:
> Please give me the time-stamp for the next 10 minutes. 1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX 2/22/18 12:43:52 PM Tweak = 62

specified target hash, and the target hash changes over time. ANTONOPOULOS, *supra* note 39, at 235–37.

109 *See supra* Part V.B.1.

110 *See supra* Part V.B.1.

SHA-256 Hash:
0c9b492a8cbe10b45c44caba79c3cc7ca296ff6882f9c30e12f3769
f13e17471

Generating five leading zeros requires almost 2.7 million searches:

Text:
Please give me the time-stamp for the next 10 minutes. 1CLrrRUwXswyF2EVAtuXyqdk4qb8DSUHCX 2/22/18 12:43:52 PM Tweak = 2739639
SHA-256 Hash:
0000079fefdafb0c93058976ff600fc0e0e5539cda1c0797c90e7db
c736ef02d

Generating ten leading zeros (as required by the example) would take a lot of time or computing power. Since each leading zero is a one-in-sixteen chance, finding the tweak that generates ten leading zeros is roughly a one in a trillion shot.[111] In other words, it is possible for a computer to find the qualifying tweak, but it will need to test a lot of numbers, roughly one trillion, before we can expect to stop.

The little contest described above is actually quite close to what Bitcoin uses as its mining puzzle. Miners select a nonce (a tweak) that they use to generate a hash with a certain number of leading zeros.[112] In the real-world Bitcoin context, the first miner to solve the puzzle is recognized as the winner. The winning miner will then add a new block to the blockchain. The new block contains valid transactions that have not previously been confirmed. For example, the new block might contain the 50 BTC from your uncle to you. By confirming this transaction, the miner is in effect time-stamping. Later, if your uncle tries to transfer the same 50 BTC to your cousin, his attempt will fail because the transfer to you is already on the blockchain.

Let us return to our initial concern, namely that dishonest users might control the time-stamp function and destabilize Bitcoin. Initially, we thought that awarding the time-stamp randomly would work. Dishonest users, however, might simply create multiple Bitcoin identities in order to swamp the system and control the time-stamp. Bitcoin mining does not award the time-stamp to users on a per identity basis. Rather, it forces users to compete on the basis of computing power and energy consumption.

Why should this competition help ensure honesty? If every actual user had the same computer and internet access, then the mining contest would indeed allocate the time-stamp randomly among actual users (or at least

---

111 16^10 = 1,099,511,627,776.

112 More preciously, the hash must be less than a certain number called the hash target. *See* NARAYANAN ET AL., *supra* note 13, at 106. The method of representation results in several leading zeros for a qualifying hash. For an example of leading zeros, note that 00072 is a way of writing "seventy-two." Writing it this way makes sense if possible values could be up to 99999 (e.g., 00001 to 99999).

among actual users who bothered to enter the contest). Multiple identities under common control would not help anyone win the contest because computing power would need to be allocated among the multiple identities. If computing power is distributed evenly across users, then the mining contest ensures the "ordinariness" of the users who control the time-stamp. The contest does not, strictly speaking, measure anyone's good or bad intentions.

4. Mining and the Coinbase Transaction

Over time, Bitcoin mining has evolved dramatically. In the early days of Bitcoin, hobbyists on their laptops could reasonably expect a periodic prize (called the "coinbase transaction") of 50 BTC for playing along with a quirky internet creation. Today, the prize is only 12.5 BTC, but the economic value is far higher, with Bitcoin prices over $10,000 in early 2018. Mining has become more commercialized and specialized. Successful miners do not use ordinary computers. They buy specialized machines built for the sole purpose of Bitcoin mining. The machines require energy to run and need to be kept cool. Thus, geography plays an important role in Bitcoin mining. Locations with cold environments, cheap energy, and good internet access are the best.[113]

With this evolution, the mining process actually measures the level of investment in Bitcoin mining. Miners with the fastest computers, the cheapest source of powering them, and the cheapest method of cooling them, will win. With the level of investment required to mine successfully, we might even conclude that miners will find it in their economic interest to see Bitcoin thrive. The payment to miners comes in the form of Bitcoin; miners who destabilize the system would cause themselves significant economic losses.

