1-1-2017

The Commercial Law of Bitcoin and Blockchain Transactions

Stephen M. McJohn
Suffolk University, smcjohn@suffolk.edu

Recommended Citation
47 Uniform Com. Code L.J. 187 (2017-2018)

The Commercial Law of Bitcoin and Blockchain Transactions

By Stephen McJohn and Ian McJohn

Draft 11.16.16

Electronic copy available at: https://ssrn.com/abstract=2874463

There is great potential in Bitcoin,[1] the peer to peer cryptocurrency. Bitcoin allows payments without any intermediary, such as a bank, wire transfer office, or check cashing store. Bitcoin's underlying blockchain technology has many potential applications, from smart contracts to new methods of settling securities sales to transparent property ledgers. As the New York Times recently put it, "Against long odds, and despite an abstruse structure, in which supercomputers "mine" the currency via mathematical formulas, Bitcoin has become a multibillion-dollar industry. It has attracted major investments from Silicon Valley and a significant following on Wall Street."[2] Bitcoin and blockchain raise a host of legal issues, from regulation to taxation to basic property law. This paper focuses[3] on some issues likely to arise under the Uniform Commercial Code as Bitcoin and the blockchain find more uses.

Bitcoin and the Blockchain

Bitcoin[4] is a decentralized digital currency. This section describes how Bitcoin transactions work,[5] going into technicalities only as relevant to the paper's discussion of Bitcoin

---

The authors would like especially to thank Sarah Jane Hughes, Stephen Chow, Lorcan.Tiernan and Gary Monserud, who, along with Steve McJohn, discussed Bitcoin and blockchain, in Current Challenges with Payment Systems, at the conference Selling Goods into Foreign Markets, New England Law Boston (October 6, 2016); Stacy-Ann Elvy, for incisive comments on a draft; and Lorie Graham for inspiration.

1 The foundational papers on Bitcoin and smart contracts respectively are Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf; Nick Szabo, The Idea of Smart Contracts.

2 Nathaniel Popper, How China Took Center Stage in Bitcoin's Civil War, New York Times (JUNE 29, 2016), http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html

3 Among the many other issues are those of intellectual property. See Bailey Reutzel , The Looming War for Blockchain Patents (September 24, 2016), http://www.coindesk.com/looming-war-blockchain-patents/. Because software patents may be quite broad, many existing software patents may read on blockchain technology. The patents invalidated by Supreme Court's leading software patent case, Alice Corp. v. CLS Bank International, 573 U.S. __, 134 S. Ct. 2347 (2014), could be read to cover some smart contract systems. See claim 1 of US Patent No. 5970479 ("A computer-based data processing system to enable the formulation of customized multi-party risk management contracts having a future time of maturity . . ."); Alice at 2359 (""[t]he computer is itself the intermediary."").

4 On the general issues of regulating Bitcoin, see Sarah Jane Hughes and Stephen T. Middlebrook, Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries, 32 Yale Journal on Regulation (2015). For a very clear description of Bitcoin and analysis of its advantages and disadvantages and likely future, see Böhme, Rainer and Christin, Nicolas and Edelman, Benjamin G. and Moore, Tyler, Bitcoin: Economics, Technology, and Governance (July 15, 2014). Journal of Economic Perspectives, Vol. 29, Issue 2 - Spring 2015.

Electronic copy available at: https://ssrn.com/abstract=2874463

and commercial law.[6] Bitcoin's elegant design potentially offers a payment system with possible advantages over existing systems.[7]

Bitcoin relies on public key encryption, which enables people to send and receive encrypted messages even with total strangers. Each user needs two enormous numbers, comprising a private key and public key pair. A message can be encrypted with the private key or the public key, but can be decrypted only with both the private and public key. Each user keeps her private key private but can freely publish her public key, so others can send her encrypted messages and decode messages from her. Lee can send an encrypted message to Megan by encrypting the message with Megan's public key. If anyone intercepts the message, they cannot read the encrypted message. Megan alone can use her private key to decrypt the message. In the other direction, Megan can send a message to Lee and encrypt it with her private key. Anyone who intercepts this message, this time, can easily decrypt it with Megan's public key. The purpose is not to hide the message's contents, but rather to show that it indeed came from Megan, because only she has the private key. So Megan could post a public message signed with her private key, allowing anyone to read the message and to verify that it came from Megan, by decrypting with Megan's public key. If Megan wants to keep her message to Lee private, she simply encodes it with Lee's public key (and she can also sign with her private key, to authenticate that it came from her).

Althea has downloaded and installed bitcoin software, which is freely available.[8] Many people who use bitcoin do not use the bitcoin software, but rather work through an intermediary such as an exchange, that handles all the following on their behalf, somewhat like a bank acting as an intermediary handling the processing of checks and other items. Althea has 5 bitcoin sent to her by Orrin. Althea wishes to send the 5 bitcoin to Barkevius. Althea needs a bitcoin address

---

[5] This description relies on the masterful book, Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies (O'Reilly Media 2014). For a good collection of articles on Bitcoin and blockchain, see http://codingvalue.weebly.com/blockchain-reading-list.html; Brett Scott, AN EPIC LIST OF BITCOIN RESEARCH (ENGLISH), https://docs.google.com/spreadsheets/d/1VaWhbAj7hWNdiE73P-W-wrl5a0WNgzjofmZXe0Rh5sg/htmlview?usp=sharing&pli=1&sle=true.

[6] There are plenty of issues relating to Bitcoin and blockchain beyond those discussed here. See Jeanne L. Schroeder, Bitcoin And The Uniform Commercial Code, 24 U. Miami Bus. L. Rev. 1 (2016)(suggesting that bitcoin is a general intangible under Article 9 of the UCC, which could impede secured transactions, and that this may be mitigated because bitcoin could be sold through intermediaries selling Article 8 securities, and that smart contracts could be uncertificated securities under Article 8).

[7] See Schroeder, note 6 supra, at 6 ("The World Bank reports that, although they have fallen in recent years, international remittance fees (i.e. the money transmittal fees charged by intermediaries to migrants, frequently sending money to their families back home) average well over 7%. If a bitcoin transaction could be achieved for 1%, we could increase the aggregate family income of these typically impoverished people by billions of dollars virtually overnight.").

[8] Bitcoin software is open source, consistent with its goal of promoting transparency and avoiding centralized control. In addition, many would be reluctant to use it without access to the source code, given its capabilities.

for Barkevious, which is derived from his public key.[9]She formulates (her Bitcoin software will do all this) a message that basically says (using account numbers only, rather than names):

Input: Althea's account received 5 Bitcoin from Cesar's account

Output: Althea's account sends 4.9995 Bitcoin to Barkevious' account

In effect (we are signaling here that this description does not seek technical accuracy), she also signs the transaction with her private key, to authenticate it comes from her, and signs it with Barkevious' public key, so that only he can direct the Bitcoin onward, so now they effectively belong to him. Note that there is slightly less bitcoin going out than in – the difference is a transaction fee, which Althea offers to get the transaction processed, as we will see below.

Althea does not send the transaction to Barkevious. Nor does she send it to some central bitcoin processing center. Rather, she sends it to everyone on Bitcoin, meaning everyone who uses Bitcoin software, which networks the users together. To do so, she sends it to a few people on Bitcoin, and their software will quickly send the transaction to others, who send it on ("flooding" the network) and within seconds it will reach pretty much everyone on Bitcoin. No single ledger records bitcoin transactions. Rather, every user has their own[10] copy of the blockchain, a database that records every valid bitcoin transaction ever. On receiving Althea's transaction, it is trivial for each user's software to verify that the transaction is valid, meaning that Althea's account had unspent bitcoin to transfer, that she signed the message, and various technical requirements are met.

Everyone on the bitcoin network can very quickly verify that the transaction is valid. But the transaction does not yet get added to the blockchain, the list of valid bitcoin transactions. To do so would raise a risk of double-spending. Right after sending her transfer to Barkevious, Althea could cleverly make another transfer to someone else. If Althea's timing is good, that person would check the blockchain but not find the transfer to Barkevious, if it had not yet been propagated.

