ANNUAL REVIEWS

Annual Review of Law and Social Science

The Law and Economics of Blockchain

Richard Holden[1] and Anup Malani[2,3]

[1]School of Economics and AGORA Centre for Market Design, Business School, University of New South Wales, Sydney, New South Wales, Australia; email: richard.holden@unsw.edu.au

[2]Law School, University of Chicago, Chicago, Illinois, USA

[3]National Bureau of Economic Research, Cambridge, Massachusetts, USA

Annu. Rev. Law Soc. Sci. 2022. 18:297–313

First published as a Review in Advance on July 18, 2022

The *Annual Review of Law and Social Science* is online at lawsocsci.annualreviews.org

https://doi.org/10.1146/annurev-lawsocsci-011921-060322

Keywords

blockchain, distributed ledger, regulation, law, contracts

Abstract

This article examines the implications of Distributed Ledger Technology (a.k.a. blockchain) for several areas of law. While cryptocurrencies have received much attention, the implications of DLT are potentially far reaching. DLT raises interesting and important questions relating to rules of evidence, surrounding issues like hearsay and authentication. The advent of initial coin offerings has implications not only for how firms are financed but also for securities law in regulating such offerings. Cryptocurrencies themselves (e.g., Bitcoin) have raised serious issues for tax avoidance and taxation law. Relatedly, the rise of cryptocurrencies raises issues regarding the relationship between private and nationally issued currencies, and even the role and efficacy of monetary policy. Finally, DLT has practical implications for election law and voter turnout, with such technology already begun to be used for security purposes in online voting and permitted in 32 US states.

1. INTRODUCTION

1.1. What Is Blockchain, or Distributed Ledger Technology?

Blockchain, or more precisely Distributed Ledger Technology (DLT), is a computer-science technology. It was introduced by Satoshi Nakamoto (2008)—a person whose true identity remains unknown—in 2008 to verify records and transactions in a decentralized manner, rather than by a central authority like a financial institution or a government. Such records or transactions may concern ownership of assets such as a digital currency or rights to real property. An example of centralized verification is your checking account at a traditional bank like Citibank; that bank verifies and records your incoming and outgoing cash flow. Blockchain is decentralized in the sense that uninterested parties verify and record the digital assets tracked on the blockchain ledger.

A key advantage of DLT is that, by not requiring the involvement of a central authority, it removes concerns about the security or trustworthiness of the central authority. In our checking example, you may prefer decentralized over centralized verification because the bank has an interest in your money: It literally makes interest off your deposits and may want to, e.g., slow recording of a withdrawal. DLT may also have certain cost advantages, because existing exchange involves either substantial frictions or intermediaries with market power.

Although Nakamoto originally developed blockchain to facilitate financial transactions, DLT more generally can be thought of as supporting the decentralized digital documentation of any statement or enforcement of any promise or contract. Understood in this light, it is easy to see why it not only has wide commercial application but also, importantly for our purposes, touches many different areas of law. To ground ideas, we begin by offering a simple example and explanation of a DLT transaction (based heavily on our previous work in Holden & Malani 2021).

Consider two parties, A and B, who want to agree that A will rent an apartment to B for $1,500 per month. This is, of course, a very familiar and natural contract that is often enforced either by a central authority (a court or regulator) or by reputational forces where the parties are deterred from cheating on the contract because they do not want to lose their reputation for being a valuable party with whom to contract.

This rental can be decomposed into two parts. The first is a statement by A that they will give B access to the apartment each month. The second is a statement by B that they will pay A $1,500 per month in a timely manner. A standard (i.e., pre-DLT) approach to arranging this transaction is for parties A and B each to write down their statements in a manner that is witnessed ex ante or verifiable ex post by some third party—ideally one who does not favor either of the contracting parties.

