The Blockchain Economy: A beginner's guide to institutional cryptoeconomics

Cryptoeconomics Follow
Sep 26, 2017 · 14 min read

Chris Berg, Sinclair Davidson and Jason Potts are from the RMIT Blockchain Innovation Hub, the world's first social science research centre into the economics, politics, sociology, and law of blockchain technology.

. . .

The blockchain is a digital, decentralised, distributed **ledger**.

Most explanations for the importance of the blockchain start with Bitcoin and the history of money. But money is just the first use case of the blockchain. And it is unlikely to be the most important.

It might seem strange that a ledger—a dull and practical document associated mainly with accounting—would be described as a revolutionary technology. But the blockchain matters because ledgers matter.

Ledgers all the way down

Ledgers are everywhere. Ledgers do more than just record accounting transactions. A ledger consists simply of data structured by rules. Any time we need a **consensus** about **facts**, we use a ledger. Ledgers record the facts underpinning the modern economy.

Ledgers confirm ownership. Property title registers map who owns what and whether their land is subject to any caveats or encumbrances. Hernando de Soto has documented how the poor suffer when they own property that has not been confirmed in a ledger. The firm is a ledger, as a network of ownership, employment and production relationships with a single purpose. A club is a ledger, structuring who benefits and who does not.

Ledgers confirm identity. Businesses have identities recorded on government ledgers to track their existence and their status under tax law. The register of Births Deaths and Marriages records the existence of individuals at key moments, and uses that information to confirm identities when those individuals are interacting with the world.

Ledgers confirm status. Citizenship is a ledger, recording who has the rights and is subject to obligations due to national membership. The electoral roll is a ledger, allowing (and, in Australia, obliging) those who are on that roll a vote. Employment is a ledger, giving those employed a contractual claim on payment in return for work.

Ledgers confirm authority. Ledgers identify who can validly sit in parliament, who can access what bank account, who can work with children, who can enter restricted areas.

At their most fundamental level, ledgers map economic and social relationships.

Agreement about the facts and when they change—that is, a consensus about what is in the ledger, and a trust that the ledger is accurate—is one of the fundamental bases of market capitalism.

Ownership, possession, and ledgers

Let's make a distinction here that is crucial but easy to miss: between **ownership** and **possession**.

Take passports. Each country asserts the right to control who crosses its borders, and each country maintains a ledger of which of its citizens have the right to travel. A passport is a physical item—call it a **token**—that refers back to this ledger.

In the pre-digital world, possession indicated ownership of that right. The Australian passport ledger consisted of index cards held in by the government of each state. Border agents presented with a passport could surmise that the traveller who held it was listed on a distant ledger as allowed to travel. Of course this left border control highly exposed to fraud.

A Belgian passport held by the Australian National Archives, A435 1944/4/2579

Possession *implies* ownership, but possession is *not* ownership. Now modern passports allow the authorities to confirm ownership directly. Their digital features allow airlines and immigration authorities to query the national passport database and determine that a passenger is free to travel.

Passports are a relatively straightforward example of this distinction. But as Bitcoin has shown: **money is a ledger, too**.

Possession of a banknote token indicates ownership. In the nineteenth century the possessor—'bearer'—of a banknote had a right to draw on the issuing bank the value of the note. These banknotes were direct liabilities for the issuing bank, and were recorded on the banks' ledger. A regime of possession indicating ownership meant that banknotes were susceptible to be both stolen and forged.

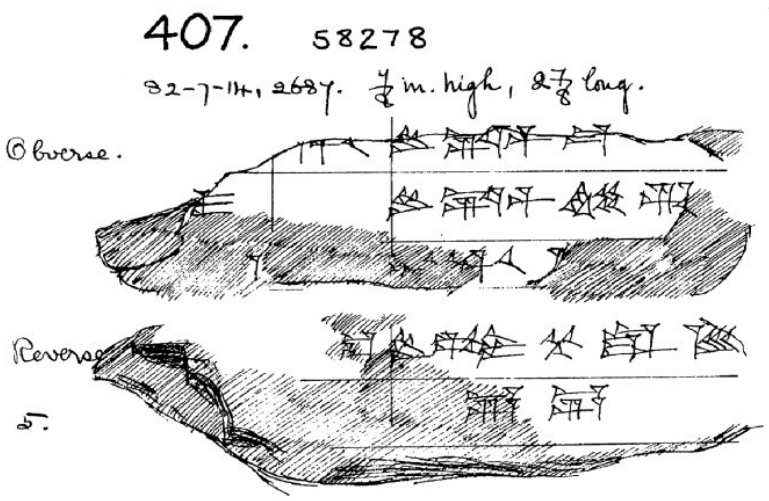
In our era fiat currencies a five dollar bill cannot be returned to the central bank for gold. But the relationship remains—the value of the bill is dependent on a social consensus about the stability of the currency and government that issued it. Banknotes are not wealth, as Zimbabweans and Yugoslavians and Weimar Republic Germans have unfortunately learned. A bill is a call on a relationship in a (now

synthetic) ledger and if that relationship collapses, so does the value of the bill.

