1. Introduction

This book introduces a new field of economic inquiry. What we call 'institutional cryptoeconomics' is the application of the transaction cost economics of Ronald Coase, James Buchanan, Oliver Williamson, and Elinor Ostrom to blockchains; the distributed ledger technology first invented by the pseudonymous Satoshi Nakamoto for the development of the Bitcoin cryptocurrency. Where cryptoeconomics is the study of the economics of blockchain consensus mechanisms – a field of game theory and mechanism design – institutional cryptoeconomics is the study of how blockchains interact with our existing and future social institutions, from the nature of contracts, to the shape of the firm, to the structures of global trade, all the way to the dynamics of capitalism and geopolitics.[1]

An economic analysis can be called institutional if it studies the social institutions that coordinate and govern exchange. Adam Smith discovered the function of markets in arranging production and distribution through incentives.[2] Friedrich Hayek uncovered the function of dispersed information and its relationship to prices.[3] Ronald Coase revealed the role of the firm, pioneering the transaction cost tradition which informs this book.[4] Duncan Black and Anthony Downs conceptualised the role of democratic government.[5] James Buchanan discovered the role of clubs.[6] Elinor Ostrom revealed the commons as a mechanism for economic coordination.[7] Institutional cryptoeconomics adds another institutional form to this schema: blockchains. Blockchains are an economic infrastructure, alongside markets, the firm, governments, clubs, and the commons, for

[1] On cryptoeconomics, see Vitalik Buterin, 'Introduction to cryptoeconomics', Ethereum Foundation (2017).

[2] Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (University of Chicago Press, 1976 [1776]).

[3] Friedrich A. Hayek, 'The use of knowledge in society', *American Economic Review* 35, no. 4 (1945).

[4] Ronald H. Coase, 'The problem of social cost', *Journal of Law and Economics* 56, no. 4 (1960); Ronald H. Coase, 'The nature of the firm', *Economica* 4, no. 16 (1937).

[5] Duncan Black, *Theory Committees and Elections* (Cambridge University Press, 2011); Anthony Downs, *An Economic Theory of Democracy* (Harper, 1957).

[6] James M. Buchanan, 'An economic theory of clubs', *Economica* 32, no. 125 (1965).

[7] Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (Cambridge University Press, 1990).

coordination and exchange. They have distinct economic characteristics that give them the potential to complement, and in some circumstances directly compete with, this existing suite of institutional choices.

Institutional innovation at this scale is rare. If our analysis is right, distributed ledgers are an institutional innovation with comparable significance to the invention of the joint stock company in the sixteenth century or the spread of representative democracy in the nineteenth: they are a new mechanism with which we govern and coordinate economic activity. The rarity of institutional innovation is one reason that institutional cryptoeconomics is such an exciting field. Markets, firms, governments, clubs, and the commons existed long before they were formally identified and understood by economists. The Smithian division of labour was mature – his pin factory example has no less than 18 steps – when the *Wealth of Nations* was published. Duncan Black and Anthony Downs were able to understand the economics of government by looking at the sophisticated party democracies of the developed world. The blockchain industry is young, just a decade old at the time of writing. Many of the technologies that make it so interesting are even younger. The consumer-facing and business back-end applications of distributed ledgers are still in their experimental phase. The consequences of the joint stock company took hundreds of years to become evident. Yet through a straightforward application of new institutional economics to this new class of technologies, we can make predictions about the long-run future of the economy.[8]

This book is a contribution to that project – understanding the long-run implications of a new institution – and a contribution to economic theory in its own right. Blockchains are a technology of trust; what *The Economist* called the 'trust machine'.[9] This book offers an analytic framework by which we can understand the role of trust and ledgers in economic coordination. What do we mean by trust? Trust is the belief or assurance that another party will not exploit our vulnerabilities.[10] Oliver Williamson pointed out that many of our economic, social and political institutions have evolved in order to safeguard against opportunism – 'self-seeking with guile', as Williamson put it – by providing *ex ante* or *ex post* compensation for the uncertainty that rules will be followed.[11]

We recast this as the following: economic institutions provide a trust

---

[8] Davidson, Filippi, and Potts.