Blockchain or DLT is simply a new technology to witness such a transaction. Crucially, DLT uses a different approach to witnessing the statements ex ante: It takes advantage of so-called cryptographic algorithms that are mediated by a computer network. Blockchains like Bitcoin or Etherium are networks of nodes that are just computers on the network. When A and B decide to transact, they each announce their statement to the network. Any such network involves a method by which the nodes can observe A's and B's messages and then, crucially, produce evidence that they have heard the messages. This is known as validating the messages.

A critical tool that blockchain networks use is a type of one-way function in mathematics known as a hash function. A one-way function is a function whereby if you know the inputs, you can produce the outputs, but if you have only the outputs, you cannot know for sure the inputs (Antonopolous 2017).

When A and B send messages to the network, it transforms each message into a hash. The key feature of the hash is that people who observe it know that the nodes must have witnessed A saying they would provide access to the apartment and B saying they would pay $1,500 per month.

The key innovation of blockchain networks is that they choose the node that gets to add that hash to the blockchain record or ledger in a manner that ensures that node is not interested in that transaction and is therefore a trustworthy witness to the messages sent by A and B. How a blockchain chooses who gets to add the hashed message to the blockchain is called the ledger's consensus protocol. Proof of Work is one such protocol, though not the only one.

Proof of Work chooses which node gets to record a message on the official blockchain ledger by posing a cryptographic game and allowing only the node that solves that game to record the message. The game employs hash functions a second time: The first node that can produce a hashed output that satisfies certain conditions is the winner (for a detailed description, see Nakamoto 2008 or the Bitcoin Developer Guides, available at **https://bitcoin.org/en/developer-guide#blockchain**). The advantage of this ordeal is that the winner is, for practical purposes, uninterested in the transaction between A and B, and thus a reliable recorder of the exchange. The main downside of the game is that nodes, called Bitcoin miners, must use specialized computers and large amounts of energy to search for the solution to such problems—especially as they have become more complex over time.

The very nature of a hash function means that the node chosen to record the hash of A's and B's messages would not have done so unless it had indeed observed the statements of A and B. In this sense, the recording of the hash validates that the overall rental transaction between A and B was announced. The complete list of all transactions recorded on a network in this manner is called the blockchain. Because the blockchain is a list of transactions, it is also called a ledger. Because a copy of that ledger is held by all the nodes on the network, rather than by a single central authority, it is known as a distributed ledger.

1.2. Legal Areas Touched by Distributed Ledger Technology

The example we just gave is a contracting one, and some important applications are to contract theory and contract law. We discuss this below when focusing on how a DLT expands the frontier of contracting technology, allowing some new forms of contract to become possible and changing the demarcation with which transactions take place in firms and which take place in markets (as in Holden & Malani 2021).

Perhaps more surprisingly, DLT raises interesting and important questions relating to rules of evidence, surrounding issues like hearsay and authentication. The advent of initial coin offerings (ICOs) has implications not only for how firms are financed but also for securities law in regulating such offerings.

Nakamoto's original—and still in some sense the best known—application of DLT to cryptocurrencies (e.g., Bitcoin) has raised serious issues for tax avoidance and taxation law. Somewhat related to this, the rise of cryptocurrencies raises issues regarding the relationship between private and nationally issued currencies, and even the role and efficacy of monetary policy.

A final issue we cover in the article is the role of DLT in voting and election law. Such technology has already begun to be used for security purposes in online voting, and online voting is permitted in 32 US states (Fowler 2020). This could increase voter turnout and meaningfully affect election outcomes but also raises important questions about security and hacking, paper trails, and the overall integrity of elections.

1.3. Legal Rules as Structured Economic Interactions Using Distributed Ledger Technology

The overarching perspective of this article is that legal rules create economic incentives that govern behavior and provide incentives or disincentives for different kinds of economic activity.

The design of these rules and institutions must be attentive to their implications for economic activity. Because blockchain/DLT are relatively new and evolving, they present important opportunities and challenges for legal design. These, in turn, invite and reward collaborations between legal scholars, economists, computer scientists, and other fields within the social sciences broadly understood.

