"SMART" CONTRACT MARKETS: TRADING DERIVATIVES CONTRACTS ON THE BLOCKCHAIN

TREVOR I. KIVIAT[1]

ABSTRACT

Trust is an age-old construct, hardwired into our biological blueprint and reflected in the institutions that we have built and maintain. Modern global economic relationships are possible because of third-party intermediaries that establish trust and thus reduce transaction costs. Financial institutions, for example, establish trust by providing credit and security. A modern paradigm is the central counterparty clearing system.

The central clearing model establishes trust between counterparties, and in doing so, also serves legitimate economic and policy functions. First, it manages counterparty risk by imposing strict eligibility and margin requirements. Second, it promotes transparency by making information on market activity and exposures available to regulators and to the public. This advanced system is enabled by technology, and recent innovations in the field of cryptography hold promise for increased efficiencies.

This paper examines whether and how blockchain technology—an innovative, cryptographic protocol—can impact the trading-clearing-settlement value chain. The blockchain facilitates the "trustless exchange" of value over a transparent, universal ledger. Trustless exchange means, for the first time, parties may confirm ownership, verify identity, and transfer value over digital networks without a trusted third-party. Additionally, these transactions may contain "smart" contracts: programmable messages that monitor and enforce the legal and economic terms of an agreement.

Such a system holds promise for reducing transaction costs in economic relationships requiring trusted third-party intermediaries. This paper considers whether and to what extent an opportunity for disruption exists specifically with respect to the trading and enforcing derivatives contracts. It considers whether a programmable technology may fit within the existing market structure. It discusses the extent to which the market structure would be disrupted by such a paradigm shift. And it identifies the most prominent barriers to such a transition.

[1] Duke University School of Law, J.D. / LL.M. expected 2016; Syracuse University, B.S. 2011.

CONTENTS

> *"For he that performeth first, has no assurance that the other will performe after; because the bonds of words are too weak to bridle mens ambition, avarice, anger, and other Passions, without the feare of some coercive Power."* [2]

INTRODUCTION

Trust is an age-old construct. It is hardwired into our biological blueprint,[3] and it is reflected in the institutions that we have built and maintain.[4] Modern economies are characterized by institutions that support trade and contracting—institutions that establish trust.[5] In the absence of institutions, many of the economic relationships that we take for granted would be highly constrained or non-existent because the associated counterparty risks[6] would be too great[7] to sustain "the bonds of words" alone.[8]

This story begins with the Champagne fairs of the Middle Ages, one of the successful pre-modern economic institutions.[9] These "veritable nerve centers" of trade attracted merchants from all over Europe.[10] Successful merchants often found themselves

---

[2] THOMAS HOBBES, LEVIATHAN 70–71 (1651) (Guernsey Press Co., 1983) (explaining why problems of trust—counterparty risk, essentially—support a policy against the enforceability of promises for future performance).
[3] Paul J. Zak, *The Neuroscience of Trust*, 37 PEOPLE & STRATEGY J. 14 (2014).
[4] *See* DOUGLAS C. NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 33–35 (1990) (explaining that modern economies are enabled by institutions that establish trust and reduce transaction costs).
[5] Paul R. Milgrom, Douglass C. North, & Barry R. Weingast, *The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, & the Champagne Fairs*, 2 ECON. & POL. 1, 2 (1990).
[6] "Counterparty risk" is simply the risk that the other party to an agreement will fail to meet their contractual obligation. *See infra* note 73 and accompanying discussion.
[7] Milgrom, et al., *supra* note 5 at 6 (noting the one exception to this is barter transactions in which physical commodities are exchanged on the spot); *see also* Richard A. Posner, *A Theory of Primitive Society, With a Special Reference to Law*, 23 J. L. & ECON. 1, 36 (1980) ("[T]he law of contracts in primitive society usually involves simultaneous (or virtually simultaneous) performance.").
[8] *See supra* note 2.
[9] The Champagne fairs were annual trading fairs held in the Middle Ages in France's Champagne and Brie regions. The Champagne fairs evolved from local agricultural and stock fairs into a central economic institution in medieval Europe. JANET L. ABU-LUGHOD, BEFORE EUROPEAN HEGEMONY: THE WORLD SYSTEM A.D. 1250–1350 50 (1991). For an interesting analysis of the Champagne fairs through a game theoretic framework, see Milgrom, et al. *supra* note 5 at 6–9.
[10] ABU-LUGHOD, *supra* note 9.

unable to satisfy the present demand for goods at market.[11] So consequently, they would enter into forward contracts[12] to satisfy their customers.[13]

The Champagne fairs fascinate economists because they are an anomaly.[14] This is not because forward contracts were novel instruments in the Middle Ages—those had been around for quite some time.[15] Rather they are an anomaly because parties to these agreements *routinely honored* their obligations.[16]

Agreements requiring future performance pose issues of information and incentives. This is especially true in pre-modern and developing economies: information costs are too high,[17] incentives to cheat are too great, and[18] enforcement systems are weak.[19] Simply, trust in "the bonds of words" alone is too low.[20] As a result, parties in this scenario confine their activities. To reduce information asymmetries, they engaging in small-scale, personalized, local exchange.[21] Parties rely on repeat dealing and

[11] Milgrom, et al. *supra* note 5 at 6.
[12] Forwards are "financial contracts in which two counterparties agree to exchange a specified amount of a designated product for a specified price on a specified future date or dates. ALAN N. RECHTSCHAFFEN, CAPITAL MARKETS, DERIVATIVES AND THE LAW 155 (2d ed. 2014).
[13] Milgrom, et al. *supra* note 5.
[14] *See, e.g.*, Milgrom, et al. *supra*, note 5; *see also* Avner Greif, *Institutions and International Trade: Lessons from the Commercial Revolution*, 82 AM. ECON. REV. 128, 131–32
[15] Many simple derivatives contracts can be traced back to ancient history. *See* GARY E. KALBAUGH, DERIVATIVES LAW & REGULATION 25 (2014) (citing Aristotle's explanation of a simple futures contract in *Politics*). In the Old Testament book of Genesis, Jacob enters into what one might consider the first recorded derivative. *See Genesis* 29:1–30 (describing Jacob's purchase of an option—at the price of seven years of labor—on the right to marry Laban's daughter Rachel).
[16] Milgrom, et al. *supra*, note 5.
[17] *E.g.*, Clifford Geertz, *The Bazaar Economy: Information and Search in Peasant Marketing*, 68 AM. ECON. REV. 28 (1978); *see supra* note 7. And, even in the case of spot transactions for physical commodities, how does one know—in the absence of scales—that the quantity paid equates to the quantity received? For a similar analysis raising enforcement issues inherent in the insurance contracts of "primitive societies," see Posner, *supra* note 7 at 10–12. Further, absent a repeat dealing setting (where reputation is a crucial concern), parties would have incentives to cheat. In other words, it would be profitable and economically rational for parties to breach these forward contracts. Milgrom, et al. *supra* note 5 at 6–9.
[18] Milgrom, et al. *supra* note 5 at 6–9.
[19] NORTH, *supra* note 4 at 27–35.
[20] *See* HOBBES, *supra* note 2.
[21] NORTH, *supra* note 4 at 34.

reputation to reduce information costs.[22] But the Champagne fairs did not follow this paradigm: It drew diverse participants from far and wide—participants who honored agreements made with relative strangers.[23]

Institutions are the "critical underpinning" of modern economies, and the Champagne fairs are an early example one such institution.[24] Institutions provide parties to an exchange with trust in the face of uncertainty. They do this primarily through third party recordkeeping and enforcement.[25]

The Champagne fair's member-organizers achieved successful institutional economies through private ordering.[26] These parties reduced information asymmetries and incentivized the honoring of agreements by gathering information, reporting disputes, and adhering to judgments.[27] Recordkeeping was centralized, and participation was conditional upon remaining in "good standing."[28] In doing so, it supported impersonal exchange relations over time by lowering the associated transactions costs.[29] With trust established, comes greater certainty, and with certainty comes the complex contracting necessary for modern economic growth.[30] In that light, one can see modern contract law

[22] Milgrom, et al. *supra*, note 5 at 6–9.
[23] Milgrom, et al. *supra*, note 5.
[24] NORTH, *supra* note 4 at 35.
[25] "Third-party enforcement is never ideal, never perfect, and the parties to exchange still devote immense resources to attempting to clientize exchange relationships." DOUGLAS NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 35 (1990).
[26] "Private ordering" is used here in the sense that these were norms and conventions that were regulated and enforced by a consortium of non-State actors. For a thorough introduction to "private ordering," the various shades of activities covered under the term, and the public goals it may achieve, see Steven L. Schwarcz, *Private Ordering*, 97 N.W. L. REV. 319 (2002).
[27] Avner Greif, *Contract Enforceability & Economic Institutions in Early Trade: The Maghribi Traders' Coalition*, 83 AM. ECON. REV. 525, 525 (1993).
[28] *Id*.
[29] Such bilateral exchanges were prohibitively costly throughout much of history due to the high costs of gathering information. *See* Posner, *supra* note 7 at 5. Uncertainties in such a setting include the probability that the counterparty will perform and the quantity delivered at sale will equate to the quantity bargained for. *Id*.
[30] NORTH, *supra* note 4 at 35.

as an institution designed to "facilitate transactions in which the performance of one or both parties takes considerable time."[31] Such mechanisms for certainty and redress strengthen "the bonds of words."[32]

Simply, trust pushes societies and economies forward:[33] The "trustworthier" its institutions, the more a society may advance.[34] In a broad sense, trust underpins core components of our legal, economic, and technological frameworks.

