A Comprehensive Contracting Solution using Blockchains

Prateek Goorha[*]

Abstract

Purpose: This paper develops the idea of comprehensive contractual solutions using the blockchain as a foundation. A comprehensive contractual solution is a template for engaging in all manner of complex contractual relationships while remaining tethered to the same underlying technology.

Approach: This paper introduces the idea of a platform contract as a practical method for contending with a range of incomplete contracts and mechanisms over a centralized platform network. It suggests why a platform contract, as a product of the network economy, represents essential inefficiencies; the paper addresses how these inefficiencies can be ameliorated by disintermediating platform networks using blockchains to develop comprehensive contractual solutions. Given the more limited nature of smart contracts, achieving this ideal on a blockchain has been a hard problem; the paper discusses proposed solutions that bode well for realizing this ambition.

Value: This paper suggests a very significant opportunity represented by blockchains that is generally underemphasized: A comprehensive contractual solution provided over a secure blockchain application that has broad acceptance, such as Bitcoin, has the very real potential to enable consistent and reliable contractual transactions to occur globally. The paper, therefore, also discuss how governments can assume a valuable role in encouraging these solutions by developing smart institutional intermediaries.

Keywords: Comprehensive Contractual Solutions; Blockchains; Platform Contracts; Disintermediation; Smart Institutional Intermediation

[*]Independent Researcher. Contact email: goorha@sent.com

Consider the 'hawala' system for sending and receiving payments between individuals who are geographically separated and who wish to avoid using state-sanctioned and formally regulated channels. Hawala is popular across several African and south Asian countries and it predates the introduction of wire transfers. It involves the use of a number of intermediaries, spread across several parts of the world, called 'hawaladars'. Typically, a sender approaches a local hawaladar with the remittance she wishes to make. The hawaladar provides a password to the sender which he also reveals to his counterpart hawaladar in the location of the recipient. The recipient then simply collects the payment from the counterpart hawaladar by providing the password to him, which he receives directly from the sender.

What is interesting is that this simple system works entirely on the basis of trust and reputation, while also simultaneously serving to 'disintermediate' traditional channels. Indeed, the word 'hawala' has the connotation of trust in Hindi-Urdu. The hawaladars usually provide better exchange rates than do the banks, and the payments can be effected fairly rapidly. Moreover, since the 'ledgers' that the hawala system employs are far from immutable, they provide an effective way for scores of expatriates to circumvent onerous tax burdens.[1]

Blockchains, of course, spring to mind as a technology that stands in stark contrast to such a system. This is true for a host of reasons, but here I wish to underscore two.

First, the more immutable a ledger technology becomes the less central is the potential role of trust and reputation as a competing basis for using the matrix of institutions that define the rules of coordination and exchange throughout a society. Yet, as the example of the hawala system hints at, sometimes the objectives of transacting parties are best served by finding the optimal level of intermediation, rather than steadfastly aiming for a binary choice of all or nothing. This is precisely the realization that several technical developers, especially for the Bitcoin blockchain, are contending with square on in the context of solving the scalability problem.

Second, the extended effects of selecting an append-only and publicly verifiable technology for the creation of immutable ledgers of transactions that are also stored across a distributed network are most vividly understood as redefining the principles

[1]The scandalous case of several top-rung politicians in India using the system to funnel money in the early 1990s was later dismissed by the country's Supreme Court in part on the basis of the fact that the ledgers maintained by the hawaladars could *not* be trusted.

of social exchange based on two interrelated aspects – assortative centralization *within* a pool of information created by a ledger technology and disassortative mixing *across* pools of information. The power of traditional ledger technology deployed on platform networks is that they strongly emphasize the former; the power of blockchains is best appreciated as enabling the latter.

In this paper, I examine these two effects by first introducing the idea of platform contracts, which are common across the network economy and have enabled a vast and staggering range of opportunities for redefining social, political and economic organization. I then suggest that the nature of platform networks – as instantiated by platform contracts – is such that they are inherently less efficient than the relevant efficient market ideal; a comprehensive contracting solution based on blockchains that serves to disintermediate platform networks, therefore, represents significant gains in efficiency. However, there are also associated costs of disintermediation that must be recognized in any such evaluation; in this regard, I concentrate attention on the looming problem of scaling blockchain throughput, which delimits the usefulness of blockchains in comparison with legacy ledger technologies. Addressing this issue would enable comprehensive contracting solutions, which are a vital and powerful construct for the blockchain economy. I end the paper with a simple framework for how the development of comprehensive contracting solutions can be significantly enhanced by assistive policy from governments in the form of smart institutional intermediation.

1 Background: Disruption with Distance-Reduction

To appreciate the idea of a platform contract as inherently amenable to the structure of a network economy, it is worthwhile beginning with a definition of the network economy as distinct from the traditional economy. The idea of a unique 'network economy' was popularized in a now famous article by Kevin Kelly that appeared in *Wired* magazine in 1997. Kelly subsequently formalized his ideas more expansively in Kelly (1999). [2]

[2]In economics, the idea of a new type of economy emerging as a significant and usefully different phenomenon to the traditional economy was proposed in the guise of a 'weightless economy' by Quah (1996). There have been several notable contributions on a knowledge economy (see, Thurow (2000) for example) and, more obliquely, several calls to examine the significance of 'ideas' – beyond merely as being embodied as a parameter for technology – in economic growth theory (such as Lucas (2009)) and development economics (as in Rodrik (2014)). And, the impact of the internet on a range of markets has been broadly examined ever since its advent. However, Quah is notable for suggesting the

While the internet is, of course, central to enabling a network economy, the network economy is a catchall conceptualization of an economic system that is entirely built on integrated markets that employ information networks. As such, it reimagines an economy as a network of networks. The dynamic value of a network economy arises from its ability to leverage the power of network externalities (which principally arise from scale economies on both the supply *and* demand sides of the market) to further extend and intensify the range of networks that operate across an economy. In the context of information networks, this permits economic value to be derived directly from the innovation of ideas rather than through optimization of physical processes.