The evolution of the ledger

For all its importance, ledger technology has been mostly unchanged … until now.

Ledgers appear at the dawn of written communication. **Ledgers and writing developed simultaneously** in the Ancient Near East to record production, trade, and debt. Clay tablets baked with cuneiform script detailed units of rations, taxes, workers and so forth. The first international 'community' was arranged through a structured network of alliances that functioned a lot like a distributed ledger.



A fragment of a late Babylonian cuneiform ledger, held by the British Museum, 58278

The first major change to ledgers appeared in the fourteenth century with the invention of **double entry bookkeeping**. By recording both debits and credits, double entry bookkeeping conserved data across multiple (distributed) ledgers, and allowed for the reconciliation of information between ledgers.

The nineteenth century saw the next advance in ledger technology with the rise of large corporate firms and large bureaucracies. These **centralised ledgers** enabled dramatic increases in organisational size and scope, but relied entirely on **trust** in the centralised institutions.

In the late twentieth century ledgers moved from analog to **digital ledgers**. For example, in the 1970s the Australian passport ledger was digitised and centralised. A database allows for more complex distribution, calculation, analysis and tracking. A database is computable and searchable.

But a database still relies on trust; a digitised ledger is only as reliable as the organisation that maintains it (and the individuals they employ). It is this problem that the blockchain solves. The blockchain is a distributed ledgers that does not rely on a trusted central authority to maintain and validate the ledger.

Blockchain and the economic institutions of capitalism

The economic structure of modern capitalism has evolved in order service these ledgers.

Oliver Williamson, the 2009 Nobel laureate in economics, argued that people produce and exchange in markets, firms, or governments depending on the relative **transactions costs** of each institution. Williamson's transactions cost approach provides a key to understanding what institutions manage ledgers and why.

Governments maintain ledgers of authority, privilege, responsibility and access. Governments are the trusted entity that keeps databases of citizenship and the right to travel, taxation obligations, social security entitlements, and property ownership. Where a ledger requires coercion in order to be enforced, the government is required.

Firms also maintain ledgers: proprietary ledgers of employment and responsibility, of the ownership and deployment of physical and human capital, of suppliers and customers, of intellectual property and corporate privilege. A firm is often described as a 'nexus of contracts'. But the value of the firm comes from the way that nexus is ordered and structured—the firm is in fact a ledger of contracts and capital.

Firms and governments can use blockchains to make their work more efficient and reliable. Multinational firms and networks of firms need to reconcile transactions on a global basis and blockchains can allow them to do so near-instantaneously. Governments can use the immutability of the blockchain to guarantee that property titles and identity records are accurate and untampered. Well-designed permissioning rules on blockchain applications can give citizens and consumers more control over their data.

But blockchains also compete against firms and governments. The blockchain is an institutional technology. It is a new way to maintain a ledger—that is, coordinate economic activity—distinct from firms and governments.

Before 2009				
	Hierarchy			
	Government	Firms	Market	
After 2009				
Government	Blockchain	Firms	Blockchain	Markets

The new economic institutions of capitalism

Blockchains can be used by firms, but they can also *replace* firms. A ledger of contracts and capital can now be decentralised and distributed in a way they could not before. Ledgers of identity, permission, privilege and entitlement can be maintained and enforced without the need for government backing.

Institutional cryptoeconomics

This is what institutional cryptoeconomics studies: the institutional consequences of cryptographically secure and trustless ledgers.

Classical and neoclassical economists understand the purpose of economics as studying the production and distribution of scarce resources, and the factors which underpinned that production and distribution.

Institutional economics understands the economy as made of rules. Rules (like laws, languages, property rights, regulations, social norms,

and ideologies) allow dispersed and opportunistic people to coordinate their activity together. Rules facilitate exchange—economic exchange but also social and political exchange as well.

What has come to be called cryptoeconomics focuses on the economic principles and theory underpinning the blockchain and alternative blockchain implementations. It looks at game theory and incentive design as they relate to blockchain mechanism design.

By contrast, ***institutional*** **cryptoeconomics looks at the institutional economics of the blockchain and cryptoeconomy.** Like its close cousin institutional economics, the economy is a system to coordinate exchange. But rather than looking at rules, institutional cryptoeconomics focuses on ledgers: data structured by rules.

Institutional cryptoeconomics is interested in the rules that govern ledgers, the social, political, and economic institutions that have developed to service those ledgers, and how the invention of the blockchain changes the patterns of ledgers throughout society.

The economic consequences of the blockchain

Institutional cryptoeconomics gives us the tools to understand what is happening in the blockchain revolution—and what we can't predict.