[9] *The Economist*, 'The trust machine', 31 October 2015.

[10] J.L. Morrow Jr, Mark H. Hansen, and Allison W. Pearson, 'The cognitive and affective antecedents of general trust within cooperative organizations', *Journal of Managerial Issues* 16, no. 1 (2004). See the discussion in Sinclair Davidson, Mikayla Novak, and Jason Potts, 'The cost of trust: a pilot study', *Journal of the British Blockchain Association* 7 (2018).

[11] Oliver E. Williamson, *The Economic Institutions of Capitalism* (Free Press, 1985).

layer to govern complex exchange. Blockchains industrialise this trust layer.[12] Proof of work blockchains such as Bitcoin convert energy into economically valuable trust. Alternative consensus mechanisms convert economic coordination tools like voting or costly signalling (such as staking capital) into trust. That trust is provided as an immutable consensus over shared facts (the blockchain's distributed ledger) that maps property and contractual relationships to identities. By building into this shared ledger self-executing 'smart contracts' – better understood as algorithms that automatically execute transfers of value when preprogrammed conditions have been met – exchange contracts on a blockchain potentially eliminate *ex post* opportunistic behaviour by contractual counterparties. Williamson's framework allows us to see how human rules and organisations mitigate against the human constraints of opportunism, bounded rationality, and asset specificity. Blockchains are mechanical institutions to mitigate those same constraints.

BLOCKCHAINS AND CRYPTOCURRENCIES

A blockchain is a type of distributed digital database, or ledger, with two critical properties: decentralisation and immutability. Formally, a distributed ledger technology is a:

> system of electronic records that (1) enables a network of independent participants to establish a consensus around (2) the authoritative ordering of cryptographically validated ('signed') transactions. These records are made (3) persistent by replicating the data across multiple nodes, and (4) tamper-evident by linking them by cryptographic hashes. (5) The shared result of the reconciliation/consensus process – the 'ledger' – serves as the authoritative version for these records.[13]

Blockchains were invented by pseudonymous Satoshi Nakamoto in order to power the decentralised digital currency Bitcoin.[14] The Bitcoin White Paper, published in 2008, described the problem this currency

---

[12] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press, 2018); Melanie Swan et al. (eds), *Blockchain Economics: Implications of Distributed Ledgers: Markets, Communications Networks, and Algorithmic Reality* (World Scientific, 2019).

[13] Michel Rauchs et al., 'Distributed ledger technology systems: a conceptual framework', *SSRN* (2018).

[14] Rainer Böhme et al., 'Bitcoin: economics, technology, and governance', *Journal of Economic Perspectives* 29, no. 2 (2015); Joseph Abadi and Markus Brunnermeier, 'Blockchain economics', 2018, https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v3g.pdf.

was trying to solve.[15] As Satoshi described it, internet commerce relies on payments systems managed by trusted third parties (that is, financial intermediaries) to process payments. Digital payments are reversable, reducing the reliability of the system and raising the possibility of fraud. Satoshi related the reversibility of electronic payments to the existence of the trusted third parties: terrestrial financial intermediaries 'cannot avoid mediated disputes', governed as they are by terrestrial law and national and international legal systems. Bitcoin would be a non-reversible digital currency 'based on cryptographic proof instead of trust'.

The idea of a native digital currency was a recurring dream of internet entrepreneurs and activists in the 1980s and 1990s. There were two distinct, although not mutually exclusive, goals that inspired the development of these currencies. First was the idea that the internet needed a native digital currency to facilitate payments. A digital communications system should have a digital cash to accompany it, not simply the terrestrial payments and monetary system bolted onto the internet. The second goal was more ambitious. A group of 'crypto-anarchists' or 'cypherpunks' saw the twin developments of the public internet and the advances in cryptography in the last two decades in strikingly political terms: a radical shift in political and economic power away from big governments and big businesses towards free citizens. Timothy C. May's 'Crypto Anarchist Manifesto', first presented in 1988, declared that cryptography 'will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation'.[16] In a subsequent essay, May explicitly linked cryptography to the goals of the libertarian movement, writing that 'it will be easier to form certain types of libertarian societies in cyberspace than in the real world of nations and physical locations'.[17] While their ambitions were broader than digital cash, the centrality of the monetary system to an exchange economy – alongside libertarian concerns