Naturally, networks feature in several traditional economy markets as well; however, networks of the network economy enable a 'distance-reduction' between the production and consumption of knowledge products, making network participants for a good both its consumers as well as potential producers of the same or related goods.[3]

Chief among its characteristics is the simple fact that a network economy is particularly adept at enabling each participant to perceive value – independently from the good itself – directly from network characteristics, such as its rate of growth and overall connectedness. Thus, Metcalfe's law, which proposes that the value of the network depends on the square of its size, is important to the archetypical network of the network economy, whereas Sarnoff's law (where a network's value depends solely on the network's size) is more typical of what a network in a traditional economy can yield.

In standard economic markets, club goods have stood as examples of a good where the number of other consumers positively affects the good's desirability; in traditional markets, such goods permit a limited scope for scalability, and are studied as examples of the efficiency costs that arise from the imposition of membership rules of some description to control participation. Club goods exhibit the same problem as does the class of goods that are examined with the framework of a commons; essentially, liberal access rules permit rates of use for a private good that are unsustainable. In knowledge markets, by contrast, access rules can afford to be more liberal since the good in question is usually more amenable to scaling, often even displaying rising positive externalities through overuse. The root of this difference is the ability for a range of knowledge-based

evolution of an altogether new type of economy.

[3]On the idea of distance-reduction in the knowledge economy see Quah (1999), and Goorha (2009a) on a framework for designing effective policy for such an economy.

goods to blur the line between a defined group of consumers and producers.

It is this aspect of distance-reduction that is illustrated by two-sided markets. Though not exclusive to the network economy, two-sided markets are quintessential products of the network economy. These markets have, to say the least, become ubiquitous as a direct result of the growing influence of the network economy.[4] We are, to some degree, all familiar with them. Any product or service we use with two or more distinct sets of actors, interacting by way of an intermediating platform that interfaces their transactions, serves as an example. Credit cards, all manner of matchmaking services, and search engines are the typical examples, since they represent a *platform* that enables distinct networks of actors to interact through a shared mechanism – merchants interact with consumers by way of the credit card provider or the search engine. All shared-use goods are also illustrative examples of two-sided markets, be they based on sharing cars, houses, workspaces or computing time on personal computers; such goods are 'two-sided' in the sense that they have a group that owns the asset, another group that is willing to purchase its use on a fractional basis, and an intermediary who helps make the market by using its platform to act as a clearinghouse might.

The reason that the platform owners in such markets often derive high and exponentially rising economic rent over a sustained duration owes much to the simple idea that the utility for individuals in groups on either side of the platform grows quadratically, which is to say that it depends on the good as well as on externalities produced from others who participate on the platform.

Two-sided markets suffer, however, from a number of key features that deserve consideration.

First, they operate on the basis of facilitating the creation of meta-networks; that is to say, they create new networks by intermediating entire groups of actors. In any resulting *platform network* of their making, they are then able to assume the role of the most central node. In other words, they centralize across two (or possibly more) networks, and work on the basis of intermediation.

Platform operators understand the key role of distance-reduction in a network economy, and base their task of intermediation accordingly. To see this we need only observe that the manner in which an operator serves to intermediate transactions across the network is directly related to measures of centrality for a given network's configuration.

[4]See Rysman (2009) for a useful review.

The ability of a participant in a network to have more direct connections with other participants, while useful, is a poor measure for the power that this actor might have as an intermediary for the entire network. The location of the participant on the network is crucial, especially when there might be two or more distinct types of participants in the market that the network is describing. As the market evolves, the actor who simply wishes to intermediate by having the most connections on the network would always hold the risk of becoming a fringe player, admittedly in a larger group, but nevertheless less relevant across the entire platform network.

Effective intermediaries, however, proceed by seeking a low 'closeness' value among network participants, where closeness is a measure of the average path-length required to reach other participants. To the extent that there is value to be derived in reducing latency in communication across different types of participants over the network, it becomes necessary to have as low a closeness score as possible.

Platforms as intermediaries in two-sided markets on networks, therefore, operate on the principle of maximizing their 'betweenness centrality', which is to say that they premise their profit-maximizing objective on the basis of locating themselves on the network such that they appear on the overwhelming majority of the shortest paths of communication between *any* two network participants. A high degree, or number of direct connections, becomes but a side-effect of pursuing this objective.[5]

Second, key characteristics of the platform are deliberately planned and developed in two-sided markets, and they are managed and maintained by a firm with extraordinary market power. This firm, by creating a single focal point across two or more subnetworks, itself constitutes a point of possible systemic, physical and market failure. In addition, platform operators become the curators of the identities of individuals across the networks that use them as intermediaries. Aspects of an individual's identity may, of course, vary based on the type of two-sided market, but can include, among other things, a range of data that uniquely identifies them and their evolving preferences. Besides being an invasion of privacy when an individual may wish for such data not to be publicly known, she also receives no economic rent from the use of her identity, even when she may choose to provide such information voluntarily.

