THE JBBA

PEER-REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-1-2-(4)2018

Competing Interests:
None declared.

Ethical approval:
Not applicable.

Author's contribution:
PG[1] designed and coordinated this research and prepared the manuscript in entirety.

Funding:
None declared.

Acknowledgements:
None declared.

Blockchains as Implementable Mechanisms: Crypto-Ricardian Rent and a Crypto-Coase Theorem

Prateek Goorha[1] PhD

Correspondence: goorha@sent.com

Received: 13 August 2018 **Accepted**: 20 September 2018 **Published**: 28 September 2018

Abstract

We suggest that the promise of blockchains is to be found not merely in the more proximate fact that they are immutable ledgers, but the broader impact that comes from blockchains as a template for mutable design. We discuss mechanism design theory to suggest where blockchains may or may not be seen as implementable mechanisms. We further discuss the idea of defining self-identity as an `elastic asset' using the blockchain in order to generate Ricardian rent from the cryptoeconomy. We suggest how this connection might be exhibited by the Bitcoin blockchain mechanism by discussing the shape of the cryptoeconomy it produces. Finally, we develop an application of the Coase theorem for the cryptoeconomy as a method for analyzing interactions between the traditional economy and the cryptoeconomy.

Keywords: *Blockchain, Cryptoeconomics, Mechanism Design, Ricardian rent, Coase theorem, Identity, Asset elasticity.*

JEL Classifications: *D02, D86, L22, O30, P4*

1. Beyond Markets and Firms

In his seminal article, Coase [2] essentially developed the definitive economic axiology, proposing the market and planning (where his particular emphasis was on the scope of a firm) as two alternate methods for the organization and creation of economic value. In a short article published recently in the JBBA, Goorha [5] suggested that, while blockchains may not violate the logic in Coase's argument, they do suggest an incipient intermediate third form, whereby self-organization replaces some of the need for top-down planning and some of the imperative to 'discover' market prices, without obviating the need for either entirely; this third form was termed a cryptographic stigmergy.

In order to examine whether this view has deeper merit, in this article we consider where blockchains broadly fit in the overall picture of the classical theory of the firm. In doing so, we will develop the idea that the promise of blockchains is to be found not merely in the more proximate fact that they are immutable ledgers, but the broader impact that comes from blockchains as a template for mutable design. We articulate this idea from the principles of industrial organization in economics by discussing mechanism design theory and examining the case for blockchains as a class of implementable mechanisms.

Let us begin with some elementary background. The Coasian transactions-cost framework (or TC model) for the organization of production in firms, as opposed to markets, was further developed by appealing to the idea of appropriability of specific asset investments made in the pursuit of any joint production of economic value [i]. Such at-risk investments generate a quasi-rent that is specific to the relationship and is consequently appropriable through a range of post-contractual opportunistic behaviors.

A systematic consideration of these behaviors and the range of options available to contracting parties to ameliorate their deleterious effects became a powerful motivation for the property-rights approach to the firm. This was chiefly because it made the explicit consideration of a key problem necessary: If contracts can only be specified incompletely, so that the actors involved do not fully internalize the full value of their association (and, thus, have reason to engage in

opportunistic behavior) who then should have residual control over the productive assets of a firm?

The answer, as per the Grossman-Hart-Moore (or GHM) model, was that the optimal boundaries of the firm are dependent on this consideration and the actor who provides the most crucial investment should, therefore, be the owner; the mere act of transferring ownership, in effect, increases the incentives to make more optimal investments.[ii] This mutable alteration of asset ownership is an idea that we shall return to again in this article, and it is in part why we examine the idea of identity itself as an asset, especially in the context of cryptoeconomics.

It is important to underscore the significance of this topic. Apart from the firm or the market, no third alternative form of organization has ever truly been on the radar.

This rarity is understandable when one considers the fact that, for some such third form of organization to exist, it would need to have the ability to permit ownership to be dynamically transferred between entities, based on the logic of the GHM model. The cost of such adjustment would need to be less than the costs of market-based transactions, while also being based on incomplete information that was completed symmetrically for all actors involved over time. In other words, the ex post renegotiation of contractual relationships would not be based on asymmetric information, but only on the revelation of a truer state of the world; the force of logic in the GHM view of the world would alone suffice to then motivate the evolution of the organizational form.

Moreover, such an organizational model would need to be self-organized, much like a market, otherwise it would hold little appeal over a market. However, this self-organization would need be of a specific nature, proscribed within parameters over information that can be well-defined, but not simply based upon market prices for which market transactions would trivially suffice. It would need to be information that is both relevant to a transaction ex ante and amenable to being used for its verification ex post. And it would be the sort of information where the role of market prices is only indirectly instantiated into its mechanism.

These are insurmountable odds to say the least. Yet, Goorha [5] suggests that blockchains do provide such a form of organization: blockchains are a crypto- graphic stigmergy; the name emphasizes the fact that a blockchain creates features of a contained environment from which a set of actors take their cues in order to self-organize. Structure itself inspires self-organization. In this paper, we wish to examine some features of the cryptographic stigmergy more carefully, partly by contrasting features of the blockchain technology with its most preeminent application in Bitcoin. In the next section, we begin by developing the argument that the role of the blockchain technology is not merely as an immutable ledger technology, but as a mutable template for mechanism design. We then consider the Bitcoin network as an exemplar to illustrate how the blockchain can be leveraged to generate a specific kind of economic value for its participants; in order to make this clear we develop the simple intuition of a Crypto-Ricardian rent. Finally, we introduce a version of the well-known Coase theorem for the case of blockchains to serve as guide for how we can expect interactions between the cryptoeconomy and the traditional economy; and, to underscore the relevance of identity in such an assessment, we introduce the idea of identity as an elastic asset.[iii]

2. Immutable Ledger, Mutable Design

A plethora of claims are made on behalf of blockchains.[iv] Those who subscribe to the most emphatic version of its potential are certain that its application will impact the course of humanity and change societies *en masse*. If one can attribute centuries of growth and development to the potent combination of markets and firms operating in free-market economies, then surely the addition of an organizational form that promises to unleash gains in efficiency should enable improvements that span all aspect of societies.