Blockchains are an experimental technology. Where the blockchain can be used is an entrepreneurial question. Some ledgers will move onto the blockchain. Some entrepreneurs will try to move ledgers onto the blockchain and fail. Not everything is a blockchain use case. We probably haven't yet seen the blockchain killer app yet. Nor can we predict what the combination of ledgers, cryptography, peer to peer networking will throw up in the future.

This process is going to be extremely disruptive. The global economy faces (what we expect will be) a lengthy period of uncertainty about how the facts that underpin it will be restructured, dismantled, and reorganised.

The best uses of the blockchain have to be 'discovered'. Then they have to be implemented in a real world political and economic system that

has deep, established institutions that already service ledgers. That second part will not be cost free.

Ledgers are so pervasive—and the possible applications of the blockchain so all-encompassing—that some of the most fundamental principles governing our society are up for grabs.

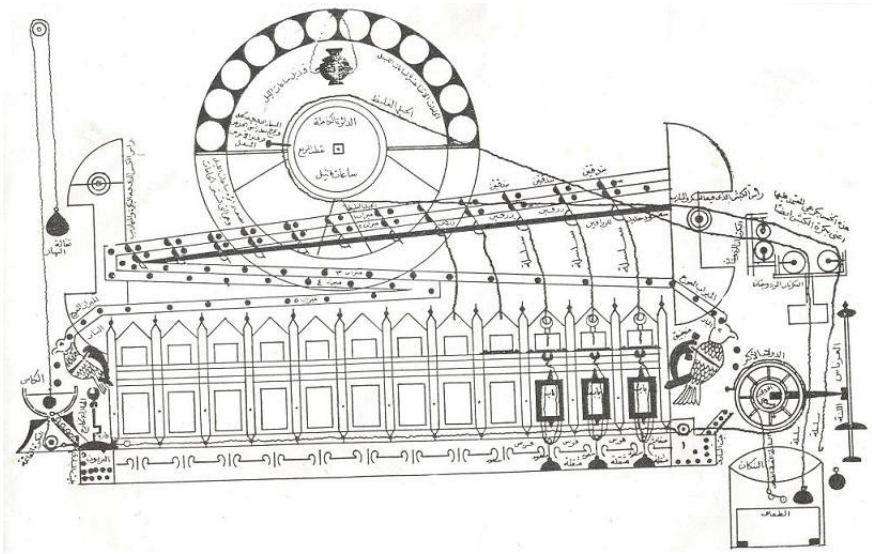
Institutional creative destruction

We've been through revolutions like this before.

It is common to compare the invention of Bitcoin and the blockchain with the internet. The blockchain is Internet 2.0—or Internet 4.0. The internet is a powerful tool that has revolutionised the way we interact and do business. But if anything the comparison undersells the blockchain. The internet has allowed us to communicate and exchange better—more quickly, more efficiently.

But the blockchain allows us to exchange *differently*. **A better metaphor for the blockchain is the invention of mechanical time.**

Before mechanical time, human activity was temporally regulated by nature: the crow of the rooster in the morning, the slow descent into darkness at night. As the economic historian Douglas W. Allen argues, the problem was variability: "there was simply too much variance in the measurement of time … to have a useful meaning in many daily activities".



The 12th century Jayrun Water Clock

"The effect of the reduction in the variance of time measurement was felt everywhere", Allen writes. **Mechanical time opened up entirely new categories of economic organisation that had until then been not just impossible, but unimaginable.** Mechanical time allowed trade and exchange to be synchronised across great distances. It allowed for production and transport to be coordinated. It allowed for the day to be structured, for work to be compensated according to the amount of time worked—and for workers to know that they were being compensated fairly. Both employers and employees could look at a standard, independent instrument to verify that a contract had been performed.

Complete and incomplete smart contracts

Oliver Williamson and Ronald Coase (who was also an economics Nobel prize winner, in 1991) put contracts at the heart of economic and business organisation. Contracts are at the centre of institutional cryptoeconomics. It is here that blockchains have the most revolutionary implications.

Smart contracts on the blockchain allows for contractual agreements to be automatically, autonomously, and securely executed. Smart contracts can eliminate an entire class of work that currently maintains, enforces and confirms that contracts are executed—accountants, auditors, lawyers, and indeed much of the legal system.

But the smart contracts are limited by what can be specified in the algorithm. Economists have focused on the distinction between complete and incomplete contracts.

A **complete contract** specifies what is to occur under every possible contingency. An **incomplete contract** allows the terms of the contract to be renegotiated in the case of unexpected events. Incomplete contracts provide one explanation for why some exchanges take place in firms, and why others take place in markets, and provides a further guide to questions surrounding vertical integration and the size of the firm.

