THE BRIDGING MODEL: EXPLORING THE ROLES OF TRUST AND ENFORCEMENT IN BANKING, BITCOIN, AND THE BLOCKCHAIN

Catherine Martin Christopher*

Bitcoin has long been touted as a currency and a payment system that relies on cryptography and mathematics rather than trust. But is Bitcoin really trustless? And if so, would that be a good thing? This article undertakes a critical deconstruction of Bitcoin and the blockchain, their themes of democracy and transparency, and the idea that they are trustless. The article then proposes a new conceptualization of the role of trust in business and contracting: the bridging model, which allows for a more nuanced understanding of the interplay between enforcement and trust in contract formation. The bridging model is applied first to traditional banking, to illustrate and analyze the enforcement mechanisms underpinning the U.S. dollar as currency and the banking system as a whole, and to demonstrate that the enforcement mechanisms (government backing and regulation) are not as robust as generally believed. The bridging model is then applied to Bitcoin, to show not only that the system requires more trust than is generally understood, but also that both currency and payment systems benefit from the involvement of trusted intermediaries in response to problems and crises.

* Associate Professor, Texas Tech University School of Law. J.D., University of Pittsburgh. Grateful thanks to the following for the opportunity to present and discuss drafts of this paper in its various stages: the 2015 Texas Legal Scholars Workshop and Nathan Cortez, Dave Fagundes, Douglass Moll, Jessica Roberts, W. Keith Robinson, Saurabh Vishnubhakat, and Kellen Zale; the New Scholars Colloquium of the Southeastern Association of Law Schools and Judd Snierson; the 11th International Conference on Contracts (KCON) and Daniel Barnhizer, Shawn Bayern, Mark Burge, Colin Marks, and Angela Walch. Thanks also to those who read drafts of the paper and gave valuable feedback: Sally McDonald Henry, Tracy Hresko Pearl, M. Alexander Pearl, Kristen van de Biezenbos, and Kyle Velte. I am also grateful to Jamie Baker, J.D., M.L.S., and Katherine Mendiola, who provided excellent research support. This work was made possible by the support of the Texas Tech University School of Law.

TABLE OF CONTENTS

INTRODUCTION 140
I. BITCOIN AND BLOCKCHAIN BASICS 142
A. Mechanics 143
B. Recordkeeping and Double-Spending 146
C. Bitcoin's Themes: Transparency and Democracy 148
D. Third-Party Intermediaries 151
II. THE INNOVATION AND POTENTIAL OF THE BLOCKCHAIN 152
III. TRUST 155
A. Trust Models 158
B. Proposed Model: Bridging 161
IV. THE BRIDGING MODEL APPLIED TO TRADITIONAL BANKING 166
A. Currency and the Money Supply 166
B. Deposits and Lending 170
V. THE BRIDGING MODEL APPLIED TO BITCOIN AND THE BLOCKCHAIN 172
A. Bitcoin as Currency 172
B. Bitcoin as Payment System, Blockchain as Recordkeeper 175
C. Third-Party Intermediaries 177
D. Government Enforcement? 179
CONCLUSION 180

INTRODUCTION

In 2008, the world realized that trillions of dollars were gone. Individual homeowners had taken on outsized home mortgages, and those mortgages were bundled and sold—as were derivative products based on those mortgages—to, well, everyone. The feeding frenzy of buyers who couldn't get enough of these doomed assets has been well documented in books,[1] movies,[2] and the popular press.[3]

---

[1] *See generally, e.g.*, ALAN S. BLINDER, AFTER THE MUSIC STOPPED: THE FINANCIAL CRISIS, THE RESPONSE, AND THE WORK AHEAD (2013); KEITH GESSEN, DIARY OF A VERY BAD YEAR: INTERVIEWS WITH AN ANONYMOUS HEDGE FUND MANAGER (2010); NEIL IRWIN, THE ALCHEMISTS: THREE CENTRAL BANKERS AND A WORLD ON FIRE (2014); MICHAEL LEWIS, THE BIG SHORT: INSIDE THE DOOMSDAY MACHINE (2010); ROGER LOWENSTEIN, THE END OF WALL STREET (2010); HENRY M. PAULSON, JR., ON THE BRINK: INSIDE THE RACE TO STOP THE COLLAPSE OF THE GLOBAL FINANCIAL SYSTEM (2010); RAGHURAM G. RAJAN, FAULT LINES: HOW HIDDEN FRACTURES STILL THREATEN THE WORLD ECONOMY (2010); ANDREW ROSS SORKIN, TOO BIG TO FAIL: INSIDE THE BATTLE TO SAVE WALL STREET (2009).

[2] *See generally, e.g.*, THE BIG SHORT (Plan B Pictures 2015) (based on the book of the same name by Michael Lewis, *supra* note 1); INSIDE JOB (Sony Pictures Classics 2010).

[3] *See generally, e.g.*, Jed S. Rakoff, *The Financial Crisis: Why Have No High-Level Executives Been Prosecuted?*, 61 N.Y. REV. BOOKS, no. 1, Jan. 9, 2014, http://www.nybooks.com/articles/2014/01/09/financial-crisis-why-no-executive-prosecutions/ [https://perm

It turned out that the houses were overvalued, the homeowners couldn't pay, and as a result, the mountains of financial products that had been built on the backs of those mortgages were worthless.[4] Tears need not be shed, perhaps, for the hedge funds and speculators who went broke, but the unfairness of ordinary people's money market accounts and pension funds being thoughtlessly invested in these and other complex derivative products is infuriating.

The indignities continued: Taxpayer dollars were used to bail out banks, securities firms, mutual funds, and insurance companies—private, for-profit companies which had never before been entitled to government support.[5] Lehman Brothers was allowed to fail while other firms weren't, and no one understood how the lines were being drawn.[6] As foreclosure rates spiked, some bankers used those government bailout funds to pay themselves huge bonuses.[7]

Against this backdrop came Bitcoin.[8] Introduced quietly in late 2008 to a very small group of computer programmers, Bitcoin promised to be a currency and an entire payment system that bypassed bankers altogether, allowing people the freedom to trade reliable units of currency directly and immediately between themselves, without having to trust anyone on Wall Street or in Washington.[9]

With a zeal bordering on the religious, Bitcoin advocates trumpeted the trustlessness of Bitcoin.[10] A financial system without intermediaries meant no lying and no one to make mistakes. Instead, a democratic, transparent system

---

a.cc/L7LX-F2ZE]; James B. Stewart, *Eight Days: The Battle to Save the American Financial System*, NEW YORKER, Sept. 21, 2009, at 58; *The Origins of the Financial Crisis: Crash Course*, ECONOMIST, Sept. 7, 2013, at 74; *25 People to Blame for the Financial Crisis*, TIME, http://content.time.com/time/specials/packages/completelist/0,29569,1877351,00.html [https://perma.cc/YPD2-QJY4] (last visited Aug. 30, 2016). The Huffington Post has an entire page devoted to the Financial Crisis. *See Financial Crisis*, HUFFINGTON POST, http://www.huffingtonpost.com/news/wall-street/ [https://perma.cc/VLS9-N6UM] (last visited Aug. 30, 2016); *see also* Manoj Singh, *The 2007–08 Financial Crisis in Review*, INVESTOPEDIA, http://www.investopedia.com/articles/economics/09/financial-crisis-review.asp [https://perma.cc/4LA8-L9Q2] (last visited Aug. 30, 2016).

[4] *See* BEN S. BERNANKE, THE FEDERAL RESERVE AND THE FINANCIAL CRISIS 71 (2013).

[5] *See generally The Financial Crisis Timeline*, FED. RES. BANK ST. LOUIS, https://www.stlouisfed.org/Financial-Crisis [https://perma.cc/UQK3-MCHT] (last visited Aug. 30, 2016).

[6] *See Fed Transcripts: Bernanke Chose to Let Lehman Fail*, FORTUNE (Feb. 21, 2014, 7:27 PM), http://fortune.com/2014/02/21/fed-transcripts-bernanke-chose-to-let-lehman-fail [https://perma.cc/N8HR-BKE9].

[7] Louise Story & Eric Dash, *Bankers Reaped Lavish Bonuses During Bailouts*, N.Y. TIMES (July 30, 2009), http://www.nytimes.com/2009/07/31/business/31pay.html?_r=1 [https://perma.cc/4M6H-N6SH]; Dan Gerstein, *The Bailout Bonus Smackdown*, FORBES (Feb. 5, 2009, 12:01 AM), http://www.forbes.com/2009/02/04/stimulus-obama-daschle-opinions-columnists_0205_da n_gerstein.html [https://perma.cc/YQB7-NXVU].

[8] *See generally* NATHANIEL POPPER, DIGITAL GOLD: BITCOIN AND THE INSIDE STORY OF THE MISFITS AND MILLIONAIRES TRYING TO REINVENT MONEY (2015).

[9] *See generally infra* Part I.

[10] PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND THE BLOCKCHAIN ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 70–72 (2015).

based on mathematical certainty would create a perfectly reliable financial system.

But is Bitcoin really trustless? And if so, is that a good thing?

The innovative contributions of this Article are two-fold. First, this Article proposes a new model for the conceptualization of trust in business and contract, called the "bridging" model. A new model is needed because existing literature on trust either ignores or oversimplifies the role that enforcement mechanisms play in parties' decisions to enter into a transaction. The bridging model allows for a more nuanced understanding of how enforcement and trust combine to allow parties to overcome their reluctance to transact.

Second, this Article applies the bridging model to Bitcoin and blockchain transactions. The popular Bitcoin narrative suggests that it is an entirely mechanized payment system and currency, requiring no trust by its participants. The bridging model facilitates a deeper understanding of Bitcoin, however, demonstrating that more trust is required from market participants than the popular narrative suggests. Moreover, this Article posits that some component of trust may actually be preferable in currency and payment systems.

This Article proceeds as follows. Part I is a critical deconstruction of Bitcoin and the blockchain—how they work, their ideological underpinnings, and the problems they purport to solve. Part II briefly outlines the innovative potential of the blockchain. Part III summarizes existing social science and legal scholarship on trust, explains why they do not adequately incorporate the role of enforcement mechanisms, and proposes the bridging model to address this deficiency. The bridging model is then applied first to traditional banking in Part IV, which demonstrates that the enforcement mechanisms of government backing and regulation may not be as robust as they are generally assumed to be. In Part V, the bridging model is then applied to Bitcoin and the blockchain, demonstrating not only that their cryptographic enforcement mechanisms require more trust than people realize, but also that some component of trust is actually preferable in currency and payment systems.

I. BITCOIN AND BLOCKCHAIN BASICS

Bitcoin is software that is best understood first as a payment system. The payment system is run on volunteer computers that are all networked together over the Internet.[11] This is called being "distributed" or "decentralized"; there is no central processor.[12] The Bitcoin payment system transacts units of "currency" also called bitcoins. To provide some clarity, this Article will use capital-B

[11] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159, 163 (2012).
[12] *Id.* at 162, 180.

"Bitcoin" to refer to the payment system and the network as a whole, while lower-case-b "bitcoin" will refer to the units of currency themselves.[13]

Bitcoin is sometimes referred to as a "virtual currency," because it exists only online; it is also sometimes referred to as a "cryptocurrency," because of the complex encryption that keeps the information secure.[14] Either of these descriptions is fine. Bitcoin is not the only cryptocurrency, but it is the most popular, with the most name recognition.[15] Just as the Kleenex corporate name is a functional synonym for facial tissues, the Bitcoin name is sometimes used loosely as a generic name for all virtual currencies. Likewise, "a Kleenex" is a single unit of tissue, just as "a bitcoin" is a single unit of the virtual currency.

A. Mechanics

The Bitcoin software was written by an anonymous programmer (or group of programmers), known only by the pseudonym "Satoshi Nakamoto."[16] Nakamoto introduced Bitcoin in a white paper published in 2008.[17] Nakamoto remained engaged in the burgeoning online Bitcoin community for several years, but disappeared in 2011, with only the vague explanation that he had moved on to other projects.[18] His (or her, or their) identity remains unknown, but the software lives on.

Individuals who wish to become part of the Bitcoin ecosystem do so by downloading the freely available Bitcoin software onto their computers and joining the network.[19] By doing so, they volunteer their computer's processing power to run the payment system.[20] Again, there is no central processor and no

---

[13] While not universal, this distinction in capitalization is becoming the convention. *E.g.*, Shawn Bayern, *Dynamic Common Law and Technological Change: The Classification of Bitcoin*, 71 WASH. & LEE L. REV. ONLINE 22, 24 n.5 (2014), http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1001&context=wlulr-online [https://perma.cc/GS9D-W2FR].

[14] Mark Edwin Burge, *Apple Pay, Bitcoin, and Consumers: The ABCs of Future Public Payments Law*, 67 HASTINGS L.J. 1469, 1500–02 (2016).

[15] *See Crypto-Currency Market Capitalizations*, COINMARKETCAP, https://coinmarketcap.com [https://perma.cc/C4RU-SVK6] (last visited Aug. 30, 2016).

[16] Grinberg, *supra* note 11, at 162.

[17] SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM, https://bitcoin.org/bitcoin.pdf [https://perma.cc/3KWX-L8FE] (last visited Aug. 30, 2016).

[18] Joshua Davis, *The Crypto-Currency: Bitcoin and Its Mysterious Inventor*, NEW YORKER, Oct. 10, 2011, at 62. Nakamoto re-emerged only once. Newsweek magazine reported on March 6, 2014 that it had (incorrectly) identified a California man named Dorian Satoshi Nakamoto as the creator of Bitcoin. Leah McGrath Goodman, *The Face Behind Bitcoin*, NEWSWEEK (Mar. 6, 2014, 6:05 AM), http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html [https://perma.cc/8TG2-29VL]. This caused a firestorm of attention on a demonstrably bewildered and unhappy Mr. Nakamoto, and the real Nakamoto—or someone using his account—resurfaced briefly to post a simple message online: "I am not Dorian Nakamoto." VIGNA & CASEY, *supra* note 10, at 75–76.

[19] Grinberg, *supra* note 11, at 162.

[20] *Id.* at 163.

specific computer (or set of computers) that are designated as the central hub of action; the system is powered entirely by a decentralized network of computers.