The crux of the optimistic argument rests on suggesting that there is unprecedented value inherent in an openly available ledger that faithfully and immutably records transactions in a system. Ledgers have always existed in societies; indeed, they are quite logically necessary to any system premised on transactions. After all, the TC model's thrust is that the existence of transactions costs is fundamental to assessing the distributional efficiency of property rights in a society, just as it is pivotal to assessing a firm's boundaries; ledgers and contracts are, therefore, useful tools in this regard. Yet, if the function of a blockchain is not much more than providing a new ledger technology with improved reliability or enabling smart contracts, then its impact is delimited to marginal improvements over a subset of existing applications.

Specifically, it is delimited by the net gains in the costs of maintaining a more reliable ledger than extant variants. Two factors impact this assessment. First, the blockchain is built upon sequentially, through a distributed system-wide consensus mechanism that incentivizes the validation of blocks of transactions before they can become part of the history of the ledger. Consensus algorithms can principally be seen as relying on proof of work, proof of stake, or some variation or combination thereof.[v] The selection across such algorithms is a choice between the relative costs of using the blockchain as a ledger versus the relative benefits of immutability they enable. Second, the blockchain ledger dispenses the need for third-party verification, which, of course, has been the raison d'être for centralizing trust within a multitude of institutional orderings (from the earliest tribal hierarchies to the sprawling modern bureaucracies) that collectively curate ledgers.

There are at least three problems with this view of blockchains seen principally as 'super-ledgers'.

1. *Blockchains inherently do not make 'truth' more likely.* Blockchains preserve and perpetuate a state-based information set blindly and without reference to whether some aspects of the information in here in some larger set of social or economic facts that are true or not. The chief application of blockchains at present, in smart contracts, makes the point vivid, since they can only be instantiated for computationally-specifiable transactions. The vast majority of contracts in practice are not computationally-specifiable, and even if they were, contract theory has given us some good reasons for why it may be desirable to leave a host of contracts deliberately incomplete in practice. ([18]).
2. *Blockchains are not universally 'public'.* Blockchains are quite trivially not public when they can be implemented as a permissioned private blockchain for a select group of entities, serving as a shared ledger that may, potentially, reduce the need for reliance on third-party verification for some aspects of a contract. More broadly, though, to say that making any distributed ledger 'public' automatically also provides a set of participants the incentives to care is an egregious misunderstanding of the functioning of markets. Any misalignment of individual incentives with transactions costs for verification logically presages the emergence of third- party verifiers of some other kind than the one being avoided at the outset. The Coase theorem's message in this context resonates quite powerfully: disintermediation in the limit requires an absence of transactions costs; intermediation on the blockchain is to some degree both rational and has thus far been inevitable, even if it were possible to use some consensus algorithm that does away with asymmetric computational power across a network's participants.
3. *Blockchains are not synonymous with immutability.* Immutability is a feature that depends on the protocols for verification selected. A poor verification protocol will not magically make a blockchain immutable merely because it is a blockchain, after all. So, the qualities of the decentralized and distributed ledgers are only ever as good as the attributes of the blockchains they are based upon.[vi]

The point we wish to make is that the promise of the blockchain technology is made much clearer by looking at it as a set of tools for the range of applications that can be addressed with the principles of *mechanism design*.

Long before the blockchain existed in our collective conscience, the field of mechanism design in economics had already emerged as an approach for problems that took dispersed information as sacrosanct. Before we were exploring blockchain applications to voting, trade, regulation, finance, monetary policy, land property rights, and so forth, the application of mechanism design in these areas had already been examined to a degree that justified a Nobel prize in economics.[vii]

The observation that Hayek [8] made on information being distributed – embodied within the most decentralized actors – in a society, gave him an unimpeachable basis for the unique role of the market as a fundamental coordinating mechanism. It was, of course, inspired by his belief that such calculations were beyond the reasonable realm of possibility for any centralized agency to deliberately engineer. Mechanism design begins with the premise that the economic system for a given objective is unknown or inaccessible and must be designed in a manner that it improves upon the status quo, which almost never abides by the assumptions that permit the idealized efficiency of the free market. In other words, it broadly simulates a market process and assumes that actors with private information on a range of preferences and parameters are capable of carrying out calculations. Its very basis is to devise a computational process that does away with, to the degree possible, the imperative for information and any computation to be exchanged across actors horizontally or vertically. [9]

Mechanisms are built to implement a Bayesian game structure over a set of n actors and specifically for a set of X outcomes.[viii] The actors are characterized idiosyncratically by their distributed and private information, θ_i, which defines the overall type space, Θ. All actors know the probability distribution of the types, but the exact type of an actor is private information. Since a given actor's utility is $u_i(x, \theta_i)$, the ex post efficiency of a given collective outcome, $f(\theta_1, ..., \theta_n) \in X$, ought to be sensitive to the distribution of types across all actors.[ix]