The unknown inventor of Bitcoin devised a brilliant, if laborious, method to keep the blockchain trustworthy, free of double-spending and similar exploits. Althea's transfer will be added to the blockchain only once, in a manner that prevents double-spending. A block of transactions may be added to the blockchain only by a *miner* who wins the race to add the next block to the blockchain.

---

9 To guard his identity, Barkevious' software may in fact generate a new public keys and bitcoin address for every transaction, which will in turn require him to safeguard the same number of private keys.

10 Not every user (or node) elects to have a copy of the blockchain, which by now is over 5 gigs of storage. Rather than being a "full node," users can use Bitcoin software that does not have a copy of the blockchain, or does not have other capabilities, such as the ability to mine Bitcoin, which is so resource intensive that now only miners with considerable resources are likely to win the right to add a block. See Antonopolous, supra note 5, at 142.

As a block of transactions is added to the blockchain, miners around the world begin the race to add the next block. To win the right to add a block of transactions to the blockchain, a miner must do the equivalent of guessing a number between 1 and 4,000,000,000,000.This somewhat absurd contest consists of assembling a block of recent transactions, verifying that they are valid, adding a nonsense number, then hashing that assembly of data. Hashing filters the data through a one-way process to get a number. If the resulting number falls within a very narrow range, the miner may put together a valid block. If not, the miner tries again, using a different nonsense number. The puzzle is trivial in a mathematical sense, because the miner will succeed if the miner tries enough times. But in all likelihood, it will take quadrillions of tries to get lucky. The lucky miner to first get a valid number sends out the valid block to the bitcoin network. The miner chooses which transactions to include in the block. That is why Althea provided a small transaction fee, as an incentive for miners to include her block. Bitcoin software around the world can verify the miner's hash, verify once again that the transactions in the block are valid, and add the block of transactions to the blockchain. Only now does Althea's transaction become part of the blockchain. This prevent double spending, because any other transaction that she tried to do with the same bitcoin cannot be in that block (or it would not be a valid block) or in a subsequent block (because that would not be a valid block).

Mining is laborious indeed. In the olden days (say, 2010), miners could run mining software using spare computing time while their computer also did other things (a little bit like the SETI project). For a computer, it's a long tedious wait between a user typing letters while word-processing. The computer could keep busy during the interim mining bitcoin. But as miners became more productive over time, the Bitcoin software increases the difficulty over time, to maintain the time between new blocks at ten minutes or so. Now, a successful miner needs lots of computing power, most likely in the form of arrays of circuits designed specifically for mining bitcoin.[11] The amount of processing power devoted to bitcoin worldwide is huge.[12] All bitcoin originate by being mined. The lucky miner that adds a block receives a chunk of bitcoin (hence, "mining" bitcoin), and also the transaction fees in the transfer. That is why Althea included a transaction fee. Had she not included it, miners would be less likely to include her transaction in a block. The bitcoins received per block is also programmed to diminish over time. In addition, the bitcoin software sets a limit on the number of bitcoin to be created. Once 21 million bitcoin have been created, there will be no more. At that time, miners will receive only transaction fees, which may have to increase to provide sufficient incentive. Note that although transaction fees paid by the parties to a bitcoin transaction are low, the transaction costs (mined bitcoin, the cost of electricity and computing) are considerable.[13] From the buyer's point of view,

[11] At first, miners just ran bitcoin software on their PC's. Then someone figured out that graphics cards could be efficiently used for bitcoin mining. Now, vendors sell ASIC's (Application Specific Integrated Circuits) that have been specially designed for bitcoin mining.

[12] Mining is costly in terms of computing power and the electric power to run it – if the miner pays for it. See Dutch Brothers in Court for *Bitcoin* Mining With Stolen Power, New York Times (Sept. 21, 2016). See also http://arstechnica.com/security/2016/09/thousands-of-infected-ftp-servers-net-attackers-88k-in-cryptocurrency/.

[13] https://www.bloomberg.com/view/articles/2014-01-02/bitcoin-is-an-expensive-way-to-pay-for-stuff.

this is not unlike credit cards, where a buyer does not appear to pay for using the card in a transaction, whereas the merchant may well pay considerable fees. For the recipient, however, the costs are shifted to the blockchain generally, as opposed to being borne by the merchant as with credit cards.

We can put that same process chronologically, to emphasize elements that will be important for applying commercial law to bitcoin. Bitcoin are created when a miner receives a transfer of bitcoin for mining a block. The miner may then transfer that bitcoin to someone else, who may transfer it on. A user does not have a collection of bitcoin. Rather, to have bitcoin means that the blockchain has a record of a valid transfer of bitcoin to an account of the user and the blockchain does not yet have a record of a transfer of that bitcoin to someone else. Because a block can be added to the blockchain only by a miner showing "proof of work," the blockchain provides a robust, trustworthy record of all valid bitcoin transfers that have ever occurred.

Bitcoin is not an anonymous system.[14] No one's name need be used. But every transfer identifies an account number of the sender and an account number of the recipient. A bitcoin user may have lots of accounts, even using a different one for every transaction. This is often called a pseudonymous system, because every participant is identified by a number, his or her account number. It may be possible to match the account number to a name using other information available online.[15] But matching numbers to names is not necessarily easy. In particular, software used often generates a new account for every transaction. In other payment systems, banks take care of all the details, in return for considerable fees. Many people who use bitcoin avoid these complexities by using an intermediary to handle their accounts and transactions.

Beyond bitcoin and other cryptocurrencies,[16] the underlying blockchain technology has excited many imaginations.[17] A blockchain, also known as a distributed ledger or distributed

---

[14] One consequence is that bitcoin transactions are not beyond legal discovery mechanisms. See Alice Huang, Reaching Within Silk Road: The Need for a New Subpoena Power That Targets Illegal Bitcoin Transactions, 56 B.C.L. Rev. 2093 (2015).

[15] Cf. Misha Tsukerman, The Block Is Hot: A Survey Of The State Of Bitcoin Regulation And Suggestions For The Future, 30 Berkeley Tech. L.J. 1127, 1137 (2015) ("The public key address contains no information about the user, and though Bitcoin users do enjoy a much higher level of privacy than users of traditional digital-transfer services, staying completely anonymous can be quite difficult. Without knowing to whom a public key address corresponded, in one experiment, researchers found that behavior-based clustering-techniques were able to reveal 40 percent of Bitcoin users.")

[16] Some see Bitcoin as unlikely to supplant existing payment systems, even if the underlying blockchain technology finds wide application. See *Bitcoin Seen as Little Threat to Payment Firms* (Feb. 24, 2014), BLOOMBERG, http://www.bloomberg.com/news/2014-02-24/bitcoin-seen-by-payment-networks-as-little-threat-to-dominance.html

[17] See Schroeder, note 6 supra, at 5 ("Putting aside a vocal minority of radical libertarians and anarchists, however, many bitcoin enthusiasts are concentrating less on its use as an alternative currency, per se, but on how its underlying technology--the blockchain--can be put to use for wide variety of uses, ranging from smart contracts to securities trading.")(footnotes omitted); Wright, Aaron and De Filippi, Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia (March 10, 2015). Available at SSRN: https://ssrn.com/abstract=2580664 (imaginative discussion of many possible applications of the blockchain); Don

database, could replace many centralized databases, such as ledgers or recording systems. A blockchain (unless access is restricted, requiring permission) allows anyone interested to see what valid transactions have occurred, allows free access without permission of a bank or government, and could be more efficient[18] than having all the parties keep separate ledgers or sets of books.[19] Financial firms have invested in developing blockchains for stock trading.[20] Blockchain ledgers could prove much more efficient and transparent in areas from real and personal property records[21] to patent ownership and assignment.[22] Vermont has enacted a statute providing that blockchain records will be legally effective in broad range of areas, including contracts, property records, and other types of record-keeping.[23] Centralized services like airbnb

---

Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World (Portfolio, 2016)(thorough description of many applications of the blockchain, with analysis of benefits and possible obstacles and costs).

[18] Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL. 837 (2015)

[19] Nathaniel Popper, DealBook|Central Banks Consider*Bitcoin's* Technology, if Not *Bitcoin* New York Times-Oct 11, 2016, http://www.nytimes.com/2016/10/12/business/dealbook/central-banks-consider-bitcoins-technology-if-not-bitcoin.html?_r=0 ("The central bankers do not want their institutions to own or use Bitcoin itself. Instead, they hope they can use the decentralized method of record-keeping introduced by Bitcoin — known as the blockchain or distributed ledger — to complete and record transactions in the real economy more efficiently, quickly and transparently.").

