

J. DAX HANSEN | PARTNER

+1.206.359.6324 DHansen@perkinscoie.com JOSHUA L. BOEHM | ASSOCIATE

+1.602.351.8161

JBoehm@perkinscoie.com

PerkinsCoie.com/Blockchain





About Perkins Coie's Blockchain Industry Group

Perkins Coie features the world's largest and leading Blockchain Technology & Digital Currency industry group because we were here when it all began. Our firm started advising clients about tokenization and bitcoin, and has since expanded to helping our clients pioneer numerous and diverse uses of blockchain technology.

LEADER, NOT A FOLLOWER

Established in May 2013, this industry group represents more of an evolution than a genesis. As part of the greater Electronic Financial Services group, Perkins Coie has a long history representing technology companies that provide consumer and financial services, including mobile payment providers, tokenized in-game assets, e-commerce companies, and marketplace payment service providers. Naturally, when the first bitcoin and other decentralized virtual currency companies emerged, Perkins Coie was uniquely situated to launch an industry group focused specifically on blockchain technology and digital currency that now has over 40 lawyers advising clients across a range of issues. This group has helped more than 200 clients reconcile complex regulatory compliance questions, assess intellectual property opportunities, negotiate with regulators, and educate the greater population about the promises of blockchain technology.

WE ARE HELPING SHAPE THE INDUSTRY

Our team participates as observers to the Uniform Law Commission Study Committee in its drafting of a model Regulation of Virtual Currency Businesses Act. We work closely with Coin Center, The Chamber of Digital Commerce, and the Bitcoin Foundation, the world's leading trade associations representing the digital asset and blockchain industry. We are founding participants in many industry and academic initiatives including COALA's Blockchain Workshops, The Digital Assets Accounting Consortium, The Berkman Klein Center for Internet & Society's Blockchain Roundtables, The Smart Contracts Alliance, and the DC Blockchain Center.

YOUR LEGAL PARTNER IN INNOVATION

Our multidisciplinary group is on the front lines, helping clients address the complex legal issues faced by bitcoin and other virtual currency businesses and partnering with those who are pioneering new blockchain and other distributed ledger solutions to many of today's market challenges. We provide regulatory compliance counseling, litigation support, consumer protection counseling, and business transaction assistance for a range of bitcoin and digital currency systems, services, and products. Our clients include virtual currency exchanges, blockchain innovators both large and small, payment processors, investors, and industry associations.

We counsel virtual currency industry clients with respect to various regulatory issues, including compliance with the Bank Secrecy Act, FinCEN regulations, and securities and commodities laws and regulations. We help them draft anti-money laundering policies and organize their internal policies and practices for compliance. We have also assisted these clients in the face of inquiries and investigations by federal and state law enforcement and regulatory agencies. Our experienced Investigations and White Collar Defense group regularly defends corporate clients and individuals against criminal and civil allegations of fraud, money laundering, and other misconduct. Our defense practice includes particular experience in defending clients and property against government asset seizures and forfeitures.





Table of Contents

INTRODUCTION	4
PART 1: TREATMENT OF BITCOIN UNDER U.S. STATE PROPERTY LAW—AN ILLUSTRATIVE ANALYSIS	5
KEY CHARACTERISTICS OF BITCOIN OWNERSHIP AND TRANSACTIONS	5
APPLICABLE PRINCIPLES OF CALIFORNIA PROPERTY LAW	7
TREATMENT OF BITCOIN UNDER APPLICABLE CALIFORNIA PROPERTY LAW	
VESTING OF PROPERTY RIGHT	9
PART 2: SCHOLARLY CONSIDERATION OF BITCOIN OWNERSHIP RIGHTS UNDER PROPERTY LAW GENERALLY	10
PART 3: TREATMENT OF BITCOIN AS PROPERTY UNDER OTHER U.S. LEGAL REGIMES	11
FEDERAL MONEY SERVICES BUSINESS REGULATION AND RELATED CIVIL FORFEITURE LAWS	11
COMMODITY LAWS	11
TAXATION LAWS	12
BANKRUPTCY LAWS	12
NEW YORK "BITLICENSE" REGULATION	13
TRUST AND ESTATE LAWS	
UNIFORM COMMERCIAL CODE	13
PART 4: POSSIBLE CHALLENGES TO TREATING BITCOIN AS PROPERTY	14
PSEUDOANONYMITY	14
LIMITED NUMBER OF PROPERTY TYPES ("NUMERUS CLAUSUS")	14
MULTI-SIGNATURE ARRANGEMENTS	15
TRACEABILITY LIMITATIONS	16
PART 5: PROPERTY INTEREST IN BITCOINS HELD IN CUSTODY	16
OVERVIEW OF SPECIAL AND GENERAL DEPOSITS	17
IMPORTANCE OF PARTIES' AGREEMENT TO CLASSIFICATION OF DEPOSIT	
POSSIBLE IMPLICATIONS FOR BITCOIN CUSTODY	18
ENDNOTES	20

BY J. DAX HANSEN¹ AND JOSHUA L. BOEHM²



Introduction

In this white paper, we analyze the treatment of bitcoin under applicable U.S. property law. We conclude that property interests should exist in bitcoin under such law, and that multiple sources of persuasive authority provide additional support for that conclusion. We proceed in five parts:

PART 1: TREATMENT OF BITCOIN UNDER U.S. STATE PROPERTY LAW—AN ILLUSTRATIVE ANALYSIS

Surveys the relevant technological characteristics of bitcoin and assesses how bitcoin is treated under U.S. state property law. Using California law as a benchmark, we conclude that intangible property rights should exist in bitcoin.

PART 2: SCHOLARLY CONSIDERATION OF BITCOIN OWNERSHIP RIGHTS UNDER PROPERTY LAW GENERALLY

Discusses scholarly articles on this topic by U.S. law professors, which generally corroborate the view that intangible property rights should exist in bitcoin.

PART 3: TREATMENT OF BITCOIN AS PROPERTY UNDER OTHER U.S. LEGAL REGIMES

Addresses how bitcoin has been treated under other U.S. legal regimes, including money services business law, civil forfeiture law, commodities law, bankruptcy law, taxation law, state cryptocurrency regulation, trusts and estates law, and the Uniform Commercial Code, all of which have been interpreted (through court opinions, regulatory guidance or informal market practice) to operate on the premise that bitcoins are property.

PART 4: POSSIBLE CHALLENGES TO TREATING BITCOIN AS PROPERTY

Discusses potential obstacles to recognizing or enforcing property rights in bitcoins, including challenges raised by multi-signature arrangements and the pseudoanonymity and lack of traceability of specific bitcoin units, as well as by traditional property law concepts that favor formal categorization of property rights (which might exclude a novel concept like bitcoin). While certain of these obstacles may limit the exercise of bitcoin property rights to some extent, they do not undercut the legitimacy of such rights or create unmanageable enforcement issues.

PART 5: PROPERTY INTEREST IN BITCOINS HELD IN CUSTODY

Assumes that (pursuant to the analysis in Parts 1–4) direct property rights exist in bitcoins and goes further to assess property law implications arising from bitcoin custodial arrangements. In particular, it uses banking law analogies to outline conditions under which a bitcoin depositor would retain title in deposited bitcoin (in a bailor/bailee relationship) rather than transferring title in such deposited bitcoin to the custodian (in a creditor/debtor relationship).

>> The authors wish to thank Andrew Beal of Ernst & Young, Jerry Brito and Peter Van Valkenburgh of Coin Center (coincenter.org), and Patrick Murck of the Berkman Klein Center for Internet & Society at Harvard University for their thoughtful comments and contributions to this white paper.







TREATMENT OF BITCOIN UNDER U.S. STATE PROPERTY LAW—AN ILLUSTRATIVE ANALYSIS

The U.S. Supreme Court has explained that the "types of interests protected as 'property'" in the United States "are varied and, as often as not, intangible, relating 'to the whole domain of social and economic fact." However, property interests in the United States are "not created by the Constitution," but instead defined "by existing rules or understandings that stem from an independent source such as state law."4

Accordingly, U.S. state law provides the starting point for determining whether ownership interests may exist in bitcoin. 5 Because a full, 50-state survey is outside the scope of this white paper, we focus on California law for illustrative purposes. California is the most populous state in the United States, serves as the operational base for a large number of companies active in the cryptocurrency industry, and generally has well-developed precedent in legal issues involving technological innovations.

Additionally, while the analysis may ultimately differ under other states' laws, it is our understanding that U.S. state laws are generally similar on foundational concepts of what may give rise to a property interest. Thus, even though bitcoin's status under a particular state's property laws would still require specific analysis, we believe that this high-level analysis under California law should be broadly useful for illustrative purposes.

