THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-2-2-(1)2019

The Contractual Cryptoeconomy: An Arrow of Time for Economics

Prateek Goorha
Independent Scholar, Greater Boston, USA
Correspondence: goorha@sent.com
Received: 11 March 2019 **Accepted**: 18 April 2019 **Published**: 2 May 2019

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
PG designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Abstract
We consider the potential blockchains have for building a framework for all manner of contracts that can characterize an economy using the unifying idea of control over their duration. Such a contractual cryptoeconomy (CCE) would accommodate a broader variety of contracts than smart contracts, which are suitable for a relatively small portion of the set of all feasible contracts. We proceed by examining the idea of a contract's natural life as a common feature shared across all contracts, be they incomplete or complete. This simplifying idea suggests why providing flexibility over a contract's duration on a blockchain – through innovations such as HTLCs — is necessary to increasing the variety of contracts that can be feasibly represented. We also assess participation in a CCE that features blockchains with differing degrees of security. We do so by focusing on how the value of a contract is related directly to its natural life for both its immediate participants and, through externalities across the CCE, to a wider set of users. A key idea provides the overall impetus: When contracts rely on third-party intermediation, at least some contractual surplus is dissipated in arbiter rent, making the quality of third-party arbitration as important as its scale. By contrast, blockchains create contractual mechanisms that act as Coasian exchanges that can internalize this arbiter rent. However, crucially, the degree to which their use requires forgoing contractual complexity and absorbing the cost of externalities can determine the relative benefits provided by a CCE.
Keywords: *Arbiter Rent; Contracts; Duration; HTLCs; Blockchains; Thomas Jefferson; Economic Arrow of Time; Coasian exchange; Contractual Cryptoeconomy*

1. Introduction

'The Earth belongs, in usufruct, to the living.' - Thomas Jefferson [1].

While its specific focus is blockchains, the impetus for this article came from Thomas Jefferson's observation cited above. It is extracted from a letter he wrote to James Madison in 1789, impelled by his belief that a contract's length should be set at a fixed period.

Jefferson's actuarial skills had enabled him to calculate that – owing to the average life span of individuals then – by the end of that period one of the parties would likely have died. Contracts, he proposed, should be rescinded every 19 years. The clock should, in other words, be reset so that the usufruct of contracts can more correctly reflect their true creators and beneficiaries.

It is on the nature of this link between the usufruct of a contract on the one hand and its duration on the other that we shall focus our attention on in this paper; it is, we shall see, key to the class of contracts that can be feasibly represented on a blockchain.

Yet there is also a second aspect of Jefferson's thought process that is worth appreciating: The idea that this usufruct is at risk of being delimited and squandered, and that a mandated reset of some kind is the only tool at hand to prevent this undesirable eventuality. Is a resetting of the clock necessary to realign usufruct across blockchains too, and can such a tool feasibly even exist for blockchains without necessarily violating its immutability characteristics? In relation to this idea we shall also consider a particular source of risk to a contractual cryptoeconomy (CCE) that emanates from the externalities between its

JEL Classifications: *D01, D02, D23, D86, O30*

different blockchain instantiations, and even between the CCE and the traditional economy based on legacy contractual mechanisms.

It is clear that Jefferson believed that successors to a contract should not be forcibly shackled to the actions of its predecessors, and that events from a time in the past should not take hostage those who create events at a time in the future. Given the linear and immutable nature of blockchains, does a CCE not meet this standard? We shall see how an appreciation of contractual variety, and developing mechanisms for a CCE to accommodate them, suggests quite the opposite.

Jefferson understood moral hazard all too well. On placing a hard duration on contracts, he wrote in his letter:

'This would put lenders, and the borrowers also, on their guard. By reducing too, the faculty of borrowing within its natural limits, it would bridle the spirit of war, to which too free a course has been procured by the inattention of money lenders to this law of nature, that succeeding generations are not responsible for the preceding.' [1]

His thinking inspires considering the following broader question: Do all contracts have some notion of a natural life in common? Perhaps more generally: What is the foundational role of time in transactions and contracts? Is it to provide an absolute and final verdict, like some digital super-precise photo-finish line in a race? Or is to serve as the permissive referee who taps an unseen wristwatch significantly, merely to encourage a dawdling participant to adopt a somewhat swifter pace of progress?

These are sweeping questions, but here we shall examine these issues more narrowly in the context of blockchains, for which a key characteristic is precisely that of the inherent immutability of transactions they enable alongside an impartial adherence to a linear process that features time-stamping as a tool to appeal to time as the ultimate impartial arbiter.

When time is connected with a sequence of transactions – say as with an uncomplicated supply chain or assembly line – the linearity of a secure blockchain can trivially be used to reliably and usefully bolster the operations with verifiability. However, a large swath of research in economics examines the myriad of situations where such linearity isn't quite so obvious. Often sequential investments are not fully specifiable ex ante, which is to say that there is no obvious chain to follow for contracting parties. In several cases such incompleteness is actually desirable to both parties in a contract, for example when the nature of incompleteness is itself a basis for setting expectations yet leaving room for creativity around a shared goal. And, frequently, the sequence should become terminable ex post to protect the value of an investment, as in cases where recontracting becomes necessary; in such cases, the prospect of recontracting limits the ability of the inefficient ex post allocation to endure.[i]

For blockchains to be a genuinely useful tool for contracting – and actualize a CCE – would seem then to depend not merely on their ability to serve as the proverbially dispassionate 'arrow of time', but also to enable guiding such an arrow's direction tractably when a contractual application requires it. This is to say that a CCE needs an 'economic arrow of time' that appeals to time as the arbiter, but in a manner better suited to maximizing contractual usufruct.