Complete contracts are impossible to execute, while incomplete contracts are expensive. The blockchain, though smart contracts, lowers the information costs and transactions costs associated with many incomplete contracts and so expands the scale and scope of economic activity that can be undertaken. It allows markets to operate where before only large firms could operate, and it allows business and markets to operate where before only government could operate.

The precise details of how and when this will occur is a challenge and a problem for entrepreneurs to resolve. Currently, **oracles** provide a link between the algorithmic world of the blockchain and the real world, trusted entities that convert information into data that can be processed by a smart contract.

The real gains to be made in the blockchain revolution, we suggest, are in developing better and more powerful oracles—converting incomplete contracts to contracts that are sufficiently complete to be written algorithmically and executed on the blockchain.

The merchant revolution of the middle ages was made possible by the development of merchant courts—effectively trusted oracles—that allowed traders to enforce agreements privately. For blockchain, that revolution seems yet to come.

Whither government?

The blockchain economy puts pressure on government processes in a whole host of ways, from taxation, to regulation, to service delivery.

Investigating these changes is an ongoing project of ours. But consider, for instance, how we regulate banks.

Prudential controls have evolved to ensure the safety and soundness of financial institutions that interact with the public. Typically these controls (for example, liquidity and capital requirements) have been justified by the fact that depositors and shareholders are unable to observe the bank's ledger. The depositors and shareholders are unable to discipline the firm and its management.

Bank runs occur when depositors discover (or simply imagine) that their bank might not be able to cover their deposits, and they rush to withdraw their money.

The bank run in Mary Poppins (1964)

One possible application of the blockchain would allow depositors and shareholders to continuously monitor the bank's reserves and lendings, substantially eliminating the information asymmetries between them and the bank management.

In this world, market discipline would be possible. Public trust in the immutability of the blockchain would ensure no false bank runs occurred. The role of the regulator might be limited to certifying the blockchain was correctly and securely structured.

A more far reaching application would be a **cryptobank**—an autonomous blockchain application that borrows short and lends long, perhaps matching borrowers with lenders directly. A cryptobank structured algorithmically by smart contracts would have the same transparency properties as the bank with a public blockchain ledger but with other features that might completely neglect the need for regulators. For example, **a cryptobank could be self-liquidating**. At the moment the cryptobank began trading while insolvent, the underlying assets would be automatically disbursed to shareholders and depositors.

It is unclear what regulatory role government should have in this world.

Tyler Cowen and Alex Tabarrok have argued that much government regulation appears to be designed to resolve asymmetric information problems—problems that, in a world of information ubiquity, often do

not exist any more. Blockchain applications significantly increase this information ubiquity, and make that information more transparent, permanent, and accessible.

Blockchains have their uses in what is being called **'regtech'**—the application of technology to the traditional regulatory functions of auditing, compliance, and market surveillance. And we ought not to dismiss the possibility that there will be new economic problems that demand new consumer protections or market controls in the blockchain world.

Nevertheless, the restructuring and recreation of basic economic forms like banks will put pressure not just on how regulation is enforced, but what the regulation should do.

Whither Big Business?

The implications for big business are likely to be just as profound. Business size is often driven by the need to cover the costs of business hierarchy—in turn due to incomplete contracts and technological necessity of large scale financial investment. That business model has meant that shareholder capitalism is the dominant form of business organisation. The ability to write more complete contracts on the blockchain means that entrepreneurs and innovators will be able to maintain ownership and control of their human capital and profit at the same time. The nexus between operating a successful business and access to financial capital has been weakening over time, but now might even be broken. **The age of *human capitalism* is dawning.**

Entrepreneurs will be able to write a valuable app and release it into the "wild" ready to be employed by anyone and everyone who needs that functionality. The entrepreneur in turn simply observe micro-payments accumulating in their wallet. A designer could release their design into the "wild" and final consumers could download that design to their 3D printer and have the product almost immediately. This business model could see more (localised) manufacturing occur in Australia than at present.

The ability of consumers to interact directly with producers or designers will limit the role that middlemen play in the economy.

Logistics firms, however, will continue to prosper, but the advent of driverless transportation will see disruption to industry too.

Bear in mind, any disruption of business will also disrupt the company tax base. **It may become difficult for government to tax business at all**—so we might see greater pressure on sales (consumption) taxes and even poll taxes.

Conclusion

The blockchain and associated technological changes will massively disrupt current economic conditions. The industrial revolution ushered in a world where business models were predicated on hierarchy and financial capitalism. The blockchain revolution will see an economy dominated by human capitalism and greater individual autonomy.

How that unfolds is unclear at present. Entrepreneurs and innovators will resolve uncertainty, as always, through a process of trial and error. No doubt great fortunes will be made and lost before we know exactly how this disruption will unfold.

Our contribution is that we have a clear understanding of a model that can be deployed to provide clarity to the disruption as and when it occurs.