As we have seen, in addition to confirming (time-stamping) transactions, the winning miner also receives a reward of Bitcoin. Currently, this reward is 12.5 BTC. As of mid-February 2018, this reward translates into almost $140,000. The reward (called the coinbase transaction) creates new bitcoin. In addition to coinbase transactions, successful miners also earn transaction fees that users voluntarily designate for miners. Transaction fees are a much smaller portion of the miners return, worth perhaps 0.2 BTC per block in mid-February 2018.

Periodically, the reward is cut in half. It started at 50 BTC when Bitcoin began in January 2009. The reward fell to 25 BTC in November 2012 and fell again to 12.5 BTC in July 2016. In mid-2020, the reward will fall again

[113] *See, e.g.*, Jacques Marcoux, *Cheap Electricity, Cold Weather Provide 'Huge Marketing Opportunity' for Manitoba to Attract Bitcoin 'Miners'*, CBC (Dec. 20, 2017, 5:00 AM), http://www.cbc.ca/news/canada/manitoba/manitoba-bitcoin-1.4457486.

to 6.75 BTC.[114] At some point, the reward will be eliminated, and miners will rely solely on transaction fees for the return on their investment. Presently, the payment to miners is currently borne by all Bitcoin owners because the expansion of supply dilutes their ownership. In the future, payment to miners will be borne increasingly by parties to Bitcoin transactions.

Mining is the most important innovation of Bitcoin and allows it to function without reliance on the law, the government, or any central institution. It is not far-fetched to say that Bitcoin mining is a system of automated dispute resolution. An uncle gives the same 50 BTC to you and to your cousin. Lawyers readily recognize this problem, and would likely imagine centralized institutions and courts as the means for solving it. Satoshi Nakamoto saw a problem that could be solved with technology and incentive engineering.

VI. THE ROLE OF THE LONGEST BLOCKCHAIN

A. *Consensus and the Longest Blockchain*

In the prior section, we discussed how miners compete for the mining prize and, in effect, time-stamp unconfirmed transactions by including them in a "block" of transactions. This block is then appended to the blockchain, which includes all Bitcoin transactions since Satoshi Nakamoto announced the "genesis block" in early 2009. This new block rewards the miner with a special transaction (the coinbase transaction) that gives the miner a reward of (currently) 12.5 BTC.[115]

Thus, every confirmed transaction will appear on the Bitcoin blockchain. Anyone can examine the Bitcoin blockchain using several user-friendly internet sites.[116] Going back to our earlier comparisons with real property deeds, the blockchain resembles the deed books at a public records office. By inspecting the deed book (or blockchain), one can learn who owns what real property (or Bitcoin).[117]

The Bitcoin blockchain is not, however, created by any government or other central party. It is maintained in identical form by the community of Bitcoin users. The Bitcoin community reaches a consensus about the blockchain because it recognizes the longest blockchain as being the valid one. Why recognize the longest blockchain? Because it contains the most

---

114 *See supra* note 30 and accompanying text.

115 Since the coinbase transaction gives the miner Bitcoin, the block includes the miner's Bitcoin address. Thus, every miner will attempt to create a distinct block (one that pays the miner the coinbase transaction), thereby making the puzzle different for every miner. *See generally* ANTONOPOULOS, *supra* note 39, at 221–26 (describing the coinbase transaction).

116 *See* ANTONOPOULOS, *supra* note 39, at 64–65.

117 *See* Fairfield, *supra* note 17, at 812.

complete set of transactions and represents the most work done by Bitcoin miners. As of late February 2018, the longest Bitcoin blockchain contained more than 500,000 individual blocks[118] created since the original "genesis block" of early 2009.