[15] We refer to this as Satoshi's Bitcoin rather than Nakamoto's Bitcoin following the naming convention of the fundamental unit of a bitcoin as a Satoshi, not as a Nakamoto. The Satoshi identity went silent after 2010. Satoshi's last post is on the Bitcoin forum is https://bitcointalk.org/index.php?topic=2228.msg29479#msg29479. Despite much effort by journalists and amateur internet detectives, his, her, or their true identity is still unknown.

[16] Timothy C. May, 'The crypto anarchist manifesto', 22 November, https://www.activism.net/cypherpunk/crypto-anarchy.html.

[17] Timothy C. May, 'Libertaria in cyberspace, or cyberspace more hospitable to ideas of liberty and crypto anarchy', 1 September, https://www.activism.net/cypherpunk/libertaria.html. See also Timothy C. May, 'Thirty years of crypto anarchy' (paper presented at the Hackers Congress Paralelní Polis, Prague, 1 October 2017); Timothy C. May. 'Crypto anarchy and virtual communities', Satoshi Nakamoto Institute, https://nakamotoinstitute.org/virtual-communities/.

about central banking – made the development of a digital payments system a priority.

Accordingly, the 1990s and 2000s saw numerous developments in digital cash. Prominent early attempts include eCash (launched in 1990 by the computer scientist David Chaum), PayPal, and e-gold, which exchanged physical gold for digital assets. These early attempts tended to founder on their reliance on services provided by existing organisations (such as banks) or central trusted authorities to provide security and mitigate against what has come to be known as the 'double spending problem'. The double spending problem comes from one of the most attractive features of the digital world: the ability for users to make infinite copies of a single digital item (such as a string of text or a file) that is an exact replica of the original. This characteristic of digital goods has led to the advances in communication and given us email, file sharing, social media, and digital archiving, but is a terrible characteristic for money. Infinite copying of a digital financial asset is, in the fiat currency world, described as counterfeiting. For a digital cash system to function, there needs to be a mechanism to prevent a single unit of digital money from being copied and spent twice. Relying on a single source of authority – call it a 'central bank' – to validate that transactions had not been double spent left the entire digital cash system vulnerable if that authority was to be compromised, or suffer technical problems, or try to extract monopoly rents.[18]

Bitcoin solved the double spending problem through an ingenious distributed consensus mechanism.[19] Security against double spending in Bitcoin is provided by distributed agreement about the validity of transactions. Bitcoin records all transactions on a shared ledger (held on thousands of voluntary nodes around the world) which can in principle be audited by any user of the network. A special class of self-selecting users, called 'miners', listen for new transactions on the network, group those transactions into blocks and add those blocks to the chain of prior transactions – hence 'blockchain' – each with a digital pointer referring to the previous block.

While relying heavily on cryptography, the active prevention of double spending is provided by economic incentives. Miners compete against each other to be first to produce the next block by solving a computationally

---

[18] A good overview of the state of electronic payments at the turn of the century is N. Asokan, Phillipe A. Janson, Michael Steiner, and Michael Waidner, 'The state of the art in electronic payment systems', *Computer* 30, no. 9 (1997). See also Jaap-Henk Hoepman, 'Distributed double spending prevention' (paper presented at the International Workshop on Security Protocols, 2007).