The Bitcoin payment system keeps a ledger of all bitcoins and their transaction history.[21] Each unit of bitcoin currency is unique, and the ledger contains entries for the date each bitcoin was created, as well as a history of each wallet (akin to a Bitcoin account) where each bitcoin has ever resided.[22] At any moment, the ledger reflects not only the current wallet location of each bitcoin, but also the complete history of that bitcoin's ownership.[23] This ledger is called the blockchain.[24]

A hasty caveat is in order: the blockchain is encrypted, so while it is technically visible to the public, its contents make no sense to humans.[25]

Transactions on this payment system are bundled together periodically and processed in batches, called blocks. Each block confirms all the current transactions being processed, while also confirming the validity of the block before it.[26] Because each block confirms the previous block, each new block also thereby validates the entire blockchain.[27] A block is processed simultaneously yet independently on computers all across the network and is confirmed and added to the blockchain only once a majority of the computers agree that the processed block is correct.[28] So long as a majority of the network is "honest," that is, non-malicious, the blockchain will be accurate.[29]

The consensus mechanism also makes the blockchain resistant to revision. In order to change a previous block, a consensus would again have to be reached. The computers on the network would never go back and redo a previous block, however—the software instructs them to confirm the previous block and then never look back.[30] In order to change a previous transaction, someone would have to rapidly introduce enough additional computing power to suddenly become a majority of the network. This is functionally impossible—to date, the Bitcoin network is hundreds of thousands of times bigger than the world's

---

[21] Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 149 (2014).

[22] Grinberg, *supra* note 11, at 162–63; Brito et al., *supra* note 21, at 150.

[23] Brito et al., *supra* note 21, at 149–50.

[24] ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES 159 (2014); Brito et al., *supra* note 21, at 149.

[25] See *Last Bitcoin Blocks*, BLOCKR, https://btc.blockr.io/ [https://perma.cc/E4EJ-T7RL] (last visited Aug. 30, 2016), for a list of recent blocks, and click on each one to see its respective contents.

[26] NAKAMOTO, *supra* note 17, at 2.

[27] ANTONOPOULOS, *supra* note 24, at 159.

[28] NAKAMOTO, *supra* note 17, at 2.

[29] *See id*.; Grinberg, *supra* note 11, at 176 n.72.

[30] *See* NAKAMOTO, *supra* note 17, at 3. *But see infra* Part V.B.

largest supercomputer. The idea that someone could amass enough *additional* computational power to become 51 percent of the network is preposterous.[31]

This inviolability is appealing, but it also prevents error-correction in the event of mistake or, more commonly, theft by hacking.[32]

A new block is added to the blockchain about every ten minutes.[33] As a byproduct of this number-crunching, encrypted strings of letters and numbers are produced, which are the new bitcoins.[34] New bitcoins are created at a predetermined rate, with the number of bitcoins produced with each block halving every few years, so the rate of production slows over time.[35] The software is programmed to stop producing new bitcoins when 21 million have been produced.[36] This is expected to happen in about 2140.[37] After that, the blockchain will continue to confirm transactions and verify previous blocks, but it will no longer produce new bitcoins. The supply of bitcoins is thus relatively stable and predictable.[38]

Once generated, a new bitcoin is awarded, lottery-style, to one of the computers on the network.[39] This is known as "mining" bitcoins, and it is one of the incentives for joining the network in the first place.[40] Some individuals and companies make big business of building ever-larger computers to contribute to the Bitcoin ecosystem—larger computing power increases the odds of winning the new-bitcoin lottery.[41]

---

[31] *See* Jörg Becker et al., *Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency*, *in* THE ECONOMICS OF INFORMATION SECURITY AND PRIVACY 135, 148 (Rainer Böhme ed., 2013); CAMPBELL R. HARVEY, BITCOIN MYTHS AND FACTS 5 (2014); *November 2015*, TOP 500, http://top500.org/lists/2015/11 [https://perma.cc/48BH-APU9] (last visited Aug. 30, 2016).

[32] *See* NAKAMOTO, *supra* note 17, at 3.

[33] ANTONOPOULOS, *supra* note 24, at 27; Grinberg, *supra* note 11, at 163 n.16; EDWARD V. MURPHY ET AL., CONG. RESEARCH SERV., BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 6 (2015) (stating transactions can take ten to sixty minutes).

[34] ANTONOPOULOS, *supra* note 24, at 25–26.

[35] Grinberg, *supra* note 11, at 163–64.

[36] *Id*. at 163–64, 178–79. Bitcoin production is logarithmic, so the maximum will be approached but never reached. *Id*.

[37] ANTONOPOULOS, *supra* note 24, at 2.

[38] *See generally* NAKAMOTO, *supra* note 17, at 3.

[39] ANTONOPOULOS, *supra* note 24, at 26–27.

[40] Transaction fees are also paid to processing computers; once the maximum number of bitcoins has been reached, transaction fees will be the only financial incentive for joining the network. Grinberg, *supra* note 11, at 165; Becker et al., *supra* note 31, at 138; *The Trust Machine: The Promise of the Blockchain*, ECONOMIST, Oct. 31, 2015, at 13 [hereinafter *Trust Machine*]; MURPHY, *supra* note 33, at 6; NAKAMOTO, *supra* note 17, at 4.

[41] *See* VIGNA & CASEY, *supra* note 10, at 138–46; Grinberg, *supra* note 11, at 167, 181 n.90 (discussing "mining collectives"). Bitcoin miners' computing power is measured in "hashes," that is, how many hashing calculations can be performed in a second. One mining company, CoinTerra, has enough computers in its Salt Lake City location to make nearly four thousand trillion calculations per second. *See* VIGNA & CASEY, *supra* note 10, at 143–44. Some mining operations are based in cold climates like Iceland simply to help keep the mining computers from overheating. *Id*. at 142.

The lottery system, based on processing power rather than a one-computer-one-ticket system, has been criticized as being undemocratic because those with more resources to build faster computers increase their odds of mining bitcoins.[42] The system has also been criticized for disproportionately awarding early adopters who participated in a smaller network when bitcoins were being produced at a faster rate.[43]

The network is now so large that an individual user is unlikely to mine a bitcoin in a meaningful timeframe. The rate of bitcoin production slowed—by half—in July 2016.[44] Someone wishing to obtain bitcoins but unwilling to play the lottery can purchase them, either in person or online, at a digital currency exchange.[45]

Bitcoins are famous for their price volatility.[46] In their brief time on earth, bitcoins have been valued at fractions of a penny, $1,388 apiece, and everything in between.[47] So, what's a bitcoin actually worth?[48] Put bluntly, a bitcoin is worth what someone will pay for it. This is true of everything, even things that are electronic and nerdy.[49]

B. Recordkeeping and Double-Spending

The blockchain's recordkeeping goes beyond that kept by banks on behalf of their customers. Banks track specific debits and credits (including exact payment amounts, dates, and some counterparty identifying information), as

---

[42] *See* VIGNA & CASEY, *supra* note 10, at 138–44.

[43] *See* Grinberg, *supra* note 11, at 163–67.

[44] Margie Smithurst, *Bitcoin's 'Halving' and the Future of the Cryptocurrency*, ABC NEWS (July 12, 2016, 11:25 PM), http://www.abc.net.au/news/2016-07-13/bitcoin's-'halving'-and-the-future-of-the/7626260 [https://perma.cc/E6LS-M23Q].

[45] *See* Grinberg, *supra* note 11, at 167; *see also infra* Part I.D.

[46] *See* Grinberg, *supra* note 11, at 164.

[47] *See What is the Highest Price Paid for a Bitcoin?* QUORA, https://www.quora.com/unanswered/What-is-the-highest-price-paid-for-a-bitcoin [https://perma.cc/5EJ7-HETT] (last visited Aug. 30, 2016) (A sheepish anonymous post admitted paying 83,333 rupees, or $1,388, for a bitcoin, even though "The exchange price was around $1100 at that time, and this was the best buy [the buyer] could get at that time in India."). *See generally Bitcoin Price Index Chart*, COINDESK, www.coindesk.com/price/ [https://perma.cc/7S7B-G97Z] (last visited Aug. 30, 2016) (providing present and historical bitcoin prices). The first purchase price of a bitcoin, in 2009, was based on the amount of electricity it took to generate one: one dollar bought about 1,000 bitcoins. POPPER, *supra* note 8, at 38.

[48] See CoinDesk.com for current and historical bitcoin prices. COINDESK.COM, http://www.coindesk.com [https://perma.cc/GMC8-7QRK] (last visited Aug. 30, 2016).

[49] I can't understand why anyone would pay $140 million for a Jackson Pollock painting, but apparently someone wanted to. Carol Vogel, *A Pollock Is Sold, Possibly for a Record Price*, N.Y. TIMES (Nov. 2, 2006), http://www.nytimes.com/20 06/11/02/arts/design/02drip.html [https://perma.cc/CBV4-R8WY].

well as account balances. Much of this information is reported to a customer in the form of monthly statements.[50]

Imagine if, in addition to all this, the bank was also keeping track of the serial number on each bill flowing into and out of an account. Of course, tracking serial numbers is both impractical and impossible. It's impractical because dollar bills are fungible, in that one is exactly as useful as any other. There is no utility in keeping track of which *specific* dollars were used to pay a restaurant tab versus those used to buy a magazine—that information just isn't important enough to track. Tracking serial numbers is unnecessary, but it's also impossible; huge numbers of transactions are made electronically, and so there are no identifiable physical dollars involved.[51]

With the blockchain, however, every bitcoin is identifiable, and before a transaction is logged in the ledger, the payment system network has confirmed not merely an account balance, but also which *specific* bitcoins are being sent.[52] Although this practice would be pointless with dollar bills, it serves two necessary functions with Bitcoin. First, a ledger that identifies the creation of a unique unit of currency prevents counterfeiting.[53] A fake bitcoin cannot be introduced into the ledger from the outside, because the ledger cannot verify its provenance. Second, the blockchain prevents double-spending, a problem that dogged previous attempts at creating digital currencies.[54]

Double-spending is normal and expected in traditional banking practices. When a bank customer deposits one hundred dollars in a checking or savings account, the bank will likely then make a loan to another customer with about ninety of those dollars.[55] Doing this means the bank increases the amount of money in circulation and the size of the economy: one hundred dollars has become one hundred and ninety.

By making this loan, though, the bank has put itself in a somewhat precarious position: if the checking or savings account customer shows up the next day and wants to withdraw the hundred dollars, the bank is obligated to return them, even though ninety of them are gone. The bank will have to use ninety dollars from anther depositor to repay this customer. The bank tracks all of this

---

[50] *See FAQs: Bank Account Statements*, BANK AM., https://www.bankofamerica.com/deposits/manage/faq-account-statements.go [https://perma.cc/AB4P-6CVW] (last visited Aug. 30, 2016).

[51] In 2012, for example, about 122.8 billion payments were made electronically in the United States. GEOFFREY R. GERDES ET AL., FED. RESERVE SYS., THE 2013 FEDERAL RESERVE PAYMENTS STUDY 13 (2013). That's not $122.8 billion in total amount transacted—it's 122.8 billion different transactions.

[52] VIGNA & CASEY, *supra* note 10, at 123.

[53] Ruoke Yang, *When Is Bitcoin a Security Under U.S. Securities Law?*, 18 J. TECH. L. & POL'Y 99, 120 (2013).

[54] *Id*.

[55] *See* RICHARD SCOTT CARNELL ET AL., THE LAW OF BANKING AND FINANCIAL INSTITUTIONS 40–43 (4th ed. 2009).

on its private ledgers—using aggregate balances, that is, not debiting specific customer accounts to repay other customers' withdrawals.

On a large scale, it is unlikely that all checking and savings account customers will want their deposits back at the same time. A few of them will make withdrawals, but the bank will usually have enough cash on hand to cover them. Banks also regularly borrow money from each other overnight to cover any shortfalls.[56]

In traditional banking, double-spending maximizes economic resources. Lumps of money that would otherwise be just sitting in savings accounts are instead circulated in the form of loans, which stimulate economic growth and also earn interest for the bank.[57]

With digital currencies, however, double-spending is a different kind of problem.[58] A unit of digital currency is merely a computer file, and computer files can typically be duplicated. As players in the book publishing and music industries know, duplication of digital goods can be problematic.[59] For currencies, however, it would be catastrophic; if any participant in the economy can duplicate units of currency, the result would be hyperinflation and the devaluation of the currency.[60] Moreover, no one could be sure they were getting an original unit of currency, as opposed to a duplicate, which renders every unit of the currency untrustworthy.

With the blockchain, however, the ledger verifies the authenticity of each bitcoin as well as its ownership, meaning that a bitcoin can be in only one place at one time, and once a person has spent it, they can't spend that same one again.[61]

C. Bitcoin's Themes: Transparency and Democracy

One of the innovations of Bitcoin, both as a payment system and a currency generator, is that it operates without a central processor. This is deliberate. Bitcoin's original author was critical of currency and payment systems that required central banks and other trusted financial intermediaries, and Bitcoin was framed specifically as "an electronic payment system based on cryptographic proof instead of trust."[62] The blockchain, that automated electronic ledger, thus operates without any one person or entity hitting a "confirm" button; rather, networked computers crunch the numbers and once consensus is reached, the

---

[56] *Id*.

[57] *See* Becker et al., *supra* note 31, at 136 ("Widely trusted (but not necessarily trustworthy) financial institutions handle electronic payments and ensure the integrity of the system's global state. In return, they charge society for this service.").

[58] *See* VIGNA & CASEY, *supra* note 10, at 123.

[59] *See* R. Joseph Cook, Comment, *Bitcoins: Technological Innovation or Emerging Threat?*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 535, 563 (2014).

[60] *See id*.

[61] *See* ANTONOPOULOS, *supra* note 24, at 18; VIGNA & CASEY, *supra* note 10, at 123.

[62] NAKAMOTO, *supra* note 17, at 1.

blockchain automatically confirms the present transactions as well as verifies all previous transactions.[63]

Two themes of Bitcoin philosophy thus emerge: transparency and democracy. Both are nuanced, and they are thrown into relief when comparing the Bitcoin payment system to traditional banking.

Bitcoin transactions are transparent in that they are published. Transactions must be processed and published by an open global network of computers. Contrast this with traditional banks, which publish almost nothing publicly and share information only with the customer and government regulators.[64] Most individual customers appreciate this, naturally, but it creates a system-wide opacity, in that citizens simply have to have faith that the banks are keeping accurate records and managing their leverage, capital reserves, and other financial affairs appropriately. The need for faith is somewhat reduced by the fact that banks are examined and audited by government regulators, but here too, customers need to trust that the regulators are investigating thoroughly and making sound judgments.[65]

Bitcoin again differs from traditional banks when it comes to identifying transacting parties. Although Bitcoin transactions themselves are published, the transacting parties are identified only by wallet numbers, and wallets are established without any personal identifying information.[66] Thus, the transaction's players are unidentified, but the facts of the transaction—its time and amount, as well as the wallet numbers of the parties—is public.[67] This is called being "pseudonymous," anonymous but for a pseudonym.[68] Contrast Bitcoin's user identity shielding with the practice of traditional banks, which are required to comply with extensive reporting and know-your-customer regulations.[69]

Bitcoin is also touted as being democratic in two senses.[70] First, blockchain blocks are not confirmed until a majority of the nodes in the network verifies

---

[63] *Id*. at 3.

[64] *See* 12 U.S.C. § 3403 (2012).

[65] *See infra* Part IV.B.