The point to note is that platform operators in a two-sided market can, and routinely do, fail, and when such failures occur in a network market, the effects are broad and

[5]See Freeman (1979) for more on this measure of centrality on a complex graph.

potentially invidious. When Sony's online PlayStation service was hacked in April of 2011, in what was one of the largest data breaches of all time, the personal details of 77 million users was leaked. A relatively recent outage across the Visa network in Europe suggests, if the official explanation is to be credited, that even vulnerabilities to localized hardware faults can cause widespread disruption of services. And the full impact of the breach of private data held by Facebook for 87 million of its users – pertaining to not just a user's personal data, but also details on her extended network – is yet to be known; under the guise of market research, and without much by way of informed consent from its users, a platform provider potentially played an indirect and crucial role in the 2016 US Presidential Election by enabling an unscrupulous political messaging firm and turning a blind eye to the exploitation of the platform itself by agents working at the behest of an unfriendly nation.

The need, then, to acknowledge the wanton power of platform operators in two-sided markets on networks is urgent, since the risks of systemic failure are at least as staggering as the potential to unlock economic value from the creation of and participation in such markets.

1.1 The problem with platform contracts

Platform operators in two-sided markets comprise an especially interesting type of firm, in that they expressly consider – even give precedence to – the role that the overall dynamic structure of the network that they operate in has to their business. Rather than take this as an exogenous factor, they make the network's scale and characteristics essential and endogenous to their strategy.[6] By understanding the network's shape and growth dynamics, they are then better able to position themselves within it in such a manner that their platform becomes *more* indispensable to the network, as well as a crucial part of the overall value that the network represents to its various sets of participants.

Among these characteristics of the network, building centrality is crucial; the firm that owns the most essential platform is also the one to have the highest centrality.

[6] In a comprehensive study, covering 40 years worth of financial data on the companies listed on the S&P 500, four models for the strategies on capital investments were identified – those based on physical assets; those relating to service provision; those concentrating on technology IP, and, for platform-based firms, a strategy of investments based on "network orchestration". (Libert et al., 2014)

Moreover, this centrality is predicated directly upon *increasing* the operator's ability to intermediate the component networks of participants on each side of the platform, enabling it to erect a larger overall network. Rival businesses may well become central *within* a given component of the overall network – to one 'side' of the platform, as it were – as long as the operator's platform retains unchallenged relevance in intermediating *across* the overall network's components. Stated differently, any actor on the network who has *higher* degree centrality poses little threat to the platform operator, so long as the platform operator maintains the highest betweenness centrality across the network.

The effect of this approach is that platforms also introduce a focal point in the overall network that serves to centralize a variety of costs associated with all transactions, anywhere in the network; likewise, by virtue of their overwhelming centrality, any friction that they create in associating component networks is magnified across the entire network.

This role of an intermediator that the platform-operator assumes, perforce gives it the characteristic of being a de facto (and often also a de jure) contractual nexus. Every participant to the network must, should it want to reach the other side of the market, enter into some contractual arrangement with the platform operator. Whereas for the typical firm it is the initial assignment of ownership rights over essential assets that motivates the basis for its overall set of contracts[7], it is important to recognize that the contractual nexus for a platform operator represents a much more complex set of arrangements.

The reason for this is simple. With positive Coasian transactions costs associated with price discovery in a market, the rationale for a firm rests in a set of *feasible* contractual outcomes, rather than a first-best. Since the platform in a two-sided market represents the set of *all* market transactions between its network's participants, it imposes an additional source of transactions cost over and above Coasian transactions costs.

The platform operator, therefore, represents a larger feasible set of contractual orderings than does a traditional firm; platform contracts are determined by network characteristics that are largely irrelevant to traditional firms. The information on a platform operator's network is a simpler representation of the information process of the underlying market; the relative degree to which information is lost through the use

[7]Grossman and Hart (1986)

of this network, therefore, represents a tradeoff between the increased transactions cost and additional value created by the platform relative to purely market-based transactions.

Further, if growth of the network *must* be made conditional on the platform operator maintaining highest betweenness centrality, then the growth of the network is not panacea in terms of ensuring increasingly better approximations of the market process.

It is useful to briefly visualize this point in terms of network topology. *Figure 1* provides representative illustrations.

A *fully connected network* or a 'complete graph' is one where every node on the network is connected directly with every other node; in other words, every participant has an identical degree and, therefore, no participant is any more central than another. The length of the path any participant contends with to reach anyone else across the network is the lowest possible, or 1. A fully connected network, therefore, depicts a situation of a market with *full* information. There are no frictions that any participant must contend with in order to connect with any other participant.

Practical networks in the real-world are usually characterized by a host of costs in connecting.[8] Without any structure over information and very high costs of organization, we leave ourselves with the possibility of *random networks*, where network participants are connected at random, and, as a result, contend with a range of transactions costs that vary dramatically depending on whom they wish to reach across the network.

In contrast to the two extremes, a platform operator's network can be seen as compromise. It is, in essence, a *small-world network*, in that all participants, on any side of the platform, are able to connect with one another within a very short path length. The costs of connection are lower than they would be on a random network. And it approximates a fully connected network, though with a higher average path length and with a higher concentration of connections across some key nodes, most importantly the platform operator.