This paper ties together ideas from economic theory and modern computer science. It explains the basic economic functions of institutions and ties this concept to the role of trusted third-parties[35] (TTPs) in electronic transactions. It explores the efficiencies offered by one economic institution—derivatives clearing houses. It describes new technological advancements that allows for "trustless" transactions. And it questions whether and to what extent a trustless technology can disrupt the trading-clearing-settlement value chain, a system traditionally requiring trusted financial intermediaries. A hypothetical "smart contract market" for futures provides the vehicle for this analysis.

In short, the blockchain[36] is an innovative "trustless" technology.[37] "Trustless" means that—for the first time in history—exchanges for value over a network can be

---

[31] *See* ANTHONY T. KRONMAN & RICHARD A. POSNER, THE ECONOMICS OF CONTRACT LAW 3–4 (1978).
[32] *See* HOBBES, *supra* note 2.
[33] *See* NORTH, *supra* note 4 at 58 ("The inability of societies to develop effective, low-cost enforcement of contracts is the most important source of both historical stagnation and contemporary underdevelopment in the Third World.").
[34] *See id.* at 34.
[35] *See infra* Part I.A.2. for a discussion of TTPs.
[36] Legal academic discussion in this space has focused almost exclusively on bitcoin *as a currency system*—in other words, as used for money transfers and payments. *See, e.g.*, Joshua J. Doguet, Comment, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119 (2013) (weighing the costs and benefits of transacting with "decentralized virtual currency"); Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159 (2012) (considering the sustainability a virtual currency system). Authors have contemplated the application of existing regulatory schemes to virtual currency. *See, e.g.*, Kelsey L. Penrose, Note,

verified, monitored, and enforced without the presence of a trusted-third party (TTP) or central institution.[38]

Because the blockchain is fundamentally an authentication and verification technology,[39] it can enable more efficient title transfers and ownership verification.[40] Because it is programmable, it can enable conditional "smart" contracts.[41] Because it is decentralized, it can perform these functions with minimal trust without using centralized institutions.[42] Because it is borderless and frictionless, it can provide a cheaper, faster infrastructure for exchanging units of value.[43] The potential for innovation is hard to overstate.[44]

This combination of features has broad disruption potential in the financial services sector because it implicates many services and capabilities traditionally performed by trusted third-party intermediaries. Specifically, the trading-clearing-

---

Banking On Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws, 18 N.C. BANKING INST. 529 (2014) (anti-money laundering schemes); Ruoke Yang, *When is Bitcoin a Security Under U.S. Securities Law?*, 18 J. TECH. L. & POL'Y 99 (2014) (federal securities regulation); Matthew Kien-Meng Ly, Note, *Coining Bitcoin's "Legal-Bits": Examining The Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J. L. & TECH. 587 (2014) (contemplating whether and which existing legal frameworks may be used to regulate bitcoin); Paul H. Farmer, Jr., Comment, *Speculative Tech: The Bitcoin Legal Quagmire & The Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85 (2014) (exploring the appropriate legal definition for "bitcoins," based upon their intended and actual use).

[37] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* 8 (2009) (self-published white paper), *available at* https://bitcoin.org/bitcoin.pdf.

[38] *Id*. at 8.

[39] *See, e.g.*, Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, & Pieter Wuille, *Enabling Blockchain Innovations Through Pegged Sidechains* (Oct. 22, 2014) (self-published white paper), *available at* http://www.blockstream.com/sidechains.pdf

[40] *Id*.

[41] *Id*.

[42] Nakamoto, *supra* note 37 at 1.

[43] *See* TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 67 (2014).

[44] One might use venture capital investment data as rough proxy for perceived innovation opportunities in this area. Investments have rocketed from $100 million in 2013 to $360 million in 2014—roughly $576 million in the aggregate (from January 2013 to April 2015). *See* COINFILTER, *Funding*, http://www.coinfilter.com/bitcoin-funding/ (compiling data from various sources, including SEC filings). To be sure, this is just a fraction of investment activity in the general "payments technology" space. *See* CB INSIGHTS, *Payments Tech Investment Report—$5.19b Invested Across 811 Deals Over the Past Five Years*, (Aug. 21, 2014), https://www.cbinsights.com/blog/payments-tech-venture-capital-report-2014.

settlement value chain is ripe for disruption, as the blockchain vertically integrates several key functions—recordkeeping, auditing, monitoring, enforcement, or asset custody (i.e. escrow). This paper analyzes the feasibility of such an undertaking. It integrates literature on select elements of the derivatives trading industry with current research from leading computer scientists and cryptographers. The aim is two-fold: first, this paper is aimed at financial industry stakeholders, seeking to understand a new technology with disruption potential; second, this paper is aimed at entrepreneurs in the cryptography space, seeking to examine a hypothetical use case for blockchain-enabled smart contracts. It proceeds in three parts.

Part I explores central counterparty clearing from an economic and technological perspective. First, it describes the economic theory of institutions and how that manifests itself in the digital world, through the cryptographic concept of the trusted third party ("TTP"). Second, it explores one modern economic institution, the central clearing house and describes its core economic and policy features and the three-part value chain from clearing, to settlement, to custody.

Part II describes the blockchain, an innovative, cryptographic protocol that facilitates the trustless exchange of value over a transparent, universal ledger. "Trustless exchange" means, for the first time, parties may confirm ownership, verify identity, and transfer value over digital networks without a trusted third-party. First, it walks through the mechanics of a blockchain transaction. Next, it explains the concept of "smart" contracts: programmable messages that monitor and enforce the legal and economic

terms of an agreement. Ultimately, this section is designed to highlight the features most pertinent to the smart contracts market hypothesis.[45]

Part III questions whether and to what extent the central clearing model can be disintermediated by the blockchain technology. Building on top of the technological groundwork established in Part II, it imagines a hypothetical smart contracts market with special attention to the core blockchain features that could enable such a market. Next, it identifies specific elements from the current model that could be disrupted by the blockchain technology. It closes with a look at the challenges to adoption—technological, economic, and otherwise—that incumbents and challengers in this space are grappling with. This paper does not address the market for derivatives contracts with respect to "bitcoin" as the underlying commodity.[46]

I. CENTRAL COUNTERPARTY CLEARING

A. Trust: Institutional Theory and the Trusted Third Party

As shown above, institutions play a critical role in modern societies by reducing uncertainty and establishing a trusted framework for economic relationships.[47] As transactions increasingly occur online via computer networks, new institutions have emerged—"new kinds of intermediaries" that establish trust in online transactions.[48] This section connects concepts of economic theory of institutions to a modern cryptographic concept: the trusted third party ("TTP"). TTPs are institutions stand between

[45] For a full primer on the blockchain technology, see SWANSON, *supra* note 43.
[46] On that topic, see Jerry Brito, Houman Shadab, & Andrea Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144, 155–71 (2014).
[47] DOUGLAS NORTH, INSTITUTIONS, INSTITUTIONAL CHANGE AND ECONOMIC PERFORMANCE 6 (1990).
[48] E-BUSINESS: KEY ISSUES, APPLICATIONS, AND TECHNOLOGIES 144 (eds. Brian Stanford-Smith, et al., 2000).

counterparties in an online transaction—certification and registration authorities, payment clearing, and notarization, for example.[49] TTPs do not have any commercial interest in the transaction itself, and all transacting parties accept them.[50] In short, they are conceptually similar to the Champagne fairs of the Middle Ages in the sense that they stand between relatively anonymous counterparties to establish trust, increase certainty and, ultimately, reduce counterparty risk.

1. Institutions and Transactions Costs

In 1937, Ronald Coase famously observed that transaction costs are the basis for the existence of the firm.[51] Indeed, institutions exist for the very purpose of reducing uncertainties arising from incomplete information with respect to the behavior of other individuals.[52] In economic terms, these uncertainties introduce information costs and enforcement costs to the transaction.[53] Information costs can be thought of as the "costs of measuring the valuable attributes of what is being exchanged."[54] And enforcement costs can be thought of as "the costs of protecting rights and policing and enforcing agreements."[55]

[49] *Id*.
[50] *Id*.
[51] *See* R.H. Coase, *The Nature of the Firm*, 4 ECONOMICA 386 (1937).
[52] NORTH, *supra* note 4 at 25.
[53] *Id*. at 73 ("If information and enforcement were costless, it would be hard to imagine a significant role for organizations.").
[54] *Id*. at 27. Consider the purchase of an automobile. The buyer gets a particular color, acceleration, style, interior design, leg room, gasoline mileage—all valued attributes. Yet it is only the automobile itself that is purchased. The value of the exchange to the parties is the value of the different attributed lumped together. It takes resources to define and measure the rights that are transferred. *Id.* at 29.
[55] *Id.* at 32–33. ("Enforcement poses no problem when it is in the interest of the other party to live up to the agreements. But without institutional constraints, self-interested behavior will foreclose complex exchange, because of the uncertainty that the other party will find it in his or her interest to live up to the agreement.")