Situations can easily be imagined where one or more actors have the incentive to strategically lie about their true type, regardless of whether the outcome is a private or a public good. This problem of information revelation constrains what outcomes can feasibly be achieved. Being able to somehow leverage the private information of actors in order to achieve ex post desirable outcomes is a key motivation for implementation theory; the rules of the game that help implement an ex post efficient social choice function defines a mechanism. In other words, rather than directly asking an agent to reveal the nature of their private information, the agent's participation in the mechanism indirectly serves to assist a collective choice that is ex post efficient. A mechanism is denoted by $\Gamma = (S_1, ..., S_n, g(\cdot))$ since it is designed to allow the participants access to permissible strategies, S_i, and a rule, $g(\cdot)$, that converts these strategies into a collective outcome.

As a field, mechanism design has always assumed that individuals have incentives to conceal private information, therefore, its chief concern has been with finding mechanisms that can implement the designer's broad objective for the game by motivating the actors to undertake optimal actions. When this is done the mechanism is effective; it satisfies the objective of being optimal and 'trustless'.

It is easy to see that, through its design features, a blockchain can feasibly operate as a template for a mechanism.[x] when instantiated effectively, a blockchain does define, largely inviolably, an allowable action space for each of its participants, S_i, and a mapping, g, from the actions to an outcome, or a distribution over outcomes. This it does in such a manner that the equilibrium outcome is implemented by the allowable actions in the blockchain eliciting the information over the blockchain participants' private information necessary for

achieving ex post efficiency.[xi] Each block of transactions in the chain can be seen as representing a snapshot over this dynamic game. When there are several equilibrium outcomes, the objective of the blockchain's initial designers naturally takes precedence, which makes it all the more important for this objective to be clearly and unambiguously stated for the participants.

Seen as implementable mechanisms, blockchains represent powerful design templates for collective choices. They also force into discussion, coequally in importance with their technological details, a few key elements, including:

1. The desirability of a collective choice to participants in a mechanism (Will participants care enough? Is the participation constraint satisfied?);
2. The relevance of individual types to the objective (Is truthful revelation of relevant private information crucial to achieving the objective?);
3. The specifiability of the permissible rules for participation in the mechanism, including mandatory inclusion (Can a set of feasible rules that enable the outcome be ethically, legally and practically articulated for the participants in the mechanism?);
4. The relative cost of implementing the mechanism over using a market-based scheme or explicit planning (Is it worth implementing a blockchain?).

Across an economy several competing blockchain applications can be imagined. Two observations on the effects are worth making. First, the ability for blockchains to operate as co-dependent mechanisms – working in concert with one another seamlessly, with fully interoperable protocols – is key in order for blockchain technology to emerge as a viable meta-mechanism. Such interoperable blockchains are enabled to iteratively develop more efficient economy-wide outcomes based on the articulation of different aspects of distributed information inherent with the privately known types of individuals relevant for any given mechanism. This variegated definition for private information, as we shall see below, is a key component of identity seen as an elastic asset.

Second, a key problem with private 'permissioned' blockchains and public blockchains that require broad voluntary participation for the mechanism to be viable is the participation constraint; in cases where blockchains do not meet the participation constraint for a critical set of actors for any period in their development, theory tells us that the mechanism will fail, or participation will need to become mandatory.

3. Crypto-Ricardian Rent and Identity

The analogy with mechanism design makes a forceful case for blockchains as design templates for implementable mechanisms that delineate an action space defined by a pool of participants. They also make disaggregated atomized identities an essential feature of the rules of the game, so that, as participation increases, the size of this space necessarily increases.

We now adumbrate the purpose of blockchain technology as a mutable design template for implementation, as best illustrated at present by Bitcoin. This connection is especially plain to see when we consider a straightforward application of the idea of a Ricardian rent to the 'cryptoeconomy', or the economic markets that are enabled by a payment system that is dissociated from third-party inter- mediation.

Much has been written in the financial media over about the speculative nature of the price of bitcoin. While a number of factors are germane to the assessment of its volatile price dynamics, what matters in our more limited context here is the 21 million maximum limit for the number of bitcoins that is specified in the system's design. This hard limit is an interesting feature since it provides participants to the mechanism access to a Ricardian rent. The mining and purchase of bitcoins can then be seen as the acquisition of essential infrastructure for an incipient economy associated directly with the Bitcoin mechanism.

Stated differently:

As the size of a cryptoeconomy associated with a particular blockchain mechanism grows, the Ricardian rent available to participants proportionately increases. We can see this as the blockchain mechanism's crypto-Ricardian rent.

There are a few moving parts to this observation that are worth some thought.

First, the idea of the *atomization of identity* requires some clarification. A blockchain strings together transactions that are immutably linked with identity without reference to third-parties, and so it behooves us to define and review the merits of atomizing identity.

Second, the point of examining Bitcoin as an exceptional cryptocurrency is not merely that it is the blockchain's first, longest enduring and most well-known application. It is that the blockchain-based design for Bitcoin was adopted by Satoshi Nakamoto, *in spite* of its inherent inefficiency. The blockchain provided an algorithmic solution to the Byzantine Generals' Problem – essentially the problem of consensus over a distributed system – by using the proof of work consensus protocol, and thereby permitted decentralization for an internet-based payment system; it achieved this, however, by raising the costs astronomically for the attendant moral hazard problem and, as a consequence, reducing the throughput of the system overall. Some of the most ardent debates among the developers of Bitcoin's open source software to this day revolve around the issue of ameliorating the throttling effects of this initial handicap, while preserving the function it served. Among these resolutions we find insight on what the cryptoeconomy might actually look like, should it come to pass and as it is imagined by its proponents.