2. The Contractual Cryptoeconomy

While constitutions, transnational pacts, purchase agreements and employment contracts can all be seen as forms of 'contracts', they have several obvious and several subtle differences that justify their examination within the purlieus of separate fields of study. Indeed, whether a constitution can be considered a (social) contract in any real and useful sense is hardly an uncontentious idea. [2] provides several useful references and a general discussion, and, interestingly, also considers their applicability within the context of piratical constitutional contracts. See, also, [3].

Economists, for example, have long studied the difference between a complete contract and an incomplete contract. The incompleteness stems from the fact that a vast majority of contracts in the real world cannot be made fully contingent on a specifiable state of the world. Smart contracts, by contrast, are premised on fully specifiable states of the world and are, in this respect, an interesting example of complete contracts. For incomplete contracts, moral hazard is a prime motivator. In other words, incomplete contracts focus on ownership of productive assets because their use can often not be fully specified ex ante, nor can it frequently be monitored. It has been argued that such incomplete contracts could, in theory, be made equivalent to complete contracts provided only that the parties are averse to risk and we assume that they can at least provide a probability distribution for future outcomes, even if they cannot predict exact features of the possible future states of the world. This works, provided we have access to an incentive compatible mechanism that motivates the parties to declare the state that does eventuate truthfully. [4]

It is not, therefore, hard to understand why incomplete contracts are ubiquitous in the real world. For a discussion of the difference between complete and incomplete contracts in the context of blockchains, see [5], [6] and [7].

Abstracting from differences between the variety of applications of contracts and their broad types, here we wish to focus thought on an essential similarity observed by the third president: the idea of a natural life. Time – its duration; its ability to be reset; its impending horizon – is central to all contracts, and it is this shared basis of a 'progression across a series of transactions', each linked in some direct or indirect manner to time, that makes their association with blockchains an interesting subject to consider.

2.1 Internalizing Arbiter Rent

Blockchains operate on the essential principle of time-stamping a batch of transactions and permit the possibility of doing so immutably, verifiably and in a decentralized manner; crucially, depending on features of their particular instantiation, the degree to which these features are secured from sabotage varies. This lends them to be particularly useful for at least two functions: providing a reliable infrastructure for broadly accessible capital markets and serving as a basis for reifying and securing property rights.

It has long been recognized in the development literature that a government's ability has to credibly secure property rights and encourage well-functioning financial markets are key to its capacity to signal its commitment to private-sector investment, especially of the variety that is accretive to longer-term growth. (See, as examples, [8] and [9].)

Between these two functions, there is little doubt that weak property rights do more insidious damage to growth prospects than weak financial markets. [10] However, it has been shown time and again that the temptation for governments to spurn this advice and turn to rapacious rent-seeking activities remains a real threat to stunting economic growth and development prospects. On this point, [11] is particularly convincing.

This broader observation is important for the context of contracts, since third-party arbitration is key not just to a contract's enforceability but to the overall set of contracts that can eventuate in an economy. This function of arbitration, enforcement and verification that governments provide – primarily through their legal code and system of courts – yields them valuable economic rent, which we can see as 'arbiter rent'.

For a contractual space based on blockchains, however, the economic value that is represented by the arbiter rent is internalized within the same system that employs actors on the decentralized network to function as independent and neutral verifiers. Traditional arbiter rent, in this broad sense at least, is reimagined by blockchains. It is retained within the transactional parameters defined by the contractual space a blockchain's design implements. It is not, however, retained entirely within a given contract directly.

To see this point, contrast the contracts that rely on third-party verification provided by institutions with those contracts that entirely dispose of them, operating purely on the basis of trust between parties.

When third-party arbitration is essential, the general institutional quality (see, for example, [12]) and the reliability and efficiency of courts (as argued in [13]) becomes paramount to the extent that a contract can generate surplus. The potential for regulatory distortions resulting in higher arbiter rent and lower contractual surplus for the participants looms large over the market.

Since institutions also provide the broader context to societal trust, or 'social capital' between contracting agents, it is hard to separate the effects of each. However, it has been shown that, even controlling for such endogeneity, social capital still plays a very strong role in enabling beneficial contracts; [14] provides a discussion on the relative role that social capital plays in financial contracts in the context of southern versus northern Italy. Frequently such trust-based contracts are used by those who would otherwise be priced out of any feasible arbiter-enforced contract for a service that entails some form of direct or indirect arbiter rent. As such, 'trust' provides a useful social benefit for contracting.

More generally, the ability to remove the extractive influence of arbiter rent reduces the inframarginal cost and enables greater contractual surplus.