In order to apply the relevant state law property principles to bitcoin, however, we first review the key characteristics of how bitcoins are owned and transacted. In the interest of brevity, we assume basic familiarity with bitcoin and its underlying technological platform, the blockchain.6

>> KEY CHARACTERISTICS OF BITCOIN OWNERSHIP AND TRANSACTIONS

Generally speaking, ownership of bitcoin is established through successful completion and recordation of transactions on the bitcoin blockchain.



THIS PROPOSED TRANSACTION is broadcast to the bitcoin network, where it is processed and verified by other participants in the network known as miners; if the transaction is valid, it will be included in a subsequent block of transactions on the blockchain, rendering it effectively irreversible.

These transactions specify the sender and recipient of bitcoins by their respective public addresses. Each public address corresponds to a set of digital keys: one "public" key and at least one "private" key. Public and private keys are independent of the bitcoin protocol and a user's software can generate them without reference to the blockchain or access to the Internet.8 The public key is derived from the private key using a mathematical procedure called elliptic curve multiplication and the bitcoin address is in turn derived from a cryptographic "hash" function of the public key.9

To conduct a transaction, a sender must digitally sign the proposed transaction with her private key to the public address of the recipient.¹⁰ The source of funds in the bitcoin transaction is tied to one or more prior transactions that the sender had completed and were verified on the blockchain.¹¹ Thus, when a transaction is consummated between a sender and recipient of bitcoins, the sender's signature with her private key essentially affirms that





bitcoins previously transferred to her (e.g., by a third party) should now belong to the recipient.¹² This proposed transaction is broadcast to the bitcoin network where it is processed and verified by other participants in the network known as "miners." If the transaction is valid, it will be included in a subsequent block of transactions on the blockchain, rendering it effectively irreversible.

From an ownership perspective, the key component of transactions is the so-called "unspent transaction output," or "UTXO." UTXOs are "chunks of bitcoin" that are "locked to a specific owner [using a so-called locking script], recorded on the blockchain, and recognized" as units belonging to that specified owner by the entire network. 13 Thus, bitcoin value associated with a particular public address may be dispersed in multiple UTXOs that are recorded in various blocks on the blockchain. 14 Note that, as a practical matter, a single user may control multiple public addresses with corresponding private keys (and in many ways, this is desirable from a security perspective). A user's wallet application can calculate a user's total "balance" by scanning the blockchain and adding up all UTXOs that are associated with accounts that the user controls. 15

The "inputs" for a bitcoin transaction must be drawn from a sender's UTXO in whatever amounts the user has available. That is, a user cannot send part of a UTXO as an input. So, if a user has only one UTXO in the amount of 5 BTC but only wants to send 1 BTC to a recipient, the user would need to specify two "outputs": (1) output to the recipient and (2) another output to the user's own address. This is akin to spending a \$5 bill on a \$1 item and receiving \$4 back in change. Beyond this "change" structure, a sender may also designate multiple third-party outputs for the inputted UTXOs in her transaction. Generally, there must also be a small output designated as a miner "fee" in each transaction to help incentivize miners to process the transaction.

To "unlock" the UTXOs designated as inputs for a transaction, so as to transfer ownership of those UTXOs (or a portion thereof) to another public address, an unlocking script must be run. ¹⁸ Generally, this is done by the sender signing the transaction with her private key to prove ownership of the bitcoin address that is associated with the locking script. ¹⁹ So, in the example noted above, the sender would sign (and thus "unlock") the UTXO input worth 5 BTC and generate (1) a nominal output representing miner fees; (2) one UTXO output worth 1 BTC associated with the recipient's public address; and (3) a second UTXO output worth slightly less than 4 BTC associated with the sender's own public address (equal to the 5 BTC input, minus the 1 BTC third-party transfer, minus the nominal fee).

Notably, while the blockchain easily permits tracking of which UTXOs (or portions thereof) are transferred from one public address to another public address, the bitcoin amounts comprising each UTXO are not "earmarked" (e.g., as with a stock certificate) such that a specific bitcoin could be traced through a series of transactions on the blockchain.²⁰

The foregoing discussion should yield an important factual premise for the subsequent property law analysis in this white paper. Specifically, ownership rights in bitcoin appear to be rooted in the ability to control the disposition of UTXOs that are recorded on the blockchain. As a default matter, therefore, control of sufficient credentials—in the form of private key or keys—to unlock a given UTXO should confer ownership of the bitcoin value represented in that UTXO. We discuss implications beyond this default rule later in this white paper (e.g., regarding the ability to override this rule by contract).²¹

With this technical background in mind, we now turn to whether bitcoin ownership should be recognized as a property right under California law.





>> APPLICABLE PRINCIPLES OF CALIFORNIA PROPERTY LAW

Under California statutory law, "[t]he ownership of a thing is the right of one or more persons to possess and use it to the exclusion of others" and "the thing of which there may be ownership is called property."²² Consistent with the principles articulated by the U.S. Supreme Court, as discussed above, California courts have described property as a broad concept that includes "every intangible benefit and prerogative susceptible of possession or disposition."23

In 1992, the U.S. Court of Appeals for the Ninth Circuit distilled three criteria that remain the prevailing standard for when California law will recognize a property right: "First, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity."24

Several cases help illustrate how this standard is applied across the spectrum of electronic data.

In a widely cited 2003 case, Kremen v. Cohen, the Ninth Circuit concluded that Internet domain names are a form of intangible property under California law.²⁵ In reaching this outcome, the court applied the prevailing three-part test as follows: first, like a "corporate stock or a plot of land, a domain name is a well-defined interest"; second, "[o]wnership is exclusive in that the [domain] registrant alone makes" the decision as to what is on the associated webpage; and third, there is a legitimate claim to exclusivity given the act of registering a domain name and the investment involved in developing and maintaining a webpage.²⁶



CALIFORNIA COURTS HAVE described property as a broad concept that includes 'every intangible benefit and prerogative susceptible of possession or disposition.'

Subsequent courts applying California law have found that other forms of electronic business data are intangible property protectable by a conversion remedy, including computer code, confidential information regarding contracts with customers, business plans and product plans.²⁷

However, courts have rejected more generalized claims that caches of "personal information" collected in an iPhone (such as zip codes, user location, and device identifier) were property subject to conversion remedies after a data breach. To illustrate, in a 2012 order In re iPhone Application Litigation, a Northern District of California judge held that such information does not constitute an interest "capable of precise definition" and that "it is difficult to see how" it is "capable of exclusive possession or control." Other courts have reasoned similarly. Although cases in this area are very dependent on facts and circumstances, a key factor in assessing property interests in electronic data appears to be whether such data would have any economic value on an independent basis (i.e., apart from any collection in which it may have been stored).30

>> TREATMENT OF BITCOIN UNDER APPLICABLE CALIFORNIA PROPERTY LAW

Applying the prevailing three-part test for property interests articulated by the Ninth Circuit, ownership of bitcoin should be considered an intangible property interest under California law.





First, there is an interest "capable of precise definition." At any given point in time, a user may claim ownership in each of the UTXOs on the blockchain that are linked to her public address. Each UTXO is associated with a precise number of bitcoins (or fractions thereof), thus satisfying the definitional requirement of a property interest.

Second, a user's ownership interest in each UTXO is capable of "exclusive possession or control." Once generated as an output in a transaction to a particular public address, a UTXO is "locked" on the blockchain with a locking script. Only when the UTXO is used as an input in a valid subsequent transaction—which requires such transaction to be "unlocked" with the private key (or keys) corresponding to the public address of the input UTXO—may ownership of the UTXO be transferred to a different public address (or addresses). If a party attempts to conduct a transaction without the requisite private key signature, the network of bitcoin miners will quickly recognize the transaction as invalid and refuse to process it, and the input UTXO will remain locked as it was on the blockchain.

Given the requirement to have the correct private key to transfer ownership of UTXOs, bitcoin ownership is much more analogous to the domain address at issue in Kremen, where the domain registrant could fully control the site associated with an address, than the generalized caches of data at issue in In re iPhone Application Litigation, which were found to be incapable of exclusive control. Thus, the "possession or control" requirement of a property interest should also be satisfied.

Third, users have a "legitimate claim to exclusivity" in their UTXO ownership interests. In Kremen, the court cited two factors underlying a "legitimate" claim to exclusivity for purposes of property rights. We address these as follows:

One factor discussed in Kremen is that a domain name owner's address is publicly registered, "like staking a claim to a plot of land at the title office," thus informing others "that the domain name is the registrant's and no one else's." Similarly, in a proposed bitcoin transaction, the transaction is broadcast to the entire bitcoin network to determine the validity of the underlying UTXO ownership interest so as to ensure that there is no fraudulent transfer of interest. Once the transaction is validated, the transferred ownership interest is irrevocably recorded in the form of the new, output UTXOs that correspond to specific public addresses on the blockchain (which is available for anyone to see).31



IN A PROPOSED bitcoin transaction, the transaction is broadcast to the entire bitcoin network to determine the validity of the underlying UTXO ownership interest so as to ensure that there is no fraudulent transfer of interest.