3.1 Atomization of Identity

The roots of several accomplishments in society are enabled by the ability of an individual to project her identity across a myriad spheres of life—economic, political, legal and social, usually simultaneously—and, thus, be able to benefit from the value that obtains from production through collaboration. This mapping between an individual and the social groups she participates is enabled by the instruments at the disposal of a planner. Traditionally, states have made use of institutions to formally and deliberately 'ascribe' an identity to an individual, so that a mapping is created or severed between individual and ownership.

This function of states has been underemphasized in the literature. Economists, for decades, have concentrated on the principal role of the state as that of protecting ownership; in practice, markets have worked, for centuries, on the basis of contracts that rehash individual identities, frequently by fiat, into teams that generate economic value, which is then distributed according to rules seldom seen in any economics textbook.[xii] Similarly, political scientists, for decades, have concentrated on examining the effects of electoral rules on effective enfranchisement; the practice of government, for centuries, has concentrated on mechanisms that monopolize the processes for defining the individuals that 'matter'.[xiii]

The blockchain mechanism as it is reified within the Bitcoin architecture appealed to its earliest adopters along these grounds; its raison d'être was grounded in enabling societies to adopt a financial system built without the need to rely on trusted third parties to intermediate. The removal of such dependence on third parties purportedly has the effect of 'atomizing' institutionally sanctioned identities; it disaggregates collectively defined identities within institutional rules and, at one fell swoop, moves towards a system that advantages atomistically defined identity, where the individual has more control over which elements that comprise and individual's private information is relevant to a P2P payment transaction.[xiv]

The value of the atomization of identity *away* from institutions is derived from a commensurate realignment of individual incentives with the local information and the distributed knowledge that they represent. As such, the ex-ante incentive for truth-telling on private information in a mechanism design setting is increased.

The Bitcoin blockchain showcased a method for tapping into the value inherent in local and contextual information; admittedly the impetus for doing so was at least equally inspired by the global financial crisis and a growing disenchantment with some of the principles that have informed policy-making based upon aggregates.[xv] This then became a key reason for why 'decentralization on the blockchain' became the poster-child, catch-all concept; the blockchain technology provides a mechanism for arrogating self-identity away from all the repositories of hierarchical organization, where it relies on the power of the state for its safekeeping. Yet when we see blockchains as templates for mechanisms it becomes clearer that their use is not necessarily panacea in all circumstances. The true value of self-identity is only 'unlocked', as it were, when it can be projected and diminished based upon individual needs.

3.2 Redefining Identity

Besides the Hayekian distinction on the value of *contextual* information in contrast to *collective* information, the other source of conviction on using blockchains as mechanisms for the atomization of identity comes from suspecting any institutional curation of individual identity.

Mises [13], for example, made a useful distinction between *classes* and *castes* in societies, convincingly pointing out that the former comprise fluid groupings of individuals who are free to associate across classes of asset ownership while the latter are reified in rigid institutional borders and serve to delimit mobility across them. Classes of asset ownership are, thus, conducive to redefining identity based on individual liberties, but castes are not.

We realize, intuitively, that state power is derived from the collective databases of identities that undergird their legitimacy. Sovereignty over oneself is, therefore, instantiated at those levels.[xvi] We are forced to concede—indeed, we seldom reflect on this—that the very processes of life, liberty and the pursuit of happiness (or the pursuit of *property*, if you prefer Locke's original) are all co-mingled within the identities that come into existence by state mandate. And, so long as an individual maintains any desire of realizing socially sanctioned objectives, there they must remain.

A key appeal of blockchain mechanisms such as Bitcoin has been to favour finance based on cryptographic proof rather than on implicit trust in a state's formal institutional matrix. The more general appeal of a blockchain-based implementable mechanism can be stated as challenging the assumption, taken for granted in much of economics, that the ultimate outside option to a contractual relationship – the external reference point guiding the behaviour of the parties to a transaction – must necessarily be a state regulator.

The blockchain 'revolution' is pivotally in denying the hitherto axiomatic premise that willingly relinquishing control over features of a range of social and market transactions to an intermediary—which is to say, centralization—is the only re-course to building a degree of trust within them.

At least two objections can be made to this vision for using blockchains as mechanisms to reclaim sovereignty of individual identity.

First, the blockchain is patently not suitable for a whole host of applications that may nonetheless meet an individual's participation constraint. This is clearest when one sees the blockchain as a template for mechanism design. When one considers the list of reasons why a blockchain may not be

preferable to a centralized database, the shine does seem to wear off a little. Besides a fairly restrictive set of qualifying features for the class of transactions that warrant the instantiation of a blockchain [xvii], even its strengths—immutability, security, decentralized consensus, privacy— tend to be taken as practical realities, rather than as compromised theoretical ideals across a range of applications. Second, in the particular case of Bitcoin, it bears noting that it competes alongside a burgeoning number of other cryptocurrencies and tokens. Why then should Bitcoin deserve special attention? And if that is true, in what sense can identity be said to have been 'reclaimed' across an expanding set of blockchain applications.