Institutions reduce information costs in a variety of ways. First, institutions may reduce information costs about the attributes of the parties themselves[56]—for example, by establishing eligibility requirements based on creditworthiness or some other certain specific status. Second, institutions may reduce information costs about the goods or services exchanged within their purview[57]—for example, by establishing standard terms, (e.g. price, size, or quantity) and certain other specifications. As seen below, derivatives clearing houses and exchanges are financial institutions that fit well within this paradigm. Clearing houses reduce information costs about parties by imposing strict eligibility requirements;[58] exchanges reduce information costs about the contracts themselves by promoting standardized terms.[59]

Institutions also reduce enforcement costs. First, institutions may reduce enforcement costs by providing mechanisms to incentivize self-enforcement[60]—for example, centralized recordkeeping to efficiently monitor the rights, obligations, and reputations of repeat players. Second, institutions may reduce enforcement costs by providing incentives to act in ways that will avoid formal adjudication[61]—for example, arbitration proceedings, which are costly and unpredictable.[62]

---

[56] *Id.* at 27–35.
[57] *Id*.
[58] *See infra* Part I.B.
[59] *See infra* note 170 and accompanying text.
[60] NORTH, *supra* note 4 at 27–35.
[61] *Id.* at 27–35.
[62] *See* Inka Hanefeld, *Arbitration in Banking and Finance*, 9 NYU J.L. & BUS. 917, 935–37 (2013) (describing uncertainties and challenges in arbitrating disputes in the banking and finance sector).

2. The Trusted Third Party

Trade has become evermore globalized and transactions increasingly impersonal.[63] And, with online transactions, have emerged "new kinds of intermediaries" called trusted third parties (TTPs). Such institutions are highly common in electronic commercial transactions,[64] and their sole purpose is to establish trust between two parties.[65] They do this by reducing information costs, and thus lowering counterparty risk in any given transaction.

For example, Party A and Party B wish to transact over a computer network. Like our Champagne fair merchants, they have never met before and have no reason to trust one another. Stopping here, the transaction would not occur; the counterparty risk is too great. But now introduce Party T—a third-party who is trusted by Party A and trusted by Party B. If Party A and Party B each trust Party T,[66] they need not trust each other.[67] One common example of TTPs are certificate authorities—entities that issue digital trust certificates.[68] Such documentation establishes the identity of a party to a digital transaction and guarantees its authenticity.

TTPs have real world analogues. Consider the notary public, an institution dating back to medieval Rome.[69] As a "broker of public trust,"[70] notaries, under the authority of the State, may certify documents, authenticate signatures, and perform certain other

---

[63] *See generally* DAVID SINGH GREWAL, NETWORK POWER: THE SOCIAL DYNAMICS OF GLOBALIZATION (2008).
[64] *See generally* RAYMOND T. NIMMER & HOLLY K. TOWLE, 1 THE LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS (2003).
[65] E-BUSINESS, *supra* note 48.
[66] Party T has no commercial interest in the transaction itself.
[67] *Id*.
[68] HENRY H. PERRITT, LAW & THE INFORMATION SUPERHIGHWAY 592 (2001).
[69] LAURIE NUSSDORFER, BROKERS OF PUBLIC TRUST: NOTARIES IN EARLY MODERN ROME 1 (2009).
[70] NUSSDORFER, *supra* note 69 at 4.

official acts.[71] Such endorsements carry a degree of trustworthiness; such authenticity falls "very high on the scale of proof."[72] TTPs then, are brokers of trust between parties to an electronic transaction.

Simply, before the blockchain, parties needed a trusted third party intermediary—a bank, a clearing house, a credit card network—reduce counterparty risk in online transactions for value. This has been true for all of history, and it has followed us into the Internet Age through TTP technology. The blockchain technology may change this because it decentralizes trust. After turning to a description of the derivatives trading industry in Part I.B, this paper will explain how a "trustless" technology works and explore its implications.

B. The Economic Case for Central Clearing

Central counterparties ("CCPs") are institutions in the economic sense described above. They are said to increase transactional efficiency primarily by reducing counterparty credit risk—the risk arising from the possibility that the counterparty may default on amounts owed on a derivative transaction.[73] They do this by imposing strict eligibility requirements and margin requirements.[74] Thus, CCPs are a classic example of institutions because they are designed to reduce the uncertainties involved in human interaction.[75] This section explains the concepts of counterparty risk and credit risk; describes the CCP model, with attention to its role in reducing these risks; and dissects the value chain of central clearing for an analysis of its component parts.

[71] BLACK'S LAW DICTIONARY (10th ed.) (defining "notary public").
[72] NUSSDORFER, *supra* note 69 at 15.
[73] THE NEW PALGRAVE DICTIONARY OF MONEY & FINANCE 502 (1992) (defining "counterparty risk").
[74] RECHTSCHAFFEN, *supra* note 12 at 188. See NORTH, *supra* note 4 at 47 (describing "formal constraints")
[75] *See* NORTH, *supra* note 4 at 25.

1. Counterparty Risk: Problems of Information and Enforcement

Counterparty risk is not a new concept. The above example of the Champagne fairs illustrates two points: (1) as long as parties have entered agreements for future performance, counterparty risk has been an issue; and (2) modern economies mitigate this risk via economic and legal institutions that establish trust through recordkeeping, monitoring, and enforcement. To be sure, today the stakes are higher and potential difficulties greater due to the rise in financial markets' interdependence and complexity.[76] Financial instruments are becoming ever more novel; transaction chains are becoming ever more complex.[77] A settlement failure by any counterparty in the chain can lead to disruptions across markets.[78]

Counterparty risk correlates directly with the costs of information and enforcement. First as to information costs, counterparty risk represents information asymmetries regarding the counterparty's resources and ability to meet the terms of the contract. Second as to enforcement costs, counterparty risk represents the possibility that the counterparty has incentives to breach the agreement. For example, incentives to breach could stem from limited liability and resource constraints or imperfect enforcement.

2. Two Models for Dealing with Risk: CCP and OTC Contrasted

Absent the CCP model, derivatives contracts are traded in a two-party over-the-counter ("OTC") model. Without a third party institution (i.e., the clearing house),

[76] *See generally* Dan Awrey, *Complexity, Innovation, and the Regulation of Modern Financial Markets*, 2 HARV. BUS. L. REV. 235 (2012).
[77] *Id*.
[78] *Id*.

counterparties enter into bilateral, customized contracts.[79] In other words, Party A buys the long position; Party B buys the short. Both parties thus assume the market risk of the contract[80] and the counterparty risk.[81] All things equal, one would expect parties to mitigate these risks by imposing their own capital and margin requirements with varying degrees of robustness.[82]

By contrast, the "central clearing model" interposes a trusted intermediary, i.e. a "clearing house" between counterparties.[83] Through the process of novation,[84] the clearing house holds offsetting long and short positions. In other words, it is not exposed to the market risk of the underlying instruments.[85] Further, parties to the transaction are no longer exposed to the counterparty risk of the other side; each party is in privity with the clearing house itself.[86] However, under the CCP model, some risk still remains. Ultimately, the clearing house assumes the risk that one party will default on its contractual obligations.[87] In other words, the intermediary guarantees the performance of each contract; payments from clearing members fund this guarantee.[88]

[79] *See* RECHTSCHAFFEN, *supra* note 12 at 188.
[80] The "market risk" is the risk that the contract's value will diminish based on changes in the underlying asset. *Id*.
[81] *Id.*
[82] *See id.*
[83] *Id.*
[84] Richard Heckinger & David Mengle, *Derivatives Overview*, FED. RES. BANK CHI., 2, 8 (2013). In this process, the clearing house becomes the buyer to every seller and the seller to every buyer. *Id*.
[85] *Id.*
[86] *See supra*, note 78 and accompanying text.
[87] *See* RECHTSCHAFFEN, *supra* note 12 at 188.
[88] *Id*.