B. *Impossibility of Re-Mining the Longest Blockchain*

Suppose Alice perceives the following weakness in Bitcoin. Since the system does not rely on any central authority, nothing stops Alice from creating her own blockchain starting with the original genesis block of early 2009, which we will call block #0. So, in early 2018, Alice begins the mining process from block #0 and the process for creating an alternative block #1. At the time, the reward was 50 BTC, which Alice now claims as a reward under her alternative block #1. She continues this process, mining off block #1 to create an alternative block #2, and so forth. Alice's ultimate goal is to create an alternative blockchain that gives her ownership of all Bitcoin created after the genesis block. Since there is no central authority, Alice could claim that her blockchain is procedurally no less valid than any other blockchain so long as she properly mines each block by creating a sufficiently small hash.

Recall that successful miners must solve a computationally intense puzzle.[119] Even though Alice is, in effect, re-mining previously created blocks (#1, #2, etc.), the previously discussed solutions do not help her at all. For Alice's scheme to work, the re-mined blocks must be different than the originals; they must pay to her the mining prize (or coinbase transaction). Alice's Bitcoin address would appear in the re-mined blocks, instead of the original miner's. The mining puzzle requires a hash with several leading zeros, and a small tweak to the text will completely change the hash of the text.[120] As a result, Alice's re-mined blocks would take just as much work to produce as the originals. Suppose that Alice re-mines a few early blocks (#1, #2, etc.). Alice has created an alternative blockchain that, as a matter of Bitcoin protocol, is completely valid.

As a matter of Bitcoin-community consensus, however, her alternative blockchain accomplishes nothing. The Bitcoin community respects the longest blockchain as being authoritative. When Alice starts her scheme in early 2018, the longest blockchain has more than 500,000 blocks. Alice has a lot of work to do to catch up! But, while she is busily re-mining blocks #1, #2, etc., the rest of the community is mining blocks #500,001, #500,002, etc. It is as if Alice is 500,000 points down at a sporting event. While she is

---

[118] Block #510,000 was mined on February 19, 2018. *See Block #510,000*, BLOCKCHAIN, https://blockchain.info/block/00000000000000000000152678f83ec36b6951ed3f7e1cc3b04c5828cab8017329 (last visited Oct. 13, 2018).

[119] *See supra* Part V.D.3.

[120] *See supra* note 108 and accompanying text.

trying to erase the deficit, other Bitcoin miners are racing to extend the community's 500,000 point lead.

C. *Why Miners Generally Build on the Longest Blockchain*

As previously noted, the Bitcoin community generally acknowledges the longest blockchain as authoritative.[121] The Bitcoin community simply wants the most complete set of valid transactions, which should be contained in the longest blockchain.[122] This norm affects the behavior of miners. Suppose that Bob and Chelsea are both mining block #500,001. Bob arrives at a solution first and announces the new block, which contains a 12.5 BTC prize for Bob. Bob has a strong incentive to communicate this solution immediately. If Bob delays, Chelsea might arrive at a solution later in time, but still announce it before Bob makes his announcement. By delaying, Bob risks losing the 12.5 BTC prize to Chelsea or some other miner. Suppose Bob announces his solution immediately. Hearing this announcement, Chelsea has a strong incentive to stop mining block #500,001 and switch her efforts to finding a solution to block #500,002. The mining process tests computational power and requires energy consumption. Even if Chelsea "wins" block #500,001, the community would not recognize this win. Chelsea would have to win both block #500,001 and #500,002 in order to create the longest blockchain. Because of these incentives, almost all Bitcoin mining focuses on adding to the longest known blockchain.

VII. BLOCKCHAIN INTEGRITY

A. *Introduction*

Without a centralized authority, Bitcoin works only if users reach a consensus on the history of all past transactions, which are recorded in the Bitcoin blockchain. The Bitcoin blockchain is stored by many (potentially all) members of the Bitcoin community, which must reach a consensus about its contents. Thieves, however, might attempt to re-write the blockchain to make it appear as if they own more Bitcoin than they actually own. Fortunately, the blockchain is structured in a way that makes such tampering obvious[123] and also supports the consensus required of the community.