[19] John P. Conley, 'Encryption, Hashing, PPK, and Blockchain: A Simple Introduction' (working paper, Vanderbilt University, 2017).

difficult puzzle known as 'hashcash', where miners perform a cryptographic hash function operation on a combination of data drawn from the network and random data until a hash with a certain number of leading zeroes is returned. There is no intrinsic benefit from a hash with many leading zeroes; the constraint only exists to make producing new blocks hard. The Bitcoin network increases the difficulty periodically, to keep up with advances in hashing technology. Miners are rewarded by being able to place into the next block a new quantity of Bitcoin (currently 12.5 Bitcoin, although the reward is halved automatically every four years) that they can send to themselves.

It is that combination of a difficult task and a strong reward that makes the network secure against double spending; miners are incentivised to protect and validate network transactions. But that security comes with a cost: the computational difficulty of the proof of work scheme, combined with the highly competitive mining industry, means that proof of work is extremely energy intensive. Estimates vary about the energy costs of maintaining the Bitcoin ledger, but a 2018 study suggested that the network consumes 2.55 gigawatts of electricity, comparable to the electricity consumption of Ireland.[20]

As far as we know Satoshi did not develop any of the constituent technologies that go into Bitcoin. Public key cryptography dates back to the 1970s, Bitcoin's ledger structure ('the Merkle tree') was first proposed in 1980, Hashcash was first proposed in 1997 to prevent email spam, and arguably the first peer-to-peer network was ARPANET itself, in which each university research node had equal peer status with each other.[21] The Satoshi innovation – the genius – was combining these technologies in a way that aligned economic incentives to maximise security even assuming the network would operate in a low-trust environment. The problem of achieving consensus in an environment where not all parties can be trusted is described in the context of blockchains as the Byzantine Generals' Problem, a problem named in 1982, but which describes the problem of coming to consensus over information in the presence of faults.[22] In Bitcoin, consensus has to be achieved in in a world of criminals and faulty

[20] Alex de Vries, 'Bitcoin's growing energy problem', *Joule* 2, no. 5 (2018).

[21] For the academic progenitors of Bitcoin see Arvind Narayanan and Jeremy Clark, 'Bitcoin's academic pedigree', *Communications of the ACM* 60, no. 12 (2017). For peer-to-peer networking see A. Oram, *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (O'Reilly Media, 2001).

[22] The problem was named in Leslie Lamport, Robert Shostak, and Marshall Pease, 'The Byzantine generals problem', *ACM Transactions on Programming Languages and Systems* 4, no. 3 (1982); but more clearly stated in Marshall Pease, Robert Shostak, and Leslie Lamport, 'Reaching agreement in the presence of faults', *Journal of the ACM* 27, no. 2 (1980). Leslie Lamport traces the original problem to NASA's work on Software Implemented Fault

communications infrastructure. But the key to understanding the Bitcoin network provides an economic, rather than technical solution to the problem of trust. We have described blockchains as machines that industrialise trust, but the fuel for those machines is high-powered economic incentives.

This approach allows us to clarify the relationship between blockchains and cryptocurrencies. The Bitcoin cryptocurrency (what we will refer to as BTC, to distinguish it from the network) is an essential part of ensuring that incentives are aligned. Good behaviour by miners is rewarded in BTC, and all users have high-powered incentives to defend the network to protect BTC they already hold. But in this sense the cryptocurrency has an instrumental purpose: to maintain and ensure consensus over a distributed, decentralised ledger. Cryptocurrencies are artefacts – 'tokens' – that can be traded and valued as money-like assets, and have become an asset class with some significance for the future of the monetary and payments system.[23] But their function is to ensure consensus over the shared ledger. In Bitcoin the ledger primarily tracks transactions of the cryptocurrency. But users can place unrelated data into the blockchain. Nakamoto's first transaction on the Bitcoin blockchain included the text 'The Times 03/Jan/2009 Chancellor on brink of second bailout for banks'.[24] (January 2009 was a fascinating time to create a payments system that did not rely on existing financial institutions.)