3. Risk Management Devices in the CCP Model

CCPs reallocate risks through several distinct mechanisms.[89] The two primary mechanisms are (1) strict requirements for the eligibility of counterparties to become a member of the clearing house, and (2) the posting of original and variation margin.[90] First, eligibility requirements allow clearing houses to impose minimum capital requirements[91] and credit strength on their members.[92] In Part III.C., this paper considers the extent to which a "permissioned" blockchain[93]

Second, CCPs require firms entering into derivatives transactions to post margin (i.e., collateral) on each trade at its initiation.[94] Posting margin at the outset, gives a party recourse in the event of a default; it can seize its counterparty's collateral to cover some, or all, of the amount owed.[95] In the OTC setting, this is open to negotiation.[96] By contrast, CCPs always require the posting of margin at the outset ("initial margin"), and periodic adjustments to reflect market fluctuations ("variation margin").[97] Initial margin is usually set based on an estimate of the transaction's riskiness *ex ante*,[98] calculated according to one of a couple standard formulas.[99]

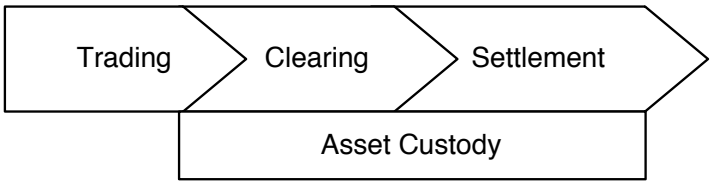
---

[89] Craig Pirrong, *The Economics of Central Clearing: Theory & Practice*, 6 (ISDA Discussion Paper Series No. 1, May 2011). Five such devices are netting, collateralization, insurance, equity, and mutualization. *Id*.
[90] *Id*. Initial margin is given to the clearing house at the inception of the trade and is used as a good-faith deposit, akin to posting a security deposit for rental housing. Variation margin is updated daily based on price movements in the underlying instrument, ensuring that counterparties account for these fluctuations by posting additional margin if necessary.
[91] This mitigates counterparty risk in the event that a derivatives contract subjects a clearing member to losses. *Id*.
[92] This ensures that all members meet a minimum level of financial stability. *Id*.
[93] This stands in contrast to the original Bitcoin blockchain, which is "permissionless."
[94] *Id.* at 8.
[95] *Id.* at 7.
[96] *Id.* at 8. ("Parties . . . negotiate whether collateral will be posted; who will post it; the amount of collateral; and how collateral postings are adjusted over the life of a transaction.").
[97] *Id*.
[98] *Id*. Higher margin may be warranted on instruments that take a CCP longer to cover in the event of a default—for example, those with above average price volatility and below average liquidity. *Id*. Initial margin is typically is not determined by the creditworthiness of the party to a contract. *Id*.
[99] *See* DAVID LOADER, CLEARING, SETTLEMENT, AND CUSTODY 85 (2002).

4. The Value Chain of Central Clearing[100]

The value chain[101] of the central clearing model can be broken down into three main functions: trading, clearing, and settlement.[102]

Figure 1. The trading-clearing-settlement value chain



The trading stage is the genesis of the transaction, where price discovery and trade execution occurs.[103] But trade execution is just the beginning of a process driven by complex systems.[104] At the clearing stage, a transaction is processed in preparation for the transfer of ownership and the fulfillment of all obligations.[105] In other words, it is prepared for settlement by matching, recording, and processing the given "instructions" or terms of the transaction.[106]

[100] This section provides a generalized overview of the "baseline" model for clearing, settlement, and custodial services. For a more detailed analysis of these functions and current developments in the market structure of the central clearing industry, see generally BANK INT'L SETTLEMENTS, *Market Structure Developments in the Clearing Industry: Implications for Financial Stability* (Nov. 2010), http://www.bis.org/cpmi/publ/d92.pdf.

[101] *See* MICHAEL E. PORTER, COMPETITIVE ADVANTAGE: CREATING AND SUSTAINING SUPERIOR PERFORMANCE 33 (1985) (defining "value chain" as the "strategically relevant activities" a firm must undertake "in order to understand the behavior of costs and the existing and potential sources of differentiation"). Here, the term is used more broadly to also encompass what Porter refers to as the "value system." *See id.* at 34–35.

[102] *See generally* LOADER, *supra* note 99.

[103] BANK INT'L SETTLEMENTS, *supra* note 100.

[104] LOADER, *supra* note 99 at 1. This paper addresses the technological systems. Of course, there are complex organizational systems at work here too. *See generally id*.

[105] At this stage, several additional value-add services may be performed—for example, the netting of obligations for increased processing and cash flow efficiency.

[106] *Id*. at 1. The clearing stage encompasses several activities such as trade capture and verification; trade matching, affirmation, and legal confirmation; trade reporting; position and payment netting; portfolio compression; novation; trade and portfolio valuation; portfolio reconciliation; and collateral management.

At the settlement stage, the actual exchange of cash or assets and transference of ownership occurs.[107] To facilitate this exchange, the processes is inherently linked with asset custodial services.[108] For example, when a party buys or sells a futures contract, it does not pay the full value of the contract; it only pays the initial margin requirement.[109] This deposit—a sort of "insurance" that delivery obligations can be fulfilled—is held in custody throughout the time the position is maintained.[110] Significantly, margin is costly because typically it must be posted in liquid assets that yield less than competing investments[111]—cash or government securities, for example.[112]

As this paper will show, the blockchain technology offers a combination of features that could allow parties to safely and securely post margin bilaterally to cryptographic escrow account without the need for a third-party clearing agent or custodian.[113]

II. THE BLOCKCHAIN & SMART CONTRACTS

The blockchain is a "trustless" technology: Parties may bilaterally confirm ownership, verify identity, and transfer value over digital networks.[114] Additionally, these transactions may contain "smart" contracts, or programmable messages that monitor and enforce the legal and economic terms of an agreement. Incumbent firms and emerging financial technology ("fintech") players are deploying substantial resources to discover how software-enabled "smart" transactions can disrupt the traditional payments, clearing,

---

[107] *Id*.
[108] *Id*. at 2.
[109] *See supra* notes 97–98 and accompanying text.
[110] LOADER, *supra* note 99 at 85.
[111] In other words, margin requirements impose real opportunity costs on businesses.
[112] Michael L. Hartzmark, *The Effects of Changing Margin Levels on Futures Market Activity, The Composition of Traders in the Market, and Price Performance*, J. Bus. 59 (1986).
[113] *See infra* Part II.B.
[114] *See generally* Nakamoto, *supra* note 37.

and settlement landscape.[115] This section introduces the blockchain technology and explains the aspects that are most integral to its disruption potential in this space. It provides a high-level overview of the mechanics of a blockchain transaction; explains the significance of "smart" contracts; and explores some current trends at the frontier of this rapidly developing field.

A. The Blockchain: A Trustless Exchange Technology

In the physical world, security requires locks, vaults, and signatures;[116] in the digital world, it requires cryptography.[117] The blockchain is a cryptographic technology[118] that solves an important technological problem: For the first time ever, secure electronic transactions for value can occur without the presence of a trusted third-party.[119] In other words, outside of the blockchain, electronic transfers of scarce resources require a trusted third-party (TTP) intermediary—a commercial bank or brokerage or PayPal, for example.[120] Such institutions establish trust and security by preserving a centralized ledger[121] to track account-holders' balances and, ultimately, vouch for a transaction's authenticity.[122] Without intermediaries (and off the blockchain), electronic units of value can be copied and spent twice, just as any digital document can be copied

[115] *See, e.g.*, Anna Irrera, *UBS to Open Blockchain Research Lab in London*, WALL ST. J. (Apr. 2, 2015), http://blogs.wsj.com/digits/2015/04/02/ubs-to-open-blockchain-research-lab-in-london; *see also supra* note 44 and accompanying text.
[116] *See supra* Part I.A.2.
[117] Cryptography is "the scientific study of techniques for securing digital information, transactions, and distributed computations." JONATHAN KATZ & YEHUDA LINDELL, INTRODUCTION TO MODERN CRYPTOGRAPHY: PRINCIPLES AND PROTOCOLS 3 (2007).
[118] Nakamoto, *supra* note 37 at 1. It is also and it is the core innovation driving the bitcoin currency platform. A discussion of bitcoin, the alternative digital currency is outside the scope of this paper. For a thorough primer on the bitcoin ecosystem, see generally Grinberg, *supra* note 36; *see also* Trevor I. Kiviat, *Beyond Bitcoin*, 65 DUKE L.J. (forthcoming Dec. 2015) (exploring current innovation and issues surrounding the Bitcoin platform and blockchain technology generally).
[119] *Id*. at 8.
[120] *See generally* SINGH, *supra* note 49.
[121] This used to be a physical ledger, now it is a centralized server network. *See id*. at 323.
[122] *Id*.

ad infinitum.[123] This scarcity-destroying property is called the "double spending problem," and it has riddled engineers for decades.[124]

This section proceeds in two parts; each addresses an essential feature of the blockchain technology. First, it explains the decentralized, transparent public ledger and analogizes it to a form of "triple-entry" accounting. Second, it explores the concept of "frictionless" settlement and clearing. To be sure, the blockchain protocol has several novel and interesting features, most of which are beyond the scope of this paper.[125]

1. "Triple-Entry" Accounting: A Decentralized, Transparent Public Ledger[126]

The blockchain enables secure electronic transactions of scarce units of value without a centralized ledger and without double spending risks.[127] Instead of a centralized ledger, it makes the entire user base the collective accountant by distributing a shared (i.e., "decentralized") public ledger—a complete record of all past transactions on the

[123] The recorded music industry is still recovering from the painful implications of this fact. *See* David Byrne, *Survival Strategies for Emerging Artists—and Megastars*, WIRED, Dec. 18, 2007, *available at* http://archive.wired.com/entertainment/music/magazine/16-01/ff_byrne (explaining how peer-to-peer file sharing transformed the economic model of the recorded music industry); *see also* Karim R. Lakhani & Marco Iansiti, *Taylor Swift and the Economics of Music as a Service*, HARV. BUS. REV. ONLINE, (Nov. 6, 2014), https://hbr.org/2014/11/taylor-swift-and-the-economics-of-music-as-a-service (exploring the industry's continued struggle to capture value with respect to recorded music).