[20] Larissa Lee, New Kids on the Blockchain: How Bitcoin's Technology Could Reinvent the Stock Market, 2 Hastings Business Law Journal (2016)

[21] See generallyJoshua A.T. Fairfield, Bitproperty, 88 S. CAL. L. REV. 805 (2015); Trevor I. Kiviat, Beyond Bitcoin: Issues in Regulating Blockchain Transactions, 65 DUKE L.J. 569 (2015).

[22] Reuben Grinberg, Bitcoin: An Innovative Alternative Digital Currency, 4 HASTINGS SCI. & TECH. L.J. 159 (2012); (discussing legal issues of regulating Bitcoin as currency, a security, or a commodity); Kevin V. Tu and Michael W. Meredith, Rethinking Virtual Currency Regulation in the Bitcoin Age, 90 Washington Law Review 271 (2015); Mitchell Prentis, Digital Metal: Regulating Bitcoin as a Commodity, 66 Case W. Res. L. Rev. 609 (2015); Gregory M. Karch, Bitcoin, the Law and Emerging Public Policy: Towards a 21st Century Regulatory Scheme, 10 Fla. A&M U. L. Rev. (2014)(recommending that " Policymakers, starting with U.S. Congress and state legislatures, should develop public policies that recognize Bitcoin and digital currencies as possessing all of the following characteristics: currencies, payment systems, commodities, properties, investments, systems of commerce, and even systems of contracts.").

Commentators vary considerably on the basic question of how much regulation of Bitcoin is appropriate.Compare Derek Dion, Note, I'll Gladly Trade You Two Bits on Tuesday for a Byte Today: Bitcoin, Regulating Fraud in the E-Conomy of Hacker-Cash, 2013 U. ILL. J.L. TECH. & POL'Y 165 (2013)(analyzing regulation of Bitcoin under such regimes as counterfeiting, the Stamp Payments Act, and the Securities and Exchange Acts, and concluding "that Bitcoin should not be strictly outlawed" but rather regulated carefully); and Nikolei M. Kaplanov, Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation, 25 LOY. CONSUMER L. REV. 111, 1114 (2012)(arguing against "the notion of applying any sort of regulation to bitcoin use, arguing that it would be ineffective and contrary to the interest of the United States consumers"); Daniela Sonderegger, A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation, 47 Wash. U. J. L. &Pol'y 175 178 (2015) (arguing that " that Bitcoin should be allowed to function within a loosely defined legal framework and permitted to develop with only a minimal degree of governmental intervention"); Olivia M. George, Bridging Bitcoin's Gender Gap, 12 N.Y.U. J.L. & Bus. 423, 424 (2016)(providing "potential solutions to Bitcoin's gender problem, including targeted marketing and legal regulation that could in turn lead to the cryptocurrency's mainstream acceptance").

See also, Nathaniel Popper & Peter Lattman, *Winklevoss Twins Plan First Fund for Bitcoins*, N.Y. TIMES (July 1, 2013), http://dealbook.nytimes.com/2013/07/01/first-name-in-the-first-fund-for-bitcoins-winklevoss (discussing developing investment vehicles linked to price fluctuations of bitcoin)..

[23] See 12 V.S.A. § 1913, § 1913. Blockchain enabling:

or uber could face competition from blockchain models that are peer to peer.[24]Insurance could perhaps be a peer to peer business.[25]A blockchain based corporate structure could provide for broader participation in the governance of the entity.[26] A blockchain might function to provide a framework of rules equivalent to a legal regime.[27] The future of blockchain seems bright.[28]

Some advantages of a blockchain are that every user could have a copy of a single database, accessible to all (or a blockchain can have limited access or require permission, although that could detract from transparency), with records of every single transaction, and

---

(3) The following presumptions apply:
(A) A fact or record verified through a valid application of blockchain technology is authentic.
(B) The date and time of the recordation of the fact or record established through such a blockchain is the date and time that the fact or record was added to the blockchain.
(C) The person established through such a blockchain as the person who made such recordation is the person who made the recordation.
(D) If the parties before a court or other tribunal have agreed to a particular format or means of verification of a blockchain record, a certified presentation of a blockchain record consistent with this section to the court or other tribunal in the particular format or means agreed to by the parties demonstrates the contents of the record.
(4) A presumption does not extend to the truthfulness, validity, or legal status of the contents of the fact or record.
(5) A person against whom the fact operates has the burden of producing evidence sufficient to support a finding that the presumed fact, record, time, or identity is not authentic as set forth on the date added to the blockchain, but the presumption does not shift to a person the burden of persuading the trier of fact that the underlying fact or record is itself accurate in what it purports to represent.
(c) Without limitation, the presumption established in this section shall apply to a fact or record maintained by blockchain technology to determine:
(1) contractual parties, provisions, execution, effective dates, and status;
(2) the ownership, assignment, negotiation, and transfer of money, property, contracts, instruments, and other legal rights and duties;
(3) identity, participation, and status in the formation, management, record keeping, and governance of any person;
(4) identity, participation, and status for interactions in private transactions and with a government or governmental subdivision, agency, or instrumentality;
(5) the authenticity or integrity of a record, whether publicly or privately relevant; and
(6) the authenticity or integrity of records of communication.

[24] Tapscotts, supra note 17, at 115.

[25] With all deliberate speed. See Michael Abramowicz, Cryptoinsurance, 50 Wake Forest L. Rev. 671, 673 (2015)(" Nonetheless, this Article will argue that radical financial disintermediation in insurance is possible--perhaps not in the next decade, though possibly in the next half century.").

[26] Theodore W. Reuter, Bitcoin: A New Tool for Structuring Agreements and Managing Entities, 32 COMPUTER & INTERNET LAW. 16 (Jan. 2015).

[27] Michael Abramowicz, Cryptocurrency-Based Law, 58 Ariz. L. Rev. 359 (2016)(" A cryptocurrency can also be used to generate rules or other written codes. Peer-to-peer law might be useful when official decision-makers are corrupt or when agency or transactions costs are high.").

[28] It is worth remembering the old saw that predictions are difficult, especially about the future. One from 2003: "Ten years from now, people seeking routine legal advice might not even think of contacting their lawyer for help. Instead, a computer will use advanced artificial intelligence (AI) technology to answer questions, present options, prepare and file pleadings, and send them on their way. Where will lawyers fit in? They'll be busy writing software for these "legal expert systems." This is the forecast of Dr. L. Karl Branting, a lawyer and computer scientist who has written extensively about artificial intelligence and legal reasoning. "In the long run, there's no stopping it," says Branting."). As of 2013, lawyers were still handling routine matters and Siri was not. But just what was meant by routine matters was not clear, and the speaker made a distinction: "I think the routine practice of law will become automated, while the creative aspect won't be — that will remain the reserve of human experts."

transactions can be validated and recorded in minutes. That could provide transparency,[29] make transactions simple and streamlined, and allow anyone who wishes to use the system. For example, if a blockchain were used to record ownership of shares of a corporation, buyers and sellers could quite simply settle their transaction with a message to the block chain, without paying an intermediary, without the transaction going through the books of the numerous entities that are now required in settling stock sales, and without delay – the blockchain recording will take minutes, where stock sales today take days to finally settle.

Some disadvantages of a blockchain are that every user could have a copy of a single database, accessible to all, with records of every single transaction. Not everyone would like their every stock transaction permanently saved on a freely accessible database. If the database is open to all, that could permit gathering of information for all kinds of purposes (advertising, crime, data mining), the flip side of transparency. A blockchain register, however, might be configured to provide more privacy than some public records that are presently completely open.[30] Finally, putting everything into a single database is putting all the eggs in one basket. As Hilary Allen has pointed out, this creates a type of systemic risk.[31]For example, a majority of miners could work together to take control of the blockchain.[32] Someone could also exploit a flaw in the software to wreak havoc, as happened with the DAO, a blockchain-based investment vehicle, which sought to use blockchain technology to provide a new form of peer-to-peer corporate governance.[33] The very inefficiency of some existing recording systems may be a security feature.