[8]There are at least two such costs. One is based on the cognitive capacity of the human brain to associate with other members in a social network. Dunbar (1998), for example, has famously argued that this ceiling is roughly 150 people in cases where connections are motivated by a clear crisis, and usually far less. A second is based on technical limitations pertaining to available bandwidth and processing power.

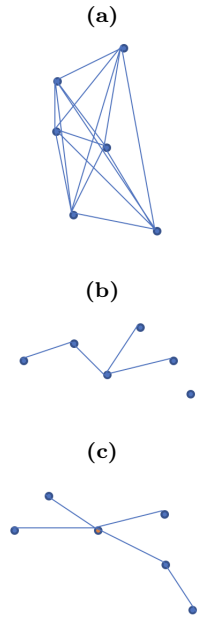

Figure 1: *Examples of network topologies with six nodes. (a) fully connected network; (b) random network, and (c) small-world network*

2 Unpacking the platform with blockchains

As alluded to in the previous section, a platform contract can be seen as a complex set of contracts that the platform operator engages in to preserve a favored network topology; as such, it represents a *feasible* institutional arrangement established by the infra-marginal transactions costs of participating in such a network.

Consequently, the relevant efficiency contrast when considering platform contracts ought to be with the underlying market that comprises *complete* Hayekian distributed information; since a platform network operates on the principles of intermediation and betweenness centrality, its structure of information flows can not replicate those of an entirely decentralized free market based on such sources of information.

Further, a platform contract interposes a secondary source of transactions costs over and above the Coasian transactions costs that justify the creation of a firm based on incomplete contracts. A platform contract can be seen as a meta-contract that seeks to deliberately engineer or 'design' the platform network. To achieve this, the operator must do two things that enable it confine the flow of information in ways that

are advantageous to its preferred network topology. First, it must use an incentive compatible mechanism (the platform) for its users to seek its intermediation services, and, second, it must serve as the nexus of all incomplete contracts that permits it to retain residual control over all indescribable future contingencies that the network faces.

A significant opportunity that blockchains represent is in their potential to unpack the black box of the platform contract. By decentralizing a large range of the platform operator's intermediation services among the network's users, blockchains have the potential to reduce that part of the transactions costs that are imposed by the centralized network topology of a platform-based market.

However, the efficiency gains from decentralization must be contrasted against the costs of implementing and maintaining a blockchain for the infrastructure of the market.

Chief among these costs is the consensus protocol that is selected for a blockchain implementation in order to achieve network-wide consensus over the validity of any proposed block of transactions. Every blockchain application needs a method to ensure that the users of the shared digital ledger have a strong incentive to verify its integrity and keep it secure. In its hallmark application of Bitcoin, for example, the underlying blockchain uses a PoW (proof of work) consensus algorithm for this purpose, which requires the 'miners' to batch new transactions into blocks in return for a reward comprising a set number of bitcoins and a transaction fee.[9] This block reward serves as an incentive for the miners to compete among each other in solving cryptographic problems with increasing degrees of difficulty in order to earn the right to link the next block to the chain. Alongside miners, any user on the network retains the ability to verify the history of transactions on the blockchain as well.

Since the PoW protocol effectively encourages an arms race in dedicated computing power devoted to solving the cryptographic hash problems among miners, we have seen resource consumption burgeon over the past few years.[10] It is often argued that this makes the Bitcoin network thoroughly inefficient, unethical even; this, of course, is missing the point, since the purpose of selecting a deliberately costly consensus protocol

[9]Over time, the block reward scales in favor of higher transaction fees as the total number of bitcoins mined approaches the maximum number that have been designed into its core software framework, making the bitcoin reward payable to the miners for every block lower.

[10]It has been estimated, for example, that the electricity consumption of the Bitcoin network will approach a level in between that of the entire national consumption in Ireland and Austria by the end of 2018. (de Vries, 2018)

is to make the ledger of transactions *increasingly* immutable through time, in lock-step with the network's value, and across a growing number of users, of which some proportion will always be adversarial (have an incentive to attempt attacks that seek to alter the ledger in their favor).[11]

This underlying blockchain on the Bitcoin network is known as its 'settlement layer' since its function is to record transactions immutably, thereby 'settling' accounts between users in a definitive manner. It is easy to see that scaling a blockchain-based network to accommodate a multitude of transactions is a deeper problem than it is for a platform operator on a platform network.[12] A blockchain database operates on the principle of *open* verifiability enabling a *distributed* consensus system in order to give precedence to the overarching principle of ensuring that only the version of the blockchain with highest credibility for immutability represents the status quo; this perspective is fundamentally different to a database that is centralized, closed to public scrutiny and where credibility of the database is coequal with the credibility of the platform operator. Transactions, therefore, may scale poorly on a centralized network, but are bound to scale much worse on a blockchain.

Solving this problem has yielded possibly the most compelling rationale for a blockchain-based contractual solution for all manner of market transactions.

2.1 Implementable comprehensive contracting solutions

A large variety of *incomplete* contracts always exist in the real world, where a future transaction can not be specified fully ex ante, yet this does not preclude it from occurring, even when the prospect of the contract being renegotiated ex post remains a possibility. Incompleteness is, as it were, retained in the contract for the duration of the contract between the transacting entities in several markets. Such contractual relationships are routinely subject to a host of unforeseeable contingencies and a variety of outcomes that aren't always verifiable, and, consequently, not readily made subject to third-party intermediation.