Kremen also emphasized the public policy interest in recognizing that domain name registrants "invest substantial time and money" to develop websites, and that protecting property interests in domain names therefore "promote[s] the growth of the Internet overall."32 Similar policy interests underpin the legitimacy of bitcoin owners' property interest in their UTXOs. A great deal of risk, innovation, and investment has gone into the creation of the bitcoin/ blockchain ecosystem since its inception, and it has already yielded numerous business use cases and promises more in the future.³³ Moreover, bitcoin owners themselves have developed and sought robust protections for their bitcoins—including "cold storage" and back-up mechanisms, multi-signature arrangements, paper wallets, and insurance—and have gravitated toward vendors who provide such protections. Protecting the investment-backed expectations of bitcoin owners is essential to promoting the further growth of this system, just as protecting domain name ownership interests was critical to promoting Internet development.³⁴

For the above reasons, we believe that an intangible property right should exist in bitcoin under California law.





>> VESTING OF PROPERTY RIGHT



PARTIES MAY ENTER into contractual arrangements in which one party entrusts partial or complete control of such private key(s) to a third party while still maintaining formal title to the bitcoin value represented in applicable UTXOs.

Further to the technological overview above, it appears that a bitcoin property right should be vested (as a default matter) once a party has the ability to control the disposition of UTXOs. Although "vesting" has specialized definitions across various categories of rights, the basic concept is understood to mean the possession of "a completed, consummated right for present or future enjoyment," which is "not contingent," "unconditional," and "absolute."35



OBTAINING THE ABILITY to unlock and thus control UTXOs should be the default rule for when bitcoin ownership vests.

Parties may, as we discuss further below, enter into contractual arrangements in which one party entrusts partial or complete control of such private key(s) to a third party while still maintaining formal title to the bitcoin value represented in applicable UTXOs. These kinds of contractual arrangements are commonplace in custodial, trust, and escrow settings, which have generated well-developed legal principles that should generally translate to bitcoin custodial contexts.

But aside from such contractual arrangements (or any indications that private key(s) were obtained illicitly³⁶), obtaining the ability to unlock and thus control UTXOs should be the default rule for when bitcoin ownership vests. At that point in time, the possessor of such UTXOs should have a completed, non-contingent, and absolute right to dispose of the value represented in such UTXOs, which satisfies the general criteria for a vested property right. Other areas of law concerning intangible property rights employ a similar default rule of "control" with the possibility of contractual override, and we believe that this is likely the most logical approach for the bitcoin context as well.37





SCHOLARLY CONSIDERATION OF BITCOIN OWNERSHIP RIGHTS UNDER PROPERTY LAW GENERALLY

Property law scholars who have encountered the bitcoin ownership issue in the context of broader, more theoretical undertakings have reached (or assumed) the same general conclusion from Part 1 of this white paper—that is, interests in bitcoin should be protected by property law.³⁸

In their articles, these professors also highlight important shortcomings under existing property law that could hinder the development of the bitcoin marketplace.

Prof. Joshua Fairfield, for instance, argues that the traditional focus of property law on the tangibility of assets yields a number of undesirable outcomes as applied to intangible assets (such as bitcoin), and that property law should be recast as a protocol for the "transmission, security and verification of information." As relevant to this white paper, though, it is clearly a premise in Prof. Fairfield's argument that bitcoin is and should be "ownable" under property law. Indeed, his prescriptions flow from the basic observation that current property law needs to be reformed to better protect and promote ownership of digital assets (including, but not limited to, bitcoin).⁴⁰



CURRENT PROPERTY LAW needs to be reformed to better protect and promote ownership of digital assets.

Prof. Shawn Bayern argues that bitcoin "does not fit neatly into" classical property categories and, as such, bitcoin is, "in a meaningful sense," a new kind of asset.⁴¹ For that reason, Prof. Bayern emphasizes the importance of assessing bitcoin-related property rights from a "functional" perspective to avoid arbitrary and unfair outcomes that could result from formal categorization under traditional property law. 42 The fact that bitcoin is "an important economic right to many who participate in the network" makes it "clearly proper to criminalize its theft," according to Prof. Bayern; moreover, it "matches parties' expectations if bitcoin is treated as intangible, movable personal property."43

Although outside the scope of this white paper, we encourage further exploration of the broader reform proposals set forth by Profs. Fairfield and Bayern to ensure that property law applies appropriately and fairly to bitcoin and other emerging digital asset use cases (e.g., to prevent arbitrary legal treatment from arising simply because of the intangible character of digital assets). For the purposes of this white paper's narrower focus on bitcoin's "ownability" under existing U.S. law, though, it is notable that Prof. Fairfield's work is partly premised on the legitimacy of ownership rights in bitcoin (among other digital assets) and that Prof. Bayern's work posits that bitcoin should be treated as "intangible, movable personal property."



BITCOIN HAS BEEN widely treated as property for purposes of other state and federal statutory regimes.







TREATMENT OF BITCOIN AS PROPERTY UNDER OTHER U.S. LEGAL REGIMES

Although the concept of "property" is fundamentally a matter of state law in the United States, it is also important that bitcoin has been widely treated as (or assumed to be) property for purposes of other state and federal statutory regimes. These treatments and assumptions have already had substantial consequences for the bitcoin sector. They therefore constitute informal but persuasive legal precedent further indicating that bitcoin can be owned as property.

>> FEDERAL MONEY SERVICES BUSINESS REGULATION AND RELATED CIVIL FORFEITURE LAWS

The U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") has issued guidance providing that an administrator or exchanger of a virtual currency like bitcoin is required to register as a money services business ("MSB") with FinCEN.44 Accordingly, a money transmitting business that operates in bitcoins must register with FinCEN. Failure to register is a violation of 18 U.S.C. § 1960, and "[a]ny property, real or personal," involved in transactions that violate § 1960 is subject to civil forfeiture. 45

In the United States, "civil forfeiture is an in rem proceeding" initiated by the government that is "directed against ... property."46 According to a leading U.S. civil procedure treatise, "[t]he essential function of an action in rem is the determination of title to or the status of property located—physically or legally—within the court's jurisdiction. Conceptually, in rem jurisdiction operates directly on the property and the court's judgment is effective against all persons who have an interest in the property."47



BECAUSE CIVIL FORFEITURE proceedings are in rem, which involve property by definition, it is notable that bitcoins have been the subject of a civil forfeiture action.

Because civil forfeiture proceedings are in rem, which involve property by definition, it is notable that bitcoins have been the subject of a civil forfeiture action in connection with a violation of 18 U.S.C. § 1960. In United States v. 50.44 Bitcoins, a federal magistrate judge recommended that bitcoins seized from an unregistered MSB be forfeited to the U.S. government, concluding (as relevant here) that such bitcoins were property subject to forfeiture under applicable federal law.⁴⁸ This proceeding provides further support for the conclusion that property interests exist in bitcoin, since the U.S. government would not have been legally permitted to seize the 50.44 bitcoins at issue if they were not property.49

Even to the extent bitcoins are treated as a currency for purposes of FinCEN regulations, it remains that traditional fiat currency is "property" subject to in rem civil forfeiture proceedings. 50 Indeed, to establish their standing to challenge the government's seizure of such currency, claimants must show that they have a "colorable interest in the property," which "includes an ownership interest or a possessory interest."51 This case law further suggests that currency is "ownable" akin to other forms of personal property.

>> COMMODITY LAWS

In September 2015, the status of bitcoin under the Commodity Exchange Act ("CEA"), and the related rules thereunder promulgated by the Commodity Futures Trading Commission ("CFTC"), was largely resolved when





the CFTC released an enforcement action and settlement order (the "Coinflip Order"). ⁵² In that order, the CFTC specifically concluded that "Bitcoin and other virtual currencies are [encompassed in the definition and] properly defined as commodities." ⁵³ Further, the CFTC treated bitcoin as an exempt commodity, putting the virtual currency into the same category as a precious metal. ⁵⁴ The treatment of bitcoin as an exempt commodity in the Coinflip Order may be characterized as providing support for the notion that the transfer of bitcoin property interests should be approached in the manner consistent with the transfer of property interests in respect of any other exempt commodity.