---

[29] Christina Batog, Blockchain: A Proposal To Reform High Frequency Trading Regulation, 33 Cardozo Arts & Ent. L.J. 739 (2015)(suggesting that blockchain technology's transparency would remedy some of the ills of high-speed securities trading).

[30] See Tom W. Bell, Copyrights, Privacy, And The Blockchain, , 42 Ohio N.U. L. Rev. 439 (2016)

[31] Allen, Hilary J., $=€=Bitcoin? (May 18, 2016). Suffolk University Law School Research Paper No. 15-33. Available at SSRN: https://ssrn.com/abstract=2645001.

[32] Nathaniel Popper, How China Took Center Stage in Bitcoin's Civil War, New York Times (JUNE 29, 2016), http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-ch. ina.html ("At the time of the meeting, held at the Grand Hyatt hotel, over 70 percent of the transactions on the Bitcoin network were going through just four Chinese companies, known as Bitcoin mining pools — and most flowed through just two of those companies. That gives them what amounts to veto power over any changes to the Bitcoin software and technology. . . . But China's clout is raising worries about Bitcoin's independence and decentralization, which was supposed to give the technology freedom from the sort of government crackdowns and interventions that are commonplace in the Chinese financial world.")

[33] Nathaniel Popper, *Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency, New York Times (*JUNE 17, 2016), http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html. ("A hacker on Friday siphoned more than $50 million of digital money away from an experimental virtual currency project that had been billed as the most successful crowdfunding venture ever — taking with him not just a third of the venture's money but also the hopes and dreams of thousands of participants who wanted to prove the safety and security of digital currency."). An interesting question is whether the taking, which simply exploited the code, was a breach of contract or following the contract as implemented in the code. See Matt Levine, Blockchain Company's Smart Contracts Were Dumb

There are other possible technical considerations. Bitcoin-like blockchain technology could be used for the Internet of Things, in which every device from light fixtures to thermostats may be connected and programmable. But those devices may need only minimal computing power to function. Asking them to store a copy of a blockchain, recording billions of transactions of no relevance to them, may be quite inefficient. The devices presently in use have now[34] notoriously low levels of security, which could mean that someone might take control of them, including private keys giving authority to make blockchain transactions. Likewise, mining with its proof of work devours a lot of electricity, where there may be more efficient means to accomplish the tasks. There are likewise possible technical responses. Some blockchain schemes use proof of stake, allowing stakeholders to vote to verify transactions, as opposed to doing quadrillions of calculations.

Most relevant to the UCC, a blockchain could be a platform for smart contracts, transactions that are executed automatically.[35] Provided that the parties can code the conditions of the contract, once started it could proceed automatically, with coded consequences for performance or default by either party, making it unnecessary for either party to rely on the other or on the courts for enforcement. Some envision smart contracts as playing a role in communication between computers in the Internet of Things. Robots already do lots of the work in industrial settings, such as welding and assembling automobiles in factories. A future robot in a Detroit flying car factory might have the authority order necessary parts online, concluding a transaction with a fellow robot in the supplier's warehouse. Supply-chain financing might be an area where the numerous repeated similar contracts between the same players (buyers, sellers, and financers) might lend itself to smart contracts.[36]

Other applications (or "use cases") of blockchain smart contracts include "trade clearing and settlement" of securities transaction, which now "often entails labor-intensive activities that include various approvals and/or complex internal and external reconciliations."[37] Transactions that involve changes in electronic records of many stripes, from data involving health records to property records, could be handled in blockchain transactions. Music licensing could be

---

(JUNE 17, 2016), http://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb.

[34] David E. Sanger And Nicole Perlroth, A New Era of Internet Attacks Powered by Everyday Devices, New York Times, New York Times (OCT. 22, 2016) http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html. Although blockchain smart contracts are as yet mainly speculation, there are already concrete issues in the interplay of security issues and contract law for the Internet of Things, see Stacy-AnnElvy, Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond (August 1, 2015). Hofstra Law Review, Vol. 44, No. 839, 2016.

[35] For a paper identifying issues and analyzing how existing contract law and theory would fit with smart contracts, See Max Raskin, The Law of Smart Contracts, 2 GEO. TECH. REV. (forthcoming March 2017)

[36] Stephen Chow suggested this at the New England Law/Boston conference.

[37] Getting smart about smart contracts, http://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html

implemented through smart contracts. Digital copies of music included code that offered licensing, for a range of uses, subject to specified conditions and implemented through blockchain royalty payments. The fact that smart contracts may require no legal enforcement may make them attractive for illegal transactions[38] or legitimate transactions where privacy is prized. The increasing use of arbitration has already taken many commercial transactions out of the area of judicial enforcement. Smart contracts, within the set of contracts that could be so implemented,[39] could substitute pre-agreed outcomes for enforcement of the contract by third parties, while increasing certainty and reducing costs of monitoring performance

Tracing

An important practical issue for the commercial law of bitcoin is, whether bitcoin are traceable. If someone purloins a private key and absconds with the owner's bitcoin, can they be traced? If – an important issue for finance of entities that use bitcoin – bitcoin is used as collateral, can a lender trace bitcoin that has been[40] transferred?

As a technical matter, bitcoin may often be untraceable. One might think that, if every bitcoin transfer ever is recorded on the blockchain, tracing bitcoin should be simple.[41] If Althea transfers five bitcoin to Barkevious, who transfers them to Cordelia, who transfers them to Degas, then those five bitcoin could be readily traced. But the transfers are often not unitary, rather add some complexity to the issue. Many (perhaps most) transfers involve multiple input and/or output accounts. A typical transaction might see Althea use as inputs 5 bitcoin from Orrin and 6 bitcoin from Toni, with the outputs being 8 bitcoin to Fran and 3 bitcoin back to Althea's

---

38 A. Juels, A. Kosba, and E. Shi. The Ring of Gyges: Investigating the Future of Criminal Smart Contracts. (2015). For a collection of papers on smart contracts, see http://www.initc3.org/publications.html.

39 Gideon Greenspan, Why Many Smart Contract Use Cases Are Simply Impossible (April 17, 2016), http://www.coindesk.com/three-smart-contract-misconceptions/.

40 http://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-getting-smart-contracts.html

41 Some commentators appear to take this view. See Schroeder, note 6 supra, at 42 ("Each bitcoin transaction is unique and identifiable and all transfers are recorded. Accordingly, ownership in bitcoin is, therefore, not truly anonymous, but can be pseudonymous. Although the secured party may have difficulty identifying many owners of an encumbered bitcoin, it will always be able to identify the encumbered bitcoin itself. Consequently, if the original debtor defaults on the secured transaction, and the unencumbered bitcoin ever comes into the hands of an identifiable transferee, then the secured party would have the right to "repossess" it. Consequently, one of the advantages of using the blockchain for the transfer of value is that does away with the confusing metaphors of tracing rules that apply to deposit accounts and replace them with the reality of actual tracing."); Böhme et al, supra note 4, ("Indeed, each individual bitcoin can readily be traced back through all transactions in which it was used, and thus to the start of its circulation."); Sometimes tracing seems to be assumed. See Tsukerman, supra note 15, at 1128 ("The blockchain acts as an online record keeping system that tracks the ownership of specific Bitcoins from their creation (in a process called mining) through every subsequent transaction."). Others have flatly stated that bitcoins are not traceable. See, e.g., See Patrick Murck, Property Law and the Blockchain, at 19.13, 22.10, https://www.youtube.com/watch?v=nqmkAa5VNGc ("While transactions are traceable, the coins attached to those transactions are not traceable . . .You're not tracing the coins . . .The title to those coins is not colored because you can never fully establish that in the first place.).

account. The transaction simply lists input and outputs. One cannot say, as a technical matter, of the 11 input bitcoins, which 8 went to Fran and which 3 went back to Althea. Bitcoin do not have serial numbers or physical tokens. Similarly, a business might use as inputs all the bitcoin it has received in a single day to a particular account and output the sum back to another same account, to consolidate things for simplicity and to reduce transaction fees later on. Or someone who has received bitcoin might then use them as input to a transfer that divides them between various parties. To make things even murkier, "mixers" offer the service of masking bitcoin transactions specifically to make tracing impossible, by using many intermediate transactions to through any hounds off the scent.