[11] Though there are a host of other alternatives to PoW, the strongest contender is a proof of stake system, where miners are replaced with validators who are selected through a randomization process, usually based on the stake that they venture as collateral in verifying a block. The tokens in a PoS system are, therefore, 'pre-mined', in that they exist at the outset.

[12] At present, the Bitcoin settlement layer can process roughly 5 transactions per second. Contrast this with the Visa network which can process roughly 1,700 transactions per second.

In contract theory economics, the theoretical counterpoint to this justification for incomplete contracts is the 'irrelevance' result, owing to Maskin and Tirole (1999), which essentially suggests that, so long as the distribution of payoffs is ex ante specifiable, the actual contingency becomes largely irrelevant. This suggests that optimal contracts ought to apply in all cases, whereby all information that is relevant to a contract can be completely contracted upon ex ante. Naturally, 'irrelevance' still relies on a suitable method to ensure that the state is verifiable or that the actors reveal pertinent information truthfully by participating in an incentive compatible mechanism.

This is not an innocuous requirement by any means. Even merely signaling private information to mitigate the problem of adverse selection involves undertaking private costs which can represent large social costs when considered cumulatively across markets. (Gale, 1996) Besides, incompleteness in contracts can exists for other theoretical reasons, such as the complexity of the future states in a contractual relationship (Segal, 1999), and it may even be useful to *deliberately* build incompleteness into a contract in practice to serve as a common reference point for admissible actions between contracting parties (Hart and Moore, 2008).

For either reason, practical or theoretical, if a generic platform for contracts is to be imagined it must be able to provide *comprehensive* contractual solutions, which, in turn, require a flexible mix of incentive compatible mechanism designs, comprising 'complete' contracts, *and* the possibility to contextualize contracts to the complexities of particular situations with a range of incomplete contracts. In other words, mutable design is essential to accommodate contractual variance in practice. Equally, no comprehensive solution for contracting has much value if it is not also simultaneously disciplined by the prospect of an immutable set of laws governing its structure.

With platform contracts, the mechanism of the platform represents the incentive compatible complete contract, and a range of incomplete contracts exist between participants of the network over services provided using the platform and over indescribable contingencies over the evolution of the network. All of these contracts are, usually quite amorphously, bundled into the overarching platform contract as part and parcel of the intermediation benefits that participation in the platform network represents over the market. There is little room for a mutable design template for contractual variance that is still compatible with the structure of a platform network.

However, by introducing blockchains to a platform network the platform contract

can theoretically be unbundled; the centralizing tendency of the platform mechanism can be dulled using the decentralized basis of a blockchain's operation. However, this is far from a straightforward process in practice. To see why, consider that an essential part of using blockchains to unpack the platform contract is through the use of smart contracts. A smart contract between two entities is the simplest incentive-compatible implementable complete contract one can imagine. The idea behind a smart contract is to use the immutable database and time-dependent nature of the blockchain to automate a transaction algorithmically between parties such that property can be recorded on-chain and rights to it can be transferred between the parties. Since the underlying blockchain effectively stands as a verification mechanism as well as a secure method for conveying property rights, a smart contract should entirely obviate the need for third-party intermediation, hence representing a significant opportunity to reduce associated transactions costs.

Naturally, a smart contract requires *complete* specifiability of the property or action. For complex property with several attributes that cannot be securely recorded or which materially alter during the course of a transaction, automation is not panacea if the transfer of rights is itself incomplete. This creates the need for the consideration of alternate methods to support smart contracts.

Chief among these is the idea of a network of different types of 'oracles' or 'trust agents', who all serve as independent verifiers of the various terms to a contract.[13] If this sounds like a roundabout way of reintroducing the role of the courts and traditional methods of third-party intermediation for a range of traditional contracts marked by an inherent incompleteness, that impression is understandable. However, the decentralized basis for the operation of smart contracts is a strong feature that developers wish to retain, and so the oracles that have been proposed usually themselves reside on the network supported by the blockchain. They may even expressly become part of a multi-signature contract that requires N of M participants to validate a transaction, or they make their validation work for smart contracts publicly verifiable. At this stage, it remains unclear as to what incentivizes their participation with the same standard

[13]One such service has been built by Oraclize for a range of blockchain applications, including Bitcoin, Ethereum and private blockchains. See www.oraclize.it. Another service, Bitrated, creates a marketplace of 'trust agents' who can be hired to manage a contractual relationship established through a multi-signature account. See www.birated.com.

of trustless-ness that is applicable to the root blockchain of Bitcoin or Ethereum.[14]

So, while the blockchain can serve to disintermediate a platform network, there are other problems that still require attention. Significant among them, as we have seen above, is the issue that blockchains are inherently less efficient than a traditional platform network in terms of accommodating high transaction throughput. This makes it a suboptimal choice for a range of practical applications.

Moreover, it is possible to imagine a series of transactions that do not directly correlate in lockstep with the linearity of a blockchain, in that some component of their particulars may need to be worked out 'off-chain' *before* making the transactions subject to the verifiability standard of the blockchain again. While the indelible timestamp of a blockchain supported by a strong consensus protocol is doubtless valuable in erecting a mechanism with the same durability of a reputable complex of institutions, buyers and sellers in practice would shun this setup for a range of contractual relationships if time-stamping transactions irrefutably itself becomes a source of additional holdup costs through opportunistic behavior by any actor who uses the quasi-rent that the funds in the multi-sig account represents, as well as the investments that may need to be made by a seller off-chain that a multi-sig account may not adequately capture.