[124] The double spending problem is also referred to as the "Two Generals' Problem," and is illustrated best through the following hypothetical: Imagine two generals, each preparing his troops to attack a common enemy. Each squadron is situated on separate hills, flanking the enemy. The generals can communicate only by courier. Each message sent carries a risk of interception by the enemy. While the two generals have agreed to attack, they haven't agreed upon a time. Assume that a successful attack requires both squadrons to attack the city simultaneously. The issue is this: The two generals must agree on an attack time, and each general must know that the other general knows that they have agreed. This is difficult because acknowledgement of receipt can be lost as easily as the original message. Thus a potentially infinite chain of messages is required to reach consensus. *See* Jim Gray, *Notes on Data Base Operating Systems*, IBM RES. LABORATORY 465 (Summer 1977) (coining the name "Two Generals' Problem"); *see also generally* E.A. Akkoyunlu, et al., *Some Constraints and Tradeoffs in the Design of Network Communications*, 9 ACM SPECIAL INT. GROUP ON OPERATING SYS. 5, 73 (1975) (documenting the problem for the first time).

[125] Again, for a full primer on the blockchain technology, see SWANSON, *supra* note 43.

[126] Modern financial accounting is a double-entry system—a system of recordkeeping that allows firms to maintain records of what the firm owns and owes and what the firm has earned and spent over any given period of time. "Triple-entry" accounting refers to the idea that transactions on the blockchain are essentially accounting entries that are cryptographically sealed, preventing tampering and enabling near real-time auditing.

[127] Nakamoto, *supra* note 119.

network.[128] This ledger is the blockchain.[129] When two parties wish to engage in a transaction, they must broadcast it to the entire network,[130] effectively asking network participants to determine its authenticity.[131] The network validates the transaction—or guards against the threat of double spending—through a "proof-of-work" validation system.[132] If the transaction is validated, the ledger is updated, and network users collectively update their copies of the blockchain.[133] Alternatively, a request for dishonest transaction "falls off" the chain and therefore the transaction never occurs.

2. "Frictionless" Exchange

The second essential feature of the blockchain—right behind the decentralized, transparent public ledger—is the promise it holds for reducing frictions specifically at the clearing stage. "Friction" generally refers to the transaction costs of an economic

---

[128] *Id*. at 3.

[129] *See id*. Although the term "blockchain" was not used in Nakamoto's original paper, it has become synonymous with this technology. *See, e.g.*, Back, *supra* note 39 at 3. Basically, a "block" contains a series of transactions; the ledger can be traced sequentially back to the first block, thus forming chain of blocks.

[130] *See id*. at 3.

[131] *Id*.

[132] *Id*. The "proof-of-work" validation system is essentially a competition among network participants to validate transactions. The transactions are time-stamped to ensure validity. Network users participate in this competition by exercising computational power. Under this system, a user's ability to influence validation—to double spend—is limited by the total proportional computational power they can harness. Users are incentivized to bear the computational costs of validation because successful participants are rewarded with new units of value. Accordingly, this process is called "mining" because the "[computational] time and electricity that is expended" is "analogous to gold miners expending resources to add gold to circulation." As long as the miners' marginal cost remains below the market price, they will continue to mine. *See* Nakamoto, *supra* note 119 at 2–4. Eventually there will be nothing left to "mine" because the total outstanding supply is limited. Grinberg, *supra* note at 163–64. When that happens, the incentive to validate transactions will likely be transaction fees. *See* Kerem Kaşkaloğlu, *Near Zero Bitcoin Transaction Fees Cannot Last Forever*, INT'L CONF. ON DIGITAL SECURITY AND FORENSICS 91, 91–93 (Jun. 2014) *available at* http://sdiwc.net/digital-library/near-zero-bitcoin-transaction-fees-cannot-last-forever.html (arguing that zero or infinitesimal transaction fees is not be sustainable, given characteristics of mining, securing the network from dishonest participants, and the scarce supply).

[133] *Id*. In this respect, the blockchain can be thought of as a historical record of all transactions that have occurred on the network. In other words, once a transaction has been recorded in the blockchain that transaction cannot be changed after the fact; parties may not rewrite history (unless the transaction is matched with a second offsetting transaction). *See id*. at 1; *but see* Eli Douardo, *Stop Saying Bitcoin Transactions Aren't Reversible*, *available at* https://elidourado.com/blog/bitcoin-arbitration (describing advanced features of the blockchain technology that may essentially provide participants with the ability to encode transactions to include arbitration and similar dispute resolution services).

exchange.[134] Friction is inefficient by definition because it represents the transaction costs of facilitating the exchange, not the exchange itself.[135] It can be measured in monetary terms—for example, the interchange fee paid between banks for the acceptance of card-based payment transactions. It can be measured in physical terms—for example, the merchant's act of swiping a credit card and the consumer's act of signing his receipt. And it can be measured in temporal terms—for example, the amount of time it takes for title and possession of units of value to transfer from one party to another.[136]

"Frictionless" settlement is the buzzword du jour in fintech;[137] but it is worth noting up front that a truly "frictionless" payment system is something of a science fiction. A system that is truly frictionless across the trading-settlement-clearing value chain[138] would imply instantaneous trading, clearing, and settlement with zero cost.

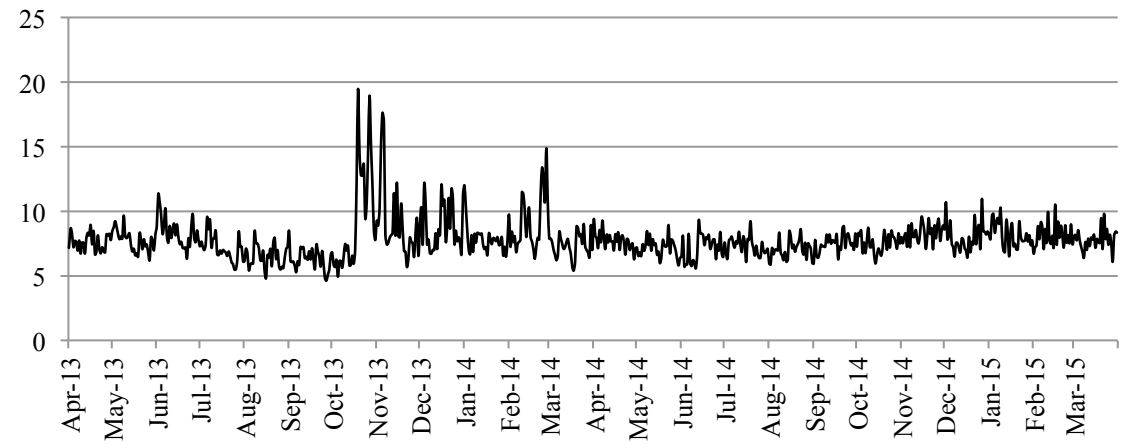
The blockchain holds promise for *reducing* friction because it vertically integrates the value chain's core components—trading, clearing, and settlement—in an elegant, efficient, mathematical way. Currently, a host of financial market utilities (FMUs) provide the infrastructure for transferring, clearing, and settling transactions among financial institutions.[139] The main friction with blockchain technology[140] is of a temporal

---

[134] *See generally* GOLDMAN SACHS EQUITY RESEARCH, *The Future of Finance: Part 3, The Socialization of Finance*, (Mar. 13, 2015) (on file with author).
[135] *See id*.
[136] *See* Jan Estep, *Same-Day ACH and the Future of Faster Payments*, AM. BANKER, (Oct. 14, 2014), http://www.americanbanker.com/bankthink/same-day-ach-and-the-future-of-faster-payments-1070471-1.html.
[137] *See generally* GOLDMAN SACHS, *supra* note 134 (using the words "friction" or "frictionless" no less than 26 times in various contexts to generally refer to the associated transaction costs in economic transfers) (on file with author).
[138] *See supra* Part I.B.4 (describing the value chain).
[139] Marc Labonte, *Supervision of U.S. Payment, Clearing, and Settlement Systems: Designation of Financial Market Utilities*, CONGRESSIONAL RESEARCH SERVICE, (Sept. 10, 2012), https://www.fas.org/sgp/crs/misc/R41529.pdf.
[140] This is current data from the Bitcoin blockchain. As discussed in Part III.B.1, innovators are currently working on various implementations of this protocol. Think of these innovations as "special purpose

nature: It takes time for the network to confirm that a transaction is, in fact, a valid transfer and not a "double spend" request. As seen in Figure 2, the average "confirmation time" for a transaction on the blockchain has hovered around the ten-minute mark for the last two years.

Figure 2. Average transaction confirmation time (Apr. 2013–Apr. 2015)[141]



* * *

So in a nutshell, the blockchain establishes trust between two parties to a transaction: Participants can trade, clear, and settle transactions for value through vertically integrated, cryptographic technology in about ten minutes. This is made possible by a decentralized public ledger and a protocol that ensures transactions cannot be changed after the fact.[142] The entire exchange process takes about ten minutes.

---

blockchains," where the creators have optimized specific parameters for certain types of designated transactions.

[141] BLOCKCHAIN.INFO, *Average Transaction Confirmation Time*, https://blockchain.info/charts/avg-confirmation-time (last visited April 17, 2015).

[142] *See* Nakamoto *supra* note 119 at 1.