Suppose Alice transferred 100 BTC to Bob in 2016. Shortly afterwards, a miner included this transaction on newly-mined block #400,000. This block became part of the consensus blockchain that forms the recorded

---

[121] *See generally* Part VI.

[122] The longest blockchain also has the greatest proof-of-work invested in it. *See* Nakamoto, *supra* note 2, at 3.

[123] *See* NARAYANAN ET AL., *supra* note 13, at 11 (calling the block chain a "tamper evident log").

history of all Bitcoin transactions. So far, so good. Let us represent this block with the following:

> Representation of True Block
> Alice gives Bob 100BTC. Nonce = 116764
> Hash of this block is
> 0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
> 47fbe3e2e4

For sake of representation, we will assume that a successful miner needs only four leading zeros.

B. *Tampering with One Isolated Block*

Alice, however, has a scheme to reclaim the 100 BTC by tampering with the blockchain. Since the blockchain is collectively maintained by all users, Alice tries to make a small alteration to block #400,000. The true block #400,000 reflects her transfer of 100 BTC to Bob. Alice maintains a copy of the blockchain and, on her computer, alters block #400,000 slightly. Rather than showing the 100 BTC transfer from her to Bob, the altered block now shows a 100 BTC transfer from Alice to herself (or to a new Bitcoin address that she controls). Alice then tries to pass this altered blockchain as the authoritative one in the hopes that she can spend the 100 BTC a second time.

> Alice's First Edit
> Alice gives Alice 100BTC. Nonce = 116764
> Hash of this block is
> 0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
> 47fbe3e2e4

The Bitcoin blockchain exposes Alice's fraud by making it internally inconsistent. Recall that successful miners must find a qualifying hash of the block they are mining.[124] With her alteration, the hash of block #400,000 would change. Any user can "hash" Alice's edited block and discover that it does not match what is reported. In order to avoid this obvious mistake, Alice alters block #400,000 again. This time, it has the correct hash of the altered block.

> Alice's Second Edit
> Alice gives Alice 100BTC. Nonce = 116764
> Hash of this block is
> 854ef3ef9f3f8a01fd96f2e02009fa2e06c8cd62cd57685764012e0
> b0a96b462

Even after this edit, Alice again has a problem.

---

[124] *See supra* Part V.D.3.

Bitcoin miners must find a nonce that creates a very small hash, one with lots of leading zeros.[125] For sake of representation, we have assumed that miners must generate a hash with four leading zeros. The original block #400,000 clearly worked. Alice's first edit of this block "worked" superficially in that it reported a qualifying hash; however, it is the hash of the original block, not the block as edited by Alice. The second edit has the actual hash of the block, but it does not qualify for addition to the blockchain as it does not contain any leading zeros.

In order to successfully continue her fraud, Alice would need to re-mine block #400,000. This would allow her to claim the mining prize for herself and generate an alternative block that complies with Bitcoin protocol (four leading zeros, in this representation). Alice generates a new "nonce" (tweak) that results in a validly mined block.

Alice's Third Edit
Alice gives Alice 100BTC. Nonce = 93590
Hash of this block is
00003615a3053a00b019975f654e467abc555ff56ee16c83637065
657ad038c5

Viewed by itself, Alice's third edit is valid and internally consistent. The reported hash matches the contents of the block and qualifies with four leading zeros. In summary, Alice has found a way to tamper with block #400,000. She simply needs to re-mine it.