Nakamoto released Bitcoin as open source, and a decade's worth of innovation on blockchains and other distributed ledgers has led to significant innovation. Blockchains have been released with innovation along almost every margin, such as different cryptocurrencies with different monetary characteristics, how private or anonymous the ledger is, and the difficulty and speed at which the consensus mechanism operates. One of the most significant areas of innovation – and one of the most critical for the future of the blockchain ecosystem – is in the consensus mechanism itself. The Bitcoin proof of work system is energy intensive and hard to scale. Alternatives such as proof of stake (where users stake tokens for the right to validate new blocks), proof of burn (where tokens are ritualistically destroyed), distributed proof of stake (where token holders vote on a limited pool of miners) are among the many innovations in this space. Private or permissioned blockchains, such as the Linux-IBM project

---

Tolerance for computer-flown aircraft, see Leslie Lamport, 'My writings', 20 September, https://lamport.azurewebsites.net/pubs/pubs.html.

[23] Our contribution to this is Chris Berg, Sinclair Davidson, and Jason Potts, 'Beyond money: cryptocurrencies, machine-mediated transactions and high frequency bartering', *SSRN* (2018).

[24] For an overview of techniques to place data into the Bitcoin blockchain see Andrew Sward, Ivy Vecna, and Forrest Stonedahl, 'Data insertion in Bitcoin's blockchain', *Ledger* 3 (2018).

Hyperledger, control who can validate new blocks and who can access the ledger. While guaranteeing much faster transaction times, these private blockchains trade off decentralisation for efficiency, resulting in a hybrid between traditional shared databases and fully distributed ledgers.

One of the most significant innovations in the blockchain space is the addition of fully operational scripting languages into the blockchain. Bitcoin is built around a highly constrained programming language called Script, which allows developers to impose restrictions (such as multi-signature keys) on how individual tokens are spent. But if any arbitrary data can be placed into the Bitcoin blockchain, why not entire computer programs? Ethereum, which was released in July 2015, claims to be fully 'Turing complete' programming language, a criteria for general purpose computing derived from the work of the computer scientist Alan Turing.[25] Ethereum programs execute as written everywhere that the Ethereum blockchain is stored; the result being distributed, censorship-proof algorithms that underpin Ethereum's goal to be a 'world computer'. Where Bitcoin was designed with the intention of an un-censorable global payments system, Ethereum generalises that to all digital algorithms. There are now a number of blockchains that offer comparably complex programming languages, whether those languages are hosted 'on-chain' (such as NEO and EOS) or 'off-chain' (such as NEM).

These features allow for the implementation of what the computer scientist and legal scholar Nick Szabo first conceptualised in 1994 as 'smart contracts'. A smart contract, wrote Szabo, is a 'computerized transaction protocol that executes the terms of a contract'.[26] Smart contracts are algorithms with contractual conditions built in, such as automatic transfers of value when conditions are triggered. Smart contracts are arguably an ironic misnomer. They execute precisely as written under any circumstances, even when unanticipated events might mean that all parties to the contract would rather they did not do so. Once a contract is published onto a blockchain, it will execute, even if it has been written poorly featuring coding bugs. Researchers have found numerous contracts on the Ethereum blockchain that might lock funds indefinitely or leak funds to unauthorised users.[27] With no central authority to appeal to, contractual terms are irrevocable even in circumstances of error. But this is a feature,

[25] There is some dispute as to whether Ethereum is genuinely Turing complete, given it is restricted by the amount of Ethereum tokens Ether (ETH) in the network. See Andrew Miller, 'Ethereum isn't Turing complete, and it doesn't matter anyway' (Consensys, 2016).

[26] Nick Szabo, 'Smart contracts', http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[27] Ivica Nikolic et al., 'Finding the greedy, prodigal, and suicidal contracts at scale', *arXiv preprint arXiv:1802.06038* (2018).

not a bug. As we shall see, a smart contract self-executes – that is, triggers, transfers payments, and enforces terms – without the need for any external agent, such as a court. Smart contracts are one of the central underlying technologies of the blockchain economy.