In June 2016, the CFTC issued an enforcement action and related settlement order involving Bitfinex, a platform that facilitated the purchase and sale of bitcoin, including on a margined basis (the "Bitfinex Order").⁵⁵ In the Bitfinex Order, the CFTC appeared to operate on the presumption that bitcoin had value and was capable of being transferred from one party as the seller of the bitcoin to another party as the purchaser of the bitcoin. Ultimately, the CFTC determined that the particular transactions at issue did not result in the actual delivery of the bitcoin within the meaning of the exception from regulation as a retail commodity transaction available under the CEA. In reaching this conclusion, the CFTC focused on the absence of possession and control over the bitcoin due to the fact that: (1) Bitfinex (the platform sponsor) continued to control the private keys to the multi-signature wallets into which the bitcoin was delivered; and (2) one of the parties to the transaction (other than Bitfinex) held a lien against those wallets. While the Bitfinex Order did not expressly address the status of bitcoin as "property," the CFTC analyzed whether a purchaser had possession and control of the bitcoin, the very conditions that constitute the basis of the state law analysis of an object's status as property.⁵⁶

>> TAXATION LAWS

In April 2014, the U.S. Internal Revenue Service issued a formal ruling expressly stating that "[f]or federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency."⁵⁷ For three years, then, persons subject to U.S. federal income tax have paid taxes on bitcoin transactions as the sale and purchase of property.

>> BANKRUPTCY LAWS

In a February 2015 bankruptcy order in the Northern District of California, a judge determined that bitcoin should be considered property for purposes of fraudulent transfer actions under Section 550(a) of the U.S. Bankruptcy Code.⁵⁸



In this case, *In re Hashfast Technologies*, the bankruptcy trustee had brought a fraudulent transfer action against a former employee to recover 3,000 bitcoins, and the question was how the bitcoins should be valued for that purpose.⁵⁹ Under Section 550(a), the trustee may recover "the property transferred, or, if the court so orders, the value of such property."⁶⁰ Thus, the trustee contended that the bitcoins were "property" and that the estate could recover either the 3,000 bitcoins or their current value, which had increased to \$1.2 million.⁶¹ The former employee argued that bitcoins were not "property" for purposes of Section 550(a), which would result in a valuation pegged at the lower U.S. dollar value at the time of the fraudulent transfer.⁶² After consideration of these arguments, the judge concluded that bitcoins were "clearly property" for purposes of Section 550(a) of the U.S. Bankruptcy Code.⁶³





>> NEW YORK "BITLICENSE" REGULATION

As of the date of this white paper, only one state has implemented a regulation specifically designed to cover cryptocurrency activity: New York, in its "BitLicense" regulation that was enacted in 2015.⁶⁴ The BitLicense regulation contains several indications that cryptocurrency is considered to be property.

First, BitLicensees are expressly prohibited from "using or encumbering *assets*, including [cryptocurrency], stored, held or maintained by, or under the custody or control of, such [BitLicensee] on behalf of another person."65 The fundamental definitions of "asset," according to Black's Law Dictionary, include "[a]n item that is *owned* and has value" and "the *property* of a person."66 Therefore, the BitLicense regulation's reference to cryptocurrency as an "asset" reflects that it is considered to be a form of property.67

Second, BitLicensees are required to maintain records of accounts and transactions "for at least five years after the time when any such [cryptocurrency] has been deemed, under the Abandoned Property Law, to be abandoned property." As its title would indicate, New York's Abandoned Property Law provides for escheatment to the state of personal property that has been abandoned for a specified time, further indicating that cryptocurrency is considered to be property under the BitLicense regulation.

>> TRUST AND ESTATES LAW

In 2015, the Uniform Law Commission approved a revised Uniform Fiduciary Access to Digital Assets Act ("UFADAA") for enactment by states. Recognizing the rapidly expanding scope of digital property in everyday life, the UFADAA is intended to make clear that the power of fiduciaries, including trustees, estate executors, conservators, and agents with powers of attorney, extends to the management of digital assets in addition to tangible property. The UFADAA frames "digital asset" in terms of property rights, defining it specifically as an "electronic record in which an individual has a right or interest. In its summary of the UFADAA, the ULC stated that "an executor that is distributing funds from the decedent's bank account will also have access to the decedent's virtual currency account (e.g., bitcoin)," thus making explicit that bitcoin is intended to come within the scope of "digital assets" under the UFADAA. In the two years since its release, roughly half the states have enacted the UFADAA or a version thereof, and other state legislatures are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it. Access to Digital Assets Act ("UFADAA") in the two years are actively considering it.

>> UNIFORM COMMERCIAL CODE75

Scholarly assessment of how bitcoin would be treated under the Uniform Commercial Code ("UCC"), as well as market actors taking security interests in bitcoin, can be viewed as providing support for the notion that bitcoin constitutes a type of property.

As a threshold matter, it is well-established that "[t]he principal focus of Article 9 of the Uniform Commercial Code (UCC) has always dealt with transactions intended by the parties to create security interests in personal property."⁷⁶ Put differently, only property can be used as collateral under Article 9 of the UCC.⁷⁷

We understand from market participants that borrowers have already pledged bitcoin as collateral to lenders. Although it remains to be seen how courts will interpret any disputes that may arise from these security arrangements, it is relevant that market actors have been operating in this area with the understanding that bitcoin is property that may be collateral under the UCC. As discussed above, under California law, the existence of such reasonable investment-backed interests is relevant to determining the legitimacy of a claim to exclusivity, which is a factor in establishing property rights as a threshold matter.⁷⁸





To that end, it is also notable that commercial law scholars and practitioners who have undertaken in-depth analyses of bitcoin's treatment under the UCC, including Prof. Jeanne Schroeder and George Fogg,⁷⁹ have operated on the premise that bitcoin is property that can be collateral subject to a UCC security interest.⁸⁰



POSSIBLE CHALLENGES TO TREATING BITCOIN AS PROPERTY

In this section, we consider four key challenges to treating bitcoin as property. The first two, which involve (a) bitcoin's pseudoanonymous characteristics and (b) the so-called "numerus clausus" principle, tend to challenge the premise that property rights may exist in bitcoin as a threshold matter. The latter two, which involve (c) multi-signature arrangements and (d) traceability issues, are less fundamental in nature and tend to challenge the practical ability of courts to recognize and enforce property rights in bitcoin. We address these challenges in turn.

>> PSEUDOANONYMITY

Some commentators have cited the pseudoanonymous character of public addresses⁸¹ in asking whether there is a "legitimate claim" to exclude others, as is required to give rise to a property right.⁸²

While there is a possibility that a court could decline to recognize bitcoin property interests on that ground, we think that, particularly if bitcoin is considered in context of analogous property interests, the mere fact of pseudoanonymity should not undercut the legitimacy of ownership in bitcoin.

This is because anonymous (or at least pseudoanonymous) ownership is permitted in other contexts of property in the United States. For example, personal or real property may be owned through trusts in some U.S. jurisdictions, with limited or no requirement that the underlying beneficial owners of such trusts be publicly disclosed (absent court order).⁸³ Functionally, that is no different than a natural person with a pseudoanonymous ownership interest in bitcoin.

Moreover, as discussed above, the test under California law for when a property interest arises does not look to public identifiability of asset ownership as a probative factor of whether the asset may be owned.⁸⁴

>> LIMITED NUMBER OF PROPERTY TYPES ("NUMERUS CLAUSUS")

Another potential challenge to the concept of bitcoin ownership arises from the doctrine of *numerus clausus*, a traditional notion that the "range of property forms should be a predetermined and closed set." Although it has influenced many areas of U.S. property law, *numerus clausus* has had a particularly strong impact on estates in land, where parties are strictly limited to certain forms of property interests (e.g., freehold interests in fee simple absolute, determinable, subject to condition subsequent, subject to executory limitation) and cannot create new forms by contract or otherwise. The rationale for *numerus clausus* derives from information cost concerns; since property rights are enforceable against the world (rather than solely against known counterparties, as in contract), maintaining a limited number of property forms helps minimize verification costs for third parties and thus promotes efficiency in property disposition.⁸⁷

Under current law, however, there is little possibility that a court would invoke *numerus clausus* in declining to recognize property rights in bitcoin. As the leading scholarly proponents of applying *numerus clausus* more widely in U.S. law acknowledge, the "*numerus clausus* is probably at its weakest in the area of intellectual property," which they construe broadly to encompass intangible property rights such as common law rights to publicity.⁸⁸ The Ninth Circuit's three criteria for recognizing intangible property rights under California law underscore that reality, as they focus solely on the functional nature of the purported right and do not look to pre-existing classifications or forms of property.⁸⁹





In other words, then, for numerus clausus to pose an obstacle to recognizing property rights in bitcoin, it would have to result from a fundamental change in prevailing legal standards governing intangible property rights (i.e., to introduce specific, formal categories of property rights). In that regard, it is notable that any effort to enact such change would likely be opposed by property scholars such as Profs. Fairfield and Bayern, both of whom argue (as discussed above) that less formalism and more functionalism is needed in property law to appropriately protect ownership rights in our increasingly digital and information-centric society.90

>> MULTI-SIGNATURE ARRANGEMENTS

Multi-signature arrangements in bitcoin arguably pose some practical challenges to using "control" as the default rule for ownership. Parties are free to implement a variety of permutations of multi-signature requirements to unlock a given UTXO; specifically, anything from a 1-of-1 to a 15-of-15 (including any combination within that range) as of the date of this white paper. 91 In cases where at least one party to a multi-signature arrangement has keys sufficient to unlock a UTXO, that party (or parties) is an owner (or co-owner) of the bitcoin value represented by the UTXO. Other parties to that arrangement (who may hold keys but not sufficient keys to transact unilaterally) do not have an ownership interest in the underlying bitcoin. It seems likely that, if no single entity has unilateral control over sufficient keys, then all holders of a necessary key (or key(s)) to unlock UTXOs would be considered co-owners of the bitcoin value represented in such UTXO, barring contractual arrangements that specify ownership.