We have already presaged the answer: To generate a crypto-Ricardian rent, the blockchain's role as an immutable ledger requires that its implementation has features that, generally and minimally, first satisfy the participation constraint. When they do not, the implementation of blockchain technology is only likely to yield short-term inframarginal rent relative to any extant contractual arrangement that it seeks to replace.

Bitcoin's role as a mutable design implementation of the blockchain, for example, only becomes apparent once its blockchain infrastructure enables the development of a cryptoeconomy representing fundamental changes across an expanding set of contractual arrangements; to be deemed 'exceptional' it would first need to pass that litmus test for its potential. Bitcoin merely as a superior form of money – the refrain among its proponents is often that it is the only 'sound money' – to all sovereign currencies does not seem to be a reasonable qualification from this perspective.

5. The Shape of a Cryptoeconomy

To address the objections raised in the previous section, it is worthwhile considering some basic principles of network structure that help us imagine the 'shape' of a cryptoeconomy.

If we were to imagine the most ideal shape for the Bitcoin network, for example, we would imagine a complete graph, as shown in *Figure 1*. Everyone would be represented as a single vertex or node on this graph and each would be connected to everyone else on the network directly. There would, in other words, be complete decentralization of all participants in the blockchain mechanism implemented by Bitcoin.

As the number of nodes grew, the number of feasible transactions would be some function of $n(n\text{-}1)/2$. The enormity of this number is less impressive than the fact that if the path length between two nodes on the network can be seen as a proxy for the transactions cost incurred then this configuration represents the lowest possible transactions cost.

Note that the identities of each of the nodes remains entirely intact in such a setup, and there is no local information specific to a transaction that must be 'lost' by virtue of having to restructure the contextual information into a smaller space of relevant information deemed sufficient by an intermediary for

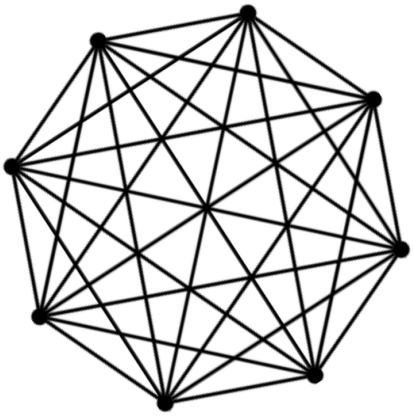

Figure 1: The Complete Graph as an Ideal for the Network of a Blockchain Mechanism

the transaction to take place.

The fact that an impossibly complex space of information that describes the infinite states of the network can, in fact, be equally verifiable by any node has remarkable implications for any implementable mechanism; such verifiability makes the behavior of participants subject to more direct observation than is feasible in most firm or market-based systems. The point is not whether a node on such a network would actually do this, but that the possibility to do so can make every node equally well-informed; information asymmetry can, in theory, no longer be the basis for inequalities upon which hierarchies of control can be erected.

A simple way to visualize the blockchain analog for the complete graph for Bitcoin's ideal-form network is by imagining a Hamiltonian path across this graph such that each node on the graph is passed exactly once. Now, when a transaction takes place between any two nodes, the information and identity data associated with the transaction need only be a minimal set that ensures it belongs to the Hamiltonian path of that graph.

In practice, this is emphatically not how a blockchain works, but this imagery is a very useful one to have nonetheless, because it tells us that decentralized participation at the level of an individual entity can form the basis for a verification mechanism. Similarly, in practice Bitcoin is not a complete graph. However, the paradox is that true atomization of identity – complete self-sovereignty – requires the mechanism meeting the participation constraint. Connection itself must be voluntary, as well as variegated; engagement across a network should be guided by the invisible hand of needs and wants.

The process of atomization of identity towards local information comprises re- gaining possession, in deliberate graduated steps, of one's identity, across a variety of spheres of life. The fact that Bitcoin commenced with financial infrastructure is critical, since financial identity pervades a vast majority of those aspects of life where we rely on alternate

mechanisms for organization—the market, the firm, the state, etc. It is this financial identity that the Bitcoin network potentially provides that can enable the creation of a foundational complete network.

Bitcoin stands as an illustrative example for the crypto-Ricardian rent that an associated cryptoeconomy can enable: the more comprehensively its underlying network infrastructure is built, the more its relevance fades in comparison to the network structure of transactions that are enabled by individual nodes providing services over the essential infrastructure.

The infrastructure of the blockchain mechanism is proxied by a complete graph, whereas the flows of crypto-Ricardian rent between participants using this foundation are represented on a scale-free network.

Yet, there is also reason for caution in assuming this to be correct shape of a cryptoeconomy.

First, the infrastructure is far from complete. The fact that adoption is still relatively marginal by global standards should give anyone pause in claiming that a 'complete network' is inevitable. Second, the process by which the Bitcoin network can accommodate variegated scaling based on the needs and desires of the holders of bitcoin is only in its infancy.

While by no means the only solution to accommodating transactions at scale, the Lightning Network is possibly the leading and most advanced candidate. It works by essentially permitting a small subset of nodes to conduct a multitude of transactions off the base or settlement layer of the Bitcoin network by opening temporary channels. This enables a much lower transactions cost and enables a broader definition of asset ownership, the import of which we shall examine below. These transactions remain entirely tractable, so that they can eventually all be settled in accordance with a verified state of the Bitcoin blockchain, thereby increasing the overall network's throughput.

Interestingly, we can readily imagine the Lightning network as a scale-free network being built atop the Bitcoin complete network. *Figure 2* provides a 3-D visualization of the Lightning Network as of September, 2018.