The trouble, of course, is that contracts that are strongly reliant on trust can only operate within the narrow swath of applications where prosocial behaviours and norms among the participants are socially embedded, which is to say, ordinarily only within extended families and smaller communities. [15] proposes a modelling framework to see the role of social capital for informal contractual enforcement in a network. The network connections themselves serve as a collateral that can be used for borrowing between participants in the network.

Contracts that are enabled by blockchains derive their basis from a third source. Neither do they directly rely on social capital – derived from interpersonal trust – nor do they need institutions that provide third-party verification and arbitration – premised upon state sanction. Instead, they replace both with a system based on a consensus protocol for their users that requires no intrinsic trust among its participants, but that creates a reliable contractual space where transactions can be made strongly verifiable.

Contracts operating on a blockchain are designed to internalize the arbiter rent, thereby creating a dedicated economic space – the 'contractual cryptoeconomy' – which is more broadly accessible than those contracts that rely entirely on social capital and less costly than those that rely on third-party arbitration.

Naturally, this is the macro-view for a theoretical motivation for the CCE. In practice, there are significant problems that make it unclear whether a CCE can indeed satisfactorily accommodate all other forms of contracts.

Consider, for example, that competing blockchain applications can be built ad nauseam without any costless manner to distinguish between their relative quality of implementation ex ante. Centralized third-party arbitration mechanisms, on the other hand, are usually maintained under a system that grants monopoly power over the arbiter's function to the state that defines the contract's jurisdiction. In theory, such proliferation can curtail the extent of the internalization of arbiter rent. Contractual surplus faces the risk of being dissipated when contracts are allocated inefficiently between the legacy contractual environment based on courts as the ultimate third-party arbiter and the contractual blockchain economy. On the other hand, proliferation might also generate positive externalities for the CCE. Much depends on whether we can make variegated blockchain implementations compatible and convergent to theoretical ideals of a contracting platform: interoperability between blockchains certainly permits such compatibility in a technical sense, though it only characterizes a fraction of all feasible implementations of blockchains. We shall develop these points further with the help of a simple model later on.

2.2 Flexibility in Contractual Time

Since the prior description of all relevant states that may affect a contract is either infeasible or impractically expensive, contracts are routinely left incomplete, without fully state-contingent clauses. Incompleteness in contracts may exist for other reasons as well, some of which are unavoidable and some deliberate.

Consider the case of a bilateral externality, for example, where the parties engage in a contract without prior information on the size of the externality that might be generated by the scale of the primary activity that one of the relevant parties engages in, and can therefore not effectively set appropriate terms. [16] Conversely, consider the case of crafting a contract to optimize on the choice of providing contractual flexibility in the terms of the contract ex ante as opposed to making them more rigid. With flexible terms established ex ante, the parties have more freedom to adjust their behavior ex post, once they have better information on how to make the division of surplus more agreeable to both parties. At the cost of some loss of control, flexibility in contractual terms can incentivize creativity, make individual initiative more likely to affect surplus, motivate the selection of more suitable projects, and so forth. This suggests that there may be a strong role for deliberate incompleteness in contracts as a tool to set the expectations for the parties involved. [17] Smart contracts, in such cases, would obviously be suboptimal.

Given the large variety of contracts in the real world that are best described as incomplete, it is worth considering the Jeffersonian idea of deliberate recontracting (in other words, the proviso of a horizon for contracts) for the particular context of contractual implementations on a blockchain.

Blockchains have potential as a theoretical construct for recreating consensual outcomes across a decentralized market structure to leverage the value that is inherent in aggregating distributed information efficiently. For economics this is nothing short of revolutionary, for the very obvious reason that we can now imagine a third alternative to the dichotomy that underpins the 'market versus organization' dilemma (or firms versus institutions) that [18] outlined. Blockchains permit market orderings for value-generation that suspend both the invisible hand of the price mechanism of markets and the direct guiding hand of hierarchies in organizations; [19] terms this third mechanism a 'cryptographic stigmergy'.

The fact that they are immutable, time-dependent databases that can be made exceedingly censorship resistant makes the market and social orderings that public blockchains enable especially durable. However, blockchains are not amenable to providing nuanced consideration of incentives and are, as a consequence, less suitable for tackling contractual complexity that such orderings must routinely grapple with. In this respect, scaling solutions for blockchains that introduce layers upon a foundational blockchain consensus protocol, and then erect a network upon it that can flexibly represent nuance that contractual incentives contain are noteworthy.

Consider the idea of a hashed time-locked contract (HTLC), which illustrates the connection between providing some degree of control over time and the types of contracts that it makes possible. An HTLC is a particular kind of smart contract that has been developed for the scalable transactional layer – the Lightning Network – built on top of the underlying Bitcoin blockchain[ii]. [20] The Lightning Network enables the creation of task-specific payment channels off-chain that permit the aggregation of several transactions that can be mapped onto fewer transactions on the base layer, thereby lowering the average transactional cost. In the limit, only two transactions on the more expensive and slower base layer suffice for a multitude of transactions on any given payment channel: the initial transaction that funds the payment channel shared by two or more agents in a 'multisig' account, and a final transaction that updates the status of accounts after the payment channel is closed off. This effectively loosens the dependency of a multi-transactional contractual relationship on the immutable time-stamping feature of the underlying Bitcoin blockchain. Transactions proceed by a process of sequential consensus over mutually preferred states that, once agreed to, simultaneously also invalidate deprecated states by instituting a penalty comprising the loss of all staked funds should the previous state be surreptitiously used to close off the payment channel and published to the blockchain.