[66] Grinberg, *supra* note 11, at 163–64.

[67] NAKAMOTO, *supra* note 17, at 6 (likening this process to the "tape" produced by stock trades). The FBI maintains that users' identities can at least sometimes be discerned through transaction patterns, IP addresses, and other clues. FBI DIRECTORATE OF INTELLIGENCE, BITCOIN VIRTUAL CURRENCY: UNIQUE FEATURES PRESENT DISTINCT CHALLENGES FOR DETERRING ILLICIT ACTIVITY (Apr. 24 2012), https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf [https://perma.cc/9WSK-JA9V].

[68] Julie Andersen Hill, *Virtual Currencies & Federal Law*, 18 J. CONSUMER & COM. L. 65, 66 (2014).

[69] *See* Catherine Martin Christopher, *Whack-A-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering*, 18 LEWIS & CLARK L. REV. 1, 6–10 (2014).

[70] Bitcoin is not "democratic" as that term applies to a system of national governance. In fact, Bitcoin is often called "anarchist" because it operates without the consent or support of any national government. *E.g*., Alan Feuer, *The Bitcoin Ideology*, N.Y. TIMES (Dec. 14, 2013), http://www.nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html?_r=0 [https://perma.cc/43SH-7F4S].

and agrees with the calculations in the block.[71] Second, the Bitcoin software is open-source, and any programmer can review it and suggest changes to the code. Once the majority adopts an updated version of the code, that version becomes the dominant and governing one.[72] This is a popular account of the process, but it glosses over an important step.

A small group of core developers—identifiable humans—has password access to the code.[73] They review and evaluate the suggestions made by other programmers, incorporate what they consider to be the good suggestions, and promulgate revised versions of the code for network adoption.[74] They approve small changes by fiat, but for larger ones they moderate a public debate about the utility of the change.[75] This bottleneck of human oversight doesn't fit the narrative of a central-bank-less currency, which may be why many advocates avoid discussing it.

Moreover, Bitcoins are only available for purchase from a few sources, for those users unwilling to wait to win the mining lottery. This also reduces the democratic nature of Bitcoin—a handful of brokers control access to bitcoins.[76] The extreme volatility of the price of bitcoins also prevents low-net-worth or risk-averse individuals from participating; the primary Bitcoin forum specifically advises against converting savings to bitcoins.[77] As a result, only wealthy people can afford the risk of investing in Bitcoin, which is hardly democratic.[78]

---

[71] *See* NAKAMOTO, *supra* note 17, at 6; *see also supra* Part I.A. The consensus mechanism solves what is known as the "Byzantine Generals' problem." ANTONOPOULOS, *supra* note 24, at 4. The expression comes from a hypothetical situation in which several Byzantine armies have surrounded a city at night and need to coordinate an attack in order to take the city in the morning. To reach consensus, envoys of negotiators must be dispatched to the various different camps, traveling back and forth between camps all night while having no idea what plans the other envoys are brokering. As the story goes, the sun comes up before a plan has been agreed to, and the siege is a failure. *See, e.g.*, MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY 2 (2015). Networked computers, on the other hand, can communicate with each other near-instantly over the internet, and can certainly reach consensus long before morning.

[72] Grinberg, *supra* note 11, at 175–76, 176 n.71.

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *See generally* Bayern, *supra* note 13.

[77] *Some Things You Need to Know*, BITCOIN, https://bitcoin.org/en/you-need-to-know [https://perma.cc/N5KR-V22Z] (last visited Aug. 30, 2016):

> The price of a bitcoin can unpredictably increase or decrease over a short period of time due to its young economy, novel nature, and sometimes illiquid markets. Consequently, keeping your savings with Bitcoin is not recommended at this point. Bitcoin should be seen like a high risk asset, and you should never store money that you cannot afford to lose with Bitcoin. If you receive payments with Bitcoin, many service providers can convert them to your local currency.

[78] David Golumbia, *Bitcoin as Politics: Distributed Right-Wing Extremism*, *in* MONEYLAB READER: AN INTERVENTION IN DIGITAL ECONOMY 117, 124 (2015).

D. Third-Party Intermediaries

A whole industry has cropped up around Bitcoin. Some merchants accept bitcoins as payment in exchange for goods and services.[79] Individuals can invest in bitcoins either by owning them directly or purchasing derivatives like futures, options, and swaps.[80]

Digital wallet providers and digital currency exchanges act as interfaces between Bitcoin and those who want to be part of the system but lack the computer literacy to participate directly. Like using a stockbroker, these intermediaries make purchases and sales on behalf of a customer, generally holding bitcoins in their own wallets on the customer's behalf.[81] This means that the individual user doesn't show up on the blockchain—the intermediary appears on the blockchain as the wallet owner, and the individual has a contractual relationship with the intermediary regarding the bitcoins.[82]

The most famous, or infamous, of these intermediaries was Mt. Gox, a digital currency exchange website established in 2010 as a place for winners of the Bitcoin mining lottery to sell their bitcoins to those who wished to buy them.[83] Mt. Gox was tremendously mismanaged by CEO Mark Karpeles; it suffered numerous hacking scandals, the largest of which drove it into bankruptcy in 2014.[84] Mt. Gox held bitcoins on its customers' behalf, and when Mt. Gox itself was hacked, the customers' bitcoins were taken.[85] The individual customers did not appear in the blockchain; rather, Mt. Gox's wallet did. Of course, because the blockchain is impersonal and inviolable, a transaction initiated by a hacker paying bitcoins to himself appears like any other transaction, and it cannot be reversed.

This critical deconstruction of Bitcoin and its blockchain has already begun to unpack several of their important ideological underpinnings, namely their democratic and transparent natures. The bridging model, proposed *infra*, will also provide a framework for deeper analysis of another touchstone: Bitcoin's supposed trustlessness. Bitcoin proponents assert that Bitcoin is an improvement on traditional banking; this section has begun the discussion of how

---

[79] *See, e.g.*, Jonas Chokun, *Who Accepts Bitcoins as Payment? List of Companies, Stores, Shops*, BITCOINVALUES.NET, http://www.bitcoinvalues.net/who-accepts-bitcoins-payment-companies-stores-take-bitcoins.html [https://perma.cc/RFA6-QS7V] (last visited Aug. 30, 2016).

[80] *See* Written Statement from Houman B. Shadab, Professor of Law, New York Law School, to Commodity Futures Trading Commission (Oct. 9, 2014), http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/gmac_100914_bitcoin.pdf [https://perma.cc/8PQ6-S25A].

[81] Bayern, *supra* note 13, at 25.

[82] *See id.* at 25–26.

[83] POPPER, *supra* note 8, at 49–52.

[84] Nathaniel Popper & Rachel Abrams, *Apparent Theft at Mt. Gox Shakes Bitcoin World*, N.Y. TIMES (Feb. 25, 2014), http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html?_r=0 [https://perma.cc/48HY-UVCN].

[85] *Id.*

Bitcoin and banking *differ*, while Part V will analyze in more depth whether Bitcoin is actually *better*.

II. THE INNOVATION AND POTENTIAL OF THE BLOCKCHAIN

Bitcoins—the currency—are fun. They're tech-y, disruptive, and volatile, all of which is very entertaining. They also provide a potential investment vehicle: buy low, sell high, like any other product. But they're not a functional currency. First of all, not everyone uses them, so they're not a useful medium of exchange.[86] Few people even understand them! The infrastructure and education necessary to make them accessible to all is prohibitive. The extreme volatility of the price, combined with irreversible transactions in the event of hacking or theft, means bitcoins aren't a useful store of value, either. The fixed supply, plus the inability of bitcoins to be double-spent, mean a lack of flexibility in response to inevitable crises. All of this is bad for a currency.

The true innovation of Bitcoin is its blockchain: the decentralized public ledger that both verifies and publishes each transaction across the Bitcoin system. "The notion of shared public ledgers may not sound revolutionary or sexy. Neither did double-entry book-keeping or joint-stock companies. Yet, like them, the blockchain is an apparently mundane process that has the potential to transform how people and businesses co-operate."[87]

To reiterate a point made above, Bitcoin and blockchain are not synonymous.[88] Bitcoin has a blockchain, but there are other blockchains that are not Bitcoin's.[89] Kleenex makes tissues, but so does Puff's, Magic Soft, Green Forest, and others. To name a few examples as of this writing, IBM, Visa, and a consortium of private banks are all in some stage of their own blockchain development.[90]

---

[86] *See generally* Becker et al., *supra* note 31; Golumbia, *supra* note 78; Popper, *supra* note 8; Brito et al, *supra* note 21; Max I. Raskin, Note, *Realm of the Coin: Bitcoin and Civil Procedure*, 20 FORDHAM J. CORP. & FIN. L. 969 (2015); Shadab, *supra* note 80; *see also* Jacob Davidson, *No, Big Companies Aren't Really Accepting Bitcoin*, MONEY (Jan. 9, 2015) http://time.com/money/3658361/dell-microsoft-expedia-bitcoin/ (noting that many companies that purport to accept bitcoins are actually just using payment processing services that accept bitcoins, and those payment processing services convert bitcoins to U.S. dollars before remitting payment to the companies). For more on the defining characteristics of a currency (medium of exchange, store of value, unit of measure), see *infra* Part IV.A.

[87] *Trust Machine*, *supra* note 40.

[88] *See supra* Part I.

[89] *See* Joshua Fairfield, *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 37 n.6 (2014), http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=1003&context=wlulr-online [https://perma.cc/54PZ-3GU2].

[90] *See, e.g.*, Jemima Kelly, *R3 Blockchain Group Adds Five Banks, Brings in Technology Heavyweights*, REUTERS (Dec. 16, 2015, 7:15 AM), http://www.reuters.com/article/us-global- banks-blockchain-idUSKBN0TZ1MF20151216 [https://perma.cc/4KQV-XJ8L]; Robert McMillan, *IBM Bets on Bitcoin Ledger*, WALL ST. J. (Feb. 16, 2016, 12:01 AM), http://www.wsj.com/articles/ibm-bets-on-bitcoin-ledger-1455598864 [https://perma.cc/ME6N-LQ8V]; Daniel Palmer, *Visa Seeks Developer for 'Secure, Scalable' Blockchain Project*,

What exactly these blockchains are trying to accomplish is not entirely clear. What problem do they solve?[91] Some speculation:

Blockchains offer security, in the sense that ownership is verified before a transaction is initiated; the transaction itself is confirmed by the disinterested, impersonal network;[92] and the transaction is non-reversible. All these features have some appeal to someone wanting to convey money or property from one party to another.

Blockchains also offer speed. Assuming it has enough processing power to handle the number of transactions, a blockchain is capable of near-immediate settlement.[93] Once a transaction has been initiated, the network begins to process it within a matter of minutes, and the transaction is confirmed and completed a few minutes later. Contrast this efficiency with the overnight clearing generally required by banks, or the potentially days-long process of signing a deed and having it recorded. Banks and recording offices are also only open on weekdays from nine to five, whereas a blockchain is available 24/7.

At its most basic, a blockchain is a ledger. Ledgers can keep track of lots of things, not just bitcoins. Consider property records again. In most of the U.S., real property is identified by metes and bounds descriptions or by a lot number, and then transferred via deeds that are recorded and publicly available. If, instead of identifying property by metes and bounds or by a lot number, each parcel of real property were represented by a specific bitcoin or similar kind of digital token,[94] buying and selling real property would become a significantly streamlined process. The blockchain could verify the seller's ownership of the parcel, eliminating the need for a title search. Upon receipt of the purchase price, the seller could direct the digital token to the buyer's account, and a few minutes later, the buyer would be confirmed as the new owner.

COINDESK (Mar. 2, 2016, 1:35 PM), http://www.coindesk.com/visa-ad-developer-secure-scalable-blockchain [https://perm a.cc/N7RV-2WLU].

[91] I loved a cartoon I saw recently on Twitter, which showed a group of bank employees around a conference table. "All our competitor banks have blockchain labs, and I want one, too!" yells the boss. The employees chime in: "We'll need some blocksperts!" "And a hipster office!" "And an actual customer problem requiring a blockchain!" Santiago Molins (@stupidcache), TWITTER (Jan. 25, 2016, 5:06 AM), https://twitter.com/stupidcache/status/691608 174147821569 [https://perma.cc/ZA5S-J9A5].

[92] A public blockchain certainly has a disinterested, impersonal network. Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM BLOG (Aug. 7, 2015), https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains [https://perma.cc/M5KZ-22ZP]. Consortium or fully-private blockchains, on the other hand, are maintained by computer nodes that have been vetted and given permission to join the network. *Id*.

[93] Elliot Maras, *Deutsche Bank Explores Outlook for Instant Payments & Blockchain Brings Options*, CRYPTOCOINNEWS (Dec. 14, 2015), https://www.cryptocoinsnews.com/deutsche-bank-explores-outlook-instant-payments-blockchain-brings-options [https://perma.cc/4VDU-TM6L].

[94] YONI ASSIA ET AL, COLORED COINS WHITEPAPER, https://docs.google.com/document/d/1AnkP_cVZTCMLIzw4DvsW6M8Q2JC0lIzrTLuoWu2z1BE/edit#heading=h.wxrvzqj8997r [https://perma.cc/CRU7-2EL8].

If this sounds bizarre, consider that it's exactly the same mechanism as a traditional recording system: ownership rights over a piece of real property are written down in some publicly-accessible place, so they can be traced over time and current ownership can be verified. Admittedly, the most hyped attempt to put real property records on a blockchain has so far been unsuccessful, but the potential still exists.[95]

The ownership or authenticity of other property could also be verified by a blockchain: artworks, designer handbags, electronic tickets to concerts or sporting events.[96]

Contractual obligations may also be recordable on a blockchain.[97] Many basic contract provisions can be reduced to computer-programming languages, because they can be reduced to a series of if-then statements.[98] If performance, then payment. If nonpayment, then default. If default, then remedies.

If tangible property is also connected to the internet, then contractual performance (or nonperformance) on the blockchain can have real-world ramifications. Imagine a leased vehicle with an internet-connected key fob.[99] If the lessee fails to make payment, the fob stops working—and the repo man's key fob *starts* working.[100] Crazy, huh?

These innovative applications for the blockchain are sometimes referred to as "blockchain 2.0."[101] If real-world assets can be tracked and transferred on a blockchain, parties can transfer ownership without an intermediary (like a Recorder of Deeds) verifying the transaction.[102]

The utility of all this may not be immediately clear; why put property records on a blockchain when we have a functional recording system in place already? A more reliable, faster recording system would always be preferable to a slow, clunky one, Moreover, blockchain technology, although initially known for its criminal implications,[103] will likely expand into other useful spaces. Sev-

---

[95] *See generally* Pete Rizzo, *Blockchain Land Title Project 'Stalls' in Honduras*, COINDESK (Dec. 26, 2015, 3:31 PM), http://www.coindesk.com/debate-factom-land-title-honduras [https://perma.cc/G33L-HQBE].