A POTENTIALLY HARDER question arises where no single entity has unilateral control or necessary keys.

But a potentially harder question arises, for instance, where no single entity has unilateral control or necessary key(s). In a 2-of-4 arrangement, to illustrate, if all four keys are held by different entities, where does ownership lie? No single key is, in itself, necessary to transact, but if three key holders refused to sign, the fourth cannot transact on her own. One could say that all four parties have equal ownership rights and can freely transfer those rights to another co-owner or a third party (again, absent any contractual restrictions). Although this rests on a probabilistic notion of "control" that departs somewhat from the default "control" rule we have developed in this white paper, it would be generally consistent with how legislatures and courts have addressed co-ownership rights in other forms of intangible property. In copyright law, to illustrate, the statute provides: "[t]he authors of a joint work are coowners of copyright in the work" and that "ownership of a copyright may be transferred in whole or in part by any means of conveyance or by operation of law."92 Further thought and analysis is needed on this issue.

Ultimately, though, practical difficulties (e.g., with respect to duties to other co-owners and coordination in enforcing rights) arising from co-ownership have led practitioners to recommend that parties draft appropriate contractual provisions to address and/or avoid co-ownership of intellectual property. 3 Although it will presumably take trial and error, we believe that analogous contractual (or protocol-based) approaches to addressing and/or avoiding coownership rights are likely to be the best avenues for addressing the practical difficulties discussed above. Indeed, we understand that multi-signature arrangements are already often governed by contractual agreements that address the respective rights of each key holder.





>> TRACEABILITY LIMITATIONS

Another possible limitation to enforcing property interests in bitcoin focuses on the lack of traceability of bitcoins between owners across serial transactions.94 This "traceability" argument starts with the premise that the structure of bitcoin transactions makes it difficult or impossible to trace particular UTXO inputs to particular UTXO outputs.95 For example, if a transaction has UTXO inputs of 1 BTC and 2 BTC, and outputs of 1.5 BTC, 1.4999 BTC, and a fee of 0.0001 BTC, there would be no way of knowing whether the fee came from the 1 BTC input or the 2 BTC input.% From that premise, this argument expresses concern that, depending on how property interests in bitcoin are characterized, traceability limitations may hinder efforts to enforce such property rights as a practical matter.

However, when looking at components of other, established forms of property, it appears that a lack of traceability is not an unusual characteristic of such property, and should not ultimately undercut courts' ability to enforce ownership rights in the asset as a general matter.

For instance, companies are permitted to recognize intangible asset values for various assets that are not interrelated and do not generate cash flow for the company, such as brand names, quality and morale of work force, technological expertise, and corporate reputation. 97 Given the challenges in breaking down individual components of intangible asset value across those areas, it would be similarly difficult to trace (for example) an increase or decrease in intangible asset value to specific changes in a particular component. But we are not aware of any material difficulties courts have faced in adjudicating and enforcing such rights. 98



CERTAIN TANGIBLE ASSETS also lack specific ownership traceability.



Certain tangible assets also lack specific ownership traceability. Oil transport is one such example: to the extent oil belonging to multiple owners is commingled in a single tank (e.g., on a tanker ship), it is no longer possible to track a particular barrel of oil as belonging to a particular owner. Yet it is well established that readily enforceable ownership rights still exist in applicable amounts of the commingled oil.

To be sure, difficulties in tracing ownership of particular bitcoin units across successive owners could cause some challenges in certain commercial use cases, such as using bitcoin as collateral for secured lending under the UCC (as discussed above).99 But, to our knowledge, defining bitcoin ownership as the ability to control certain UTXOs has not posed irresolvable problems in practical use cases. Indeed, blockchain technology itself has enabled, and will likely continue to enable, solutions to obstacles that do arise. For example, multi-signature escrow arrangements (i.e., via contract) have already been used to establish perfection of creditors' interests in encumbered bitcoins for UCC purposes. Additionally, the bitcoin blockchain permits users to attach "metadata" to UTXOs, which may also be used as a mechanism to uniquely identify certain transactional inputs and outputs.



PROPERTY INTEREST IN BITCOINS HELD IN CUSTODY

In this white paper, we have focused to this point on the fact that bitcoins are capable of being owned directly. However, a secondary property law consideration is also of critical importance to the bitcoin sector, given that many holders of bitcoin do not store such bitcoin themselves but use a third-party custodian to do so. The question is: assuming bitcoins are capable of being owned, what factors determine whether a depositor retains title or transfers title of deposited bitcoin in a custodial arrangement?





>> OVERVIEW OF SPECIAL AND GENERAL DEPOSITS

The first step in answering this question is whether a deposit would be considered a "specific" or "general" deposit.

Broadly speaking, a specific deposit arises when a custodian "accepts cash or other valuables for 'safekeeping'," creating a bailor/bailee relationship with the depositor that is not based on contract "but is instead based on property."100 Ownership remains with the depositor, and the custodian undertakes a fiduciary duty to care for the property of the depositor and return it upon demand.¹⁰¹

By contrast, a general deposit "is essentially a loan transaction" based "on contractual rights" under which a depositor lends funds in exchange for receiving credit to her account, thus creating a debtor/creditor relationship. 102 The depositor thus transfers ownership and right to use the deposited assets to the bank/custodian. 103

Before applying these concepts to bitcoin custody, it is important to understand that much of the applicable case law in this area has developed in the area of U.S. state and federal banking law, which generally prohibits the taking of "general" deposits by non-banks. We are not currently aware of any U.S. state or federal regulator who has expressly stated that the deposit-taking restrictions under its banking laws apply to custodial holdings of bitcoin (which are otherwise subject to applicable state stored value regulation), and an analysis of banking law implications is outside the scope of this white paper, in any event.

However, given the novelty of bitcoin, a court assessing parties' legal rights in a bitcoin custodial context will presumably look to the closest analogues for persuasive legal authority (even if not exactly on point). To that end, banking case law on "specific" versus "general" deposits may be a likely analogue for whether property rights have been transferred to a custodian (akin to a "general deposit") or retained by the depositor (akin to a "special deposit").104 Thus, while the cases discussed in the following sections generally refer to "banks" and deposits of "money," our citation of those cases is intended for purposes of analogy to the bitcoin custodial context. 105

>> IMPORTANCE OF PARTIES' AGREEMENT TO CLASSIFICATION OF DEPOSIT

In the absence of an agreement and proof to the contrary, a deposit is presumed to be general rather than special in the United States. 106 Under the common law of many states, a special deposit is the delivery of either money or chattel to a bank under a special agreement or under circumstances sufficient to create a trust.¹⁰⁷ Thus, proving the existence of a special deposit requires an express or clearly implied agreement that the deposit is for a particular purpose. 108



WHILE AN IMPLICIT agreement could theoretically suffice to overcome the general deposit presumption, the existence of a written agreement explicitly obligating the bank to segregate deposited funds and leaving legal title with the depositor—seems to be, practically, the dispositive issue in deciding whether a deposit is special.

However, the depositor does not necessarily rebut the general deposit presumption by proving only that a deposit was intended for a specific purpose.¹⁰⁹ In many special deposit cases, courts sought, but did not often find, an explicit contract in which the bank had a duty to segregate deposited funds from its own assets.¹¹⁰ While an implicit agreement could theoretically suffice to overcome the general deposit presumption, the existence of a written agreement—explicitly obligating the bank to segregate deposited funds and leaving legal title with the depositor—





seems to be the dispositive issue in deciding whether a deposit is special.¹¹¹ In some jurisdictions, a further requirement for a special deposit to exist is that it should be agreed that the identical money or chattel deposited should be returned. 112 Note, however, that there is also authority that a special deposit of money does not become a general one simply because the bank is not bound to return the identical money or chattel received. 113

Furthermore, if an agreement has not been made or is ambiguous, a court may look to whether the bank had actual knowledge of the deposit source.¹¹⁴ Notably, a court may determine that a special deposit was made "by implication" if the bank had actual knowledge of a third party's interest in the deposit (e.g., if the account is specifically designated as an "escrow" account).115

>> POSSIBLE IMPLICATIONS FOR BITCOIN CUSTODY

In the bitcoin context, as noted above, distinguishing between general and special deposits requires examination of the agreement between the custodial holder with the user to determine if their relationship is one of creditor and debtor or bailor and bailee. In each case, there is likely to be a written agreement (such as online terms of service) between the receiver of bitcoin and the depositor containing an integration clause, and it is therefore such agreement that courts will look to in determining whether a general or special deposit of bitcoin has been made.