B. Smart Contracts

The blockchain protocol facilitates the exchange of value[143] through a series of mathematical rules that govern the network. As described above,[144] transactions have a three-part structure: (1) Party A sends a message to the network declaring the transaction; (2) Party B accepts the transaction by broadcasting its acceptance; and (3) the network participants verify the authenticity of the transaction.[145] To be sure, this basic structure was designed for transferring ownership of "bitcoins."[146] But when people send and receive "bitcoins," they are really just transferring "containers for value."[147] Like a digital envelope, these containers can carry "coins" across the network; but they can also transmit richer forms of information, creating added utility.

A typical transaction follows a simple "script"—a set of instructions—that adheres to the three-part structure described above.[148] If the script were altered to contain additional conditions, users could engage in more sophisticated transactions. For instance, maybe Party A and Party B want to add a fourth condition to that script structure. Maybe they only want the transaction to occur at a certain time, or upon the occurrence or non-occurrence of an objectively verifiable condition. At this stage in the analysis, one begins to understand why this technology has sparked much discussion about "smart contracts."

---

[143] David S. Evans, *Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Platforms* 6–7 (The University of Chicago, Institute for Law and Economics Working Paper Series) (Apr. 2014) (The blockchain is a "protocol for sending value, receiving value, and recording value securely."); Back, *supra* note 39 ("There are assets besides currencies that may be traded on blockchains, such as IOUs and other contracts, as well as smart property."); *see also generally* SWANSON, *supra* note 43.
[144] *See supra* Part II.A.1.
[145] *See supra* notes 130–133 and accompanying text.
[146] Evans, *supra* note 143 at 4 ("Calling the container a coin causes confusion because, at least at the start of the platform, the container is not a currency, since it is not widely used, and because the public ledger platform could be viable even if the container did not evolve into being a general-purpose currency.").
[147] SWANSON, *supra* note 43 at 55.
[148] *Id*.

Smart contracts are "computer protocols that facilitate, verify, execute and enforce the terms of a commercial agreement."[149] This concept is not new, and it is not unique to the blockchain. One primitive example is digital rights management ("DRM"), a technology developed to fight copyright infringement.[150] Essentially, DRM technology embedded U.S. copyright law[151] into digital files by limiting the user's ability to view, copy, play, print, or otherwise alter the works.[152] In other words, digital audio files encrypted with DRM technology were not susceptible to the double spending problem because they contained a basic "smart contract"—instructions pointing to a *centralized* network, i.e. a server enforcing Apple's iTunes Store Terms and Conditions.[153]

1. Decentralized Smart Contracts

The blockchain enables *decentralized* smart contracts—in other words, smart contracts that leverage a secure public ledger as an enforcement mechanism. In contrast to the iTunes example, these contracts do not rely on a third-party institution or server for centralized recordkeeping and enforcement.

This fact is significant because, as described above, institutions help solve the problem of trust between counterparties to a transaction.[154] With decentralized smart contracts, parties may transact at arms length, with total strangers, without the worry of

---

[149] *See id*. at 15. An extended discussion of whether and how smart contracts fit within the legal framework of contracts law is beyond the scope of this discussion.
[150] ROSS ANDERSON, SECURITY ENGINEERING 679 (2d. ed.); *see also* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J. L. & TECH. 49, 60 (explaining the evolution of DRM technology).
[151] More specifically, it was certain provisions of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. §§ 1201–05 (2006). *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.03(A)(1)(a) (2011) (explaining the DMCA prohibits circumvention of DRM on copyrighted material).
[152] Armstrong, *supra* note 150 at 60.
[153] In 2009, Apple reversed its policy and no longer provides DRM-encrypted digital files in its iTunes store. *See* Ruth Suehle, *The DRM Graveyard: A Brief History of Digital Rights Management in Music*, OPENSOURCE.COM (Nov. 3, 2011), *available at* http://opensource.com /life/11/11/drm-graveyard-brief-history-digital-rights-management-music
[154] *See supra* Part I.A.

fraud, without the cost of third-party enforcement (i.e. recordkeeping costs, mediation costs, and other administrative and operational costs). Two parties can agree to a contract with significantly reduced counterparty risk, without the associated costs of a third-party financial intermediary. In other words, decentralized smart contracts allow for new markets to develop: decentralized contract markets in which parties do not have concern for counterparty risk.

To be sure, the task of encoding the legal subtleties and nuances that underlie even the most basic contract poses significant programming challenges. The remainder of this section addresses this concern. It shows how simple smart contracts—contracts that only involve objectively verifiable conditions about the state of the world—can be designed. Part III uses this understanding as a jumping off point to envision a hypothetical decentralized smart contract market for futures.

2. Multi-signature Transactions and Escrowing

Multi-signature ("multi-sig") transactions are transactions that involve more than two parties—for example a 2-of-3 multi-sig transaction is a transaction between three parties.[155] They are called "2-of-3" because they require approval from two parties before clearing and settlement can occur.[156] One implication of this feature is cryptographic escrow.[157] For example, Party A and Party B wish to enter a futures contract. They enlist Party M as a mediator who will sign the transaction in favor of either party upon the maturation of the agreement. Some or all of an amount to be transferred under the

[155] ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES (2014).
[156] *See id*.
[157] This idea is developed off of a concept sketched by Mike Hearn. *See* BITCOIN WIKI, *Contracts, Example 2: Escrow & Dispute Mediation*, https://en.bitcoin.it/wiki/Contracts#Example_2:_Escrow_and_dispute_mediation.

contract is cryptographically locked at the outset; parties have essentially posted initial margin through a bilateral arrangement, without the need for an asset custodian.

3. Oracles

If the contract terms to be interpreted and enforced consist of objectively verifiable digital information, the cryptographic custodian in a multi-sig transaction does not need to be human. Smart contracts that reference off-blockchain events[158]—the price of corn futures at a given time, for example—must be able to monitor real world conditions. "Oracles" are systems set up to monitor off-blockchain information and data that is essential to the effective execution of the smart contract's terms.[159] They listen to that third-party data—NYMEX quotes or the ESPN Live Score feed, for that matter—and they use it to instantaneously "arbitrate" the terms of the smart contract.[160]

This is done through multi-sig contracts.[161] In other words, at the time of execution, the original trustees cryptographically sign the contract and post escrow to a cryptographically secure account.[162] But, before the funds may be released, the oracle must also sign. It does so upon the occurrence (or non-occurrence) of the contractually specified condition.[163] This event is an off-blockchain condition that the oracle is programmed to monitor and verify.[164] At the appropriate time, the oracle enforces the

[158] "Off-blockchain" events are any measurable events that occur outside of the blockchain and thus cannot be monitored by an on-blockchain script. The current temperature in Durham, North Carolina; the spot price of Brent crude at a particular time in the future; and the results of the 2015 Formula 1 Chinese Grand Prix are all off-blockchain events that could be referenced in a smart contract and enforced by an oracle.
[159] *See* SWANSON, *supra* note 43 at 61.
[160] *See id*.
[161] *Id*.
[162] *Id*.
[163] *Id*.
[164] *Id*.

agreement, and the funds are released from escrow to the beneficiary, or otherwise allocated to the parties in some contractually specified manner.[165]

III. SMART CONTRACT MARKETS: A HYPOTHETICAL PATH FORWARD

A. The "Smart Contact Markets" Hypothesis

As established in Part II, blockchain transactions are programmable and self-enforcing. Parties can design their contractual relationship—a relationship that is automatically executed without the additional costs of monitoring or enforcement.[166] Further, these transactions may occur without intermediaries, given the decentralized nature of the blockchain.[167] And finally, these transactions are secure[168] and publicly verifiable by all market participants.[169]

These features give rise to the following hypothesis: The blockchain has disruptive potential that specifically implicates the value chain of derivatives trading, given its ability to perform functions traditionally performed by trusted third party financial intermediaries—be it recordkeeping, auditing, monitoring, enforcement, or asset custody (i.e. escrow). This remainder of this paper tests that hypothesis. Using the exchange-traded futures market as a beachhead, it identifies opportunities for disruption at specific parts of the trading-clearing-settling value chain; it recognizes certain major barriers to adoption; and it examines the extent to which smart contract markets may develop in the future.

---

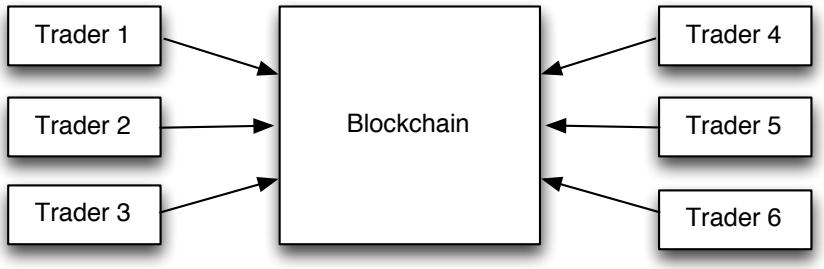
[165] *Id*.
[166] *See infra* Part II.
[167] *Id*.
[168] Security stems from the cryptographic nature of the technology. In other words, contract terms written on the blockchain are irreversible and immune to tampering. *See id*. (explaining the mechanics of a blockchain transaction).
[169] *Id*.