The network aspect of the Lightning Network permits several 'hops' across any of its nodes with open payment channels. This allows any participant to effect payments to anyone else on the network much more swiftly and cost-effectively than is possible with the base Bitcoin layer. Moreover, the open nature of the network creates a contestable market for transactions. This is important since it ensures that competitive market pressures influence the terms of all new contracts, and the terms that pertain to the division of the surplus that the contract can entail.

For our context, these developments are significant for two compelling reasons.

First, more specifically, HTLCs make the significance of a natural expiry for a contract in eliciting efficient contractual investments clearer to apprehend. An HTLC operates by first creating the hash of a secret. The secret must be revealed by the recipient in order to access some funds at stake. If the hash is kept private, we have a more constrained and state-contingent contract between a buyer and a seller. If the hash is made public, we can then imagine a tournament between a buyer and a pool of sellers who competitively exert efforts to discover the secret. An HTLC also involves an interplay between a definite time at which the contract expires and the ability to adjust the terms of the contract to the demands of a specific context by decrementing this duration sequentially. An HTLC, therefore, places emphasis on publicly specifying a 'fixed duration' before the contract's outcome becomes inviolably published to the Bitcoin blockchain, thereby ending the contract and forcing a reset.

While this reset afforded by the base layer is Jeffersonian in spirit, the HTLC permits context to provide variability in the duration itself. This is because an HTLC also features a method to introduce a 'flexible horizon' as a method to motivate and negotiate efforts that help generate contractual usufruct in the shadow of the Bitcoin blockchain. As such, HTLCs are designed and can be developed further to capture a broader swath of contracts in practice.

Second, and more broadly, note that the Lightning Network could, in theory, permit defining any arbitrary architecture for some given contractual mechanism as a subgraph of its overall network structure. In particular, it becomes feasible to specify not just any set of nodes that are involved within a transaction, but also the order in which they are involved from the time it is initiated to the time it is completed. Therefore, HTLCs can be seen as an organic and dynamic method to define a nexus of contracts that determines the boundary of a traditional firm, and it uses the underlying Bitcoin blockchain as the third-party arbiter for a wider set of contracts that inhere to traditional firms.

While this setup seems to have effectively created the precursors to decentralizing a firm on a scaling solution for blockchains, it remains far from certain that it rings in the demise of traditional firms. Issues pertaining to residual control over productive and complementary assets, management of teams, the assumption of risks, the delegation of authority across agents, and so forth are complex contractual issues that will require further developments, very likely relying on a suite of suitable technologies working seamlessly to integrate not just blockchains, but other types of ledger technologies as well.

3. The Economic Arrow of Time

The prospective role of time-stamping processes that can then be marched immutably through time looms large over applications that are considered for blockchains. There is something attractive about relying on time as an arbiter.

Of course, this view is rather limiting in its capacity for the nuanced insight needed for dealing with contractual variety in the real world. It is indeed true that some physical processes feature an 'arrow of time': closed systems with increasing entropy concretely indicate an irreversible and directional arrow through time. Most famous among these is the thermodynamic arrow of time implied by the Second Law of Thermodynamics. Other processes, however, are characterized by a 'time-reversal invariance', in that they do permit possibilities for a reversal of the process. [21] It is, therefore, even at a rather general level, infeasible to rely on the inviolability of some implied arrow of time as the essential shared foundation for real world applications. In the context of blockchains, while the law is routinely taken to unleash the value of transactional immutability, it can very well also be taken to suggest the level of difficulty required to successfully sabotage precisely that feature.

For instance, a supply chain, from initial input to final output, may appear to represent a process very conducive to the arrow of time analogy. Yet, the value of any such arrow shrinks markedly when we are interested in more than merely describing the process of sequentially linking units into a chain. By concentrating emphasis on the curation of information, a supply chain on a blockchain sets aside several interesting and important contractual issues, implicitly assuming that they can all be considered complete.[iii] This delimits the usefulness of blockchains by relegating a host of incomplete contractual transformations that affect the potential usufruct of the supply chain. By contrast, when we begin to consider aspects of the various contracts that exist between entities on a supply chain, the emphasis shifts from one of an inexorable and rigid arrow of time, to one that can be guided – perhaps better seen to be a distinct 'economic arrow of time'.

In a standard contract in economics (where the principal is risk neutral and the agent is risk averse) the prospect of renegotiating a contract serves to give the contract precisely this characteristic of time-reversal invariance. When an agent must select costly effort that is unobservable by the principal over the course of a contract and, simultaneously, must also commit to not renegotiating, she exposes herself to a degree of risk. To elicit the optimal level of effort through any form of assurance of a payoff that corresponds with the higher-level of effort, the principal would need to distinguish between agents who would select suboptimal levels of effort from those who select the optimal level; instantly, we shift the focus of the problem to one of resolving adverse selection rather than a strict sequential progression through the contractual parameters.

3.2 Aspects of time

Contracts that feature degrees of state dependency and propensities for renegotiation underscore the relevance of two aspects of time that are related but subtly different in their effects: 'timing' and 'duration'.