In some cases, tracing might well be possible. If someone wrongfully transferred a huge amount of bitcoin, then that would be less likely to be mixed up with other transactions, unless our thief was managing to steal huge numbers of bitcoins from others as well.[42]Some have proposed "blacklisting" of accounts that have wrongfully received bitcoin, meaning getting miners across the network to decline to process transfers from such accounts.

In many cases, technically tracing bitcoin would not be practicable. But that does not end the inquiry.[43] Money is likewise difficult to trace, in the sense of following the path of each dollar. Suppose Ben, a bookkeeper, has $42,000 in his checking account. Ben deposits another $10,000, from a check he embezzled from work. He later wires $7,000 from the account to Janet. We cannot say as a technical matter whether that $7,000 came from the proceeds of the stolen check. But from a legal point of view, courts have developed many tracing doctrines, to decide whether it should be deemed that property can be traced to a certain source.[44]Such doctrines as first-in-first-out or lowest intermediate balance may be applied to trace property. Likewise, those could be applied to bitcoin, especially as the blockchain keeps a record of every transaction. Suppose Althea receives 5 bitcoin from Farah and then 6bitcoin from Sam. She uses those transactions as an input that sends 7 bitcoin to Tracy and sends 4 bitcoin back to Althea's account. Using FIFO, a court could deem that Farah's 5 bitcoins and 2 of Sam's bitcoin found their way to Tracy, and the other 4 of Sam's bitcoin are still with Althea. Or a court might deem a pro rata approach more appropriate, applying a 5/11 split to each output, on the theory that the

---

42 Recovering stolen bitcoin: a digital wild goose chase https://www.theguardian.com/technology/2013/dec/09/recovering-stolen-bitcoin-sheep-marketplace-trading-digital-currency-money ("

43 As one commentator put it, "When we consider whether it is possible in law to obtain the recovery of stolen cryptocurrency units, what matters is normative, rather than technical, traceability of the stolen units." Koji Takahashi, Technical traceability and normative traceability, Blockchain and Cryptocurrency Law blog, http://cryptocurrencylaw.blogspot.jp/2015/11/technical-traceability-and-normative.html (10 November 2015)

44 Richard L. Barnes, Tracing Commingled Proceeds: The Metamorphosis of Equity Principles into U.C.C. Doctrine, 51 U. Pitt. L. Rev. 281, 296 (1990)(" This "special property right", shorthand for the contractual relationship and its breach, should be given to all innocent victims of a wrongful commingling. Thus, it would be wrong to use the first-in, first-out method to establish priority among a number of innocent victims. Nor does the lowest intermediate balance rule consider the equality of footing among the innocents. Both devices work toward a predetermined advantage where no advantage should exist among the class of innocents. In re Oatway and James Roscoe, Ltd. v. Winder appropriately treated the innocents as a class and allowed them to recover pro-rata.").

bitcoin from Farah and Sam were divided proportionately in the output bitcoin. If Tracy had been somehow colluding with Althea to defraud Sam, maybe it would be more appropriate to deem that all Sam's bitcoin went to Tracy.

Nor does legal tracing require an exact trail. Where a cashier embezzled hundreds of thousands of dollars (in the 1940, when those dollars were worth much more) before committing suicide, the victims were entitled to claim the insurance of his life insurance policy, even though they could not show that the insurance premiums were paid with the specific proceeds of his defalcation.[45]Suppose many bitcoins go missing from an online marketplace, and the pilferer's partner subsequently cannot explain how she acquired a large sum of money that she used to buy a house. That may be sufficient to support tracing those assets to a person, even without identifying the intervening steps.[46] And they could be required to return funds or bitcoin they ended up with.[47]

Legal tracing doctrines can also account for facts beyond the blockchain.[48] Likewise, parties could work together to attempt to hide a trail. Suppose Althea wanted to send 15 bitcoin to Luis without leaving a trail on the blockchain. She could simply send 15 bitcoin to Lorie, and ask Lorie to send Luis 15 bitcoin from one of Lorie's other accounts. The blockchain would record only transfers from separate accounts. But of course a court that had evidence of Lorie's cooperation with Althea could easily deem the 15 bitcoin sent to Luis to be traceable to Althea. Whether a party has engaged in wrongdoing is considered in legal[49] tracing, as opposed to technological tracing.[50] Bitcoin could also be traced by associating them with other transactions by the same party (which also illustrates that bitcoin transactions are pseudonymous, but not anonymous). One bitcoin embezzler was tracked down by online sleuthing.[51]

---

45 See Constructive Trusts - Clear Tracing Held Unnecessary to Impose Constructive Trust on Insurance Proceeds Where Premiums Paid from Account of Embezzling Bank Officer, 59 Harv. L. Rev. 462 (1946)

46 Cf. Yessi Bello Perez, Czech Police Seize $345,000 Property Linked to Bitcoin Hack (April 1, 2015) http://www.coindesk.com/czech-police-seize-345000-property-linked-to-bitcoin-hack/

47 Cf. William Strunk, The Elements of Style (Harcourt, 1918).

48 Kavid Singh, *The New Wild West: Preventing Money Laundering in the Bitcoin Network*, 13 NW. J. TECH. & INTELL. PROP. 37, 60 (2015)(" While this anonymity problem poses challenges for law enforcement in the near term, money laundering in Bitcoin usually bleeds outside of the virtual network eventually. If the owner converts her bitcoins into USD at another Bitcoin currency exchange--which is the most likely scenario--the exchange will require her to provide identifying information for transactions pursuant to CTR and SAR requirements, thus leaving a trail outside of Bitcoin for law enforcement to follow.")(footnote omitted).

49 To be technically legally accurate, tracing is an equitable doctrine, as opposed to a legal doctrine, in the narrow sense of the distinction between law courts and equity courts.

50 Peter B. Oh, Tracing, 80 Tul. L. Rev. 849, 886 (2006) ("When the wrongdoer only withdraws funds from the bank account, the victim maintains a claim to a proportionate interest in the remaining traceable value. When, however, the wrongdoer has withdrawn and also deposited value within the bank account, courts use what is known as the "Lowest Intermediate Balance" rule; because there are multiple possible sources of value, the victim can claim only up to the lowest balance between the time of the wrongdoer's deposit and tracing")(footnotes omitted)

51 Why criminals can't hide behind Bitcoin, By John Bohannon, Science Mar. 9, 2016.

There are many variations. The point is that with bitcoin, as in many areas, the law has considerable flexibility to reach an appropriate conclusion even where a purely technical analysis would prevent determining some facts.[52] Other blockchain technologies may be more difficult to trace technically, because they may use technology that, unlike Bitcoin, does not make account numbers publicly available.[53]The same general principle would apply, however, because there may be information beyond the blockchain that permits tracing.

What are the implications for commercial practice? Creditors that loan against bitcoin as collateral should be aware that if the collateral is transferred, they may well not be able to trace it. But lenders have long dealt with a similar issue, when money in a bank account is collateral. In such loans, creditors can protect themselves by having the borrower use a "lock-box" account, which the creditor is able to control, preventing the collateral from wandering away. From the other perspective, anyone that takes bitcoin may have the risk that the bitcoin is someone's collateral, meaning its possible that the bitcoin will be traced and returned to the creditor. That problem does not exist with money, because Article 9 protects innocent transferees of money from an account (a rule intended to facilitate commerce, because otherwise anyone receiving payment might have to first do due diligence on the bank account, which would put considerable friction into commercial transactions). If cryptocurrencies gain more commercial use, jurisdictions may consider legislating similar protections. In the meantime, debtors who use cryptocurrencies and also put it up as collateral may seek waiver clauses in the security agreement, in order to facilitate liquidity. Moreover, innocent recipients of funds, as noted above, are less likely to be subject to tracing, which is an equitable doctrine that considers the fairness of the parties' conduct. But replacing that fuzzy standard with clear rules could, as the UCC seeks generally, provide guidance for parties to structure their transactions.[54]

---

[52] There is some analogy here with the issue, whether and when a security can be traced after transfers through an intermediary, an issue under Article 8 of the UCC. See Kenneth C. Kettering, Repledge Deconstructed, 61 U. Pitt. L. Rev. 45 (1999)(" The Nontraceability Thesis, even in its weak form, holds that use of a net settlement system between intermediaries ordinarily makes it impossible-not undesirable, but impossible -to trace ownership claims in securities transferred through the indirect holding system. But that, plainly, is just not so.").