B. A Smart Contracts Market for Futures

Futures agreements are highly standardized to ensure that contracts can be easily traded and priced.[170] Standardization makes them an ideal test case[171] for the smart contract markets hypothesis.[172] Smart futures contracts would trade, clear, and settle in a decentralized manner—without an exchange or central counterparty.

Through a combination of scripting,[173] multi-signature escrowing,[174] and oracles,[175] the digital agreement would be self-monitoring and self-enforcing. Trades would be programmed with a contract's terms (i.e., quality, quantity, and delivery) and communicated directly to the blockchain. And the blockchain, not an exchange, would function as the sole record-keeper, arbiter, and custodian:

Figure 3. A smart contracts market for futures[176]



[170] CME GROUP, A TRADER'S GUIDE TO FUTURES 4 (2013), https://www.cmegroup.com/education/files/a-traders-guide-to-futures.pdf; ASWATH DAMODARAN, INVESTMENT VALUATION, *Valuing Futures Contracts*, http://pages.stern.nyu.edu/~adamodar/pdfiles/valn2ed/ch34.pdf; *see also* Stephen G. Cecchetti, Jacob Gyntelberg, & Marc Hollanders, *Central Counterparties for Over-the-Counter Derivatives*, BIS Q. REV. (Sept. 2009) at 49 ("[D]erivatives contracts have in many cases become more standardized. For example, over the years, interest rate swaps and foreign exchange derivatives have become highly standardized through voluntary industry initiatives.").

[171] By contrast, OTC derivatives do not offer a strong use case given their liquidity risk. In other words, agreements are custom tailored to fit parties' unique risk profiles. *See* RECHTSCHAFFEN, *supra* note 12 at 188.

[172] This model is based on a hypothetical developed by Professor Shadab in his remarks to the CFTC's Global Markets Advisory Committee. *See* Houman B. Shadab, *Written Statement to the Commodity Futures Trading Commission: Regulating Bitcoin and Block Chain Derivatives* 15, (Oct. 9, 2014), http://www.cftc.gov/ucm/groups/public/@aboutcftc/documents/file/gmac_100914_bitcoin.pdf.

[173] *See supra* note 141–148 and accompanying text.

[174] *See supra* Part II.B.2.

[175] *See supra* Part II.B.3.

[176] *See supra* note 172.

The price for each contract could be algorithmically determined with the help of an oracle that incorporates market data.[177] Once deposits are made, Party A and Party B sign the contract, which goes live on the blockchain. At any point during the contract, either party can use a blockchain explorer[178] to verify that both parties' funds are safely in escrow.

C. Opportunities for Disruption

Smart contract markets may be technically feasible. Yet, this does necessarily imply it is worth pursing. Before incumbent firms reevaluate their systems, before disruptive innovators choose to exploit this particular application of the technology, the existence of an economically viable opportunity must be reasonably clear. This section addresses specific elements of the trading-clearing-settlement value chain that present opportunities for disruption. The next section turns to the most formidable barriers that such an endeavor would likely face.

1. Trading: The Application or "Information" Layer

The blockchain protocol shares many qualities with the Internet—qualities that allow seemingly endless possibilities for innovation.[179] One such quality is the ability to support an application layer or "information layer."[180] In other words, the underlying

[177] These could include not only other financial markets, but also commodity markets that, for example, automatically enter into futures trades on behalf of an agricultural producer if projected crop prices drop below a certain level. *See* Adam Ludwin, *Bitcoin's Killer Apps*, CHAIN.COM BLOG, http://blog.chain.com/post/99177371581/bitcoins-killer-apps (Oct. 4, 2014) ("Synthetic versions of financial assets will be traded on the block chain, reducing default risk, increasing transparency, and providing universal access to financial instruments. Farmers will buy crop futures they couldn't previously access. Better still, smart farms will automatically buy and sell hedging contracts throughout the season using data about soil, weather, yields, and prices.").

[178] A blockchain explorer is an open-source web tool that allows users to view information about the blocks, addresses, and transactions. *See, e.g.*, BLOCKCHAIN.INFO, https://blockchain.info.

[179] *See generally* Andy Yee, *Internet Architecture and the Layers Principle: A Conceptual Framework for Regulating Bitcoin*, 3 INTERNET POL'Y REV (Aug. 19, 2014), http://policyreview.info/articles/analysis/internet-architecture-and-layers-principle-conceptual-framework-regulating-bitco-0.

[180] *See id*. at 3–4.

technology, i.e. the blockchain, is the "logical layer"; it transmits and receives information from user-facing applications.[181] Actors at the information layer make the underlying technology accessible to end-users by developing intuitive applications with user-friendly interfaces.[182] This allows end-users to interface with protocol, send and receive commands, and, ultimately, execute transactions.[183] In the context of the Internet, these are applications that send *information*[184]—such as e-mail, or the SWIFT wire system.[185]

This quality is essential for widespread adoption. In the context of the smart contracts market hypothesis, it means that individual traders would not need to physically translate and input their trades into raw code. Such an interface can be designed to store, monitor, and disseminate information about prices and other market data in a graphic manner that is intuitive and user-friendly.[186] It could monitor specific characteristics of the counterparties, individual positions, and entire portfolios.[187] It could execute, report, and confirm trades.[188] And finally, it could assist with the settlement and clearing process, by automating various aspects of collateral management and trade matching.[189]

---

[181] *See id*.
[182] *See id*.
[183] *See id*.
[184] *See id*.
[185] *See infra* notes 202–204 and accompanying text.
[186] *See* Shadab, *supra* note 172 at 13 (describing features of modern derivatives trading applications).
[187] *See id*.
[188] *See id*.
[189] *See id*. An analysis of whether such a system could interface with standardized messaging protocols such as Financial Information eXchange (FIX) or Extensible Markup Language (XML) or would need to replace such systems completely is beyond the scope of this paper.

2. Clearing: The Double Spending Problem

The need for a clearing house "stems from" the double spending problem.[190] A balance in USD is just an entry in a digital ledger. This ledger is the proprietary database of a given financial institution.[191] The balance is a liability of its issuer, a promise to pay backed by the assets held by a bank or custodian.[192] The clearing house mitigates counterparty risk by acting as a trusted clearing agent.[193] Otherwise, a bank could double spend—in other words, it could simultaneously send payments to multiple counterparties.[194] Instead, banks deposit funds with the clearing house, who can move assets between their accounts with enough visibility to ensure the solvency of payments. The blockchain technology solves the double spending problem by decentralizing trust over a shared public ledger. Thus if this shared public ledger can operate as the "logical" layer for settlement, then real-time, bilateral settlement can occur without a third-party clearing agent. [195]

3. Settlement: The Logical Layer

As established above, trading activity would take place on the application layer. The movement of funds—settlement and clearing—would happen on blockchain, or the

[190] *See* RIPPLE LABS, *The Ripple Protocol: A Deep Dive for Finance Professionals* 7, (Nov. 2014), https://ripple.com/ripple-deep-dive/ (registration required). For an explanation of the double-spending problem, see *infra* note 124 and accompanying text.
[191] *See* RIPPLE LABS, *supra* note 190.
[192] *See id*.
[193] *Id*.
[194] *Id*.
[195] Notably, custodial services can be grouped into two categories: (1) "core services," such as the safekeeping of assets in segregated accounts; and (2) "value-add services," such as securities borrowing and lending, or assistance with withholding tax claims. *See* LOADER, *supra* note 99 at 127–28. To be sure, this discussion is aimed at the technology's disruption of "core services" and not the "value-add services."

logical layer.[196] This vertical integration of may settle faster and at lower cost with fewer intermediaries, as illustrated by the following figure:

Figure 4. From exchange-to-settlement: The current layered model

Domestic	Layers:	**Int'l**
E.g, Trading platform	**Applications**	E.g, Trading platform
E.g., Bank of America	**Banks**	E.g., Bank of America
E.g., The Fed	**Standards**	E.g., SWIFT
E.g., ACH	**Network rules**	E.g, SWIFT
E.g., ACH	**Messaging**	E.g., SWIFT
E.g., The Fed (interbank)	**Settlement**	Complex[197]

Today, every country has its own domestic interbank transfer system[198]—for example, the Automated Clearing House (ACH) system in the U.S. or the Bankers' Automated Clearing Services (BACS) in the U.K. These are the rails that enable domestic bank-to-bank transfers.[199] As described above, such transfers are routed through a central bank as a clearing agent.[200] While the transaction costs are typically low-cost in monetary terms, they take two to five days to settle,[201] which represents a significant opportunity cost that parties can recapture with a real-time system.

While The Society for Worldwide Interbank Financial Telecommunication ("SWIFT") provides a secure, standardized and reliable network for global financial institutions to send and receive *information* about financial transactions.[202] And while it is often colloquially called "international wire," it only provides for messaging—not

[196] *See* Yee, *supra* note 179 at 3–4.
[197] *See infra*, notes 198–204 and accompanying discussion.
[198] *See* RIPPLE LABS, *supra* note 186.
[199] *Id*.
[200] And, in the derivatives trading setting, the clearing house
[201] *Id*.
[202] SWIFT, *About SWIFT*, http://www.swift.com/about_swift/index.

funds settlement.[203] Settlement occurs through "a patchwork of regional rails."[204] A shared public ledger could solve this.[205] It would be administered collectively by a network of servers would truly an international rail—a vehicle by which a consortium of worldwide banks, both central and commercial could exchange value.