[96] *See* SWAN, *supra* note 71, at 9–10.

[97] *See id*. at 9.

[98] Pioneering work in this area was done by Nick Szabo. *See* Nick Szabo, *The Idea of Smart Contracts*, NICK SZABO'S PAPERS AND CONCISE TUTORIALS (1997), http://szabo.best.vwh.net/smart_contracts_idea.html [https://perma.cc/V6AZ-7V8W] [hereinafter *Smart Contracts*]; Nick Szabo, *A Formal Language for Analyzing Contracts*, NICK SZABO'S PAPER AND CONCISE TUTORIALS (2002), http://szabo.best.vwh.net/contractlanguage.html [https://perma.cc/XR6D-BE7G].

[99] SZABO, *Smart Contracts*, *supra* note 98.

[100] *See Smart Property*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Smart_Property [https://perma.cc/8CYY-ZWAB] (last visited Aug. 31, 2016).

[101] *E.g*., SWAN, *supra* note 71, at 10. Some sources go further. *See id*. at xv–xvi (distinguishing between Blockchain 2.0 (financial contracts on the blockchain) and Blockchain 3.0 (further applications of smart contracting)).

[102] Fairfield, *supra* note 89, at 38, 41.

[103] *See* Christopher, *supra* note 69, at 19–20.

eral sources have likened the blockchain to Napster, the music-sharing service.[104] What began as a company with shady overtones turned out to be a pioneering development in peer-to-peer file sharing, a technology that has grown to encompass other useful applications.

Nakamoto understood at Bitcoin's inception that the blockchain had additional potential beyond Bitcoin, but many useful applications for the blockchain are likely in the future.[105] This overview of the blockchain's innovative applications is admittedly cursory, but the blockchain's potential is only beginning to be understood.[106] Future work should further investigate the utility and viability of blockchain technology in contracts, as well as the legal and social implications of such applications.

This future work should also consider the enforcement mechanisms inherent in the blockchain and whether they further the social goals and legal doctrines that govern and guide existing contract forms. For instance, if access to a rented apartment is governed by the blockchain and the tenant defaults on the rent, the blockchain could conceivably inhibit the tenant's access to the apartment.[107] This may, however, circumvent important bodies of landlord/tenant law.[108] Future work must consider what role a trusted intermediary—including but not limited to the judiciary—can and should play in an enforcement-based system to prevent unjust or dangerous results.

III. TRUST

Bitcoin has been touted from its inception as being a "trustless" payment system and currency, with the unexamined assumption being that a trust-based system is inherently worse than a trustless one.[109] This begs the question of what role trust does—and should—play in finance, business, contract, and economic activity generally.

Despite the fact that trust has been examined across many social science disciplines, no uniform or universal definition has emerged. Trust has been defined as "willingness to rely on an exchange partner in whom one has confidence,"[110] a generalized "expectancy held by an individual . . . that the word . . .

---

[104] Cook, *supra* note 59, at 562; *Trust Machine*, *supra* note 40.

[105] *See* NAKAMOTO, *supra* note 17, at 1 (referencing escrow services).

[106] Fairfield, *supra* note 87, at 38, 41; *see e.g.*, SWAN, *supra* note 71, at xv–xvi.

[107] I am grateful to Tracy Hresko Pearl for this hypothetical.

[108] Szabo also anticipated that there may be circumstances in which automatic enforcement may not be desirable: in discussing automatic termination of an auto lease, he pointed out that "it would be rude to revoke operation of the car while it's doing 75 down the freeway." SZABO, *Smart Contracts*, *supra* note 98.

[109] NAKAMOTO, *supra* note 17, at 1.

[110] Christine Moorman et al., *Factors Affecting Trust in Market Research Relationships*, 57 J. MARKETING 81, 82 (1993).

of another . . . can be relied upon,"[111] and, in the context of e-business, "general reliance of business actors and private citizens or consumers on other actors or systems within the Information Society."[112]

What most definitions of trust have in common is the concept of uncertainty.[113] If a thing is certain, there is no need for trust because there is only knowledge that the thing will be. Trust, then, is usually described as a belief in something despite its uncertainty.[114] Definitions of trust often contain not only words like "uncertainty," "perceived risk," and "vulnerability," but also their antitheses: words like "confidence," "reliability," and "integrity."[115]

If defining trust is difficult, measuring it is even more so.[116] The published literature relies primarily on surveys about individuals' opinions, or on human behavioral experiments with names like "basic trust game" and "gift exchange game," which are variations on the prisoner's dilemma scenario.[117] Huge numbers of variables have been analyzed with regard to whether they contribute to (or detract from) the strength of a person's trust. Studies have investigated endogenous factors like the person's risk tolerance, beliefs about other people's trustworthiness, and aversion to feeling betrayed; exogenous factors such as broader social beliefs, ethno-linguistic homogeneity, and common religion; and even neurobiological factors that suggest evolutionarily-beneficial explanations for trusting behavior.[118]

While trust is usually defined in relation to the trustor's vulnerability, some studies also investigate the trustee's reaction and its consequences. Once a trustor has initiated a trusting behavior, the trustee is in a position to exploit that trust for his own benefit.[119] However, a trustee who takes advantage of trusting

---

[111] Julian B. Rotter, *A New Scale for the Measurement of Interpersonal Trust*, 35 J. PERSONALITY 651, 651 (1967).

[112] Sara Jones et al., *Trust Requirements in E-Business*, 43 COMM. ASS'N FOR COMPUTING MACHINERY 81, 83 (2000).

[113] Deepak Malhotra, *Trust and Reciprocity Decisions: The Differing Perspectives of Trustors and Trusted Parties*, 94 ORGANIZATIONAL BEHAV. & HUM. DECISION PROCESSES 61, 62–64 (2004); GERARDO A. GUERRA & DANIEL J. ZIZZO, OXFORD INTERNET INST., ECONOMICS OF TRUST IN THE INFORMATION ECONOMY: ISSUES OF IDENTITY, PRIVACY AND SECURITY 3 (2003).

[114] *See* GUERRA & ZIZZO, *supra* note 113, at 3. For the purposes of this paper, trust is understood as an emotion that, once in existence, causes or permits a party to engage in some behavior. *But see, e.g.*, ERNST FEHR, INST. STUDY LAB., ON THE ECONOMICS AND BIOLOGY OF TRUST 3 (2008) (conflating the emotion of trust with the trusting behavior it engenders).

[115] Avinandan Mukherjee & Prithwiraj Nath, *Role of Electronic Trust in Online Retailing: A Re-Examination of the Commitment-Trust Theory*, 41 EUR. J. MARKETING 1173, 1177 (2007).

[116] *See* FEHR, *supra* note 114, at 2.

[117] *E.g.*, MICHAEL BACHARACH ET AL., OXFORD UNIV., DEP'T OF ECON., IS TRUST SELF-FULFILLING? AN EXPERIMENTAL STUDY 2–3 (2001); Ernst Fehr & Simon Gächter, *Do Incentive Contracts Undermine Voluntary Cooperation?* 3 (U. Zurich Inst. Empirical Research in Econ., Working Paper No. 34, 2002).

[118] *See* FEHR, *supra* note 114, at 2, 15, 21–22.

[119] BACHARACH ET AL., *supra* note 117, at 3; GUERRA & ZIZZO, *supra* note 113, at 2.

behavior risks punishment from the trustor(s).[120] Trustors have even been found to punish trustees for seeking verification, or otherwise taking away the trust opportunity.[121] On the other hand, some people demonstrate "trust responsiveness," in that they are more likely to behave in a trustworthy manner once they realize trust has been placed in them.[122] Unsurprisingly, the more sympathy or respect the trustee has for the trustor, the more trust-responsive the trustee will be.[123]

Some social scientists posit that trust is required when there is a lack of legal commitment, suggesting that the absence of a legal enforcement mechanism causes the very uncertainty that in turn requires trust before the parties enter into an agreement or exchange.[124] For those in the legal field, however, the mere presence of a public or private law enforcement mechanism may not be enough. The outcomes of negotiation, litigation, or other dispute resolution mechanisms are probably still uncertain enough that trust is required before entering into even legally enforceable agreements. Indeed, at least one study has measured the percentage of law students per capita across countries as a proxy for lack of trust: large numbers of law students were presumed to signal "problems in the legal enforcement of property rights and contracts in the absence of effective social norms[.]"[125]

More broadly, trust plays an important role in economic activity. Trusting economic actors invest and trade more, expanding the reach of their economic activity in spite of the uncertainty of their returns or utility.[126] Given that a trustee is by nature provided the opportunity to exploit a trustor's vulnerability, it is paradoxically necessary for a trustee to decline that self-interested opportunity in order for an economy to thrive.[127]

When business takes place solely or primarily online, trust formation is even more important.[128] Without interpersonal interaction and social and cultural norms to aid in evaluating uncertainty, trust formation can be more difficult.[129] Moreover, a trustor engaging in purely electronic business activities must place trust not only in the counterparty but also in the reliability and secu-

---

[120] *See* Ernst Fehr & Simon Gächter, *Cooperation and Punishment in Public Goods Experiments*, 90 AM. ECON. REV. 980, 980 (2000); *see also* FEHR, *supra* note 114, at 13 ("Betrayal aversion means that people dislike non-reciprocated trust. It is plausible that people who experience particularly high disutility from non-reciprocated trust have a high willingness to punish non-reciprocating players.").

[121] GUERRA & ZIZZO, *supra* note 113, at 17.

[122] BACHARACH ET AL., *supra* note 117, at 6.

[123] *Id*.

[124] *See* FEHR, *supra* note 114, at 3.

[125] *See id*. at 22.

[126] *See id*. at 23–24.

[127] *See* GUERRA & ZIZZO, *supra* note 113, at 4.

[128] *See* Mukherjee & Nath, *supra* note 115, at 1176.

[129] *See, e.g*., GUERRA & ZIZZO, *supra* note 113, at 4; Mukherjee & Nath, *supra* note 115, at 1179.

rity of the counterparty's information and delivery systems.[130] For instance, a customer's trust in an online banking system depends on whether the customer perceives the bank to share the customer's values, on the bank's responsiveness in communicating with the customer, and on the customer's sense of security that the bank will not engage in opportunistic behavior.[131] Customers particularly demand assurances regarding the privacy and security of their financial information as an antecedent to trusting behavior.[132]

The broad availability of electronic information may (at least partially) compensate for the uncertainty built into a transaction not conducted face-to-face.[133] Collecting that information may violate privacy, however, resulting in "trust tension."[134] The "absence of data impedes trust as accountability is limited, but data gathering creates trust problems regarding the use of the data in question and intrusions on privacy."[135] Another dilemma may be that electronic information is not itself well-verified; for example, online review systems are under frequent fire for being unfair.[136]

A. Trust Models

The process of establishing trust and the effects of doing so are sometimes represented in the literature as trust models—either as a kind of flow chart or as an algebraic expression. The notoriously math-phobic legal academy will no doubt be daunted by an algebraic expression:

> Henceforth we write t for the probability with which the truster R chooses T[rusting behavior] and f the probability with which the trustee E chooses F[ulfilling behavior]. We let t^* denote E's estimate of t, f^* R's estimate of f, and f^{**} E's estimate of f^*. We call f the trustee's *propensity to fulfill*, f^* the truster's *confidence*, and f^{**} the trustee's *confidence-perception*.
>
> Trust responsiveness implies that f increases with f^{**}. But this is not quite enough to characterize the intuitive notion: we must add the proviso that the function expresses a causal relation from f^{**} to f; E must be made more ready to

---

[130] *See, e.g.*, Jones et al., *supra* note 112, at 83.

[131] Mukherjee & Nath, *supra* note 115, at 1178.

[132] *Id.*

[133] GUERRA & ZIZZO, *supra* note 113, at 4.

[134] *Id.* at 5.

[135] *Id.*

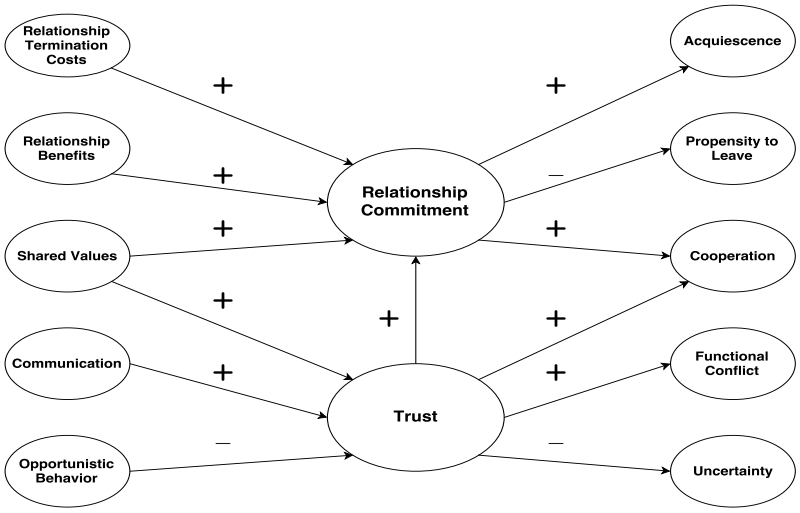
[136] *See generally* JENNIFER BROWN & JOHN MORGAN, HAAS SCHOOL OF BUS., U.C. BERKELEY, REPUTATION IN ONLINE MARKETS: SOME NEGATIVE FEEDBACK (2006), http://faculty.haas.ber keley.edu/rjmorgan/reputation%20in%20online%20markets.pdf [https://perma.cc/RK5F-5N 6J]; *see also* Daniel Roberts, *Yelp's Fake Review Problem*, FORTUNE (Sept. 26, 2013, 3:05 PM), http://fortune.com/2013/09/26/yelps-fake-review-problem [https://perma.cc/82RL-V8 S9]; Brent Underwood, *Behind the Scam: What Does It Take to Be a 'Best-Selling Author'? $3 and 5 Minutes*, OBSERVER (Feb. 23, 2016, 10:00 AM), http://observer.com/2016/02/behind-the-scam-what-does-it-takes-to-be-a-bestselling-author-3-and-5-minutes [https://perma.cc/V B32-XF35].

> play F *because* she believes that *R* expects her to. . . . In sum, a trustee is *trust responsive* if an increase in *f*** tends to bring about an increase in *f*.[137]

Got that? All this is to say that when a parent tells a child, "I'm trusting you to . . ." and the child believes them and behaves better, the child is considered "trust responsive."[138]

The flow-chart models are perhaps more accessible. The flow charts demonstrate how variables and behaviors build upon and influence each other, moving through "trust" (usually the centerpiece) towards ultimate behaviors. For example, Morgan and Hunt (Fig. 1) theorize that in order to develop long-term relationships between customers and businesses, the parties must have shared values and prompt, honest communication.[139] These, plus an avoidance of opportunistic behavior, build trust.[140] Trust, along with the acknowledgement of relationship benefits (plus higher relationship termination costs), leads to a relationship commitment.[141] Relationship commitment, again along with trust, leads to parties' acquiescence, cooperation, and "functional" conflict, while reducing uncertainty and propensity to leave the relationship.[142]

FIGURE 1: MORGAN AND HUNT MODEL: RELATIONSHIP COMMITMENT AND TRUST



[137] BACHARACH ET AL., *supra* note 117, at 6.