[53] Nathaniel Popper, Zcash, a Harder-to-Trace Virtual Currency, Generates Price Frenzy, New York Times (Oct. 31, 2016), http://www.nytimes.com/2016/11/01/business/dealbook/zcash-a-harder-to-trace-virtual-currency-generates-price-frenzy.html ("While Bitcoin was initially described as an anonymous currency, its transactions are recorded on a public ledger that can be tracked and traced by law enforcement. Each Bitcoin user has an address, made up of letters and numbers, and the authorities are often able to link an address to a real person using sophisticated data analysis. In contrast, Zcash uses a method developed by a team of cryptographers working at M.I.T. and in Israel — known as zk-Snark — that allows transactions to be confirmed by the network without anyone recording the Zcash addresses involved in the transactions. Users can opt out of this privacy function.").

[54] See Bob Lawless, Is UCC Article 9 the Achilles Heel of Bitcoin?, http://www.creditslips.org/creditslips/2014/03/is-ucc-article-9-the-achilles-heel-of-bitcoin.html.

Contracting out of contract law?

Blockchain smart contracts (not yet in wide use, but much discussed) are sometimes characterized as an alternative to legally enforceable contracts.[55] As some have put it, a smart contract is neither smart nor a contract.[56] The smart contract to sell goods, for example, is robotic, not smart. It blindly applies the conditions in the code, without any consideration of other factors. It is not a contract, some would say, because it is not legally enforceable. Rather, once the smart contract is activated, the parties have no entitlements beyond those in the code. They get what they get and cannot get upset.

As a general matter, it is well-settled that parties may opt out of contract law, in the sense that they may agree that their agreement is not a legally binding agreement. This is slightly paradoxical, with the parties making a binding agreement that they have no binding agreement.[57]

A smart contract to sell goods, however, is different than a letter of intent or a familial agreement. In those agreements, the parties intend no legally binding consequences from their agreement. The smart contract, however, is intended to have legal effect: if the goods are delivered, legal ownership of that property will pass from seller to buyer, and ownership of the payment will pass from buyer to seller . If the goods are not delivered, then legal ownership of the security will pass from seller to buyer. By contrast, with the letter of intent or familial agreement, the parties have no legal obligations, rather state a non-binding intent to take future acts that will have legal consequences.

In terms of Article 2, the parties' conduct will be sufficient to create a contract, per§ 2-207(3). Rather, if they truly choose to have their respective rights and obligations limited to those embodied in the code, Article 2 can accommodate that. An agreement to forego judicial enforcement could be characterized as a limitation on remedies. Sections 2-719 and 2-718 would generally give effect an agreement that the exclusive remedies be those that the parties have agreed to. But the sections would put outer limits on the agreement:

Smart contract law, then, might be an area that is not outside of contract law, but rather where the parties, as a matter of practice, simply do not generally use judicial mechanisms.[58]

---

[55] Note that "smart contracts" more broadly, well beyond just blockchain smart contracts, could refer to contracts made between devices or electronic agents, which raise many issues, such as which body of contract law would apply. See generally By Stacy-Ann Elvy, Hybrid Transactions And The Internet Of Things: Goods, Services Or Software?,Washington& Lee Law Review (Forthcoming Spring 2017)(analyzing whether Article 2 of the UCC should apply to Internet of Things transactions).

[56] Your authors first heard this from Dazza Greenwood and Patrick Murck.

[57] Jeff Lipshaw pointed this out to the authors: "Or maybe it's like a Liar's Paradox. A contract says "I am not a contract." To be enforceable according to its terms, it has to be a contract. But if it is a contract, it's not a contract." The parties to an international sales contract can opt out of Article 2 of the UCC, but that simply supplies a different body of governing law, the United Nations Convention on the International Sale of Goods. See generally Michael P. Van Alstine, The International Sales Contract Including the United Nations Convention on the International Sale of Goods, in International Commercial Transactions (2005).

Smart contracts compared to letters of credit

As commercial practices develop, existing law may provide analogies for principles to resolve legal issues involving blockchain transactions. To explore one analogy, for some smart contracts, the most applicable legal framework might not be contract law but rather letters of credit.

A letter of credit allows two parties to do business while limiting both their reliance on each other or on the legal system.[59] If Buyer in Boston simply contracts with Seller in Singapore to buy goods, someone may bear the risks of nonpayment and judicial enforcement. If Seller ships before payment, there is the risk Buyer will not pay and Seller will have the hazard of trying to enforce her rights in an unfamiliar legal jurisdiction. If Buyer pays in advance, Buyer takes the risk of receiving no goods or defective goods and needing to figure out how to use a foreign legal system to get her money back. The parties can reduce all those risks by using a letter of credit. Buyer has her bank (likely working through a Singapore bank) issue a letter of credit to Seller. The letter of credit obliges the bank to pay the price to Seller, upon presentation of specific documents, such as a bill of lading, customs documents, and a certificate of inspection of the goods by a specified inspector. Seller can now ship the goods, without relying on Buyer or judicial enforcement. As long as Seller has the required documents, Seller is entitled to recover from the bank. Likewise, Buyer need not pay Seller in advance. Buyer will put the money up with the bank, but may recover if Seller does not ship goods that have been duly inspected and supply the documents to get them from customs. Both parties must rely on the banks, but presumably are more comfortable with their local financial institutions than unfamiliar trading partners in far-off jurisdictions.

The key to getting the banks to participate are the doctrines of the independence principle and strict compliance. Under the independence principle, the banks' obligation to pay is independent on whether Seller is entitled to payment on the sales contract. Banks are not in the business of inspecting and testing goods. Nor need the bank decide such questions as, if the contract calls for fifty barrels of syrup, should Seller receive partial payment if she ships forty-five barrels. Rather, the bank is obliged to pay if and only the documents strictly comply with the terms of the letter of credit.

A smart contract for the sale of goods has the same structure, with the banks replaced by the blockchain. By putting control over payment on the blockchain, the buyer and seller avoid relying directly on each other. Rather, each can rely on the blockchain and knows quite specifically the conditions that trigger payment. Like the banks, the blockchain has no actual involvement in the underlying transaction. Whether or not it releases payment depends only on

---

[58] Lisa Bernstein , Opting out of the Legal System : Extralegal Contractual Relations in the Diamond Industry, 21 Journal of Legal Studies 115 (1992).

[59] See Stephen McJohn, Assignability of Letter of Credit Proceeds: Adapting the Code to New Commercial Practices, 25 UCC L.J. 257 (1993).

,whether the coded conditions are fulfilled, and those would be defined strictly in terms of the input data – such as electronic bill of lading, customs documents, and inspection certificate. The blockchain will not inspect or test the syrup. The code of the smart contract similarly imposes its own version of strict compliance. If the code requires documents showing shipment of fifty barrels, seller will not get partial payment for documents showing shipment of forty barrels.

The functional similarities between letters of credit and blockchain smart contracts would support applying some of the principles of letter of credit law to smart contracts. If an intermediary such as an exchange plays a role in the execution of smart contracts, it could be treated in a similar way to a bank that issues a letter of credit. Under the independence principle, the intermediary would not be expected to go beyond its role in supplying blockchain services to be treated as a party to the underlying transaction. Rather, similar to strict compliance, its rights and obligations would be measured by its implementation of the smart contract itself. By the same token, analogous to strict compliance, it would be entitled to reimbursement for its services only upon strict compliance with the terms of the smart contract.