It is broadly understood that timing is integral to the very rationale for a range of contracts. The sequence and ordering of investment decisions that are stipulated by a contract can determine the amount of contractual surplus generated. One of the key messages of transaction cost economics is that timing is key to ameliorating a variety of opportunistic behaviors that are inspired by appropriable quasi-rents; timing is, indeed, central to motivating efficient investments, reducing a range of social externalities and, of course, in setting the overall boundaries of a firm with respect to the market. A key difference between a simple state-dependent smart contract and an HTLC is that the latter permits a method to algorithmically delimit the appropriable quasi-rents involved in a contract.

Contracts can also vary widely in their duration. Constitutions usually have far more enduring lives while several securities contracts can have extremely short lives. Thus, a provision for flexibility over both aspects of time that affect the contractual horizon is both necessary and appropriate for any generic contractual template.

The idea of a contractual duration has been examined at some length in the literature. [22] and [23], for example, suggest that, broadly, contract length depends on the level of uncertainty the investment represents and the cost of renegotiation. Short-term contracts with the option of renegotiation have been contrasted with longer-term contracts. For example, [24] suggests that, in the absence of a commitment to refrain from renegotiation, a buyer and seller will prefer engaging in a sequence of short-term contracts. (See also [25], which contains useful references.) [26] demonstrates the efficiency of short-term contracts over the long run and [27] suggests that even spot contracts can be efficient when inter-temporal smoothing concerns are not a consideration.

Concerns with sequential short-term contracts arise when pertinent information over incentives and 6 behaviour is revealed asymmetrically and in a manner that is correlated over time so that bargaining power shifts squarely towards one party to the detriment of the other. Here, smart contracts that also strongly guarantee anonymity of the participants ex ante would incentivize undertaking a sequence of shorter-horizon contracts, thereby avoiding introducing undesirable divisions of surplus owing to the asymmetric revelation of private knowledge. [28] develops a class of contracts for the Lightning Network, called 'discreet log contracts', that provide anonymity as a feature while also reducing the scope of malfeasance by the third-party nodes that act as intermediaries.

3.2 Phases in a contract's natural life

Regardless of the nuance over aspects of time within a contract's natural life, most contracts are usually seen dichotomously – a contract either exists or it does not, whether in prospect or in fact, and whether it is tacit or explicit. However, consider that most contracts exist within contextual environments that impinge upon them and lead them through 'states' of validities over the duration of their existence. Generally, we can call these states of a contract over its natural life its 'phases' and enumerate at least three: acceptability, vulnerability and termination. Quite simply, when an extant contract accords with the intention of its participants it can be said to have acceptable validity; when, over its life, it is susceptible to being either terminated or unacceptable (at risk of renegotiation) then it can be said to have a vulnerable validity. The contract's natural life can thus be parsed into phases that describe stages of its existence, and we can subsequently consider the transitions of the contract through these phases over its duration.

While fluid transitions between phases that might exist within a contract are not explicitly considered in the literature, the general issue is recognized as one that is significant in its social welfare implications. For instance, [29], which focuses on contrasting ex ante dispute resolution arrangements with ex post dispute resolution; while ex ante arrangements enhance joint surplus, they tend not to be legally enforced.

Our consideration of a contract's natural life here is not meant as a sensationalist departure from the literature on contracts, but to draw attention to the fact that several aspects of a contract, such as its prospect for renegotiation, uncertainty, moral hazard, and adverse selection, can usefully be seen as being internal to the contract and manifested as transitions across its phases. HTLCs provide a very promising first step towards resolving such issues for contracts on the blockchain, but they are hardly flexible enough to accommodate complex transactions, multi-layered contracts, complicated property rights, and a host of other issues.

Contracts are often generic templates. They might be drawn up to be applicable across a multitude of transactions, with only limited consideration for specific circumstances, or they might be drawn up and made inviolable through the passage of time or across its applications in a given period. Several examples can be offered in support of this observation of a social, political and economic nature: primogeniture, constitutions and union-negotiated employment contracts, for instance, are contracts that, perforce, do not specify all feasible states explicitly, but their incompleteness for a particular context or contingency (intentionally or not) completely defines their phases. This restates the result in [25], but for a different reason: there the observation is that incompleteness on account of transaction costs need not be relevant so long as payoffs are known. Here, incompleteness can never be entirely eradicated even if payoffs are known so long as parties to a contract 'care' about the transitions of the contract over its phases in its duration, and that the phases are finite and foreseen. It is, of course, feasible that the phases in the duration are a mechanism relevant to the contracting parties since it retrieves information relevant for payoffs.

4. Externalities in a CCE

Recall that [18] argued that there is an inherent 'cost to discover market prices,' and that firms are motivated by the ability to suspend using the price mechanism of the market to coordinate production, permitting the firm's manager instead to direct the coordination of resources. Similarly, a blockchain can be seen as a 'Coasian exchange': Participants are brought together through an ecosystem that acts as a mechanism for the coordination of activities organically, and which is motivated by the 'cost of discovery for the market value of consensus'.

Arguably, the Lightning Network, as a second-layer scaling solution for Bitcoin, can be seen as an effort to encourage the Coasian exchange dynamics of the underlying layer by undertaking an 'intervention' to ameliorate the negative externalities from congestion on the base layer.