CUSTODIAL HOLDINGS OF bitcoin generally vary in two significant aspects: whether they are pooled or segregated, and whether the private keys are maintained by the custodian alone, jointly with the user, or not at all.

Custodial holdings of bitcoin generally vary in two significant aspects: whether they are pooled or segregated, and whether the private keys are maintained by the custodian alone, jointly with the user, or not at all. In a pooled custodial arrangement, the custodian generally has sole control over the private key to the public address holding the bitcoins, because each user obviously should not have access to the other users' bitcoins that are commingled with hers. However, in a segregated custodial arrangement where each user has her own bitcoin public address, the user can either control the private key herself, with no access to the unencrypted private key by the service provider (who in this case would not be a custodian),¹¹⁶ establish a multi-signature arrangement in which control of private key(s) is allocated between the user and custodian (or service provider),117 or have no control over the private key, relying on the custodian to follow the user's instructions with respect to the bitcoins stored at that public address.118

In the case of a service provider that does not hold or store sufficient private keys to unlock UTXOs associated with public addresses, it does not appear that any deposit exists (whether general or specific), because the provider never receives or has custody over user bitcoins. In the case of a custodian that holds sufficient or necessary private keys on behalf of users, such relationship may be deemed a deposit. As noted above, a deposit is presumed to be general unless the requirements for a special deposit are met.

The factors that would increase the likelihood of a special deposit being found by a court are the existence of an agreement specifying that the deposit is for a special purpose, obligating the custodian to segregate deposited bitcoins and leaving legal title with the depositor. The obligation of the custodian to return the exact bitcoins





deposited, rather than the equivalent number of bitcoins from another source, would also indicate a special deposit rather than a general deposit.

The cases cited above generally require segregation of custodial assets from the custodian's own assets; they do not appear to impose any requirement that the assets of individual users be segregated from each other. The Federal Deposit Insurance Corporation ("FDIC") rules for determining the owners of deposits placed at insured depository institutions by agents or custodians appear to support this inference. When such requirements are satisfied, the depositor rather than the agent or custodian is treated as the owner of the deposit.¹¹⁹

First, the agency or custodial relationship must be disclosed in the account records of the custodial institution.¹²⁰

Second, the identities and interests of the actual owners must be disclosed in the records of the custodial institution or records maintained by the custodian or other party.¹²¹

Third, the deposits actually must be owned (under the contract between the parties or any applicable law) by the named owners and not by the custodian. ¹²² By analogy, a custodian holding user bitcoins in a pooled wallet could disclose such custodial relationship and specify that the bitcoins reflect a special deposit on the blockchain (perhaps through public notes or metatags embedded within transactions depositing bitcoins into the pooled wallet). The custodian should also maintain records of the identities and interests of its users in the pooled wallet.

Accounting practices could support a finding of a special deposit under this "actual ownership" factor. For instance, we understand that hosted wallet providers, in general, only store customers' bitcoins and do not lend or use such bitcoins in any manner. Consistent with that business model, we also understand that such hosted wallet providers have historically not held customers' bitcoins on their own balance sheets.

Fourth, and finally, the contract between the custodian and its users should specify that users own the deposited bitcoins, not the custodian.

If these conditions are met, the depositors should be treated as the owners of the bitcoins held in the pooled wallet, not the custodian, and hence the deposited bitcoins are more likely to be deemed a special deposit rather than a general deposit, even if individual bitcoin balances are not segregated from one another.





Endnotes

- 1 Partner, Perkins Coie LLP. Chair of Perkins Coie's Financial Technology industry group and Blockchain Technology & Digital Currency industry group.
- 2 Associate, Perkins Coie LLP. Member of Perkins Coie's Financial Technology industry group and Blockchain Technology & Digital Currency industry group.
- 3 Logan v. Zimmerman Brush Co., 455 U.S. 422, 430 (1982) (citing various examples in which property interest was found).
- 4 Bd. of Regents of State Colls. v. Roth, 408 U.S. 564, 577 (1972); see also Logan, 455 U.S. at 430 (emphasizing that "the hallmark of property" is "an individual entitlement grounded in state law").
- 5 Note that property rights may also be conferred by federal statutes (such as the Copyright Act and Patent Act), which would preempt any conflicting rights granted under state law. See G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc., 958 F.2d 896, 903-04 (9th Cir. 1992).
- 6 For a helpful overview of bitcoin and blockchain technology, see generally Andreas Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies (O'Reilly Media, 2014) (Kindle ebook).
- 7 In multi-signature arrangements, more than one signature by a private key may be needed to prove ownership and unlock bitcoins from a public address. See Antonopoulos, supra note 6 loc. 2448.
- 8 Antonopoulos, supra note 6 loc. 1466.
- 9 Id. locs. 1494, 1513.
- 10 *ld* loc 1479
- 11 Id. loc. 2807.
- 12 Samvit Jain, et al., "Determining an Optimal Threshold on the Online Reserves of a Bitcoin Exchange," Princeton Univ., Dept. of Computer Science, http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_68-2.pdf.
- 13 Antonopoulos, supra note 6 loc. 2807.
- 14 *ld* loc 2811
- 15 Id.
- 16 *Id.* In a notable exception to this principle, so-called "coinbase" transactions are included in the first transaction in each new block as a reward to the "winning" miner (i.e., the one who solved the cryptographic puzzle generated by the bitcoin algorithm for the applicable block). Because coinbase transactions reflect newly created bitcoins, they do not technically have an "input" and thus create outputs from nothing. *Id.* locs. 2836, 2840.
- 17 *Id.* loc. 3057.
- 18 Id. locs. 2834, 3136.
- 19 Id. loc. 3136.
- 20 Oil transport serves as a useful analogy to this characteristic, as discussed in Part 4, infra.
- 21 See infra Part 4.
- 22 Cal. Civ. Code § 654 (West 2016).
- 23 Downing v. Mun. Court, 88 Cal. App. 2d 345, 350 (1948) (internal citation and quotation marks omitted).
- 24 Rasmussen, 958 F.2d at 903.
- 25 337 F.3d 1024, 1030 (9th Cir. 2003). California courts have recently and repeatedly cited *Kremen* when assessing intangible property rights. *See, e.g., Welco Elecs., Inc. v. Mora*, 223 Cal. App. 4th 202 (2014).
- 26 Kremen, 337 F.3d at 1030. Note that other jurisdictions have assessed domain names somewhat differently from Kremen, for instance, by concluding that they are a form of tangible property. See Daniel Hancock, You Can Have It, But Can You Hold It?: Treating Domain Names as Tangible Property, 99 Ky. L.J. 185 (2011).
- 27 See, e.g., Terarecon, Inc. v. Fovia, Inc., No. C 05-4407 CW, 2006 WL 1867734, at *9 (N.D. Cal. July 6, 2006).
- 28 In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012); see also Thompson v. Home Depot, Inc., No. 07CV1058 IEG WMC, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007).
- 29 See, e.g., Thompson v. Home Depot, Inc., No. 07CV1058 IEG WMC, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007).