Blockchain innovation has been intense since Satoshi published the Bitcoin White Paper in 2008, and cryptocurrencies are merely the first use-case for this new technology. While a complete survey of the applications of blockchain is neither possible or necessary here, blockchains are being used to manage supply chains in fields as diverse as agriculture and advanced manufacturing, to coordinate trade finance, for identity, certification and licence management, banking, registries for land, water energy, and intellectual property, for medical records, to organise data for smart cities, and to register legal documents such as wills.[28]

More ambitious applications exploit the possibilities of smart contracts to coordinate activity without the need for hierarchy, even human agency.[29] Distributed autonomous organisations (DAOs) are organisations built around smart contracts and a blockchain, controlled in a decentralised manner by its owners. The Ethereum game CryptoKitties, which allows users to breed and exchange unique digital cats, represents an entirely new category of intellectual property.[30] Cellarius, also built on the Ethereum network, is an ambitious attempt to build a collective storytelling platform, where users coordinate around a sci-fi world building and narrative creation structure. Throughout this book we shall explore some blockchain applications in depth. But for now, the remarkable breadth of applications that have already been developed, and the extraordinary diversity of fields in which blockchains are being trialled and applied, suggests, at a first instance, that this technology has particular economic properties that make it institutionally significant.

---

[28] Jason Potts, Ellie Rennie, and Jake Goldenfein, 'Blockchains and the crypto city', *it-Information Technology* 59, no. 6 (2017); E. Ganne, 'Can blockchain revolutionise international trade?', 2018, https://www.wto.org/english/res_e/booksp_e/blockchainrev18_e.pdf; Evangelos Benos, Rod Garratt, and Pedro Gurrola-Perez, 'The economics of distributed ledger technology for securities settlement', *SSRN* (2017); Michael Casey et al., 'The impact of blockchain technology on finance: a catalyst for change', *Geneva Report on the World Economy*, no. 21 (2018); Amy Whitaker and Roman Kräussl, 'Blockchain, fractional ownership, and the future of creative work', CFS Working Paper Series 594, Center for Financial Studies (CFS), 2018.

[29] Anthony J. Casey and Anthony Niblett, 'Self-driving contracts', *Journal of Corporation Law* 43 (2017); Richard Holden and Anup Malani, 'Can blockchain solve the holdup problem in contracts?', University of Chicago Coase-Sandor Institute for Law and Economics Research Paper, 2017; Joshua S. Gans, 'The fine print in smart contracts', NBER Working Paper No. w25443, 2019.

[30] Chris Berg, Sinclair Davidson, and Jason Potts, 'KodakOne could be the start of a new kind of intellectual property', *Conversation*, 12 January 2018.

SOME METHODOLOGICAL CONSIDERATIONS

Blockchains are an early stage technology. While Bitcoin now has a decade-long history, many of the blockchain innovations which have led to the field of institutional cryptoeconomics are only a few years old. Ethereum was only released in July 2015. The zero knowledge proof privacy coin Zcash was only released in October 2016. There are many uncertainties about the future of blockchain development as we write this book. Public blockchains tend to have low transaction throughput, at least compared to centralised systems. The proof of work algorithm used by Bitcoin and many other second and third generation blockchains is highly energy intensive, and has created many environmental concerns. Alternative mechanisms that might solve scaling problems and environmental costs – such as proof of stake, distributed proof of stake, and practical Byzantine fault tolerance – are in an earlier experimental stage of development. Even if the technical challenges are worked out, the user experience for blockchains leaves something to be desired: it is time consuming and tedious to convert fiat currency into cryptocurrency; key management can be complex and brings security risks; and there is still a non-trivial amount of technical knowledge necessary to interact with blockchains.

These limitations are what might be expected from a technology just a decade old, but it is also possible that there is some as yet undiscovered limiting condition around a critical blockchain characteristic. For example, Zooko's triangle, suggested by the developer of Zcash, Zooko Wilcox-O'Hearn, suggests that there is a trade-off between three desirable properties of identities on a network protocol: that they are human-readable, that they are secure, and that they are distributed (that is, no central authority has control over identities). Wilcox-O'Hearn suggested that identity management systems can only have two of these three properties.[31] There is a chance that researchers or developers will discover constraints around decentralisation, consensus, availability, and persistency that prevent limiting the potential of blockchain as an economic institution.