Intrinsic to these relative costs of discovery (those for the market prices versus those for the market value of consensus) are several externalities, positive and negative, that a contractual blockchain economy represents relative to the traditional economy.[iv] These externalities may inhere in the social resource costs for securing a blockchain implementation's consensus protocol. They may arise from the information costs imposed by implementations of blockchains with less desirable characteristics or the lack of interoperability between the more desirable ones.[v] They may even pertain to the developments upon it that alter its value proposition.

There is a broad source of externalities that the regulation of cryptocurrencies imposes upon this relative cost consideration. Broadly, this source inheres to the difference between the market for ideas as opposed to the market for goods. Externalities are a common basis for excessive regulatory intervention in the market for goods, especially when contrasted with a reluctance to apply similar regulatory predispositions in the market of ideas. It was Coase again ([30] and [31]) who articulated why a definitive treatment of this issue was essential to any real consideration of externalities affecting production in markets. The notion, frequently heard, that software ought to be treated by the government as speech makes this point quite clear.

4.1 A traditional modeling framework on realigning externalities

Let us briefly consider this issue of externalities as they pertain to participation in the CCE. We use a simple framework that should be instantly familiar to students of public economics.

We might imagine that the economy comprises some secure blockchain υ with a market price of p^{ν}, and other blockchain instantiations conducive to hosting contracts. We can think of this ecosystem collectively as our contractual blockchain economy, Υ.

The point is to imagine a scenario where participation in υ provides a net external value to other participants across Υ, and that it is only partially accounted for by the participants within the secure blockchain. To capture the idea that other participants in the blockchain economy experience varying degrees of externality effects from υ, the nature of which can also be multidimensional, we only need assume that the joint probability distribution $P(V, E)$ is known to all who participate in Υ, where participation in Υ yields a private benefit of V to the individual and, simultaneously, it inspires a net positive externality of value, E. In terms of our Jeffersonian premise, E can be seen to represent that part of the contractual usufructs in υ that are not directly internalized by its participants.

It is useful to see why this joint probability distribution would make sense for Υ. Information is inherently distributed, and so the secured and decentralized economic orderings enabled by υ entails more of a gain to those who are more marginalized by any of the distributively inefficient economic orderings that are more centralized and less secure than υ.[vi]

To fix ideas further, let us capture the social marginal cost that the security of υ entails on the Υ ecosystem with s. This permits us to define a net social gain in the blockchain-enabled economic system; for an individual in Υ, participation in υ yields a net social gain of $\kappa = (V + E - s)$.

All new entrants to Υ face p^{ν} for access to the most secure blockchain. Naturally, if p^{ν} exceeds the entrant's reservation price she does not participate in υ. As such, a recognition of the presence of the net positive externality makes it advantageous for Υ to institute a method to provide a social subsidy for all entrants to υ. In the case of the secure blockchain, the magnitude of this 'subsidy' can be seen as the social resource cost, R, of securing υ, and it can be written as

$$R = \int_{p^{\nu}} \int_{0} \kappa(P(V, E))dV\, dE\,,$$

where the value that a participant receives begins at p^{ν} without an upper bound whereas the externality from a given participant ranges from zero without an upper bound.

If Υ were to efficiently select a price for υ we would have:

$$\partial R / \partial p\upsilon = -\int_{0} \kappa(P(V, E))dE = 0.$$

This suggests that the efficient price for υ is

$$\widetilde{p^{\nu}} = \alpha\left(E/\widetilde{p^{\nu}}\right) - s,$$

where $\alpha\left(E/\widetilde{p^{\nu}}\right)$ represents the average externalities applicable at the efficient price; thus, the social marginal cost is equal to the social marginal gain.

In words, even an efficient price consideration for υ can do no better than lump in relevant nuances in average externalities. Those in Υ for whom the private benefit and net externality is below the social marginal cost participate in υ (V is higher than

$\widetilde{p^{\nu}}$); those for whom it is higher do not participate (V is lower than $\widetilde{p^{\nu}}$). This is undesirable, of course, because the former comprises the group of participants in υ who create fewer net positive ϒ-wide externalities and the latter group would have been participants who would be more likely to generate such positive externalities to ϒ.

It is quite obvious that any ability to price discriminate between these groups would be an immediate source for an increase in the net social externality gain from market outcomes.

In our context we can imagine higher layers on the secure blockchain υ to concern themselves with increasing the transaction throughput of υ's base settlement layer. This naturally serves as a screening mechanism between those participants who are interested in the security and immutability of the value of the data on υ through time and those who are interested, more proximately, with securing frequent transactions at low cost, which we can capture with the variable ς.