5. A Crypto-Coase Theorem for Identity on the Blockchain

Identity is an essential—possibly *the* quintessential—property right only when it comprises both a right to use as well as a right to *exclude*.

A mechanism that tractably maps information generated by an individual back to the individual immutably through time, without reference to a third party, pro- vides that individual with a verifiable right to exclude; a mechanism that enables an individual to provide access to her identity to others in the mutable creation of collaborative value, yet tractably retains her

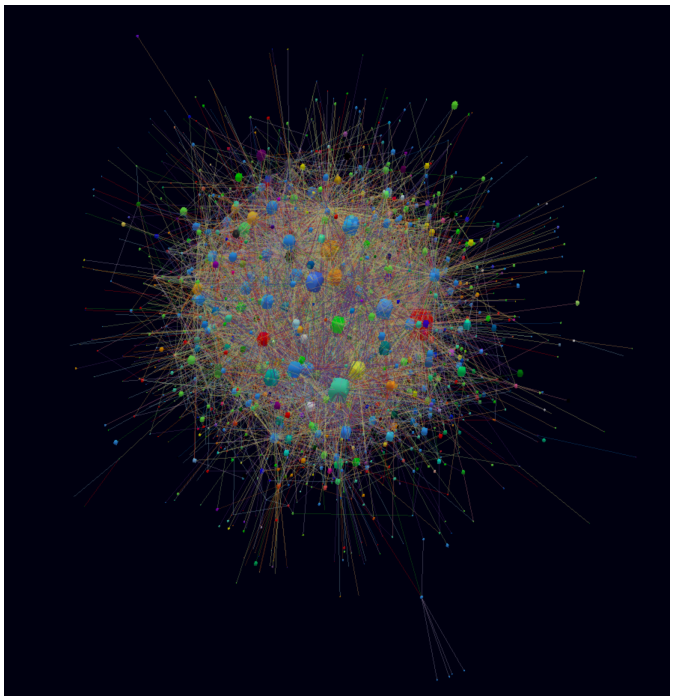

Figure 2: Scale-Free Network: A Visualization of the Lightning Network Cryptoeconomy Courtesy: lnd3.vanilla.co.za

attributable product from the association, provides her the right to use.

The right to exclude is a key strength of the blockchain; the right to use, however, requires using the blockchain as an infrastructure to access a range of value-creating activities across the cryptoeconomy. As discussed above, the Lightning Network atop the Bitcoin blockchain is a promising step in that direction, though it is yet in its infancy, and other developments may prove more rewarding. The key, however, is that a genuinely useful blockchain application would need to provide control over both rights – to use and exclude – to an individual, so that the benefits of disintermediation and decentralization that accompany moving economic activity from the traditional economy to the cryptoeconomy can accrue to the participants.

When such a mechanism becomes a reality, and identity coincides more precisely and tractably with information, we do have some guidance on what to expect. The Coase theorem suggests that the optimal distribution of property rights only occurs in an environment with vanishingly small transactions costs. However, as the definition of what constitutes property itself is atomized to include information that belongs to an individual, such 'small' transactions costs become increasingly significant. Some degree of intermediation then becomes necessary; to the extent that a complete graph ideal represents higher transactions costs than a scale-free network, the network should become more scale-free. Individuals self- organize into such networks; this stigmergic self-organization becomes a powerful alternative to organization by markets and planners.

The **crypto-Coase theorem** suggests:

In an environment of higher frictional costs imposed by market orderings on the one hand (on the basis on un- known prices of contextual information that motivates the formation of firms) and planning on the other (on the basis of the aggregation of contextual information to empower institutions), economic activity moves towards the cryptographic stigmergy, where contextual information and identity are most closely matched in a verifiable manner.

The practical import of the Coase theorem—ironically, entirely missed by most —is that the initial distribution of assets *will* almost always matter, since, in an environment of only partially tradable externalities, we will need to routinely contend with a range of significant transactions costs: compelling examples include costs that accrue on the basis of the Shirky Principle, institutional stickiness, and regulatory capture.

It is easy to see that these sources of frictional costs would, fundamentally, affect not only economic growth at the scale of economies, but remain relevant to decisions at the level of markets that operate within any given system of property rights that drives a wedge between self-identity and contextual information.

5.1 Asset Elasticity

A critical reason why the issue of the scalability of the Bitcoin network has been a matter of such critical concern can be seen as belonging to a particular class of problems in economics. These are problems that concern themselves with examining any institutional re-ordering within an economy on the basis of its ability to reduce the types of frictional costs that prevent the achievement of an efficient redistribution of property rights over any expanding set of assets.

The import of this point becomes most clear when we consider the geometric form of a collaborative enterprise on the very simple basis of three distinct kinds of information. *Known knowns* can satisfactorily be reflected in current prices or can, in an appropriately devised contractual relationship, be made to cohere within prices. The shape of the enterprise dealing only with known knowns can be imagined as essentially a simple polygon, since its area (scope of work) and perimeters (extent of activity) are all well-defined. In such a situation, self-identity remains recoverable in a straightforward manner because it retains a direct correspondence to the enterprise's output.

Known unknowns cause uncertainty of a very interesting nature. So long as the contractual relationship between parties that only ever need concern themselves with known knowns is largely similar to the relationship that can, by and large, prescribe specific actions for a contract that is affected by known unknowns, the difference between these two types of information becomes largely irrelevant. In other words, precise actions stand in as strong proxies for precise prices. Yet again, self-identity remains recoverable.