Adapting the law

Past experience in adapting the law to digital technology counsels the advantages of not formulating rules that are technology-specific.[60] Legislatures and courts do best to look past the particular technology that might prompt reform, in order to accommodate the inevitable changes in the direction of both technology and commercial practices. A good example is the Semiconductor Chip Protection Act of 1984, which gave sui generis protection to designs of computer chips. Before long, the underlying technology advanced and the type of protection afforded by the statute was no longer applicable, meaning that few cases were brought under the statute.[61]

A statutoryprovision addressing electronic promissory notes provides an example more analogous to digital currencies. Both federal and state statutes have been enacted to facilitate electronic commerce by authorizing digital signatures. In general, the statutes provide that a signature may be effective, even if it is in digital form. But the statutes make exceptions for categories of documents that might still be expected to have a manual signatures. One's last will and testament, for example, may require a manual signature under state law. Likewise, the statutes generally exclude negotiable instruments. The very nature of a negotiable promissory note is to be a piece of paper that embodies the right to be paid money. Whoever is the holder of that piece of paper has that right, provided it has been properly signed over to the holder. Permitting electronic promissory notes could undercut that role, because digital promissory notes may be so easily copied, indeed must be copied to communicate. The drafters, however, came up with their electronic version of the unique piece of paper. An electronic promissory note could be

60 Thanks to Steve Chow on this point.

61 See Altera Corp. v. Clear Logic, Inc., 424 F.3d 1079 (9th Cir. 2005)(one of the few cases decided under the statute).

negotiable provided that "a single authoritative copy of the transferable record exists which is unique, identifiable, and, . . . unalterable." Note that this rule on its face is not technology specific. It allows parties to come up with any scheme they like, provided that the result is a single, unique, unalterable electronic copy.[62] One could question whether that standard could really be met. Actually having only a single copy of a file would be technically challenging. Rather, computers make copies of files in order to use or view them, to back them up, or to send them to another computer (which might entail multiple copies being made along the way). But certainly that standard would not be met with an electronic promissory note on the blockchain. The very nature of the blockchain is that there are myriad copies of the blockchain, making it a distributed database.

Existing and potential blockchain technologies present a broad array of regulatory issues.[63] How to legally characterize bitcoin[64] and other blockchain technologies and how to regulate it, if at all, or even ban it,[65]has attracted increasing attention.[66] Tax issues have already arisen.[67] Commercial law will likewise need some adaptation.

To take one concrete proposal, Hughes and Middlebrook have persuasively suggested that Article 4A of the Uniform Commercial Code provides a model the regulatory framework for a payment system built around bitcoin.[68] Key to their analysis is the point that many people and businesses are unlikely to use bitcoin software directly. They may wish to use bitcoin, but not install, maintain and use the software, including managing multiple addresses, safeguarding

---

[62] In the reverse of adapting law to new technologies, it may be that Bitcoin serves to give effect to laws that exist but have never actually been use. See Schroeder, note 6 supra, at 1. ("In Part 3, I explain how cryptosecurities fall squarely within Article 8's definition of "uncertificated securities." Ironically, therefore, the creation of bitcoin securities may finally breathe life to little used provisions that were invented almost 40 years ago in a failed attempt to solve a completely different problem.").

[63] See, e.g., Kien-Meng Ly, Coining Bitcoin's Legal-Bits: Examining the Regulatory Framework for Bitcoin and Virtual Currencies, 27 Harv. J. L. & Tech. 587 (2013–2014)(broadly surveying governmental actions in response to Bitcoin); Jeffrey E. Alberts and Bertrand Fry, Is Bitcoin a Security?, Boston University School of Law Journal of Science and Technology (Winter 2015); Stephen Smalla Bitcoin: The Napster of Currency, 37 Hous. J. Int'l L. 581 (2015)(discussing tax law analysis of Bitcoin).

[64] Benjamin Akins, Jennifer L. Chapman, Jason Gordon, The Case for the Regulation of Bitcoin Mining As A Security, 19 Va. J.L. & Tech. 669 (2015)

[65] R. Joseph Cook, Bitcoins: Technological Innovation or Emerging Threat?, 30 J. Marshall J. Info. Tech. & Privacy L. 535 (2014)(" First, the Analysis will provide current economic and national security policies that justify the U.S.'s monopoly on currency, and why a monopoly on currency should be maintained. Second, the Analysis will address how an outright ban on Bitcoin and other DVCs would work and why this method is preferred over regulating and mitigating decentralized digital currency.").

[66] Shahla Hazratjeea, Bitcoin: The Trade Of Digital Signatures, 41 T. Marshall L. Rev. 55, 58 (2016)(proposing that bitcoins "should be broadly defined as property that can be used as a private currency, as money, or to represent ownership of assets, rights, or obligations").

[67] Sam Hampton, Undermining Bitcoin, 11 Wash. J.L. Tech. & Arts 331, 331 (2016)(" Decentralized currencies like Bitcoin pose novel and difficult regulatory questions, but mechanically applying old rules will lead to an unsatisfactory outcome. The best solution is new legislation that specifically addresses the novel issues posed by virtual currencies, fosters the use of virtual currency in transactions, and still collects tax revenues from investor").

[68] See Hughes and Middlebrook, supra note 4.

private keys, and generally dealing with issues that can arise with using encryption. Rather, intermediaries can handle all the technical details, and parties can use bitcoin just as easily as shopping at Amazon or doing online banking. UCC 4A already provides a sturdy framework for such a payment system, in which intermediaries (banks) handled payment orders (analogous to bitcoin transfers) for its customers. Hughes and Middlebrook state several advantages for providing such a framework.

If UCC 4A were to be emulated in drafting, say, UCC 4B for virtual currencies, it would be to take into account existing commercial practices, as did the drafters of UCC 4A. Some of the rules of UCC can seem downright peculiar unless considered in the light of banks' practices in connection with wire transfers. Suppose, for example, Gabriel's Oak Services issued a payment order to its bank, instructing it to transfer $100,000 to Bathsheba Everdene, account number 261840 at Madding Bank. Gabriel's Oak Services takes great care to correctly state the beneficiary's distinctive name, but makes a slight mistake in the account number, which is actually account number 261480. Gabriel's Oak Service's bank send a matching payment order to Madding Bank. Madding Bank looks only at the account number listed and puts the money in account number 261480, which belongs to William Boldwood, who disappears with the funds. One might expect Madding Bank to take the loss, where it did not take a few seconds to differentiate between Bathsheba Everdene and William Boldwood by checking the account numbers against the name listed. But UCC 4A puts the loss on Gabriel's Oak Services, who made the error, not on Madding Bank, who could so easily have detected the error. Why? Because the drafters of UCC 4A had found this to be consistent with banking practices. The nice clear rule gives all parties clear guidance: "Triple check the account number!" and avoids the difficulties of requiring a match between name and number. Names are tricky things. The originator may not use the exact legal name of the beneficiary, or the contract may be with a subsidiary but the funds going to a parent company, or the beneficiary may do business under a trade name. The account number, however, should be unique and readily determinable.

Another rule of UCC 4A which sometimes comes as quite a surprise to customers is the allocation of the risk of fraud. Suppose a crafty individual sends an email to thousands of addresses, stating that their business has updated its wire transfer system and the recipient should enter his user name and password to maintain authority to use the system. The vast majority of recipients will ignore or laugh at this phishing email. But perhaps one unfortunate and trusting recipient gets it the very day his company has, by coincidence, updated their wire transfer system. He enters his user name and password, and soon the company's funds have been wired to parts unknown. Although the transfers were not authorized, UCC 4A will deem them authorized, provided the bank followed a commercially reasonable security procedure in place.

To adapt UCC 4A for bitcoin transfers, careful attention must be paid to commercial practices.[69] These may be more difficult to ascertain. Bitcoin has been around only a few years, as opposed to decades of wire transfer practice. Many bitcoin transactions have been considerably less transparent than commercial banking practices.

Secured transactions

The use of bitcoin and smart contracts to provide collateral been frequently floated.[70] In the very paper where Nicholas Szabo coined the term "smart contracts," he suggested that one application of smart contracts would be to automatically disable a car if the loan payments were not made in timely fashion.[71]

The first question, as with contract law, would be whether the parties could opt out of Article 9 of the Uniform Commercial Code, which governs Secured Transactions ("secured transactions" in the sense that personal property is given as security for an obligation, not in the other relevant sense of "secured transactions," transactions that are encrypted in order to provide security against). Suppose Lender loans dollars to Borrower, and the parties secure the obligation with a smart contract that, upon failure to make timely payments, will send the agreed amount of bitcoin to Lender from Borrower's wallet. May the parties effectively agree that the computer code alone will control the transaction and that UCC A9 will not apply? In contract law, that raised a conundrum. Article 9, by contrast, brooks no defectors. Under Section 9-109, Article 9 applies to secured transactions, regardless of the form of the transaction.