C. *Tampering with One Block Included in the Blockchain*

When viewed as part of the blockchain, however, Alice's third edit will fail. Blocks are linked ("chained") sequentially; each block reports the hash of the immediately preceding block.[126] We previously saw how hash functions can secure the order of documents when we considered (fictitious) wills executed by Satoshi Nakamoto.[127]

Let us return to Alice. She is attempting to tamper with Block #400,000, which contains a transfer she made to Bob. The importance of the blockchain will now become clear. In a blockchain, every new block reports the hash of the block that came before. Before Alice's attempted fraud, the blockchain might be represented as follows:

Block #400,000
Hash of prior block is
0000fef5c86a7c04f269a57a4ed3d2445e96912143f636abafaba5e
ed1d724ff
Alice gives Bob 100BTC. Nonce = 116764
Hash of this block is

125 *See supra* note 108 and accompanying text.
126 *See* Nakamoto, *supra* note 2, at 2.
127 *See supra* Part V.B.

0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
47fbe3e2e4

Block #400,001
Hash of prior block is
0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
47fbe3e2e4
Chelsea gives Ellie 2.2BTC. Nonce = 78213
Hash of this block is
000076ee0f3bcb7cc729c901cdd48323337646e453beac7f1e8cee
08b8a1068a.

This sequence represents the consensus blockchain that was previously mined. Note that block #400,001 reports not only its own hash, but also the hash of the prior block. This linkage between sequential blocks creates the "chain" of the blockchain. If Alice tried to insert her tampered block #400,001 into the blockchain, it would look like the following:

Block #400,000
Alice gives Alice 100BTC. Nonce = 93590
Hash of this block is
00003615a3053a00b019975f654e467abc555ff56ee16c83637065
657ad038c5

Block #400,001
Hash of prior block is
0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
47fbe3e2e4
Chelsea gives Ellie 2.2BTC. Nonce = 78213
Hash of this block is
000076ee0f3bcb7cc729c901cdd48323337646e453beac7f1e8cee
08b8a1068a

Alice's attempt at re-writing the blockchain makes it easy to detect her fraud. Block #400,001 reports a hash of the preceding block, but this reported hash does not match the hash of Alice's tampered block.

To continue her fraud, Alice could attempt to tamper with—and completely re-mine—block #400,001 as she did with block #400,000. Block #400,002, however, would expose this attempt. Alice would have to re-mine the entire Bitcoin blockchain to conceal her fraud. Earlier, we discussed how this is probably not a feasible strategy. Not only would Alice have to re-mine the entire blockchain, but she would also need to catch up with the entire mining community. As discussed before, it seems unlikely that an adversary could re-mine significant portions of the blockchain.[128]

[128] *See supra* Part VI.B.

D. *Targeting the Hash of One Existing Block*

Alice might have one last strategy that could allow her to alter block #400,000 while maintaining an internal consistent blockchain. Alice might try to focus all of her efforts on block #400,000. What if Alice found a new nonce (tweak) that produces exactly the same hash as the one found in the original block #400,000 (i.e., 0000ec87 . . .)? If Alice could find such a nonce, the reference in block #400,001 would remain correct and Alice could plausibly alter block #400,000 in a way that would avoid detection, as her fraudulent blockchain would be internally consistent. This nonce is represented by <???> in text below:

> *Block #400,000*
> Hash of prior block is
> 0000fef5c86a7c04f269a57a4ed3d2445e96912143f636abafaba5e
> ed1d724ff
> Alice gives Alice 100BTC. Nonce = <???>
> Hash of this block is
> 0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
> 47fbe3e2e4
>
> *Block #400,001*
> Hash of prior block is
> 0000ec87190008373f39d344f901699ecce4a3caa839f78be5ee4b
> 47fbe3e2e4
> Chelsea gives Ellie 2.2BTC. Nonce = 78213
> Hash of this block is
> 000076ee0f3bcb7cc729c901cdd48323337646e453beac7f1e8cee
> 08b8a1068a.

This sounds like a simple task. Just find a nonce that produces the required hash of 0000ec87 . . . . Despite the simplicity, the task is computationally impossible given what we know about cryptographic hash functions.[129] The only way to find the required hash is by trial and error. The hash size, however, is 256 bits, or roughly 1.16 x 1077. This number is far greater than the number of atoms in the Milky Way galaxy and not much smaller than the estimated number of atoms in the entire Universe.[130] Alice is not searching for a needle in a haystack; she is searching for particular a molecule in the Universe. Her last attempt fails.