This latter group would then have a joint probability distribution of $P^{\varsigma}(V,E)$, whereas and the former group would have $\widetilde{P^{\varsigma}}(V,E)$. The social resource cost, R, of securing υ, now becomes

$$R = \int_{p^{\nu}}\int_{0} \kappa\widetilde{P^{\varsigma}}(V,E).\, dV\, dE + \int_{p^{\nu}}\int_{0} \kappa(P^{\varsigma}(V,E))dV\, dE$$

With the cost of access to the higher transactional layer as l, the efficient price for participants solely in the settlement layer abides the same condition:

$$\widetilde{p^{\nu}} = \alpha(E/\widetilde{p^{\nu}}) - s$$

whereas, for the groups on the transactional layer, the price abides:

$$s + l = \widetilde{p^{\nu}_{\varsigma}} + \alpha_{\varsigma}(E/\widetilde{p^{\nu}}).$$

The price for the group participating in the transactional layer is lower than that for the group on the base layer and the net positive externalities are higher through discrimination. Specifically, the ability to sort the participants in this manner permits participation in the base layer to exclude those for whom E was lower but V was higher, and include them in the transactional layer instead.

There is a technical limit for the number of transactional layers that are likely to be built on υ as well as a practical limit on the need for such layers. At a general level, this causes a degree of pooling of the participants across the two groups and creates limits to the ratcheting effect that curators of such layers might develop merely to price discriminate on the basis of ς more and more perfectly. See [32], who initially developed this idea in the context of a two-period incentive contract with asymmetric information on observed performance.

5. Concluding Remarks

With Jefferson's observation as the overarching impetus, we have examined the issue of a natural life for contracts as a feature they all share. Contracts do not, however, last forever, and the notion of their stability is only relevant when seen from the perspective of their vulnerability to partial failure; in other words, how contracts behave over the course of their entire life deserves attention. Blockchains draw attention to this overarching fact. They hold the potential to develop a platform, with features of a Coasian exchange, that permits the use of an economic arrow of time that can accommodate a genuine contractual blockchain economy.

The Jeffersonian standpoint of favouring the living is an acknowledgment[vii] that the contractual enabling of the usufruct is premised upon a period that comes to a close. Logically, this period can be examined as a duration with a definite commencement and expiration, but with varying states of validity as economic rent from a relationship varies over the course of the duration of the contract; the contract then can be seen to have conditional probabilities for these validities over its duration. When contractual usufruct is lost through the course of a contract's natural life, the Jeffersonian solution of recontracting makes patent sense. However, when an economic arrow of time can be appealed to that can service complete as well as incomplete contracts, recontracting does not have to be the default solution. The linear transformations that blockchains accommodate so well provide a strong basis for contractual mechanism design; the organic networks that fluidly emerge from the evolving patterns of contractual usufructs that higher-layer scaling solutions provide suggest that a much wider variety of incomplete contracts can be accommodated as well. Together this gives us a strong basis for a contractual blockchain economy.

Admittedly there is a long way to go before the contractual blockchain economy can be seen as a real alternative – indeed, one that is to be preferred in an era of technologies that favor distributed information – to the traditional economy. However, the fact that several of the necessary components exist in theory and practice even today is a real source for optimism.

References:

[1] T. Jefferson "Letter to James Madison", The Founders' Constitution, vol. 1, chapter 2, document 23, University of Chicago Press. http://press-pubs.uchicago.edu/founders/documents/v1ch2s23.Html, 1789.

[2] P.T. Leeson, "The Calculus of Piratical Consent: The Myth of the Myth of Social Contract", Public Choice, vol. 139, no. 3/4, pp. 443-459, 2009.

[3] D.D. Heckathorn and S.M. Maser "Bargaining and Constitutional Contracts", American Journal of Political Science, vol. 31, no. 1, pp. 142-168, 1987.

