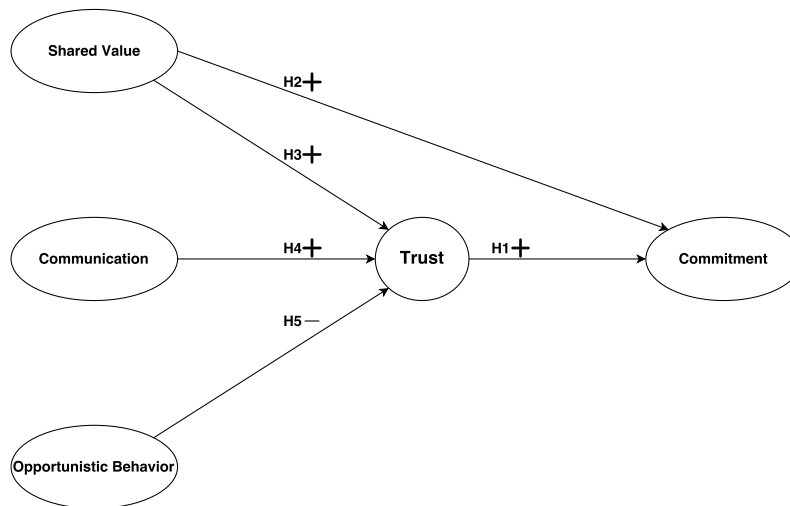


Mukherjee and Nath have written multiple papers building on the Morgan and Hunt model. In 2003, they analyzed trust-building and relationship marketing in the online banking context, proposing a slimmed-down version of the Morgan and Hunt model (Fig. 2).¹⁴³ In this model, they determine that shared values, 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

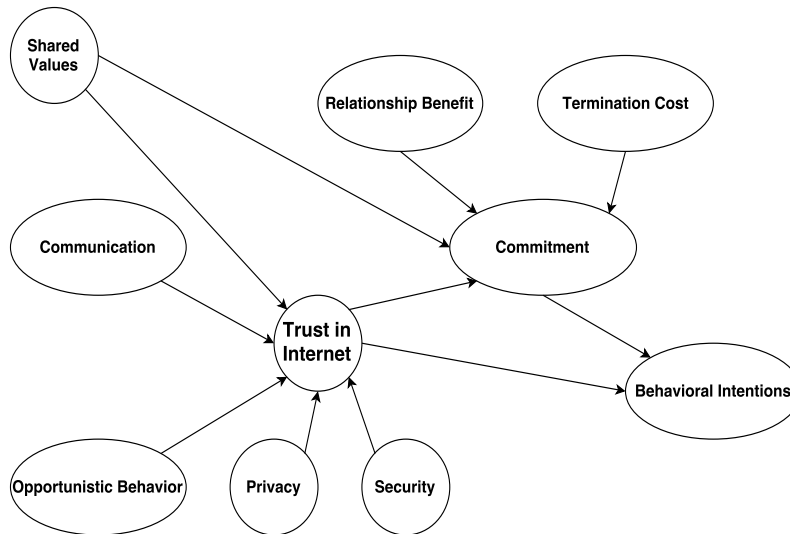
¹⁴³ Avinandan Mukherjee & Prithwiraj Nath, *A Model of Trust in Online Relationship Banking*, 21 INT'L J. BANK MARKETING 5, 9 (2003).

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.

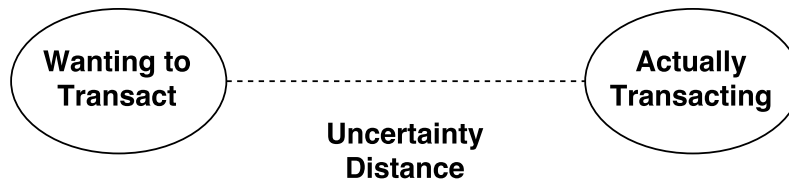
To understand better how enforcement mechanisms interact with trust in contract formation, then, a more sensitive model is necessary.

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

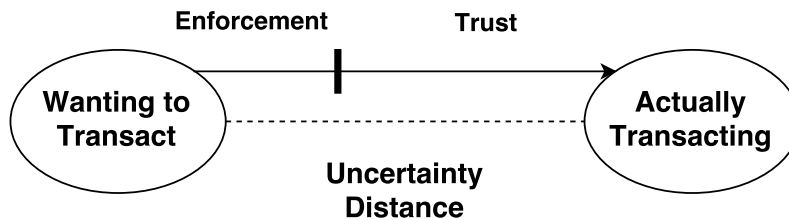
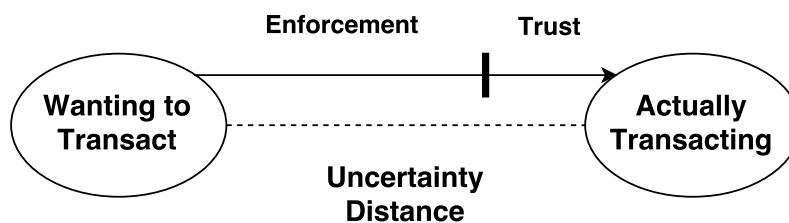
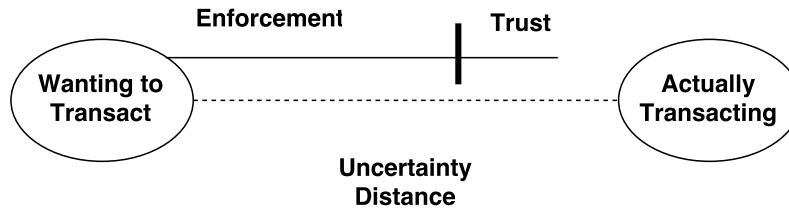


FIGURE 6: STRONG ENFORCEMENT/LOW TRUST: DISTANCE BRIDGED



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 norms¹⁴⁹ 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 Murnighan 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 parties¹⁵⁸—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 Inter-firm 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 contracts 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 Golumbia, *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 memories¹⁹¹). 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 currency²¹⁴—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-JEUV>] (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. Columbia, *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.