- 30 Courts applying the laws of other U.S. jurisdictions have employed similar reasoning regarding protectable property interests in electronic data. See, e.g., Dwyer v. Am. Express Co., 273 Ill. App. 3d 742 (1995) (sale of cardholder names to various merchants did not state a claim for tortious appropriation because cardholder's name has little or no intrinsic value apart from its inclusion on a categorized list); In re Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) ("There is ... no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large."); Thyroff v. Nationwide Mut. Ins. Co., 8 N.Y.3d 283, 292 (2007) (employee had conversion remedy against his former employer with respect to valuable personal data, including his list of professional contacts, which had been stored on his work computer and kept from the employee after his termination).
- 31 Although the bitcoin recipient (i.e., the new owner) does not take the affirmative step of registering its UTXO ownership, unlike the domain name owner in *Kremen*, the critical fact is that the bitcoin recipient's address is recorded on the blockchain just as the domain name owner's website is recorded on a registry. Thus, for relevant purposes, ownership is publicly recorded in a materially similar manner in both cases.
- 32 This was also a factor emphasized in *Rasmussen*, where the court, citing longstanding U.S. Supreme Court precedent, observed that "the law generally favors the establishment of property rights" to reward and promote creation and innovation. 958 F.2d at 900 (citing *Int'l News Servs. v. Assoc. Press*, 248 U.S. 215 (1918)); see also id. at 903 (discussing importance of protecting "reasonable investment-backed expectations" in exclusive control of property).
- 33 See generally Don Tapscott & Alex Tapscott, Blockchain Revolution (Portfolio Press 2016).
- 34 Moreover, as Peter Van Valkenburgh has argued, the manner in which value has been created in bitcoin is analogous to other forms of property, such as gold or platinum. See Peter Van Valkenburgh, "Framework for Securities Regulation of Cryptocurrencies," CoinCenter Report, at 2 (Jan. 25, 2016), http://www.coincenter.org/2016/01/securities-framework/ (follow "available here" hyperlink) (arguing that the "value placed on gold by society," like that of bitcoin, "is largely a sort of mutually shared desire" and communal "decision to value these finite solutions [i.e., to problems generated by blockchain for purposes of mining] and therefore make the effort to uncover them").
- 35 Vested, Black's Law Dictionary (10th ed. 2014).
- 36 As property law scholars have argued, there should be criminal consequences in the event that bitcoins are stolen or otherwise misappropriated. See infra note 43 and accompanying text. And as discussed above, civil law remedies (in the form of a conversion action) should also be available. See supra note 27 and accompanying text. We note, however, that a civil law conversion remedy may be unavailable in jurisdictions which (unlike California) follow the rule that intangible property can only be converted where the property rights are merged in a document. See Xereas v. Heiss, 933 F. Supp. 2d 1, 7 (D.D.C. 2013) (citing Restatement (Second) of Torts § 242 (1965)).
- 37 See 26 C.F.R. § 1.482-4(f)(3) (setting forth rules for identifying owner of intangible property for tax purposes where laws of an applicable jurisdiction are silent on the matter).
- 38 Joshua Fairfield, BitProperty, 88 S. Cal. L. Rev. 805 (2015); Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 Wash. & Lee L. Rev. Online 22 (2014).
- 39 As Prof. Fairfield explains, tangibility has long been used as a proxy for scarcity and rivalrousness, which are key rationales underlying property rights (e.g., insofar as a person has a legitimate claim to exclude others, as discussed in *Kremen*). Fairfield, *supra* note 38, at 854.
- 40 Fairfield, *supra* note 38, at 874 (observing how courts have at times "assumed that traditional property rules are simply inapplicable to online information-based resources" and that "a theory of property as information" is needed). Although outside the scope of this article, we note that the rights associated with other digital assets will become an increasingly important issue as virtual reality technology continues to develop.
- 41 Bayern, supra note 38, at 30-33.
- 42 Id. at 34.
- 43 Id.
- 44 See Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001, Department of the Treasury, Financial Crimes Enforcement Network (Mar. 18, 2013).
- 45 18 U.S.C. § 981(a)(1)(A).
- 46 U.S. v. All Funds Distributed To, or o/b/o Weiss, 345 F.3d 49, 55 (2d Cir. 2003); U.S. v. Cherry, 330 F.3d 658 (4th Cir. 2003); 3 Criminal Practice Manual § 107:4 (June 2016).
- 47 4A Charles Alan Wright & Arthur R. Miller, Federal Practice & Procedure Civil § 1070 (4th ed.).
- 48 No. CV ELH-15-3692, 2016 WL 3049166, at *1 (D. Md. May 31, 2016). Note that this magistrate recommendation for a default judgment is still pending and is subject to approval by a district court judge.
- 49 Although related to violations of money laundering laws (instead of MSB regulation), we note that bitcoins belonging to Ross Ulbricht, the former head of Silk Road, were also found to be "property" subject to civil for
- 50 United States v. \$133,420.00 in U.S. Currency, 672 F.3d 629, 637 (9th Cir. 2012).
- 51 Id. (citations omitted).





- 52 In order to be subject to the CEA and the regulatory oversight of the CFTC, a transaction must in the first instance involve a "commodity," a term that is defined very broadly by Section 1a(9) of the CEA to include, in addition to physical commodities, various financial interests (such as currencies, interest rates and financial indices), as well as all services, rights and interests on which futures contracts are based. 7 U.S.C. § 1a(9).
- 53 Press Release: PR7231-15, CFTC Orders Bitcoin Options Trading Platform Operator and its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering (Sept. 17, 2015), http://www.cftc.gov/PressRoom/PressReleases/pr7231-15.
- 54 The CEA and related CFTC rules distinguish commodities by type: agricultural commodities, excluded commodities and exempt commodities.

 Generally speaking, agricultural commodities are derived from plants or living organisms, excluded commodities are financial references such as currencies, indices and interest rates, and exempt commodities are any commodity other than an agricultural or an excluded commodity. 17 C.F.R. §1.3(zz); 7 U.S.C § 1a(19). A precious metal is an example of an exempt commodity.
- 55 Press Release: PR7380-16, CFTC Orders Bitcoin Exchange Bitfinex to Pay \$75,000 for Offering Illegal Off-Exchange Financed Retail Commodity
 Transactions and Failing to Register as a Futures Commission Merchant (June 2, 2016), http://www.cftc.gov/PressRoom/PressReleases/pr738016
- 56 Separately, we note the CFTC's 2012 interpretation regarding the circumstances under which agreements, contracts or transactions in environmental commodities will satisfy the so-called "forward contract exclusion" from the definition of swaps (which are otherwise subject to CFTC regulation). Although this interpretation did not address bitcoin and a detailed description is outside the scope of this white paper, we note that environmental commodity transactions are fairly analogous in concept to bitcoin. Since the CFTC's interpretation reasoned that environmental commodity transactions were capable of being "delivered" and "consumed"—characteristics that appear to be common to any commodity that would constitute property—this interpretation further supports the view that bitcoin may constitute property. Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping; Joint Final Rule, 77 Fed. Reg. 48208, 48233 to 48235 (August 13, 2012).
- 57 I.R.S. Notice 2014-21, 2014-16 I.R.B. 938 (April 14, 2014) § 4, A-1.
- 58 Order on Motion for Partial Summary Judgment, In re Hashfast Techs., LLC, No. 14-3011DM (Bankr. N.D. Cal. Feb. 22, 2016), see also John F. Libby & Jacqueline C. Wolff, "California Bankruptcy Judge Rules that Bitcoin Is Property, Not Convertible Currency, For Valuation Purposes Under Fraudulent Transfer Laws," Lexology, Mar. 24, 2016 (reporting on related oral ruling from judge on Feb. 19, 2016), http://www.lexology.com/library/detail. aspx?g=d80f280b-43e7-4168-bd7e-2d007a5652f5.
- 59 Libby & Wolff, supra note 58.
- 60 11 U.S.C. § 550(a).
- 61 Libby & Wolff, supra note 58.
- 62 Id.
- 63 Id.
- 64 N.Y. Comp. Codes R. & Regs. tit. 23, §§ 200.1–200.22 ("23 NYCRR"). To the extent other U.S. states regulate cryptocurrency activity, they have generally chosen to do so thus far through existing money transmitter regulation. However, note that the Uniform Law Commission ("ULC") is in the process of drafting a model cryptocurrency state regulation. See ULC Regulation of Virtual Currencies Business Act (Draft for Discussion at July 8 July 14, 2016 Annual ULC Meeting), http://www.uniformlaws.org/shared/docs/regulation%20of%20virtual%20currencies/2016AM_VirtualCurrencyBusinesses_Draft.pdf (hereafter "ULC July 2016 Draft Model Cryptocurrency Regulation").
- 65 23 NYCRR § 200.9(c) (emphasis added).
- 66 Asset, Black's Law Dictionary (10th ed. 2014) (emphasis added).
- 67 Although the ULC model cryptocurrency regulation is still being drafted, we note that the latest draft similarly refers to cryptocurrencies as an "asset." See ULC May 2016 Draft Model Cryptocurrency Regulation, supra note 63, § 207(a)(1).
- 68 23 NYCRR § 200.12(c)
- 69 1 N.Y. Jur. 2D Abandoned Property § 23; N.Y. Abandoned Prop. § 103 (McKinney 2004).
- 70 Uniform Law Commission, Legislative Fact Sheet, Uniform Fiduciary Access to Digital Assets Act, Revised (2015), http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015).
- 71 Id.
- 72 Uniform Law Commission, Uniform Fiduciary Access to Digital Assets Act, Revised (2015), http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2015_RUFADAA_Final%20Act_2016mar8.pdf.
- 73 Uniform Law Commission, Act Summary, Uniform Fiduciary Access to Digital Assets Act, Revised (2015), at p. 2, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Revised%202015/Revised%20UFADAA%20-%20 Summary%20-%20March%202016.pdf.
- 74 Uniform Law Commission, Enactment Status Map, Uniform Fiduciary Access to Digital Assets Act, http://www.uniformlaws.org/LegislativeMap.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015).