Alternatively, it is possible that blockchains might be superseded by new distributed ledger technologies. Nakamoto's data structuring technique – grouping transactions into blocks that include hash pointers to previous blocks – is unlikely to be the end state of distributed ledger development. For example, there are a number of distributed ledger protocols built around directed acyclic graphs (DAGs) which store transactions in nodes rather than blocks. Richard Goldschmidt described the first consequential

[31] Zooko Wilcox-O'Hearn, 'Names: distributed, secure, human-readable: choose two', 12 October, https://web.archive.org/web/20011020191610/http://zooko.com/distnames.html.

evolutionary mutations in biological species as 'hopeful monsters', which Joel Mokyr adapted for the study of technological innovation.[32] A hopeful monster is a macromutation; a large, ugly, surprising leap forward in evolutionary adaptation. And Bitcoin is ugly.[33] It is a complex, interlocking set of cryptographic techniques and economic incentives. It is slow, expensive, and energy inefficient by design. The need for distributed consensus has made it hard to modify in order to alter fixed limitations. But it is merely the first mutation. Its success – and, unsurprisingly, the high exchange rate between Bitcoin and fiat currency experienced during 2017 – has brought massive research resources to bear on building better blockchains, and making Bitcoin more useful.

Nonetheless, throughout this book we use the word 'blockchain' near synonymously with 'distributed ledgers'. This is for convenience and readability. Our claim is that blockchains are an incredibly successful proof of concept for distributed ledger technology. Or, more broadly, blockchains are an instantiation in economics and computer science of a new class of mechanism to achieve consensus around facts – whether those facts are who owns what cryptocurrency, or has the right to what water entitlement, or what part of a science fiction narrative should be considered 'canon' – that does not rely on central authorities, or hierarchies. As social scientists, we are keenly aware of the economic role of those central authorities in providing trust, and of the high costs of low-trust societies. Blockchains reveal to us the role of trust across a new margin. They offer a new way to provide trust, while reducing some of the costs of trust provision. A smart contract has embedded within it not only the terms and triggers of the contract event, but its own means of fulfilment and enforcement. While the role of a traditional court system – that *ex post* provider of trust – in a world of smart contracts is not zero, it is much reduced.[34] If a firm provides a trust layer for economic activity, what does it mean to mechanise that trust in a DAO?

As this suggests, we conceptualise the methodology of institutional cryptoeconomics as 'high-trust economics'. The analogy here is to high-energy physics, which uses a particle accelerator as a tool for exploring

---

[32] Richard Goldschmidt, 'Some aspects of evolution', *Science* 78, no. 2033 (1933); Richard Goldschmidt, *The Material Basis of Evolution* (Yale University Press, 1940); Joel Mokyr, *The Lever of Riches: Technological Creativity and Economic Progress* (Oxford University Press, 1990).

[33] Gwern Branwen, 'Bitcoin is worse is better', 2 January, https://www.gwern.net/Bitcoin-is-Worse-is-Better.

[34] See Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018); Darcy W.E. Allen, Aaron M. Lane, and Marta Poblet, 'The governance of blockchain dispute resolution', *SSRN* (2018).

conditions that are otherwise far removed from the observable, low-energy world. High-energy physics seeks to understand the fundamental building blocks of the universe – space, time, matter, and energy – by exaggerating the conditions of normal existence. A particle accelerator recreates on Earth conditions that otherwise pertain at the core of a star, or in the very early universe. High-trust economics offers a similar experimental method. It allows us to explore conditions in an economy in which trust is maximised. A high-trust economy is one in which contracts are self-enforcing. To reveal the fundamental nature of the economy, we do high-trust economics – we crank up the trust – which permits near perfect promise and trust. Institutional cryptoeconomics is the study of a new technology and its implications, but it is also a methodology, based on the exploration of the nature of a high-trust economy using a tool as both an actual technology in the world, and as an ideal type, a 'perfect ledger'.