In practice these problems can be solved through the use of scalability solutions that work by building a second layer atop a base blockchain application that permits a much wider variety of contractual transactions. The second layer essentially suspends the direct connection with the base blockchain, permitting contractual flexibility, but uses the base layer to discipline all forms of contractual complexity. This is best illustrated by the Lightning Network, built as a second layer over the Bitcoin blockchain.[15] What is noteworthy about the Lightning Network solution is that it generates the possibility of increasing transaction throughout on the Bitcoin network by many orders of magnitude; it permits creating state-channels between network participants directly as well as indirectly through an intermediary; and it retains the aspect of immutable settlement of the contract directly on the base layer.

[14]This is known as the 'oracle problem' in crypto-economics. A comprehensive solution for *any* source of information relevant to a contract does not exist. A partial workaround is that the oracle certifies the relevant information (usually objective data) for use in a smart contract, and gets paid for each such 'call' for information.

[15]With Ethereum a close parallel is Slock.it, which permits the creation of a largely disintermediated platform for sharable assets built over the Ethereum blockchain, albeit with a less rigorous 'settlement layer' as with Bitcoin.

By using this multi-layered approach to settlement on the blockchain, a wide range of markets that exist entirely on platform networks can be disintermediated by re-engineering platform contracts using a series of appropriate contractual solutions. For the complete contracts component, the base blockchain application provides a useful coordination mechanism[16], and for the portion of incomplete contracts required by the transactions that are sensitive to context, the secondary layer permits off-chain contracts to be designed, and intermediated by agents who are on the network.

Since all transactions – whether off-chain or directly on-chain – between participants are eventually settled on-chain, the set of contracts between any number of entities on the network are disciplined directly by the incentives structures that are compatible with the decentralized Bitcoin network. Such a contractual template holds the promise to become a *comprehensive contracting solution*, in the sense that it can be designed as mechanisms – and serve as complete contracts – while also remaining open to accommodating incomplete contracts flexibly; since this can be done without burdening the throughput of the settlement layer, the contractual system is also scalable to accommodate a wide variety of economic activity.

Recall the simple setup of the hawala system that we began with, which shows almost none of the desirable features of blockchains. Yet, a key message is that the costs of a transaction can be significantly reduced by disintermediating a platform, especially when the mechanism for doing so represents similar levels of credibility. In the context of a blockchain, a very similar system to that of hawala can be seen in the context of atomic swaps, or transfers across cryptocurrencies that have their own blockchains. The system is not unlike hawala in that the sender opens a payment channel with a given amount on one blockchain and includes the cryptographic hash of some random number. The recipient follows suit by opening a payment channel on the other blockchain for a predetermined amount permitting the recipient to collect this amount conditional on him receiving the random number from the sender. Once the sender provides this number, both parties can then conclude their transactions by closing off the payments channels and permitting the respective amounts to be registered on both blockchains.

To this simple setup if we can also add comprehensive contracting solutions for

[16] Albeit not strictly a 'mechanism' as it is meant by the literature in the economics, since participation is voluntary. For some government platforms, especially those pertaining to individual identity and property, participation *can* be made mandatory, making the parallel much closer.

transactions far more nuanced than simple remittances, we put ourselves in a position to disintermediate a much wider range of platform networks. We have seen that this would require the instantiation of an intermediary, not unlike the hawaladar for the hawala system – an intermediary who has a vested interest in maintaining the alternate decentralized platform to the same degree as the individuals involved in the contract.

While smart contracts in their current incarnation are not adequate for this lofty goal, there have already been several developments to their structure that get us much closer. Consider, for example, hashed time-lock contracts or HTLCs.

Let us suppose that the seller and buyer interact through an intermediary. The seller provides an assurance of intent by providing the cryptographic hash of a random number to the buyer. The buyer can then initiate a payment and include the hash with the condition that, before a given deadline expires, the seller must use the original random number associated with the hash to verify that the payment has been received. If the deadline expires, the payment is securely refunded back to the buyer. Notably, once the hash is received by the buyer, he can initiate a host of other action requirements by the seller.

There are several small and large issues that need to be addressed if we wish to make HTLC smart contracts the basis for a more comprehensive effort at making a variety of real- world contracts amenable to automation on a blockchain. For example, consider the duration (that is to say, the 'nLock' parameter) for an HTLC contract. The trouble with building a contractual template where the duration must be specified in advance is obviously that duration can then no longer emerge endogenously as a feature of the contract's contextual conditions. This can entail a cost of contracting that is imposed by the contract being immutable to shocks and changes in the context in which it operates that can be resolved simply by adjusting contractual length through renegotiation or automatic 'reopeners'[17]. Arguably, this is not an insurmountable issue to address for a developer. On the Lightning Network, for instance, the seller can satisfy a HTLC contract before the deadline is reached by signing it with his private key, thus terminating the open channel and including the transaction on the blockchain.

More generally, it also bears noting that this comprehensive contracting approach permits discretizing information flows across a network in such a manner that the role of any platform operator as an indispensable connecter across networks of markets on

[17]See Danziger (1995) on reopeners as a feature of contracts.

either side of the market can be significantly diminished or brought under the stronger influence of directly contestable markets.