- 75 In this section, we discuss the UCC in general terms. However, in light of this white paper's illustrative focus (where applicable) on California law, we also note that the cited UCC provisions in this section have been implemented in California statutes.
- 76 D. Fenton Adams, Sales of Personal Property as Secured Transactions Under Article 9 of the Uniform Commercial Code, 31 U. Ark. Little Rock L. Rev. 1, 1 (2008); see also id. at 3–4 (citing related principles articulated by Professor Grant Gilmore, one of the principal drafters of the UCC).
- 77 UCC §§ 9-102(a)(12).
- 78 See supra note 31 and accompanying text.
- 79 George Fogg is a partner at Perkins Coie LLP.
- 80 See Jeanne L. Schroeder, Bitcoin and the Uniform Commercial Code, Social Science Research Network, Aug. 22, 2015, at. 12, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2649441; George Fogg, "The UCC and Bitcoins: Solution to Existing Fatal Flaw," Bloomberg BNA (Apr. 1, 2015), http://www.bna.com/ucc-bitcoins-solution-n17179924871/.
- 81 Bitcoin public addresses are "pseudoanonymous" in the sense that they are not inherently traceable to a natural person, but are capable of such tracing if analyzed in context of other activities and factors. For example, if a certain bitcoin address were regularly used to purchase groceries from the same corner store, and the store's surveillance video and/or employees allowed identity of that natural person, a strong presumption could arise that the same person (or persons acting with her authority) conducted other transactions involving the same public address on the blockchain.
- 82 See, e.g., Ryan J. Straus & Matthew J. Cleary, The Law of Bitcoin: The United States 187 (Jerry Brito, ed., iUniverse 2015).
- 83 See, e.g., Myron Kove, et al., Bogert's Law of Trustes and Trustees § 249, at 2 (2015) (explaining, with regard to land trusts, that "[p]rivacy of ownership is provided since the sole document recorded is the trust deed showing only the number of the confidential trust agreement in which the identities of the beneficiaries are disclosed.").
- 84 See supra note 24 and accompanying text. As a practical matter, the pseudoanonymity of bitcoin may also be partially a function of how nascent the technology is. It may therefore diminish over time as the technology and related regulatory regimes mature.
- 85 Fairfield, supra note 38, at 845
- 86 Thomas Merrill & Henry Smith, Optimal Standardization in the Law of Property: The Numerus Clausus Principle, 110 Yale L. J. 1, 4 (2000).
- 87 Fairfield, supra note 38, at 845.
- 88 Merrill & Smith, supra note 86, at 19-20.
- 89 See supra note 24 and accompanying text.
- 90 See supra Part 4.
- 91 Antonopoulos, supra note 6, loc. 3274
- 92 Corbello v. DeVito, 777 F.3d 1058, 1064, 1066 (9th Cir. 2015) (citing 17 U.S.C. §§ 201(a), 201(d), and discussing how component parts of a copyright can be "chopped up and owned separately").
- 93 See, e.g., Anne Friedman, "Joint Ownership of Intellectual Property: Complexity That Only a Lawyer Could Love," DLA Piper (Oct. 6, 2014), https://www.technologyslegaledge.com/2014/10/joint-ownership-of-intellectual-property-complexity-that-only-a-lawyer-could-love/.
- 94 See, e.g., Patrick Murck, Presentation at Harvard Univ. Berkman Center for Internet & Soc'y: Property law and the blockchain (Oct. 20, 2015), https://cyber.law.harvard.edu/events/luncheon/2015/10/Murck.
- 95 Id.
- 96 Id.
- 97 Aswath Damodoran, Presentation at the N.Y. Univ. Stern School of Business: The Value of Intangibles, at 7, http://people.stern.nyu.edu/adamodar/pdfiles/ovhds/dam2ed/intangibles.pdf.
- 98 See, e.g., Tri Cty. Wholesale Distribs., Inc. v. Labatt USA Operating Co., LLC, No. 15-3710/3769, 2016 WL 3618970, at *7 (6th Cir. July 6, 2016) (detailed analysis of claims involving distinction between diminished brand values and lost profits).
- 99 See Fogg, supra note 80.
- 100 See Marek Dubovec, The Law Of Securities, Commodities & Bank Accounts: The Rights Of Account Holders, 120 (Edward Elgar Publishing Ltd. 2014).
- 101 *Id.*
- 102 Id. at 121.
- 103 *ld*.
- 104 Although much of the analysis in this white paper has used California law for illustrative purposes, we survey a broader range of jurisdictions in this section. In part, this is because the general vs. specific deposit concepts have been developed more thoroughly in jurisdictions where banking activity is concentrated (New York, in particular). We also look at federal banking regulations that may serve as persuasive authority.





- 105 Of course, as Prof. Bayern has discussed, there are important functional distinctions between banking and bitcoin custody that could limit the applicability of the banking law precedent discussed here. See Bayern, supra note 38, at 26 (discussing such differences and proposing that specific performance would be the appropriate remedy for a bitcoin depositor against a custodian).
- 106 Rio v. Army Aviation Ctr. Fed. Credit Union, 82 B.R. 138 (M.D. Ala. 1986); Swan Brewery Co. v. U.S. Trust Co. of N.Y., 832 F. Supp. 714 (S.D. N.Y. 1993); In re Smith, 51 B.R. 904 (Bankr. M.D. Ga. 1985); Peoples Westchester Sav. Bank v. FDIC, 961 F.2d 327, 332 (2d Cir. 1992).
- 107 See, e.g., Hudnall v. Tyler Bank & Trust Co., 458 S.W.2d 183 (Tex. 1970); Sec. Fund Servs., Inc. v. Am. Nat'l Bank & Trust Co. of Chi., 542 F. Supp. 323 (N.D. Ill. 1982); Hossain v. Rauscher Pierces Refsnes, Inc., 46 F. Supp. 2d 1164 (D. Kan. 1999); Masi v. Ford City Bank & Trust Co., 779 F.2d 397 (7th Cir. 1985).
- 108 Peoples Westchester Sav. Bank, 961 F.2d at 331.
- 109 Swan Brewery Co., 832 F. Supp. at 719 ("The fact that funds are deposited for a specific purpose is not determinative of the question of whether an account is general or specific.") (citation omitted); In re Kountze Bros., 27 F. Supp. 1002, 1003–04 (S.D.N.Y. 1938) ("The mere fact that the funds were here deposited for a special purpose ... is quite consistent with the ordinary debtor-creditor relationship.") (citations omitted).
- 110 See Peoples Westchester Sav. Bank, 961 F.2d at 331 (no special deposit because "documents generated in opening the [account] do not evidence that [the bank] assumed a duty to segregate those funds from its own general assets" and that "there was no explicit agreement ... to segregate [deposited] funds"); Keyes v. Paducah & I.R. Co., 61 F.2d 611, 613 (6th Cir. 1932) (no special deposit because the court "fail[ed] to find in any ... instruments ... any indication that it was the intention ... of the parties that the avails of the draft were to be segregated and kept as a separate fund"); In re Kountze Bros., 27 F. Supp. at 1004-05 (no special deposit when "[n]one of the reclaimants established that it ever required or requested [the debtor] to segregate the funds transmitted, from the bank's general funds, or not to use the funds in their own business").
- 111 Merrill Lynch Mortg. Capital, Inc. v. FDIC, 293 F. Supp. 2d 98 (D.D.C. 2003).
- 112 Sec. Fund Servs., 542 F. Supp. 323; First Nat'l Bank of Blue Island v. Estate of Philp, 106 Ill. App. 3d 360 (1982).
- 113 Union Elec. Light & Power Co. v. Cherokee Nat'l Bank of St. Louis, 94 F.2d 517 (8th Cir. 1938) (holding that an agreement in connection with special deposits of money that the bank need not keep for the depositor the identical money received, provided that an equal amount was maintained in the special account, does not change the character of the deposits from special to general); Genesee Wesleyan Seminary v. U.S. Fid. & Guar. Co., 247 N.Y. 52 (1928) (holding that a trust fund deposited in a bank may amount to a special deposit, although it is the duty of the bank to hold, not the identical bills or coins, but an equivalent sum, to be kept intact for the use of the depositor); Marchant v. Summers, 79 F.2d 877 (4th Cir. 1935) (holding that identical bonds need not be returned to plaintiff, but merely bonds of the same issue, denomination, and value).
- 114 Dubovec, *supra* note 100, at 121.
- 115 Id. (citing Aetna Cas. & Sur. Co. v. Atl. Nat'l, 430 F. 2d 574, 577 (5th Cir. 1970) and Carl v. Republic Sec. Bank, 282 F. Supp. 2d 1369 (S.D. Fla. 2003)).
- 116 For example, the wallet service offered through Blockchain.info, https://blockchain.info/wallet.
- 117 See supra Part 4.
- 118 For example, the wallet service offered by Coinbase, https://coinbase.com.
- 119 Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms; Notice of New General Counsel's Opinion No. 8, 73 Fed. Reg. 67155, 67156 (Nov. 13, 2008).
- 120 See 12 CFR 330.5(b)(1).
- 121 See 12 CFR 330.5(b)(2).
- 122 See 12 CFR 330.3(h); 12 CFR 330.5(a)(1).

This white paper is not legal advice. No attorney-client relationship with Perkins Coie LLP is created by review, citation or use of the information in this white paper.