[4] E. Maskin and J. Tirole, "Unforeseen Contingencies and Incomplete Contracts", Review of Economic Studies, vol. 66, no. 1 (special issue on contracts), pp. 83-114, 1999.
[5] P. Goorha, "Blockchains as Implementable Mechanisms: Crypto-Ricardian Rent and a Crypto-Coase Theorem", Journal of the British Blockchain Association, Volume 1, Issue 2, Available: 10.31585/jbba-1-2-(4)2018., 2018a.
[6] P. Goorha, "A Comprehensive Contracting Solution Using Blockchains," SSRN Working Paper, Available: http://dx.doi.org/10.2139/ssrn.3237076 , 2018b.
[7] J.S. Gans (2019) 'The Fine Print in Smart Contracts,' SSRN Working Paper, Available: http://dx.doi.org/10.2139/ssrn.3309709, 2019.
[8] D. North, Institutions, Institutional Change and Economic Performance, Cambridge University Press, 1990.
[9] D. Rodrik, "Promises, Promises: Credible Policy Reform via Signalling", The Economic Journal, vol. 99, no. 397, pp. 756–772, 1989.
[10] S. Johnson, J. McMillan and C. Woodruff, "Property Rights and Finance", American Economic Review, vol. 92, no. 5, pp. 1335–1356, 2002.
[11] A. Shleifer and R. Vishny, The Grabbing Hand: Government Pathologies and Their Cures, Harvard University Press, 2002.
[12] D. Acemoglu, D. and S. Johnson "Unbundling Institutions", The Journal of Political Economy, vol., no. 5, pp. 949-995, 2005.
[13] A. Shleifer, "Efficient Regulation", Regulation vs. Litigation, ed. Daniel Kessler, NBER and University of Chicago Press, pp. 27-43, 2010.
[14] L. Guiso, P. Sapienza and L. Zingales, "The Role of Social Capital in Financial Development", The American Economic Review, vol. 94, no. 3, pp. 526-556, 2004.
[15] D. Karlan, M. Mobius, T. Rosenblat and A. Szeidl, "Trust and Social Collateral", Quarterly Journal of Economics, vol. 124, no. 3, pp. 1307-361, 2009.
[16] R. Pitchford and C.M. Snyder, "Coming to the Nuisance: An Economic Analysis from an Incomplete Contracts Perspective", Journal of Law, Economics and Organization, vol. 19, pp. 491-516, 2003.
[17] O. Hart and J. Moore, "Contracts as Reference Points", Quarterly Journal of Economics, vol. 123, pp. 1-48, 2008.
[18] R.H. Coase, "The Nature of the Firm", Economica, vol. 4, pp. 386-405, 1937.
[19] P. Goorha, "The Return of 'The Nature of the Firm': The Role of the Blockchain", Journal of the British Blockchain Association, volume 1, no. 1, Available: 10.31585/jbba-1-1-(2)2018, 2018c.
[20] J. Poon and T. Dryja "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", Available: https://lightning.network/lightning-network-paper.pdf, 2016.
[21] B. Roberts, "When We Do (and Do Not) Have a Classical Arrow of Time", Philosophy of Science, vol. 80, no. 5, pp. 1112-1124, 2013.
[22] J. Gray, "On Indexation and Contract Length", Journal of Political Economy, vol. 86, no. 1, pp. 1-18, 1978.
[23] S. B. Vroman, "Inflation Uncertainty and Contract Duration", Review of Economics and Statistics, vol. 71, no. 4, pp. 677-681, 1989.
[24] O. Hart and J. Tirole "Contract Renegotiation and Coasian Dynamics", Review of Economic Studies, vol. 55, no. 4, pp. 509-540, 1988.
[25] M. Dewatripont, "Renegotiation and Information Revelation over Time: The Case of Optimal Labor Contracts", Quarterly Journal of Economics, vol. 104, no. 3, pp. 589–619, 1989.
[26] P. Rey and B. Salanie, "Long-Term, Short-Term and Renegotiation: On the Value of Commitment in Contracting", Econometrica, vol. 58, pp. 597-619, 1990.
[27] D. Fudenberg, B. Holmstrom, and P. Milgrom "Short-term Contracts and Long-Term Agency Relationships", Journal of Economic Theory, vol. 51, pp. 1-31, 1990.
[28] T. Dryja, "Discreet Log Contracts", undated working paper, MIT Digital Currency Initiative, last accessed: February, 2019.
[29] S. Shavell, "Alternative Dispute Resolution: An Economic Analysis", Journal of Legal Studies, vol. 24, no. 1, pp. 1–28, 1995.
[30] R.H. Coase, "The Market for Goods and the Market for Ideas", American Economic Review, vol.64, no. 2, pp. 384–391, 1974.
[31] R.H. Coase, "Advertising and Free Speech", The Journal of Legal Studies, vol. 6, no. 1, pp. 1-34, 1977.
[32] J. Laffont and J. Tirole "The Dynamics of Incentive Contracts", Econometrica, vol. 56, no. 5, pp. 1153–1175, 1988.

[i] Note that, when such inefficiencies are the source of rent for one of the parties in a contract, recontracting is undesirable to her, even if recontracting may lead to a Pareto improvement for the contract.

[ii] Recall that the base layer of Bitcoin was the first blockchain application and was created with the intention to serve as a digital payment system for networks that obviated the need for third-party intermediation. Bitcoin secures its transactions through the use of a consensus algorithm based on the idea of incontestable proof of work done; it is operationalized by nodes on the network called miners who must invest in costly dedicated computer hardware and energy to competitively solve cryptographic puzzles in order to earn the right to batch transactions into a block that then gets appended to the Bitcoin blockchain. This provides the miner a payoff comprising a fixed number of bitcoins and a smaller variable transaction fee, while enabling all participants on the network to verify the accuracy of the overall ledger of transactions independently.

[iii] For instance, along each stage of a supply chain that features a typical two-sided market, incentives provided by the reference platform linking both sides of the market may well change.

[iv] Naturally, there are several externalities that pertain to the mechanisms of a given blockchain implementation as well. These may include externalities imposed by the activities of a single node that affects the entire network, such as when it engages in transactions that increase the latency across the entire network and ties up a disproportionate share of resources. However, we are more interested here in considering externalities directly relevant to the broader contractual blockchain economy.

[v] A key benefit of contracts on interoperable blockchains is in reducing the costs of complexity in describing outcomes that pertain to a contract. For example, the nature of investments that parties make at *time 2*, once the contract has been put into operation at *time 1*, is often seen as being sufficiently complex to make them effectively beyond being independently verified by any third-party, such as a court. Blockchain interoperability can assuage this concern by folding in more and more aspects of an incomplete contract within the ambit of what can be feasibly verified publicly by a 'trusted third-party'. Such aspects can pertain to the nature of the investments, but also to the realized state of the world ex post.

[vi] Mutatis mutandis, this can be seen to extend beyond the contractual blockchain economy to the traditional economy as well.

[vii] The author readily admits that Jefferson's observation was more profound than what is made of it for the purpose of this paper!