3 Smart Institutions for Smart Contracts

Governments can greatly assist the ecosystem of comprehensive contracting solutions, and, by extension, a blockchain-economy, by realizing the enormous efficiency advantages from providing clarity in regulatory policy. Such clarity is especially important for blockchain applications since an onerous regulatory compliance procedure for contractual solutions provided on the blockchain would serve to dissuade its adoption for reasons entirely unrelated to its merits. This is because policy on the blockchain is much more directly a bandwidth problem; if regulatory compliance procedures occupy a significant fraction of available bandwidth on-chain, it would make scaling such solutions all the more difficult.

Therefore, I end this paper with a simple template for governments to take a more deliberate and purposive role in developing the framework for comprehensive contractual solutions for the blockchain economy. The template can be seen as *smart institutions*, and they would effectively work in conjunction with smart contracts on the blockchain, while providing the analytic intermediation required for more complex contracts that feature incompleteness.[18] Such incompleteness may be reduced through publicly verified input provided by the smart institutions based on soliciting independent expert advice and legal insight, and, generally, a wide variety of quantifiable contextual nuance that the contracting parties face.

The setup of a smart institution could be based on the principles of control process engineering; CPE foundations are routinely applied in automation applications across a range of complexity, from a simple electronic valve that might control the rate of flow of a liquid being poured into a container to the automation of machines, such as robots and autonomous vehicles.

Consider a simple thermostat as an example of CPE. Once set at a desired value, it sends a low-powered signal to the condenser, which undertakes higher-power effort to reduce the room's temperature. The difference between the desired temperature and

[18] As background to this approach, see Goorha (2009b). More specifically for the use of CPE in developing contextually-sensitive contracts, see Goorha (2018).

the room's temperature comprises the feedback, measured directly at the thermostat, and this error guides further signals sent by thermostat. The process constitutes a feedback loop. When the set-point temperature is reached, the thermostat switches off the condenser.

We might, of course, imagine a far more sophisticated thermostat, such as one that accommodates fuzzy logic: the thermostat may operate with the verbal instruction, "make the room cooler", rather than by requiring the input of a precise number of degrees, and it may even dehumidify the room when it hears the instruction, "it's too humid". Fuzzy logic controllers essentially convert verbal instructions into quantifiable inputs for the control process.[19] As any control process becomes more complicated – with more scope for ambiguity in target variables and, hence, more complex actuating signals – the process of metering and feedback becomes increasingly important. It is for this reason that modern controllers, informed by deep learning algorithms and big data analytics, are becoming increasingly competent at managing more complex reasoning.

In the context of contracting solutions on the blockchain, we might imagine that a simple three-party multi-signature account is established in an off-chain state channel by the buyer, with the seller and an intermediary as participants. This is shown by the gray rectangle in *Figure 2*. The intermediaries, shown within the blue rectangle, can be further decomposed into a dumb metering mechanism generating automated quantitative feedback, f, and a smart feedback mechanism that enhances feedback to f^* using more nuanced intermediation – possibly based on a fuzzy-logic control mechanism to convert qualitative input to quantitive feedback – before sending it back to the controller. This smart feedback mechanism process is where government regulators can erect their regulatory feedback protocols for use on blockchains. By adjusting the restrictiveness of this protocol, regulators would then be able to control the degree to which they permit contractual relationships to be intermediated by automated regulation relative to their regulation through traditional channels.

The strength of a blockchain is a direct function of the strength of its consensus protocol. On-chain, the Bitcoin PoW protocol serves to make its blockchain increasingly secure over time; similarly for off-chain state channels for comprehensive contracting

[19] Please see Goorha (2018) for more on how this process works.