However, when parties to a contract know that there are likely to arise eventualities in the future that will impact their payoffs, but they cannot fathom ex ante what actions they might prescribe specifically when and if any of them were to eventuate, then they need to rely on some external reference to guide behaviour.

The geometric form of a firm in such a case becomes more like an irregular polygon, in that its scope or extent might alter, though perhaps not in entirely unpredictable ways. Self-identity now *does* require some crutch—some external frame of reference or third-party—to be recovered, once the activities of the enterprise alters it from its initial form; whether this recovery will be completely satisfactory depends on the strength and validity of that crutch.

Finally, the set of *unknown unknowns* represents information that cannot systematically be used to guide the behaviour of contracting entities; more accurately, such information cannot really even be the basis of any meaningful 'contract' to begin with.[xviii]

Such information is exploratory in nature; its incidence is unknown, and so its value is unknown as well. Yet, this is precisely the sort of information that is embodied within any enterprise that begins with self-identity and local information as its inherent building blocks. The geometric form of such an enterprise is best imagined as a smudge or a cloud, with essentially no defined perimeters and with only an approximate area that indicates its scope. Firms and identifiable markets may not eventuate from this information, but innovation and creativity routinely do emerge from such collaborative enterprises. Self-identity can lose almost all meaning in such ventures; it evolves within it so fundamentally, that it becomes harder to extricate a definable identity from it that coheres exactly with what went into it at the outset.

What is needed for self-identity to have a more meaningful connotation for the cryptoeconomy is a range for its elements – crisp elements at one extreme, such as a person's name, passport number, contact details, and so forth, and fuzzy elements at the other, such as her interests, ambitions, hobbies or ideals. The ability to immutably instantiate crisp identities within any blockchain is straightforward; however, an individual would also have the ability to redefine her identity based on the information that she accumulates through participation in other applications of the technology, such as within commercial enterprises that employ the Lightning Network or a public ledger on patents, academic credentials or real estate. These enhancements to identity would occur so that, when information is shared through participation, identities would grow in an elastic manner to account for the contributions it makes to the self-identities of others in a society. This makes identity an elastic asset, rather than a plastic one.

Seeing self-identity as an elastic asset is best done when we imagine it as a particular package of contractual rights a person possesses over her productive ideas. Such rights can be specific to the individual as well as residual over the set of all specifiable and unspecifiable ideas that individuals collaborate with in an

enterprise. Where the residual rights over any given expansion of the set of ideas permits more productive use than when farmed out to other individuals, the self- identity of an individual grows. This is a fundamental insight of the incomplete contract literature. Fundamentally, what this suggests for blockchains is that until they are not interoperable across a wide set of applications, the benefit of self-identity on the blockchain is limited to not much more than digital safekeeping of its crispest elements. Similarly, Bitcoin's true value would be in realizing a world where such self-identity is added to the store of value use case on its base layer, while permitting complex interactions on its scalability solutions.

6. Concluding Remarks

Blockchains as a technology are yet in their infancy, and the trajectory of their influence is far from decided. It may well turn out that, in the years to come, we may look back and shake our heads disapprovingly at the audacity that anyone would have conceived that blockchains could actually represent a third form of organization of economic activity, sufficiently distinct from the either the market or planning.

However, at present there seems to be sufficient reason for optimism, and in this article we have attempted to spell out the economic foundations for this enthusiasm. Principally, two aspects seem to be have crucial relevance.

First, we have argued that blockchains can be seen, from the perspective of mechanism design theory, as a class of implementable mechanisms. This is an exciting way to look at blockchains because it permits us to use the language of complete contracts for them. They can be seen as mutable design templates for creating simulated markets that instantiate organic environments to inspire specific collective objectives. There are several practical limitations to this idea, and we have attempted to enumerate some of the more pressing issues in this paper.

Second, much of this paper concerns itself with the role of blockchains in enabling the property rights inherent in the concept of self-identity. This emphasis is deliberate, since we have argued that the fullest impact of blockchains is genuinely unleashed when an individual's participation constraint in a cryptoeconomy is materially different from those she faces in either a market supported by third- party intermediation or directly in state-sanctioned institutions. Specifically, when blockchains provide tractable ownership over her self-identity without appealing to an intermediary, it enables a participant to stake claims to the Ricardian rent that a blockchain mechanism enables for her in its associated cryptoeconomy. We attempted to highlight the fact that self-identity is hardly a fixed idea. Indeed, a significant challenge to the future of economies characterized by a system of blockchains is in designing methods that permit the elastic growth of self-identity to ensure that the blockchain implementations are integrated from the perspective of the individual's participant constraint as well as being seamlessly interoperable.

References

[1] O. Blanchard, "Should We Reject the Natural Rate Hypothesis?," *Journal of Economic Perspectives*, vol. 31, no. 1, pp. 97-120, 2018.

[2] R. Coase, "The Nature of the Firm." *Economica*, vol. 4, no. 16, pp. 386-405, 1937.

[3] R. Coase, "The Federal Communications Commission." *Journal of Law and Economics*, vol. 2, pp. 1-40, 1959.

[4] R. Coase, "The Problem of Social Cost," *Journal of Law and Economics*, vol. 3, no. 1, pp. 1-44, 1960.