[138] *Id*. For more on trust reciprocity, see Malhotra, *supra* note 113, at 62–64*; see also* Madan M. Pillutla et al., *Attributions of Trust and the Calculus of Reciprocity*, 39 J. EXPERIMENTAL PSYCHOL. 448 (2003).

[139] Robert M. Morgan & Shelby D. Hunt, *The Commitment-Trust Theory of Relationship Marketing*, 58 J. MARKETING 20, 22 (1994).

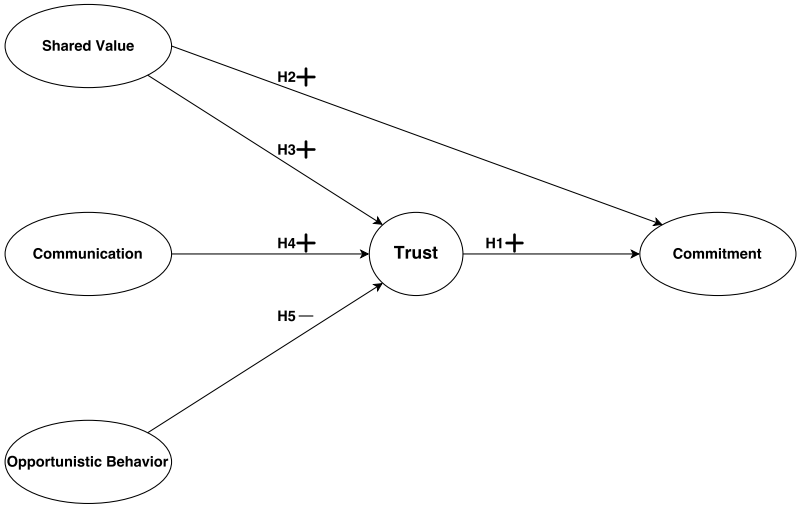
[140] *Id*.

[141] *Id*.

[142] *Id*.

Mukherjee and Nath have written multiple papers building on the Morgan and Hunt model. In 2003, they analyzed trust-building and relationship marketing in the online banking context, proposing a slimmed-down version of the Morgan and Hunt model (Fig. 2).[143] In this model, they determine that shared values, good communication, and avoidance of opportunistic behavior build trust, and that trust (along with shared values) leads to relationship commitment:[144]

FIGURE 2: MUKHERJEE AND NATH TRUST-BUILDING MODEL

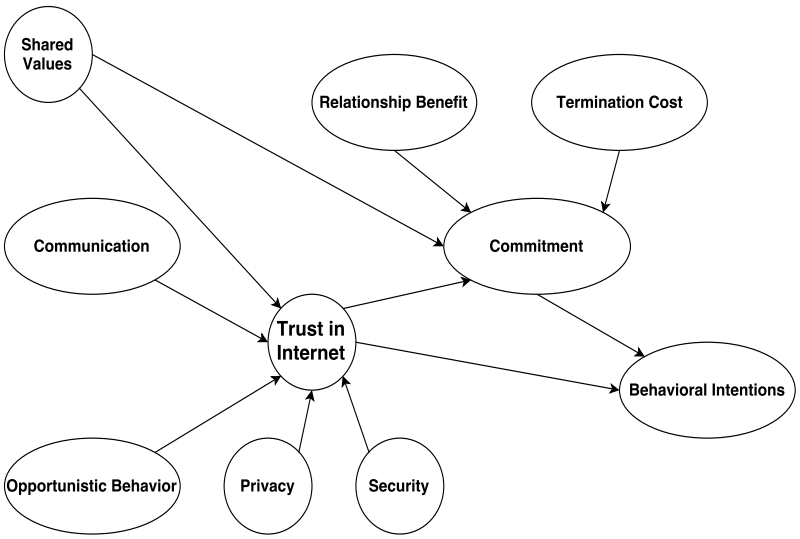


In 2007, Mukherjee and Nath analyzed relationship marketing in online retailing more broadly. Their 2007 model (Fig. 3) expands the streamlined 2003 version, introducing privacy and security as variables in trust-building and adding relationship benefits and termination costs into the formation of relationship commitment.[145] They also expand the end-product of the model, reincorporating the Morgan and Hunt conceptualization of relationship commitment as a waystation toward behavior, rather than an end in and of itself:[146]

---

[143] Avinandan Mukherjee & Prithwiraj Nath, *A Model of Trust in Online Relationship Banking*, 21 INT'L J. BANK MARKETING 5, 9 (2003).
[144] *Id*.
[145] Mukherjee & Nath, *supra* note 115, at 1183.
[146] *Id*.

FIGURE 3: MUKHERJEE AND NATH RELATIONSHIP MARKETING MODEL



These models offer qualitative analysis of the factors that build trust in an individual party and how that trust manifests itself in business decisions. Missing from these models is the legal component—the enforcement mechanisms that exist, in part, to remove the need for trust.

Some social-science work assumes that the mere existence of a legal framework supplants the need for trust, suggesting that trust is necessary only where legal mechanisms are absent.[147] As any lawyer knows, however, the mere existence of a legal system is a far cry from certainty of outcome—contract enforcement via litigation is full of risks and unknowns, and even if a judgment is obtained, it may not be collectible.

To understand better how enforcement mechanisms interact with trust in contract formation, then, a more sensitive model is necessary.

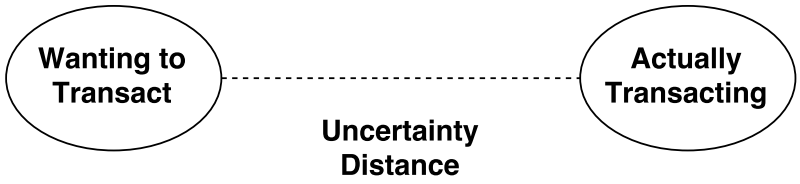
B. Proposed Model: Bridging

This paper proposes a new conceptualization of trust, with particular implications for business and law. The model begins with the premise that there is a distance between wanting to do something and doing (or committing to doing) it; this distance represents the uncertainty of the performance occurring. One party is interested in entering into a transaction or contract but is uncertain whether the other party will perform adequately. This uncertainty, visualized here as a distance, must be overcome before the parties actually enter into the transaction or contract (Fig. 4).

---

[147] *E.g.*, Jones et al., *supra* note 112, at 83–84; FEHR, *supra* note 114, at 3.

FIGURE 4: UNCERTAINTY DISTANCE



The uncertainty distance may also be characterized as the party's *reluctance* to enter into the transaction or contract. Only by overcoming this reluctance will the parties enter into the transaction or contract.

There is no attempt here to quantify the uncertainty distance. For a particularly risk-averse actor, the uncertainty distance may be wide; for a risk-tolerant actor, or for someone who is simply unconcerned with possible negative repercussions, the uncertainty distance may be minimal.

Whatever its size, the distance between wanting to transact and actually transacting is overcome by a combination of two things: trust and enforcement mechanisms. The more absent or vaguer the enforcement mechanisms, the more trust is necessary to bridge the uncertainty distance and for the parties to enter into the transaction (Fig. 5), and vice versa: the more reliable the enforcement mechanism, the less trust is necessary (Fig. 6).

FIGURE 5: WEAK ENFORCEMENT/HIGH TRUST: DISTANCE BRIDGED

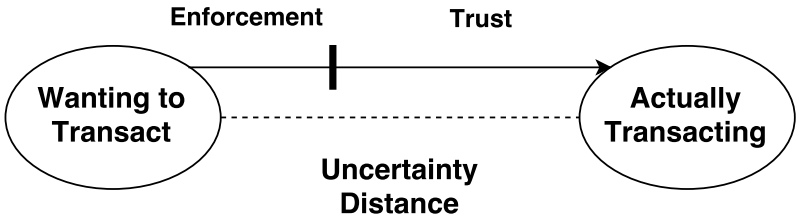
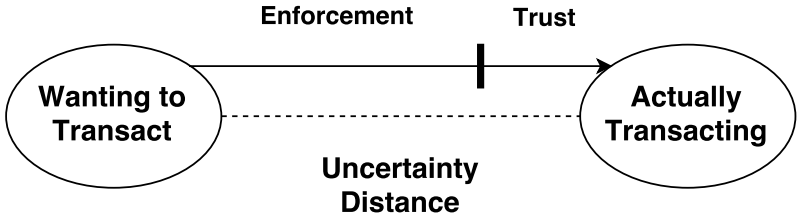
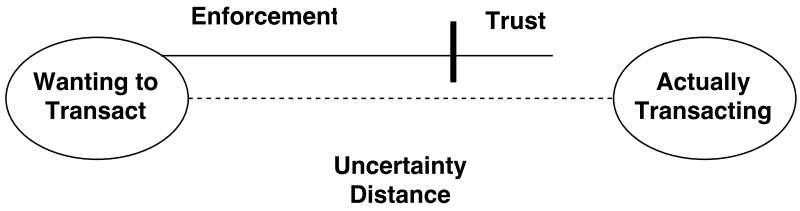


FIGURE 6: STRONG ENFORCEMENT/LOW TRUST: DISTANCE BRIDGED



It is also possible that a proposed transaction or contract will not have enough enforcement potential or trust to effectively bridge the uncertainty distance (Fig. 7). In such a situation, the parties would not bridge the uncertainty distance, and no transaction or contract would result:

FIGURE 7: LOW ENFORCEMENT/LOW TRUST: DISTANCE NOT BRIDGED



Importantly, the word *enforcement* is not used here in the sense that parties will be forced to perform under the contract. Rather, enforcement here refers to any mechanism that will make an aggrieved party whole in the event of breach or other violation. Enforcement mechanisms eliminate party risk; they may do so by requiring specific performance or the payment of damages by the counterparty, or they may be third-party reassurance, such as insurance providers.

Enforcement mechanisms may be broadly understood.[148] They may be formal, public affairs such as litigation to compel specific performance or assess money damages. Enforcement may also be informal or semiformal, private or semiprivate. Social norms[149] and relationship pressures can serve as informal enforcement mechanisms,[150] though they may be as public or as private as the enforcer effectuates—public shaming of a counterparty may be a very effective enforcement mechanism, though not necessarily a relationship-building one. Alternative dispute resolution, trade association governance, and network governance may be considered "semiformal" enforcement, in that third-party adjudication may be present (though not by a formal court).[151] Trade association

[148] The bridging model may encompass, but does not require, distinctions between types of enforcement mechanisms. For more on differentiation between enforcement mechanisms, see *e.g.*, Barak D. Richman, *Firms, Courts, and Reputation Mechanisms: Towards a Positive Theory of Private Ordering*, 104 COLUM. L. REV. 2328 (2004) (proposing a model to distinguish between firm-based, court-based, and reputation-based enforcement mechanisms, and to predict when each type of mechanism will be utilized).

[149] *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES 123–264 (1991) (exploring the development of behavioral norms and social order among cattle ranchers in Shasta County, California, irrespective of existing legal and market mechanisms).

[150] Ronald J. Gilson et al., *Braiding: The Interaction of Formal and Informal Contracting in Theory, Practice, and Doctrine*, 110 COLUM. L. REV. 1377, 1378–80 (2010).

[151] *See* Lisa Bernstein, *Beyond Relational Contracts: Social Capital and Network Governance in Procurement Contracts*, 7 J. LEGAL ANALYSIS 561, 562 (2015); *see also* CHARLES FRIED, CONTRACT AS PROMISE: A THEORY OF CONTRACTUAL OBLIGATION 21–27 (1981).

governance and network governance may be considered "semiprivate" as well, in that industry players may be informed of adjudications and enforcement, but the general public is not. Insurance may also provide a kind of enforcement mechanism, assuring parties that they will be made whole (if not by their counterparties) in the event of nonperformance.

Whatever form enforcement may take, it may be understood as an exogenous force on the party's ability to bridge the uncertainty distance. The party does not exert control over the formation or existence of the enforcement mechanism. Trust, on the other hand, is endogenous, in that it comes from within the trusting party.[152]

Current legal theory in trust and contracts can be incorporated and understood through this bridging model. Professor Fried, for instance, has explored whether contractual obligations exist because of external pressures on parties or because of internal, moral principles that compel performance of a promise.[153] Professor Fried's emphasis on the moral basis for contract law does not appear in the bridging model, but the tension of whether contracts are performed in response to internal or external forces is neatly incorporated: both external enforcement mechanisms *and* internal trust contribute to overcoming the uncertainty distance.

More recently, Professor Bernstein explores governance of master supply agreements between original equipment manufacturers, suggesting that interreliant firms in a given industry can, via procurement contracts, turn over the governance and enforcement of these agreements to a trade association or other form of social governance.[154] Likewise, Professor Richman has explored community institutions among ultra-Orthodox Jews that generate specific economic efficiencies in the diamond industry beyond what could be expected using public courts and contract law doctrines.[155] These industry-specific examples can be understood in the bridging model as specialized or additional kinds of enforcement mechanisms that reduce the amount of trust necessary to bridge the uncertainty distance between wanting to transact and actually transacting.

In a series of papers, Professors Gilson, Sable, and Scott explore contracts for innovation, or contracts between component manufacturers who are work-

---

[152] Malhotra and Murninghan also characterize trust as internal, while contract (an enforcement mechanism) is an external behavioral control. Deepak Malhotra & J. Keith Murnighan, *The Effects of Contracts on Interpersonal Trust*, 47 ADMIN. SCI. Q. 534, 536 (2002).

[153] *See* FRIED, *supra* note 151, at 5.

[154] *See generally* Bernstein, *supra* note 151.

[155] Barak D. Richman, *How Community Institutions Create Economic Advantage: Jewish Diamond Merchants in New York*, 31 L. & SOC. INQUIRY 383 (2006); *see also* Barak D. Richman, *Ethnic Networks, Extralegal Certainty, and Globalisation: Peering into the Diamond Industry*, *in* LEGAL CERTAINTY BEYOND THE STATE 31, 35 (Volkmar Gessner ed., 2009); Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. LEGAL STUD. 115, 115 (1992).

ing to develop cutting-edge technologies.[156] These contracts fascinate because the parties do not know at the outset what specifications, or even what products, are going to be produced; rather, the contracts are carefully designed to set out each party's responsibilities in an ongoing collaboration toward something inarticulable.[157] Gilson, Sable, and Scott propose that these contracts "braid" formal and informal enforcement mechanisms together, which in turn builds trust between the parties[158]—this process is in lieu of parties establishing trust first, then agreeing to these difficult-to-articulate contractual arrangements.