No matter how the parties characterize their transaction, if the substance is a secured transaction in personal property, UCC A9 applies. Contract law generally lets the parties decide on the rules governing their relationship. Article 9 is less permissive, for two reasons. First, secured transactions affect not just the two parties, but other parties. If the bitcoin is Lender's collateral, that means that other creditors of Borrower will not be able to get at the bitcoin, even if Borrower ends up in bankruptcy.[72] Article 9 provides rules about how to put other creditors on

---

[69] See Carla L. Reyes, Moving Beyond Bitcoin To An Endogenous Theory Of Decentralized Ledger Technology Regulation: An Initial Proposal, 61 Vill. L. Rev. 191, 227 (2016) (suggesting an approach to regulation use of the blockchain that is "a synthesized approach that is iterative, cooperative, focused on the functional purposes for enacting regulation, and implemented from within the market requiring regulation").

[70] For a view of the broad range of issues bitcoin transactions raise for lenders, see Pamela J. Martinson, Bitcoin and the Secured Lender, Banking & Fin. Services Pol'y Rep., June 2014, at 13 ("The growing use of Bitcoin poses potential legal issues for creditors, particularly when Bitcoin may be a source of collateral for a loan, and perfection of security interests and recovery of the collateral is integral to the deal").

[71] See Szabo, supra note 1.

[72] Many issues may arise in the inevitable intersection of bitcoins and bankruptcy. See, e.g., Chelsea Deppert, Bitcoin and Bankruptcy: Putting the Bits Together, 32 EMORY BANKR. DEV. J. ___ (2016)(analyzing the treatment of bitcoin under the Bankruptcy Code); Devin Burke Hahn, Bitcoins in Bankruptcy: Taking a Byte Out of Chapter 11, 25 No. 3 J. Bankr. L. & Prac. NL Art. 4 (2016)("As a preliminary matter, the characterization of virtual

notice. Second, Article 9 was drafted with a background of oppressive practices by some creditors. By making its rules mandatory, Article 9 prevents lenders from circumventing the protections it applies.

Szabo's classic example involves a smart contract which automatically disables a car if the debtor fails to make timely payments. Such automatic repossession might be perfectly consistent with UCC Article 9. A creditor need not get a court order or even give prior notice to the debtor before repossessing the collateral. Creditors usually do not give prior notice before repossessing cars, because that may only cause the debtor to play hide and seek with the collateral.

But repossession does not end the relationship. Writers about smart contracts often seem to assume that the creditor simply keeps the car. But Article 9 does not permit that. The creditor cannot simply keep the collateral in satisfaction of the debt. Article 9 put an end to that practice, whereby a creditor, when a debtor had almost paid off the debt, could opportunistically take back the collateral upon a default. That allows the creditor to get the entire value of the collateral by giving up only the remaining payments. Now, under UCC A9, a creditor may propose taking the collateral as satisfaction, but the debtor may decline. The creditor may resell the collateral, but must give prior notice of the sale and do everything in a commercially reasonable way, and must return the collateral if the debtor pays down the debt. Internet commerce is not yet so automated that used cars can be resold without human intervention, let alone allowing for all the contingencies that might arise if there is a question of redemption. Nor can the parties simply agree in the security agreement exactly what procedure the creditor shall follow upon default. Rather, protections given debtors (no strict foreclosure, creditor must give notice of resale and conduct resale in a commercially reasonable manner) may not be waived.

A closer consideration of default raises real questions of whether conditions could be sufficiently clearly defined to code in a smart contract. If a debtor defaults on a payment, that generally will be a default permitting the seller to repossess the collateral. But it is a rare creditor that immediately repossesses the collateral immediately upon repayment. Repossessing and reselling the collateral may be expensive. Encouraging the debtor to cure the default may, especially if the interest rate and fees are favorable, be better for the creditor. This might require some negotiation and perhaps some adjustments. A classic smart contract, which is fully programmed from the beginning, may not have the adaptability to account for such back and forth. Indeed, if the software could be so reprogrammed, then it starts to simply look like a communication channel. In addition, including conditions in a smart contract that are not on the

---

currencies for the purposes of bankruptcy law remains an open issue, clouding the outcome of potential disputes concerning (i) eligibility, (ii) property of the estate, and (iii) safe-harbors for estate causes of action. Even after bankruptcy courts resolve the legal questions surrounding this new asset, the anonymity of virtual currencies will present a significant potential for fraud, specifically the concealment of a debtor's assets.").

blockchain (such as payments from funds that are not locked in the blockchain), hazards making it impossible for the code to function.[73]

"Default" itself, as presently practiced, also would be challenging to code. Non-payment is default that permits the creditor to repossess. But loan agreements typically define default more broadly, to capture many other events that increase the risk of nonpayment. For automobile loans, default events could include failure to maintain insurance, using the car as a commercial vehicle, selling or leasing the car, filing bankruptcy, damaging the car, and so on. It would be challenging for a computer to monitor all that information, especially when the debtor has incentives to keep that information from the creditor. More generally, security agreements often have an "insecurity clause," that allows the creditor to declare default upon anything that increases the risk of nonpayment or loss of value of collateral. Such a clause is used exactly because creditors cannot in advance envision all the possible conditions that should trigger default. Coding such conditions into a smart contract would be a challenge.

The question might arise, whether Article 9 should be made more flexible in order to account for bitcoin financing and blockchain transactions. In particular, whether the mandatory protections for debtors should be relaxed, in order to accommodate smart contracts. One could argue that the parties to a loan transaction should be able to choose the conditions of their relationship, and that the chances of creditors behaving opportunistically are reduced by transparency inherent in smart contracts, because every condition and action must be specified by the parties. The counterargument seems stronger, however. Article 9 was drafted with a colorful history of oppressive behavior by some creditors. Recent years hardly show that such conduct has gone away. Predatory and discriminatory lending and taking advantage of unsophisticated consumers have been widespread, even at the same time that innovation in lending has made credit more available to borrowers. The ill practices of some payday lenders, for example, show graphically how a lender may be able to get a borrower to initially get a small loan, which spirals upward geometrically given high interest rates and fees. The Consumer Financial Protection Bureau was created in recent years largely as a response to consumer debt problems. The information asymmetries of credit (meaning, creditors are sophisticated repeat players in the game, where borrowers are likely to have much less experience and understanding) may in fact be magnified by smart contracts. Article 9 already has been amended to account for electronic practices, such as requiring that the security agreement be a "record," as opposed to a "record," and permitting electronic filing of UCC-1 financing statements. The protections given to debtors are not an obstacle to smart contracts, rather a limitation on the scope of those contracts. But Article 9 could be amended in ways that facilitate blockchain transactions without eroding debtor protections.[74] The definitions of property, for example, could be amended to

[73] See Greenspan, supra note 39.

[74] Professor Schroeder, for example, suggests amending Article 9's definition of "money" and super-negotiability rule to facilitate bitcoin financing. See Schroeder, supra note 6, at 43.

clarify where digital currencies fall. States could work together to implement a blockchain filing system for UCC-1 financing statements, using smart contracts to preserve the right of state to collect filing fees.[75] And the possibility exists that smart contracts offer a means for consumers to bargain with online businesses, where at present consumers are presented with take-it-or-leave it terms, meaning that protections could be relaxed in order to give scope in negotiation.[76] But hard evidence of such benefits should proceed legislative enablement.

Conclusion

The Uniform Commercial Code has adapted to commercial practices for over fifty years. Revisions to the code and judicial opinions have continued in the spirit of the law merchant and of Karl Llewellyn and Grant Gilmore's attention to the realities of commercial life. Commercial law likewise has the flexibility to support changes in commercial practices which may be revolutionary – and also to abide while the course of those changes unfolds.

75 See Schroeder, note 6 supra, at 46-47.

76 Joshua Fairfield, Smart Contracts, Bitcoin Bots, and Consumer Protection, 71 Wash. & Lee L. Rev. Online 35 (2014)("Online, contract law is not the law of bargained-for exchange; it has become the law of company-dictated exchange. Smart contracts--automated computer programs able to execute trades through TPLs--may offer a solution.").