4. Risk Management, Transparency, and Public Policy

As to risk management, multi-sig custodial accounts would allow parties to bilaterally post initial and variation margin in a safe and secure manner. The smart futures contract would automatically make adjustments to the custodial account, in the case of variation margin, and settle the agreement upon expiration.[206]

As to transparency, the fact that such a system would reside on a shared ledger provides previously unprecedented possibilities for managing financial controls.[207] Further, oracles would likely be audited and required to conform to specific regulations to protect against potential fraud or market manipulation.[208]

Finally, a smart contracts market may be less susceptible to manipulation in general. Assuming the blockchain is managed as a quasi-public utility, there would be "no incumbent firms stand[ing] to benefit from the revenues generated by bad actors."[209] To the extent practicable,[210] the CFTC's 23 Core Principles for Contract Markets could

[203] Ripple Labs, *The Ripple Protocol: A Deep Dive for Finance Professionals* 6, (Nov. 2014), https://ripple.com/ripple-deep-dive/ (registration required).
[204] *Id*.
[205] Such a ledger would be "permissioned" rather than "permissionless." *See infra* notes
[206] *See* Shadab, *supra* note 172; *see also* Part II.B.2.
[207] *See* Tim Swanson, *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems* 5, (Apr. 6, 2015).
[208] *See* Shadab, *supra* note 172; *see also* Part II.B.3.
[209] *See id*.
[210] Certain Core Principles require human judgment. These would be difficult, if not impossible, to reduce to objectively verifiable conditions.

be programmed as part of each futures agreement.[211] For example, the block chain could be programmed to prevent excessive orders and large positions that could manipulate or disrupt markets.

D. Barriers to Implementation

There are a host of barriers to implementation—technical barriers,[212] economic barriers,[213] political barriers,[214] and regulatory barriers.[215] Many of these are actually interrelated. While a full discussion of each is beyond the intended scope of this paper, this section address the "permissioned/permissionless" networks debate; it is intended to be illustrative of these hurdles and the degree to which they are interconnected.

The current iteration of the Bitcoin blockchain cannot facilitate smart contract markets. The Bitcoin blockchain was designed for a limited purpose: The mining and exchange of "bitcoin," a scarce, artificial commodity that could be traded and exchanged as a currency over the Internet—without trust, without financial intermediaries.[216] Accordingly, the protocol itself allows for very limited types of transactions to occur.[217] So one could not currently execute scripts of the sort described in the smart contract markets hypothesis directly on the Bitcoin blockchain. While this appears to be a

[211] *See* Shadab, *supra* note 172.
[212] "Technical barriers" refers generally to shortcomings with respect to the technology itself that must be overcome in order to facilitate a smart contracts market. The most striking example of this is the fact that the original Bitcoin protocol, in its current form is not robust enough to support a smart contracts market.
[213] "Economic barriers" refers generally to roadblocks imposed by the current market structure within the financial services industry, including the allocation of human capital and financial capital.
[214] "Political barriers" refers to the fact that the development community does not share one ideology. On the one hand, there are those who believe that this technology exists for the purpose of entirely disintermediating banks and "democratizing" the world financial system. At the more moderate end of the spectrum, there are developers who are actively enlisting the support of major financial institutions to create a more centralized version of the technology.
[215] "Regulatory barriers" refers to the fact that
[216] *See generally* Nakamoto, *supra* note 37.
[217] For a more thorough explanation of these limitations and a unique proposed solution, see generally Back, *supra* note 39.

technical barrier at first blush, a deeper inquiry reveals economic and political barriers. In other words, technical changes to the protocol are possible, and many have occurred. However, these are generally minor tweaks—not because larger changes are technically difficult, but rather they must undergo a rigorous vetting process.[218]

This is probably the appropriate place to draw an important distinction—a distinction between permissionless networks and permissioned networks.[219] A permissionless network, such as the Bitcoin blockchain, is fully decentralized.[220] Market participants may join the network, process transactions, and fully participate without any previous relationship with the ledger.[221] There is no gatekeeper; there are no suitability requirements; the "identity of participants is either pseudonomyous or even anonymous."[222] For these reasons, a permissionless network—while useful in some contexts—is probably ill suited for a smart contracts market. Participation in many aspects of the trading-clearing-settling value chain requires meeting certain membership or regulatory requirements.[223] For these reasons, it is unlikely that the Bitcoin blockchain will facilitate this vision of a smart contracts market.

By contrast, on a permissioned network, transactions are validated and processed by those who are already recognized by the ledger.[224] Market participants must have a

---

[218] *See* BITCOIN WIKI, *Bitcoin Improvement Proposals*, https://en.bitcoin.it/wiki/Bitcoin_Improvement_Proposals; *see also* BITCOIN WIKI, *BIP 0001*, https://en.bitcoin.it/wiki/BIP_0001 (explaining the process for submitting an improvement proposal to the Bitcoin protocol). Notably, improvement proposals must include an abstract of the technical issue being addressed, an explicit waiver of copyright interest, and a rationale supported by the consensus of the community.
[219] *See* Swanson, *supra* note 207 at 5.
[220] *See id*.
[221] *See id*.
[222] *See id.*
[223] *See supra* Part I.B.
[224] Interestingly, despite the fact that the Bitcoin protocol was originally designed with permissionless parameters, the Bitcoin ecosystem today is characterized by many of the on-ramps and off-ramps—exchanges, wallets, and other applications—that are permission-based.

previous relationship with the ledger in order to gain access to the market entirely, or certain specific features—depending on the designed parameters.[225] In other words, user identity is "whitelisted" through some type of know-your-customer procedure—common parlance in the world of finance.[226] This "gated approach" allows permissioned systems to clear and settle assets faster and cheaper; the tradeoff is the loss of democratization that comes with a decentralized system.[227] There are a variety of trade-offs between permissioned and permissionless systems—speed, cost reduction, censorship, reversibility and finality.[228]

Ripple is one such example of a permissioned network.[229] Like the Bitcoin blockchain, Ripple is essentially a shared, common ledger.[230] It provides the books and records of financial institutions a common language by which to communicate.[231] By integrating with financial services institutions rather than seeking to "disintermediate existing players,"[232] the developers at Ripple hope to deliver a more efficient settlement system—one that can settle funds in "three to six seconds."[233] Yet despite Ripple's stated

[225]
[226] *Id*.
[227] *Id*. at 6.
[228] *Id*.
[229] The fact that it is "permissioned" should not be conflated with "private" or "proprietary." No one owns the Ripple network; Ripple Labs does collect fees, or limit access; the software is open-sourced and free. *See supra* note 198 at 4. For a technical explanation of the Ripple Protocol Consensus Algorithm, see David Schwartz, Noah Youngs, & Arthur Britto, *The Ripple Protocol Consensus Algorithm* (2014), https://ripple.com/files/ripple_consensus_whitepaper.pdf.
[230] *See id.* at 4–5.
[231] *See id.* ("Every financial firm manages a ledger of accounts of some sort. In a digital world, payments are essentially just updates to the database. A bank can transfer funds between in-house accounts by effectively moving $1,000 from cell C1 to cell D1. The complexity arises from the fact that every firm has its own proprietary ledger, and two firms running two different systems cannot easily communicate directly.")
[232] *See id.* at 2.
[233] *See id*.

intentions, this technology—given the framework outlined above[234]—is poised to displace clearing agents at the very least.

CONCLUSION

Today, we stand nearly six years from the technology's first public unveiling.[235] To be sure, activity and interest in this space has never been greater.[236] Both incumbent firms and agile start-ups are working with an eye toward their own slice of the trading-clearing-settlement pie.

Perhaps, given the technology's ambitious and malleable nature, it is not surprising that is taking some time to come into its own. First, complex technological systems already underpin our financial markets.[237] In such a deeply entrenched technological framework, even small changes must occur gradually to avoid sending unintended shocks through the network.[238] Second, while it holds the promise to transform a wide swath of economic activity, it depends on the vision of the community—its stakeholders and its core developers.[239] What systems can benefit most from decentralization? What intermediaries are ripe for disruption?

This paper has shown that the blockchain technology presents an exciting new alternative to effectuating financial transactions, with special reference to derivatives

---

[234] *See supra* Part III.C.
[235] *See* Nakamoto, *supra* note 37 (describing the concept for the first time).
[236] *See supra* note 44 and accompanying text.
[237] *See generally* Awrey, *supra* note 177.
[238] *See generally e.g.*, NANEX, *Analysis of the "Flash Crash"*, (July 10, 2010) http://www.nanex.net/20100506/FlashCrashAnalysis_Intro.html (analyzing trading on the exchanges during the moments immediately prior to the flash crash, revealing that it was exacerbated by technical glitches in the price-reporting algorithms).
[239] To borrow from technologist Mark Stefik's words on the Internet, blockchain technology can support different kinds of dreams: "We choose, wisely or not." MARK STEFIK, INTERNET DREAMS: ARCHETYPES, MYTHS, AND METAPHORS 390 (1996).

trading and clearing.[240] A viable product is not yet in sight—but, as the saying goes, "Wall Street wasn't built (or rebuilt) in a day."

[240] *See* Part III.C.