The proposed model from this paper would incorporate the "braiding" concept differently, suggesting that braided enforcement mechanisms together increase overall enforcement capacity and reduce the amount of trust necessary to bridge the distance between wanting to transact and actually doing so.

The bridging model assumes a fixed uncertainty distance for any given transaction, so that building additional trust—while pleasant—is not necessary once the uncertainty distance is bridged. Put another way, superfluous trust is nice but not necessary. Increasing amounts of trust over time do not cause the enforcement mechanisms to shrink or the uncertainty distance to change. Rather, enforcement exists as an exogenous force on transaction formation, and it is not forced to constrict as trust expands.

It is also possible that as the relationship between two parties continues, the balance between enforcement and trust may shift. Parties may begin their relationship with one combination of enforcement reliance and trust, but enforcement mechanisms may become more or less reliable over time. For instance, Bernstein posits that trade associations and network governance can be effective;[159] the effectiveness of these mechanisms may change as industries develop. A nascent industry may have weak (or untested) enforcement mechanisms, but as the industry matures and grows, trade associations and networks may self-reinforce. The opposite is also true: a dying industry may have enforcement mechanisms with ever-dwindling authority. In either case, as the efficacy of the enforcement mechanism changes, the amount of trust necessary to bridge the uncertainty distance would also change. Of note, a dwindling enforcement mechanism and a lack of trust between parties may well mean that the uncertainty distance is no longer bridged, and transactions will cease.

---

[156] *See* Ronald J. Gilson et al., *Contracting for Innovation: Vertical Disintegration and Interfirm Collaboration*, 109 COLUM. L. REV. 431, 434–35 (2009) [hereinafter *Contracting for Innovation*]. *See generally* Gilson et al., *supra* note 150; Ronald J. Gilson et al., *Contract and Innovation: The Limited Role of Generalist Courts in the Evolution of Novel Contractual Forms*, 88 N.Y.U. L. REV. 170 (2013); Ronald J. Gilson et al., *Text and Context: Contract Interpretation as Contract Design*, 100 CORNELL L. REV. 23 (2014); Ronald J. Gilson et al., *Contract, Uncertainty and Innovation* (Colum. Law Sch. Law & Econ. Paper Series, Working Paper No. 385, 2011).

[157] *Contracting for Innovation*, *supra* note 152, at 449.

[158] Gilson et al., *supra* note 150, at 1384.

[159] *See* Bernstein, *supra* note 151, at 562.

The model does not suggest what balance of enforcement and trust is optimal. While it may seem at first blush that an entirely enforcement-based bridge is preferable, the analysis in Part V, below, suggests that the incorporation of at least some trust is inevitable—even beneficial.[160]

Information exchange can expand the quantity of both enforcement reliance and trust. Parties that are better informed about available enforcement mechanisms (formal or otherwise) will generally perceive expanded enforcement capabilities, and as parties learn more about each other (values and interests, history of past dealings, etc.) they will have the opportunity to build more trust between them.

The proposed model may undoubtedly be improved. The model, for instance, does not currently suggest what *creates* the trust that contributes to bridging the uncertainty distance. This vacuum is a departure from the social-science research summarized above, which does focus on variables and behaviors that affect trust formation.[161] The role of information sharing, especially online, including reputation formation and interpretation, might be explored. Future work may also consider additional forms of enforcement mechanisms that increase the amount of certainty in a transaction and thereby reduce the amount of trust necessary to bridge the distance between wanting to enter a transaction and actually doing so.

IV. THE BRIDGING MODEL APPLIED TO TRADITIONAL BANKING

As an illustration of the bridging model in application, this Part applies the model to traditional banking, understood roughly here to mean the brick-and-mortar U.S. banking system of the past hundred years or so.

A. Currency and the Money Supply

Traditional banking relies on money, as opposed to relying on a barter system.[162] Currency has three characteristics: it is a unit of account, a store of value, and a medium of exchange.[163]

---

[160] Relatedly, Professor Malhotra has suggested that overly complex or incentive-based contacts can be perceived as insulting, and that the proposal or presence of such contracts can actually erode preexisting trust between the parties. Deepak Malhotra, *When Contracts Destroy Trust*, HARV. BUS. REV., May 2009, at 25.

[161] In exploring this question, the work of Shapiro, Sheppard, and Cheraskin (1992) may be useful, which suggests "three broad categories (or typologies) of trust: deterrence-based trust, knowledge-based trust, and identification-based trust." Malhotra, *supra* note 113, at 61.

[162] Some sources distinguish between money and currency—money is an idea, while currency is the physical representation of value. *See* Ralph E. McKinney, Jr. et al., *The Evolution of Financial Instruments and the Legal Protection Against Counterfeiting: A Look at Coin, Paper, and Virtual Currencies*, 2015 U. ILL. J. L. TECH. & POL'Y 273, 277 (2015). The distinction is not important for the purposes of this Article, and the terms will be used interchangeably here.

[163] Angela Walch, *The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y 837, 848–49 (2015).

A *unit of account* is simply a way of quantifying how many of one thing equals how many of another. It's a way of measuring value against a consistent standard. Anything can be a unit of account,[164] but in the United States we measure value in dollars and cents. Dollars and cents can, in turn, be valued in other currencies—at the time of this writing, for instance, one U.S. dollar is worth about 0.91 Euros, 6.52 Chinese yuan, 3,309 Colombian pesos, and 0.30 Kuwaiti dinar.[165]

Currency is a *store of value* when its value is relatively consistent.[166] This ensures the buying power of a unit of currency today is about the same as it will be tomorrow, making the currency a good vehicle for savings. If the value of a currency were unpredictable and unstable, people would tend to spend all the money they obtain, because they can't be sure how much it will buy in the future.

Money serves as a *medium of exchange* because all goods and services in the economy can be reduced to their price and can be exchanged for that universally accepted item, currency.[167] This allows people to trade without bartering and facilitates price comparison.[168]

A functional currency requires a tremendous amount of trust by an entire society. This is true whether the currency is "fiat" (government-issued) or "specie" (tied to the value of some other precious commodity, such as gold or silver).[169] Specie currencies are presumed to be inherently valuable, while fiat currencies are valuable because they are backed by a government, making them legal tender for paying debts.[170]

The U.S. dollar is a functional medium of exchange because people agree to express their offered goods and services in dollar-denominated prices and agree to accept dollars in exchange for those goods and services.[171] It is a store of value because its value is relatively consistent, and people trust that their savings of U.S. dollars will generally hold value over time.

The dollar is "backed" by the government, which does not mean that dollars can be taken to the steps of the Federal Reserve and exchanged for anything (such as gold). It does mean, however, that the U.S. government takes responsibility for managing the supply of money, in terms of both the physical

---

[164] *See* Columbia, *supra* note 78, at 118; *see also Sesame Street* (PBS television broadcast Dec. 15, 2011) (Drew Brees measures Elmo's height in inches (24), potatoes (4), tubes of toothpaste (3), and footballs (3)).

[165] *Exchange Rates: New York Closing Snapshot*, WALL ST. J., (Feb. 23, 2016), http://www.wsj.com/mdc/public/page/2_3021-forex-20160223.html?mod=mdc_pastcalendar [https://perma.cc/83ZL-PA6A].

[166] *See* Walch, *supra* note 163, at 848–49.

[167] *See* Becker et al., *supra* note 31, at 2.

[168] *Money*, THISMATTER, http://thismatter.com/money/banking/money.htm [https://perma.cc/TYF7-US4L] (last visited Aug. 31, 2016).

[169] *See, e.g.*, Grinberg, *supra* note 11, at 173.

[170] *Id.*

[171] *See, e.g.*, McKinney, *supra* note 162, at 275.

bills in circulation and the total money supply.[172] As with all things, the value of a dollar is connected to its scarcity,[173] and the number of dollars in circulation is carefully monitored and managed by the federal government.[174]

Using the bridging model, the use of currency in a society can be expressed in this way: the uncertainty distance between wanting to transact in U.S. dollars and actually doing so is bridged by a combination of (1) enforcement, in the form of government backing, and (2) trust. Unpacking this a bit further, however, reveals that government "backing" may not be the lock-step enforcement mechanism many assume.

Certainly, the federal government has a monopoly on the printing and distribution of physical dollar bills.[175] The Constitution grants Congress alone the power to coin money,[176] and this process is monopolized by the Department of the Treasury.[177] Federal law establishes U.S. coins and currency as legal tender.[178] To maintain the value of the currency, counterfeiting is a federal crime,[179] and the Secret Service is tremendously efficient at stamping out counterfeiting.[180]

The management of the intangible money supply is handled by the Federal Reserve ("the Fed"). The Fed uses three main tools here.[181] First, the Fed sets the discount rate, the interest rate at which the Fed lends money to other banks, which then has a spillover effect on the interest rates those banks charge customers and each other.[182] Higher interest rates generally encourage saving and

---

[172] *See, e.g.*, *Money*, FED. RESERVE BANK DALL. (Sept. 2013), https://www.dallasfed.org/assets/documents/educate/everyday/money.pdf [https://perma.cc/J2ZR-253G].

[173] *See* Becker et al., *supra* note 31, at 2.

[174] *See infra* Part IV.A.

[175] Most of us take paper dollars for granted, but the transition from coin to paper was a dramatic Constitutional question in the latter half of the nineteenth century. *See generally* James B. Thayer, *Legal Tender*, 1 HARV. L. REV. 73 (1887).

[176] U.S. CONST. art. I, § 8, cl. 5. The very next clause authorizes Congress to punish counterfeiting. U.S. CONST. art. I, § 8, cl. 6. The states are expressly forbidden to coin money. U.S. CONST. art. I, § 10, cl. 1.

[177] 31 U.S.C. §§ 301–304 (2012). Section 301 establishes the Department of the Treasury, section 302 identifies the Department of the Treasury as the Treasury of the United States. Section 303 establishes the Bureau of Engraving and Printing (which produces paper currency), and section 304 establishes the United States Mint (which produces coins). *Id.*

[178] 31 U.S.C. § 5103 (2012). *See also* Julliard v. Greenman (The Legal Tender Cases), 110 U.S. 421 (1884).

[179] 18 U.S.C. §§ 472–473 (2012).

[180] JASON KERSTEN, THE ART OF MAKING MONEY: THE STORY OF A MASTER COUNTERFEITER 56–57 (2009).

[181] The three tools outlined here are the traditional ones. During times of crisis, the Fed may engage—and has, historically—in additional economic management tools, e.g. qualitative easing. *See* Tracy Alloway & Luke Kawa, *Say Goodbye to the Fed You Once Knew*, FORBES (Apr. 14, 2016), http://www.bloomberg.com/news/articles/2016-04-14/say-goodbye-to-the-fed- you-once-knew [https://perma.cc/B8YN-ZU79].

[182] Kathryn Reed Edge, *Bank on It: Interest Rates 101*, TENN. B. J., Aug. 2015, at 32, 33; *About the Federal Open Market Committee*, BD. GOVERNORS FED. RESERVE SYS., http://

discourage borrowing, thereby decreasing lending and the overall money supply.[183] Second, the Fed conducts open-market operations, either buying or selling securities to expand or contract the amount of money in general circulation.[184] When the Fed buys securities, it collects those securities from the public sphere and replaces them with dollars, expanding the money supply. When the Fed sells securities, the money supply contracts because the Fed is collecting dollars from other economic actors and replacing those dollars with less liquid securities. Third, the Fed, as a banking regulator, can adjust the reserve requirement, or the amount of deposits the banks are required to keep.[185] A reserve requirement of 10 percent means that $90 of every $100 can be lent out; a reserve requirement of 12 percent means that only $88 of every $100 can be lent. Increasing the reserve requirement thus decreases the money supply.

Managing the money supply steadies a currency's value; the invention of central banking demonstrably reduced the volatility of currencies and the depth of economic shocks.[186] Most economists agree that central bank management of the money supply is a social good.[187]

This management of the money supply is a form of enforcement, in that it is an exogenous force reassuring users that the vehicle is safe and reliable. To be sure, money supply management it is not automatic. Whereas Bitcoin's algorithm automatically adjusts its difficulty to ensure that production of bitcoins happens consistently every ten minutes,[188] the supply of U.S. dollars is tracked by the Fed and small adjustments are made as the Boards of Governors or the Federal Open Market Committee see fit.[189] This method is, of course, not perfectly reliable. The Fed is made up of people, who sometimes make mistakes. They're trying their best, but they're imperfect. This decreases the impact of the enforcement portion of the bridge, requiring more trust.

Nearly everyone in America uses dollars, even those who refuse to use banks.[190] This suggests that whatever deficiencies may exist in the enforcement mechanisms behind the currency, there is enough trust among Americans to

---

www.federalreserve.gov/monetarypolicy/fomc.htm [https://perma.cc/3ULA-PGHC] (last visited Aug. 15, 2016).

[183] *See* PETER CONTI-BROWN, THE POWER AND INDEPENDENCE OF THE FEDERAL RESERVE 54–55 (2016).

[184] 12 U.S.C. § 353 (2012); *see also* Mark F. Bernstein, Note, *The Federal Open Market Committee and the Sharing of Governmental Power with Private Citizens*, 75 VA. L. REV. 111, 114–18 (1989).

[185] 12 U.S.C. § 461 (2012).

[186] BERNARD SHULL, THE FOURTH BRANCH: THE FEDERAL RESERVE'S UNLIKELY RISE TO POWER AND INFLUENCE 36–40, 60–61 (2005).

[187] Grinberg, *supra* note 11, at 173 n.64; Golumbia, *supra* note 78, at 124.

[188] ANTONOPOULOS, *supra* note 24, at 25–26.

[189] *E.g.*, Jeff Cox, *Fed Raises Rates by 25 Basis Points, First Since 2006*, CNBC (Dec. 16, 2015, 2:41 PM), http://www.cnbc.com/2015/12/16/fed-raises-rates-for-first-time-since-2006.html [https://perma.cc/F9K6-P8PU].

[190] Grinberg, *supra* note 11, at 172–73; POPPER, *supra* note 8, at 16 ("The essential quality of successful money . . . [is] the number of people willing to use it.").

overcome the uncertainty distance and use dollars for daily transactions. Unless, of course, people use dollars out of inertia or ignorance—the dollar has been strong and reliable for most Americans' lifetimes, and some people may have never paused to wonder why they use dollars or whether there are other options (Americans have short memories[191]). On the other hand, in countries where the fiat currency is unreliable and untrustworthy, people do move away from using it.[192]

B. Deposits and Lending

A traditional bank, at its most basic function, takes deposits and makes loans. Why is it we're willing to deposit money with a bank? We certainly wouldn't do such a thing with strangers—hand them a wad of cash and say, "Hang on to this for me, but give it back when I ask." Why would a person want to hand over their savings to a bank, on the bank's mere promise that he or she could withdraw the money again later?