---

[129] *See generally* NARAYANAN ET AL., *supra* note 13, at 2–10 (describing cryptographic hash functions).

[130] Steve Cavill, *Number of Atoms in the Universe*, OXFORD UNIV. PRESS: OXFORD EDUC. BLOG (Nov. 24, 2015), https://educationblog.oup.com/secondary/maths/numbers-of-atoms-in-the-universe.

E. *Consensus and the Most Recent Block*

Earlier, when we discussed hypotheticals about Satoshi Nakamoto's will, we saw how documents could be ordered chronologically using a hash function.[131] Each subsequent document simply reports the hash of the immediately prior document. We also learned that Satoshi could secure all documents in his will, and their correct order, simply by publicizing the hash of the last document.

We can use this result to understand the type of "consensus" that is required for Bitcoin to operate. The community does not need to expressly agree on the history of all transactions. Instead, all the community needs to agree on is the most recent block. Suppose a miner reports a new block #510,000 before anyone else. This block has its own qualifying hash and contains a reference to the prior block (#509,999).

> Block #510,000
> Hash of prior block is 00000000000000000002292de0d9f03dfa15a
> 04dbf09102d5d4552117b717fa86
> <580 Transactions> Nonce = 3347656422
> Hash of this block is
> 000000000000000000152678f83ec36b6951ed3f7e1cc3b04c582
> 8cab8017329

Suppose the community recognizes this block as valid. The transactions it contains are considered confirmed, and miners begin working on the next block.

Since this block is considered valid, block #509,999 must be valid as well (since the two are linked). But, if #509,999 is valid, so must #509,998, and so forth. So long as someone maintains the information from these blocks, the rest of the community can confirm the information. Relatedly, the community does not need to trust those who maintain the full set of information. As we saw with Alice, attempts at tampering with the blockchain are easy to spot because they break the chain (i.e., the hashes) that links blocks and therefore lead to inconsistencies within the blockchain. Members of the community can spot these inconsistencies and disregard attempts at tampering.

VIII. CONCLUSION

The main goal of this Article is to describe Bitcoin as a legal institution. No one knows if Satoshi Nakamoto has any legal training, but his work can be viewed as clever lawyering. Indeed, his primary goal was essentially legal in nature: to create a payment system that could operate outside of the jurisdiction of any state. Because it has no centralized authority, Bitcoin has no headquarters, no agent for service of process. No court can obtain

[131] *See supra* Part V.B.3.

jurisdiction over Bitcoin, as it resides on computers throughout the world. No regulator can control the actions of Bitcoin. In literal terms, Bitcoin is merely common software and a common set of recorded transactions that users agree on.

In functional terms, Satoshi Nakamoto created a form of property that can exist without relying on the state, centralized authority, or traditional legal structures. Bitcoin shares many characteristics of real property. It is transferred by instruments that we can characterize as "deeds." To provide "title assurance," Bitcoin transfers are recorded on a "blockchain," a public repository that describes every Bitcoin transaction ever made. Before transactions can be added to the blockchain, they must be organized into a block by Bitcoin miners. Bitcoin miners, in effect, time-stamp transactions and put them into their proper order. Miners and the blockchain operate like a public records office, time-stamping deeds as they are submitted and filing them away for public inspection.

We can be amazed at the cleverness and success of this creation even if we are uneasy with some of its results. Since Bitcoin was created outside of the law, the law will struggle to regulate it. Financial regulators can easily direct traditional financial institutions to conduct themselves in certain ways (for example, by requiring them to facilitate the chargebacks that Satoshi Nakamoto wanted to avoid).[132] Because regulators direct their actions against people, not algorithms, Bitcoin regulation will prove difficult. By understanding Bitcoin as decentralized deeds, however, we can better face the challenges ahead.

[132] *See generally* Truth in Lending Act, 15 U.S.C. § 1666i (2018) (establishing certain chargeback remedies for consumers).