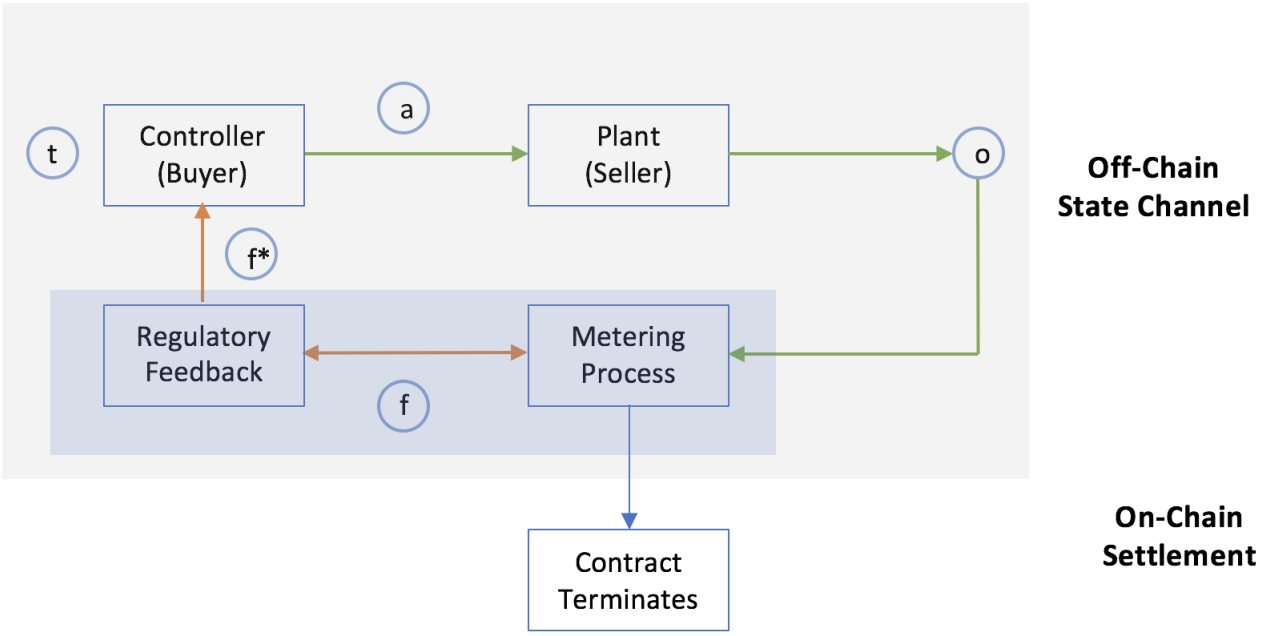

Figure 2: *The Comprehensive Contracting Solution with Smart Institutional Intermediation*

solutions the strength of the intermediation process would play a similar and vital role in ensuring that the comprehensive contractual solutions retain the same standards of security and viability as does the settlement layer. Governments can play a leading and vital role in this regard.

When the contractual parameters are simple, a smart contract (the path of which is traced by the green arrows) suffices. The metering only need be dumb since complexity is not an overriding concern with a smart contract; the contractual process need not even be looped before it is settled on chain. However, as contractual complexity grows, actuator signals may become less describable, the contract may require renegotiation, the target variable may need to be altered after a few rounds of feedback is received, and so forth. In such cases, disputations are much more likely to arise, and their ex ante expectation may even prevent such activity from being undertaken over a blockchain network. Here, it becomes much more important to have 'smarter' feedback generated. By having regulatory bodies serve as oracles on the blockchain network who can be called for input during the feedback process can serve to make such off-chain state channels extremely valuable. They would significantly ease the burden on traditional intermediation channels as well as accelerate the development of comprehensive contractual solutions for the blockchain economy.

References

[1] Danziger, Leif (1995) "Contract Reopeners," *Journal of Labor Economics*, Volume 13, Issue 1, pp. 62-87.

[2] Freeman, Linton C. (1979) "Centrality in social networks: Conceptual clarification," *Social Networks*, Volume 1, Issue 3. pp. 215–239.

[3] de Vries, Alex (2018) "Bitcoin's Growing Energy Problem," *Joule*, Volume 2, pp. 801-809.

[4] Gale, David (1996) "Equilibria and Pareto Optima of Markets with Adverse Selection," *Economic Theory*, Volume 7, pp. 207-235.

[5] Goorha, Prateek (2018) "Contextual Contracts: On a Context-sensitive Approach to Contract Theory," *Journal of Interdisciplinary Economics*, Volume 30, Issue 2, pp. 191-209.

[6] Goorha, Prateek (2009a) "Policy in the knowledge economy social network: a social capital redux," *International Journal of Social Economics*, Volume 36, Issue 9, pp. 930-944.

[7] Goorha, Prateek (2009b) "An Evolutionary Approach to Revising Modernization Theory: an introduction to the Credible Polity', *World Futures: The Journal of General Evolution*, Volume 65, pp. 176-203.

[8] Grossman, Sanford and Oliver Hart (1986) "The Costs and Benefits of Ownership: A Theory of Lateral and Vertical Integration," *Journal of Political Economy*, Volume 94, pp. 691-719.

[9] Hart, Oliver and John Moore (2008) "Contracts as Reference Points," *Quarterly Journal of* Economics, Volume 123, Issue 1, pp. 1-48.

[10] Kelly, Kevin (1997) "New Rules for the New Economy," *Wired*, September 1, 1997. https://www.wired.com/1997/09/newrules/

[11] Kelly, Kevin (1999) *New Rules for the New Economy,* Penguin Books

[12] Libert Barry; Wind, Yoram, and Megan Beck (2014) "What Airbnb, Uber and Alibaba Have in Common," *Harvard Business Review*, November 20, 2014.

[13] Lucas, Robert (2009) "Ideas and Growth," *Economica*, Volume 76, Issue 301, pp. 1-19.

[14] Maskin, Eric and Jean Tirole (1999) "Unforeseen Contingencies and Incomplete Contracts," *Review of Economic Studies*, Volume 66, pp. 83-114

[15] Quah, Danny (1996) "The Invisible Hand and the Weightless Economy," *Centre for Economic Performance* Occasional Paper No. 12

[16] Quah, Danny (1999) "The weightless economy in economic development," *Centre for Economic Performance*, Discussion Paper No. 417

[17] Rodrik, Dani (2014) "When Ideas Trump Interests: Preferences, Worldviews, and Policy Innovations," *Journal of Economic Perspectives*, Volume 28, Issue 1, pp. 189-208.

[18] Rysman, Marc (2009) "The Economics of Two-Sided Markets," *Journal of Economic Perspectives*, Volume 23, Issue 3, pp. 125-143.

[19] Segal, Ilya (1999) "Complexity and Renegotiation: A Foundation for Incomplete Contracts," *Review of Economic Studies*, Volume 66, pp. 57-82.

[20] Thurow, Lester C. (2000) "Globalization: The Product of a Knowledge-Based Economy," *The Annals of the American Academy of Political and Social Science*, Volume 570, pp. 19-31.