The difference of course between a particle accelerator and a blockchain is that blockchains now exist in the real world. We do not have to construct them as experimental domains, or theorise about their existence. Blockchains have been brought into the world and now coordinate economic activity. Much of this book is based on our observation of the development of this technology over the last decade. But institutional cryptoeconomics does not actually depend upon the success of blockchain technologies. It is sufficient for our purpose that blockchains exist as a concept: a concept of a trustless technology of governance and coordination, a new technology of trust. The idea of a blockchain is sufficient to establish institutional cryptoeconomics as a theoretical field. That they exist – that they are being built, that entrepreneurs, engineers and enthusiasts are investing enormous resources into their success – makes the study of institutional cryptoeconomics urgent.

ABOUT THIS BOOK

This book has two distinct audiences: economists and students of economics on the one side, and those who work or are interested in the blockchain industry on the other. We hope that the book will offer the tools that will allow these two audiences to communicate and share ideas. We proceed, therefore, as follows. In Chapters 2, 3, and 4 we spell out the basic foundations of institutional cryptoeconomics. Chapter 2 presents a straightforward analytical framework to understand the properties of blockchains through Oliver Williamson's transaction cost framework. Blockchains reduce opportunism and offer a institutional technology for governing specific assets. In Chapter 3 we fold out some of the broader consequences of

this analysis. We describe blockchain technology as a universal institution that can adopt the properties of the other institutions in the institutional schema. Chapter 4 provides a close analysis of the role that ledgers play in coordinating exchange. Ledgers store information about property ownership that allows buyers and sellers to trade. Institutional cryptoeconomics offers a ledger-centric view of the economy.

Chapters 5 and 6 drill down into what we consider the two major use-cases for blockchain technology: financial assets and supply chains. We explore how, despite being apparently prosaic topics, viewing blockchains through the financial asset and supply chain lenses helps us to conceptualise the full scope of blockchain applications, even in fields seemingly far removed from finance or logistics. Chapter 5 asks a simple question: are cryptocurrency tokens money? Regulators and policymakers need guidance about how to treat new technologies under current law; or some guide about how to adjust law to suit. Applying the theoretical frameworks earlier, we work through popular and institutional definitions of money and conclude that cryptocurrency tokens are 'dequity': a theoretical hybrid of equity and debt that Williamson conceptualised and named more than three decades ago, but which technological limitations prevented from being realised. Chapter 6 looks at the use of distributed ledgers for managing goods and services as they travel through a supply chain. Supply chain information in this context can be described as the creation of identity attributes at specific points in time. Framing supply chains in this way allows us to see a variety of supply chain models in industries as diverse as the finance sector, the charitable sector, and education credentials. Supply chains offer a general framework through which we can scrutinise and assess blockchain use-cases.

Chapters 7, 8 and 9 draw out the implications of this analysis for the future of the firm, for public policy, and ultimately for political economy. In Chapter 7 we explore a new mode of corporate organisation: the V-form organisation, where vertical integration is outsourced to a distributed ledger. The V-form organisation represents a blockchain instantiation of the so-called 'virtual organisation' that has been discussed since the 1980s, but has been limited by its need to establish trust between competing parties. Chapter 8 surveys some of the first-order public policy consequences of the widespread use of blockchain technology, and how a 'crypto-friendly' government should respond. Chapter 9 broadens this considerably. We present a model of the demand for regulation that stems from the political and economic consequences of corporate hierarchy – those warnings about the implications of capitalism from Karl Marx and Joseph Schumpeter – that a new, non-hierarchical, consensus driven technology to manage agreed social facts potentially disrupts. As

Paul Strassman wrote in 1985, 'The history of [information technology] can be characterized as the overestimation of what can be accomplished immediately and the underestimation of long-term consequences'.[35] This is what transaction cost economics offers us. A set of tools and techniques to understand how social institutions are shaped, and how when those transaction costs change, institutions are reshaped, with sometimes profound consequences.

[35] Paul A. Strassmann, *Information Payoff: The Transformation of Work in the Electronic Age* (Free Press, 1985), p. 199.