Banks are physically safer than keeping funds at home, provide deposit customers with cheap and reliable payment systems, and ideally pay interest on deposited funds.[193] Much of a bank's business, however, is shrouded in secrecy. Banks keep customer information private, so much information is kept where it cannot be verified by anyone other than regulators. Banks keep their private ledgers regarding customer information, and central banks keep ledgers of individual banks' accounts.[194] This is good for individual privacy, but bad in the sense that opacity can enable bad business practices and fail to find or prevent mistakes.

What allows a depositor to overcome the uncertainty that deposited funds can be withdrawn again? A combination of exogenous enforcement mechanisms and endogenous trust. Enforcement comes, most obviously, from the insurance provided by the Federal Deposit Insurance Corporation ("FDIC") that covers most funds on deposit with banks. A second type of enforcement comes from governmental regulation of banks.

---

[191] The English comedian Eddie Izzard has told audiences,

> I grew up in Europe, where the history comes from. . . . You tear your history down, man. 'It's thirty years old, let's smash it and put a car park here.' I have seen it in stories. I saw . . . something in Miami. 'We've redecorated this building to how it looked over fifty years ago.' People are going, 'No, surely not! No! No one was alive then.'

EDDIE IZZARD: DRESS TO KILL (Ella Communications Ltd. 1999).

[192] *See* VIGNA & CASEY, *supra* note 10, at 17–21, 208–10 (discussing Argentina's currency crises and public affinity for alternative financial service providers and Bitcoin).

[193] Catherine Martin Christopher, *Mobile Banking: The Answer for the Unbanked in America?*, 65 CATH. U. L. REV. 221, 226–30 (2015).

[194] *See* 12 U.S.C. § 3403 (2012); 12 C.F.R. § 204.5 (2012).

The FDIC insures funds on deposit; that is, if the bank fails and is unable to repay its depositors, the FDIC will do so, within the statutory caps.[195] This system has been in place since 1933 and remains "the cornerstone on which American consumer confidence in its banking and financial system rests . . . ."[196] Using the bridging model, this is an obvious enforcement mechanism—external assurances that allow individuals to overcome their reluctance to place their money with banks.[197]

In addition to deposit insurance, bank customers are protected by government regulation of banks.[198] Every bank in the United States is "examined" on a regular basis, during which exhaustive process the safety and soundness of the bank is tested.[199] Errors are corrected, changes are recommended, and (sometimes) punishments are imposed.[200] The majority of commentators agree that bank regulation is necessary,[201] but it is far from perfect. Banks are subject to examination by a convoluted web of government regulators,[202] which results in inefficiencies and inconsistencies across the industry.[203] Moreover, the whims of one individual examiner may have a disproportionate effect on an individual firm.[204]

So, while deposit insurance and bank regulation provide external reassurances to bank customers that the bank is safe to do business with,[205] these enforcement mechanisms are not perfect. FDIC insurance is not unlimited, and bank examination—like insurance rate management—is performed by fallible

---

[195] 12 U.S.C. § 1811 (2012); 12 C.F.R. § 303.20–.25 (2014); *see also Deposit Insurance*, FDIC, http://www.fdic.gov/deposit [https://perma.cc/N9VX-XZZE] (last visited Aug. 31, 2016).

[196] Nancy J. Coppola, Note, *Increased Federal Deposit Insurance Coverage: At What Cost?*, 6 N.C. BANKING INST. 429, 430 (2002).

[197] Not everyone overcomes this reluctance, of course. *See* Christopher, *supra* note 193, at 224–26 (discussing why some Americans are unbanked).

[198] Notes, *Compulsory Incorporation of Banks and the Fourteenth Amendment*, 23 HARV. L. REV. 629, 629 (1910).

[199] *See* Melanie L. Fein, *Functional Regulation: A Concept for Glass-Steagall Reform?*, 2 STAN. J. L. BUS. & FIN. 89, 106–14 (1995).

[200] *See* CARNELL ET AL., *supra* note 55, at 627–44.

[201] *See, e.g.*, E. GERALD CORRIGAN, FED. RESERVE BANK MINNEAPOLIS, ARE BANKS SPECIAL? (1982).

[202] *See* CARNELL ET AL., *supra* note 55, at 632. Banks may be chartered (incorporated) under either state or federal law; the selection of one over the other changes the constellation of regulators keeping watch over the bank, though not necessarily the principles of the regulations. *See* Henry N. Butler & Jonathan R. Macey, *The Myth of Competition in the Dual Banking System*, 73 CORNELL L. REV. 677, 677–78 (1988).

[203] *See* Fein, *supra* note 199, at 109–13. The bank regulation landscape has evolved since Ms. Fein's article was published, of course, but the regulatory burdens and problems she highlights have not been resolved.

[204] CARNELL ET AL., *supra* note 55, at 642 ("By raising eyebrows at a dubious practice, a bank examiner—even if officially only preparing an examination report—engages in a sort of enforcement.").

[205] Brito et al., *supra* note 21, at 194.

humans. While would-be banking customers may bridge their uncertainty distances partially with the knowledge and understanding of available enforcement mechanisms, the remainder of that distance must be bridged by the customer's trust in the bank.

These are but a few examples of the balance of enforcement and trust that exist within the traditional banking industry. More work can certainly be done in applying the bridging model to more complex banking and shadow-banking activities.

Those who would like to enter the banking system but have not yet done so must bridge their uncertainty distance with a combination of enforcement and trust: enforcement exists in the imperfect forms of money supply management and bank regulation, both primarily via the Fed. These enforcement mechanisms are not perfectly robust, however, and the remainder of the uncertainty distance must be bridged with user trust.

Bitcoin proponents, by contrast, argue that Bitcoin is a trustless system, and that such a system is superior to the traditional-yet-flawed U.S. banking system. The next Part addresses these issues.

V. THE BRIDGING MODEL APPLIED TO BITCOIN AND THE BLOCKCHAIN

Advocates trumpet the "trustlessness" of Bitcoin and the blockchain as one of the system's core virtues.[206] But Bitcoin and the blockchain are not really trustless. And that's a good thing. The bridging model is useful in understanding the issues at play.

A. Bitcoin as Currency

As a currency, Bitcoin is said to be trustless because the money supply is predetermined. Bitcoins are produced at a predictable rate, with a maximum number pre-established.[207] Bitcoins cannot be double-spent, meaning each existing coin is only in one place at one time.[208] Contrast this with the money supply in traditional banking, in which the Bureau of Printing and Engraving can increase the physical supply of currency, and the Fed can manipulate the intangible money supply by altering interest rates, engaging in open-market operations, and changing the reserve requirement.[209] With Bitcoin, on the other hand, there are no central bankers making such decisions.

Applying the bridging model to this narrative, it would appear that those who use Bitcoin as a currency rely entirely on its exogenous enforcement

---

[206] *See, e.g.*, NAKAMOTO, *supra* note 17, at 1.

[207] *See generally id.*; POPPER, *supra* note 8, at 30 (stating the ideological underpinnings of Bitcoin were as a currency).

[208] *See supra* Part I.B. *Contra* John Carney, *Of Course You Can Have Fractional Reserve Bitcoin Banks*, CNBC (Sept. 20, 2013, 9:53 AM), http://www.cnbc.com/2013/09/20/of-course-you-can-have-fractional-reserve-bitcoin-banks.html [https://perma.cc/8H5X-KN2N].

[209] *See supra* Part I.B.

mechanism—predetermined currency production—to bridge the uncertainty distance. This is not enforcement in the sense that government backing or management supports the currency, obviously, but in the sense that the Bitcoin protocol is entirely self-enforcing. Computer programming is the most mechanical of mechanisms: If X, then Y, no questions asked.[210] If Bitcoin is entirely enforcement, then, no trust is necessary (once the user is well-enough informed to understand the mechanics of the enforcement).

All currency, however, requires trust—trust that others are willing to accept that currency in exchange for goods and services.[211] Moreover, all currencies require trust in the origin source; with Bitcoin, that trust is placed in the code and the encryption process.[212] These are publicly available in a way that traditional banking methods aren't,[213] but transparency isn't everything. The majority of the population doesn't have the computer literacy to understand the code and verify that it's good. Those people are simply trusting that the programmers (from Nakamoto onward) have done the right thing.

The fixed and regular supply of bitcoins, together with their inability to be double-spent, hearkens to the appeal of gold as a currency[214]—scarcity creates value.[215] However, here's the bombshell that doesn't get much attention: since Bitcoin is a computer program, the maximum number of bitcoins, and the rate at which they are mined, can be changed.[216]

Increasing (or decreasing) the maximum number of bitcoins in circulation is not a common or even popular suggestion, but it is possible. The core developers have the ability to make this change, though they would admittedly have to convince 51 percent of the Bitcoin network to adopt the updated version of the software that contains the modification.

Making significant changes to the Bitcoin software is not without precedent, but it is also not without controversy. For instance, since Bitcoin's inception, each transaction block in the blockchain has been limited to one megabyte in size.[217] By early 2016, however, so many transactions were taking place at any one time that a single block wasn't big enough to process them all, threatening delays in the peer-to-peer settlement.[218] The debate over whether to re-

---

[210] *See* SZABO, *Smart Contracts*, *supra* note 98.

[211] *See* POPPER, *supra* note 8, at 55.

[212] *Id*.

[213] *Id*.

[214] Sarah Gruber, Note, *Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion*?, 32 QUINNIPIAC L. REV. 135, 150 (2013).

[215] Grinberg, *supra* note 11, at 168; *see also* Gruber, *supra* note 214, at 150 n.90.

[216] *See* Grinberg, *supra* note 11, at 175 n.71.

[217] Paul Vigna, *Bitcoin Developer Cites Community Rift in His Exit*, WALL ST. J., Jan. 19, 2016, at C6.

[218] One of Bitcoin's benefits over traditional banking is the close-to-real-time settlement, compared to overnight settlement in traditional banking. *See* Vivek Wadhwa, *R.I.P. Bitcoin. It's Time to Move On.*, WASH. POST (Jan. 19, 2016), https://www.washington

vise the Bitcoin code to increase the block size caused huge controversy within the community, largely because it would change the incentive system for miners.[219] One of the most prominent Bitcoin proponents even sold his bitcoins and quit the community over the drama.[220] If a proposal to change the block size can cause such disruption, surely a proposal to increase or decrease the maximum number of bitcoins would, too. It remains, however, technically possible.[221]

The fact that the maximum number of bitcoins can be changed decreases the power of the enforcement mechanism in the bridging model as applied to Bitcoin. Bitcoin isn't completely trustless—trust must be placed in the core developers and the network as a whole to adopt useful and appropriate modifications to the code as necessary.

Because the exogenous enforcement mechanism isn't perfect, some trust must exist to bridge the uncertainty distance between wanting to use Bitcoin and actually doing so. Or, put another way, individuals relying on the enforcement mechanism to keep bitcoins' value stable are not fully informed.

Moreover, central bank management of currency is generally presumed to be a good thing.[222] Yes, central bankers are fallible, but a flexible money supply helps control inflation and deflation, which can be destabilizing in an economy. Inflation occurs when the supply of money outpaces the demand for it; if salaries go up, prices must also rise to appropriately ration or distribute goods and services among increasing numbers of potential buyers.[223] Deflation occurs when the money supply is too small, and prices must shrink because too few market participants have enough money to purchase available goods and services.[224] The Fed monitors all of these factors and tweaks its monetary policy accordingly.

---

post.com/news/innovations/wp/2016/01/19/r-i-p-bitcoin-its-time-to-move-on/ [https://perma.cc/VCY5-EK73].

[219] *See* Vigna, *supra* note 217.

[220] Nathaniel Popper, *A Bitcoin Believer's Crisis of Faith*, N.Y. TIMES (Jan. 14, 2016), www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html?_r=0 [https://perma.cc/LQ7L-LQLP].

[221] Modifying the code requires a majority of nodes to consent to the change. This is different than the 51 percent attack, discussed *infra* in the text accompanying notes 231–234. It is more likely that 51 percent of the computing power of the network would agree to even a controversial modification, than that 51 percent of the network would agree to rewrite an existing block (thereby devaluing the entire blockchain).

[222] Golumbia, *supra* note 78, at 124, 127 ("[L]ack of regulation produces boom-and-bust cycles of an intensity far greater than the central bank regulation Bitcoin advocates loathe so much."); CRAIG K. ELWELL ET AL., CONG. RESEARCH SERV., BITCOIN: QUESTIONS, ANSWERS, AND ANALYSIS OF LEGAL ISSUES 7 (2014).

[223] *See* ELWELL ET AL., *supra* note 222, at 6; *see also* Cook, *supra* note 59, at 550–54.

[224] ELWELL ET AL., *supra* note 222, at 7. The price volatility alone makes Bitcoin a dysfunctional currency. Golumbia, *supra* note 78, at 124.

As the code is currently written, bitcoins will cease to be produced once 21 million have been mined.[225] It is possible that once this cap is reached, there will not be enough bitcoins in circulation for each user to buy what they want. If this happens, the natural result will be deflation: prices will shrink to the point at which inventory can be sold to an appropriate number of buyers. Bitcoins are divisible to the eighth decimal place, so increasingly small transactions are certainly possible.[226] Shrinking prices, however, encourage hoarding.[227] If one bitcoin buys a pair of shoes today, but prices are decreasing, then that same bitcoin may buy two pairs of shoes next month. The rational economic actor would then delay purchasing, which, in the aggregate, causes the economy to sputter.

For this reason, a flexible money supply is actually an economic boon. This suggests that Bitcoin-as-currency, analyzed via the bridging model, may be *too* enforcement-heavy to the extent that the maximum number of bitcoins is rigidly set. A more significant component of trust here may actually be the preferable method by which to bridge the uncertainty distance: incorporating more trust-based human flexibility to manage the supply and value of bitcoins would actually make Bitcoin a more functional currency.

B. Bitcoin as Payment System, Blockchain as Recordkeeper

As a payment system, the decentralized blockchain also operates by computational certainty. Transactions are made by users and confirmed by the network, which verifies that the sender owned the bitcoins and updates the ledger to reflect that the bitcoins are now in the recipient's wallet.[228] Here again, using the bridging model, the uncertainty distance between wanting to utilize the Bitcoin payment system and actually doing so would appear to be bridged entirely by the enforcement-based software mechanism.

Because there is no centralized recordkeeper, the Bitcoin protocol prohibits charge-backs, which further supports the entirely enforcement-based payment mechanism. Nakamoto wrote, "With the possibility of reversal, the need for trust spreads[,]" in apparent disparagement of trust.[229] This thinking directly informs the design of the blockchain: verification by consensus (rather than by trusted intermediary) by a method that cannot be undone.