[5] P. Goorha, "The Return of 'The Nature of the Firm': The Role of the Blockchain" *Journal of the British Blockchain Association*, vol. 1, no. 1, [Online]. Available: https://jbba.scholasticahq.com/article/3448-the-return-of-the-nature-of-the-firm-the-role-of-the-blockchain, 2018.

[6] S.J. Grossman. and O.D. Hart., "The costs and benefits of ownership: A theory of vertical and lateral integration," *Journal of Political Economy*, vol. 94, no. 4. pp. 691-719, 1986.

[7] O.D. Hart and J. Moore, "Property Rights and the Nature of the Firm," *Journal of Political Economy*, vol. 98, no. 6, pp. 1119-1158, 1990.

[8] F. Hayek, "The Use of Knowledge in Society," *American Economic Review*, vol. 35, no. 4, pp. 519-530, 1945.

[9] L. Hurwicz, "On the Concept and Possibility of Informational Decentralization," *American Economic Review*, vol. 59, no. 2, pp. 513-524, 1969.

[10] B. Klein, R. Crawford, and A. Alchian, "Vertical Integration, Appropriable Rents, and the Competitive Contracting Process", *Journal of Law & Economics,* vol. 21, no. 2, pp.297-326, 1978.

[11] A. Mas-Colell, M.D. Whinston and J.R. Green, *Microeconomic Theory*, Oxford University Press, 1995.

[12] E. Maskin and J. Tirole "Unforeseen Contingencies and Incomplete Contracts," *Review of Economic Studies*, vol. 66, no. 1, pp. 84- 114, 1999.

[13] L. von Mises, *Socialism: An Economic and Sociological Analysis*, Jonathan Cape, 1951.

[14] D. Mookherjee, "The 2007 Nobel Memorial Prize in Mechanism Design Theory," *Scandinavian Journal of Economics*, vol. 110, no. 2, pp. 237-260, 2007.

[15] A. Narayanan and J. Clark, "Bitcoin's Academic Pedigree," *Communications of the ACM*, vol. 60, no. 12, pp. 36-45, 2017.

[16] S. Popov, "The Tangle," version 1.4.3, unpublished manuscript. 2018, Accessed on May 8, 2018. [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[17] O.E. Williamson, *The Economic Institutions of Capitalism*. Macmillan, 1985.

[18] O.D. Hart and J. Moore, "Contracts as Reference Points," *Quarterly Journal of Economics*, vol. 123, no. 1, pp. 1–48, 2008.

[i] Chiefly, [16] and [10].

[ii] [6] and [7].

[iii] For the uninitiated, the Coase theorem was principally stated in [4], but relied on his work on the FCC, published as [3]. The theorem does not rely on mathematical formulation, but simply on trenchant observation. The essence of the theorem is that, in a market system with well-defined property rights and low transactions costs, efficiency is invariant to the distribution of the property rights.

[iv] Apart from their obvious ubiquity among cryptocurrencies and crypto tokens, there are thou- sands of private blockchain applications around the world, and several hundred in government.

[v] As an aside, while much of the technology that such consensus protocols represent relies on prior contributions in the computer science and information theory literatures, its practical application is no mean feat of intellectual ambition and vision with repercussions for a very wide-variety of problems. See Narayanan and Clark [15].

[vi] Neither, for that matter, is the blockchain unique in this regard. The premise of a transactions cost incentivizing block formation on the blockchain ledger puts a floor on the minimum value for transaction. A DAG attempts to solve this problem by making transaction validation by a node on the network conditional on its own transaction approval. A DAG is the basis for the cryptocurrency IOTA. [16]

[vii] See [14] for a review.

[viii] A very useful overview of mechanism design can be found in [11].

[ix] This is captured as a feature of the social choice function for the game.

[x] For particular applications with government adoption, participation can even be seen as mandatory, though mostly it features voluntary participation.

[xi] Whether it does so indirectly or directly depends on whether revealing private information is a dominant strategy.

[xii] This might seem like an unfairly harsh criticism, since much of industrial organization and cooperative game theory has dealt with production in groups, and the conditions that define optimal contracts for eliciting efficient marginal contributions within such teams. The fact remains, however, that most real-world contracts are neither optimal nor are they complete.

[xiii] Whether members of one race are treated as only worth three-fifths as valuable as the members of another, or, indeed, whether one race is considered worthless altogether in comparison with another, are egregious examples of state-defined individual identity. Less virulent definitions determine economic and social inequalities everywhere across the globe, though doubtless the situation is more deplorable in repressive regimes than it is in more open societies.

[xiv] Naturally, this brings up the issue of anonymity and privacy. While those are essential and interesting aspects of identity, we are side-stepping them in this paper. There are convincing arguments that KYC and tax reporting regulations on exchanges and financial intermediaries, as well as technologies that help reverse-engineer internet addresses associated with transactions severely remove the appeal of bitcoin ownership merely for the sake of anonymity (for which other cryptocurrencies are better suited anyway) or for privacy for most consumers.

[xv] It should be noted here that this critical re-evaluation is not alien to academic investigation. Critiques of the Washington consensus, for instance, are not new. For a more recent example see the noteworthy evaluation of the Natural Rate hypothesis in Blanchard [1].

[xvi] The Global Passport Power Rank is one instructive illustration of the disparity that exists across definitions of citizenship.

[xvii] See, for example, this article published by the World Economic Forum as a generic guide on the practicability of blockchains

[xviii] Broadly, you have a contract when the person signing on to one has agreed to participate and that the conditions the contract provides incentivize her to exert costly efforts; these are known, respectively, as the participation and incentive constraints.