However, a certain component of trust in a payment system may be desirable. A centralized, trusted recordkeeper can be appealed to in case of error. Fraudulent credit card charges, for instance, can be disputed, and such systems

---

[225] Grinberg, *supra* note 11, at 163.

[226] Chris Nunes, *The 10,000 Foot Future Price of Bitcoin*, MEDIUM (Apr. 17, 2015), https://medium.com/@ucnunes/the-10-000-foot-future-price-of-bitcoin-9c0ac15b7cfe#.npewwnda9 [https://perma.cc/8Y7L-8BQC].

[227] ELWELL ET AL., *supra* note 222, at 7.

[228] *See id*. at 6.

[229] NAKAMOTO, *supra* note 17, at 1.

are in place to prevent individual users from being the victims of theft or fraud. With Bitcoin, however, there's no one to complain to if a Bitcoin user sends bitcoins to the wrong address, or if bitcoins are stolen by a hacker. Such mistakes or thefts are irreversible, unless the recipient (who is functionally anonymous) voluntarily returns them.

The lack of central recordkeeping also means that if a user loses their password, there's no one to ask for retrieval. One of the more delightful ironies of the Bitcoin economy is that the best advice for keeping your password safe is to write it down on a piece of paper and keep that paper in a safe place.[230]

Attacking the blockchain would be extremely difficult, since it would require marshalling at least 51 percent *more* computing power than the network already encompasses.[231] Nakamoto was aware of this weakness, though he dismissed it on the grounds that the attacker would have no financial incentive to do so: Nakamoto assumed an attacker would be attempting to steal bitcoins, possibly by double-spending them.[232] If such an attacker were to do so, the violation of the blockchain would eliminate its trustworthiness, causing the value of all bitcoins (including those owned by the attacker) to plunge.[233] Stealing bitcoins for their value may not be an attacker's goal, however: he, she, or they may simply want to destroy Bitcoin, "as a form of terrorism."[234]

Even with honest actors, blockchain snafus are possible. On March 11, 2013, an incompatibility between Bitcoin version 0.7 and the recently-released version 0.8 caused a "hard fork," in which the network computers running version 0.7 began processing a different block than the computers running 0.8.[235] There were suddenly two different (and growing) versions of the ledger, which in turn meant that neither was reliable.[236] Programmers noticed the problem almost immediately, and core developer Gavin Andresen moved quickly to resolve the hard fork.[237] He did so simply by asking nicely: He convinced mining operation BTC Guild to revert its system to version 0.7.[238] BTC Guild controlled enough computing power within the network to shift the majority consensus back to version 0.7, and the network as a whole disregarded the fork of

---

[230] Quentin Fottrell, *To Secure Your Bitcoins, Print Them Out*, MARKETWATCH (Feb. 26, 2014, 11:09 AM), http://www.marketwatch.com/story/to-secure-your-bitcoins-print-them-out-2014-02-26 [https://perma.cc/5HMH-HBVL].

[231] *See* NAKAMOTO, *supra* note 17, at 3.

[232] *See id*. at 7.

[233] *Id*. at 4 (reasoning there's no incentive "to undermine the system and the validity of his own wealth.").

[234] Becker et al., *supra* note 31, at 4.

[235] Gruber, *supra* note 214, at 163; POPPER, *supra* note 8, at 193–95; *see also* VIGNA & CASEY, *supra* note 10, at 149 (recounting the exchange between two chat-room participants as they realized what was happening: "Luke-jr: so??? yay accidental hardfork? :x Jouke: Holy crap.").

[236] *See* Gruber, *supra* note 214, at 164.

[237] *See* POPPER, *supra* note 8, at 194; *see also* VIGNA & CASEY, *supra* note 10, at 150–51.

[238] POPPER, *supra* note 8, at 194–95.

the blockchain that had been begun to be generated by version 0.8.[239] BTC Guild lost money by abandoning the version 0.8 blockchain.[240] Without certainty as to which blockchain was valid, however, its holdings—and everyone else's—would have become worthless.[241] In another ironic instance, then, a bug in the self-executing software caused a potentially catastrophic error in the system, which was corrected by the very human intervention Bitcoin was designed to avoid.

Because of the theoretical possibility of the blockchain being violated by a 51 percent attack or by the more-likely occurrence of a hard fork, the blockchain is therefore not as inviolable as may be presumed. The enforcement mechanism is not as robust as the popular narrative suggests, and some amount of trust is still necessary for users to bridge the uncertainty distance and begin using Bitcoin and the blockchain as a payment system. Indeed, given the possibility of errors or software bugs creating unpredictable problems in the blockchain, some measure of trust may actually be desirable.

C. Third-Party Intermediaries

Because most people lack the computer literacy to participate directly in the Bitcoin ecosystem, many Bitcoin participants use the services of third parties, who act as interfaces between the individual and Bitcoin.[242] Engaging these services requires a tremendous amount of trust, because enforcement is quite uncertain.[243]

Most third-party intermediaries in the Bitcoin ecosystem hold their customers' bitcoins on their behalf—the individual customers are not reflected on the blockchain, but the intermediary is.[244] The customers thus have a contractu-

---

[239] *Id*.

[240] *Id*.

[241] *See id*.

[242] *See supra* Part I.D; *see also* Gruber, *supra* note 214, at 158–59. The Bitcoin Wiki website warns:

> When storing your bitcoins with a browser-based wallet on a third-party website, you are trusting that the operator will not abscond with your bitcoins, and that operator maintains secure systems that protect against theft, internal or external. It is recommended that you obtain the real-world identity of the website operator, ensure that sufficient recourse is available and avoid services that do not use an offline wallet (cold storage) for bitcoins that are not needed for daily transactions. Storing significant quantities of bitcoins on third party websites is not recommended.

Browser-based Wallet, BITCOIN WIKI, https://en.bitcoin.it/wiki/Browser-based_wallet [https:// perma.cc/5V39-JEVV] (last visited Aug. 23, 2016).

[243] *See* Gruber, *supra* note 214, at 207–08. Third party vendors demonstrate their trustworthiness when they identify themselves. *See* POPPER, *supra* note 8, at 46–47 (discussing the power of core developer Gavin Andresen's personal visibility in spreading trust in Bitcoin).

[244] Raskin, *supra* note 86, at 996. For example, the company Coinbase holds bitcoins on a customer's behalf, but the company Blockchain.info does not; instead, it "provides software and infrastructure to allow customers to possess their own private keys." *Id*. This requires extensive trust in the quality of service provided by the intermediary. Bitomat.pl, for exam-

al relationship with the intermediary,[245] and to forge that relationship they must overcome the uncertainty distance, not between themselves and Bitcoin, but between themselves and transacting with the intermediary.[246]

The bridge, if it is built, must consist almost entirely of trust, because enforcement mechanisms here are minimal. The intermediaries conduct their business online, but are, in fact, located in jurisdictions all across the world. Enforcing contract claims in that situation would be difficult, to say the least.[247]

Hackers steal bitcoins on a semi-regular basis. Numerous third-party intermediaries have been hacked, and customer bitcoins stolen: Bitcoin vendors Bitstamp, Bitcoin Savings and Trust, Bitfloor, Instawallet, and others have all been hacked, with hundreds of millions of dollars' worth of bitcoins stolen.[248] The most infamous of mismanaged and vulnerable intermediaries was Mt. Gox, which at one point processed nearly 80 percent of all Bitcoin transactions globally.[249] Red flags abounded for years, but the company finally collapsed after admitting in February, 2014, that 850,000 bitcoins were gone, valued at about half a billion dollars.[250] The company filed bankruptcy in Japan (and a related proceeding in the United States),[251] and about a quarter of the missing bitcoins have been recovered so far.[252]

Thus, using a third-party intermediary requires a tremendous amount of trust, since enforcement is nearly nonexistent.[253] Because most people lack the computer literacy to participate directly in Bitcoin, however, significant trust in these third-party intermediaries is necessary for meaningful expansion of

---

ple, once "incompetently lost the file that contained 25,000 bitcoins belonging to its users." Grinberg, *supra* note 11, at 198.

[245] Bayern, *supra* note 13, at 25–26.

[246] This cuts against Bitcoin advocates' argument that Bitcoin is democratic. Golumbia, *supra* note 78, at 128 ("Despite their frequent use of the word 'democratization', such efforts are profoundly anti-democratic, insisting that the introduction of devices and software by a self-identified technocratic elite trumps duly-enacted laws and law enforcement mechanisms, and that a kind of market—a market in adoption of such services—is the exclusive method society should use to judge the provision of these services.").

[247] *See infra* Part V.D.

[248] *See* MURPHY ET AL., *supra* note 33, at 8.

[249] Nathaniel Popper & Peter Lattman, *Never Mind Facebook; Winklevoss Twins Rule in Digital Money*, N.Y. TIMES, Apr. 11, 2013, at A1.

[250] *See generally* Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014, 6:30 AM), http://www.wired.com/2014/03/bitcoin-exchange [https://perma.cc/393R-DANT].

[251] Tom Hals, *Mt. Gox Files U.S. Bankruptcy, Opponents Call It a Ruse*, REUTERS (Mar. 10, 2014, 5:27 PM), http://www.reuters.com/article/us-bitcoin-mtgox-bankruptcy-idUSBREA290WU20140310 [https://perma.cc/Q2GF-5T9W]; *see also In re* Mt. Gox, Ltd., No. 3:14-BK-31229 (Bankr. N.D. Tex. Mar. 09, 2014).

[252] Scott Fargo, *The Mt. Gox Post-Bankruptcy Claims: A Detailed Guide*, BLOCKCHAIN AGENDA (May 8, 2015, 5:00 AM), http://insidebitcoins.com/news/the-mt-gox-post-bankruptcy-claims-a-detailed-guide/32357 [https://perma.cc/764R-VGWK].

[253] "Almost all bitcoin exchanges are located outside the U.S. and are largely unregulated, which introduces unnecessary counterparty risk." Brito et al., *supra* note 21, at 173.

Bitcoin. Of course, Bitcoin was designed specifically to avoid the need for trusted third-party intermediaries.[254]

D. Government Enforcement?

Bitcoin has its own internal enforcement mechanisms written into the code, but some would-be users may seek to rely on external enforcement mechanisms to bridge the uncertainty distance. Although the bridging model can incorporate a diverse definition of enforcement (network governance, public shaming, etc.), this section explores whether governmental enforcement mechanisms are reliable in the Bitcoin context.

Within the United States, government regulation of Bitcoin is minimal. This may make it a libertarian ideal, but it prevents would-be Bitcoin users from being able to rely on external enforcement mechanisms. Several federal agencies are exploring whether Bitcoin comes within their jurisdiction, but their actions are uncoordinated.[255] To the extent enforcement has been effective, it has been in the criminal context rather than the civil; various federal law enforcement agencies have had significant success in shutting down Bitcoin-related money laundering, drug dealing, and other criminal activities, but there is precious little consumer protection regulation for Bitcoin users.[256]

This may be because we are not currently able to answer a surprisingly basic question: What *is* a bitcoin? A robust debate is ongoing about whether bitcoins are a currency, commodity, security, or property.[257] If it's a currency, it's a non-governmental one, and no government support can be expected, though third-party intermediaries might conceivably be regulated under financial rules as money services businesses.[258] If Bitcoin is a security or commodity, on the other hand, then enforcement lies with the Securities and Exchange

---

[254] *See* NAKAMOTO, *supra* note 17, at 1.

[255] *See, e.g.*, MURPHY ET AL., *supra* note 33, at 10–15.

[256] *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES (2014).

[257] *See, e.g.*, Cara R. Baros, Note, *Barter, Bearer, and Bitcoin: The Likely Future of Stateless Virtual Money*, 23 U. MIAMI BUS. L. REV. 201, 202–03 (2014); Nicole Mirjanich, Comment, *Digital Money: Bitcoin's Financial and Tax Future Despite Regulatory Uncertainty*, 64 DEPAUL L. REV. 213, 213–15 (2014); Aubrey K. Noonan, Comment, *Bitcoin or Bust: Can One Really "Trust" One's Digital Assets?*, 7 EST. PLAN. & COMMUNITY PROP. L.J. 583, 584 (2015); Eric P. Pacy, Note, *Tales from the Cryptocurrency: On Bitcoin, Square Pegs, and Round Holes*, 49 NEW ENG. L. REV. 121, 122–23 (2014); Nicolas Wenker, Note, *Online Currencies, Real-World Chaos: The Struggle to Regulate the Rise of Bitcoin*, 19 TEX. REV. L. & POL. 145, 146–47 (2014).

[258] *See, e.g.*, Christopher, *supra* note 69, at 2–3; *see generally* Gruber, *supra* note 214; Mirjanich, *supra* note 258; Pacy, *supra* note 258; Kelsey L. Penrose, Comment, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. 529 (2014).

Commission or the Commodity Futures Trading Commission.[259] If it is property, as the IRS believes it is,[260] then its ownership and transfer can theoretically be enforced by a robust body of contract and property law. Until consensus emerges, the governmental regulatory response to Bitcoin questions and challenges is likely to remain fractured.

This assumes, of course, the civil procedure hurdles can be overcome: determining where to file suit, identifying and serving a pseudonymous defendant, and determining what law applies to a potentially international transaction.[261]

CONCLUSION

Bitcoin has shaken up the way the world views money: it forces us to confront how comfortable we are with a financial system dependent on trusted intermediaries, and whether transparency and democracy are preferable to opacity when it comes to our financial health. But to call Bitcoin "trustless" is an oversimplification. Although Bitcoin contains mechanisms that make it predictable and reliable—the regular production of bitcoins, the publicly verified ledger—these mechanisms still rely on human involvement. Moreover, the Bitcoin code may strip away instances where trust and human overrides are actually preferable, in that they allow considered responses to unanticipated problems.

The bridging model allows us to analyze the robustness of enforcement mechanisms in bridging the uncertainty distance between wanting to transact and transacting. It also allows us to articulate and analyze the interplay between enforcement and trust. Particularly as additional blockchain applications are explored, future work should critically analyze what roles enforcement and trust should play in the legal and social spaces.

---

[259] Sec. & Exch. Comm'n v. Shavers, No. 4:13-CV-416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013) (ruling that bitcoins are securities).

[260] INTERNAL REVENUE SERV., NOTICE 2014-21 IRS VIRTUAL CURRENCY GUIDANCE (2014). This decision has been somewhat controversial. *See supra* note 258; Nika Antonikova, *Real Taxes on Virtual Currencies: What Does the I.R.S. Say?*, 34 VA. TAX REV. 433, 433 (2015); Erin M. Hawley & Joseph J. Colangelo, *Bitcoin Taxation: Recommendations to Improve the Understanding and Treatment of Virtual Currency*, 15 J. FEDERALIST SOC'Y PRAC. GROUPS 4 (2014).

[261] *See generally* Raskin, *supra* note 86, at 970.