The article proceeds as follows. In Section 2, we discuss one of the more legal applications of blockchain technology, which is how it affects the rules of evidence and how many jurisdictions have adapted those rules to accommodate DLT evidence. In Section 3, we discuss blockchain as a new contracting technology that has implications for the boundary of the firm and the efficiency of market-based exchange. Section 4 focuses on ICOs, their role as a new financing instrument, and the implications for securities law, which has already had to adapt to these new instruments. In Section 5, we discuss the implications of blockchain technology for taxation law and the risks it poses to the revenue base of nation-states. Section 6 tackles the issue of private digital currencies and the implication this has for regular fiat currencies as well as international law. In Section 7, we turn attention to how DLT can be, and indeed already is being, used in elections to provide for more secure voting. Section 8 contains some brief concluding remarks.

Before proceeding, we note that because this is a relatively nascent field—despite its potential importance—there is comparatively little published work in it, and as a result the number of references we are able to point the reader to will be fewer than in a typical article of this kind or in this journal. At this point, there are few regulations and even fewer cases. As a result, much of the legal scholarship on blockchain is normative rather than positive.

2. BLOCKCHAIN AND RULES OF EVIDENCE

As we highlighted in the introduction, DLT provides evidence in the broad sense that it witnesses facts about the world, including a potential transfer of value from person A to person B. This description is actually a simplification. Unpacking it reveals both the extent to which blockchain relies upon other technologies and institutions to operate and the centrality of evidence law in understanding the value of blockchain.

At its core, blockchain is a ledger, a book in which one records data entries. The data may be numbers, words, or anything that can be encoded as bits of information. The distinguishing feature of the blockchain's ledger is that once entered, the data cannot be altered without great difficulty. (A great deal has been written about how difficult it is to alter the data; that is not central to this article, so we assume that entries are practically immutable.)

Evidence law regulates the data provided to a court to ensure that the data measure the actual state of the world. DLT does not regulate the content of the data entered (except in the trivial sense that it accepts only digital data).

One can ensure that blockchain may capture the true state of the world in two ways. One way is to make the data entered in the ledger be the actual state of the world. In other words, if the contract is premised not on B actually paying $1,500 to A but on B merely entering "transfer $1,500 to A" in the ledger, then the ledger prima facie measures the relevant state of the world. This approach will be central to how Bitcoin and smart contracting blockchains such as Ethereum operate. With Bitcoin, for example, the account balance of person A is literally equal to the sum of digital statements by others like B that they are transferring Bitcoin to A and statements by A that she is transferring Bitcoin to others.

The other way to make sure the data entered on the blockchain ledger are true facts about the world is to check the facts entered. Most computer scientists will think this means that you need a better oracle, a technology that observes the state of the world and enters the state into

the ledger. An example is a digital thermometer: It could measure the temperature in Chicago on January 4, 2021, and then pass that information to the ledger. The problem, however, is that we need to ensure that the thermometer is not manipulated, e.g., moved to Miami, or that the signal is not hijacked on the way to the blockchain. The DLT itself cannot do that.

But this is exactly what the law of evidence attempts to do. Courts regularly face questions such as, is the statement by this witness reliable? Is that DNA test reliable? In doing so, the court polices the process by which data are gathered and then transmitted to the court, including the chain of possession and the interests of the speaker. The goal is to reduce the risk that the message to the court is false.

Now let us step back and consider the following question. Suppose a court is called upon to enforce a contract that is conditioned on the state of the world, and the state of the world is ostensibly recorded on a blockchain. Should the court accept as fact the relevant blockchain entry?

One could attempt to consider this from a purely legal perspective, that is, accept that what the existing law does to determine the validity of evidence is normatively correct and ask whether existing law accepts a blockchain entry as fact. If the court in question were a US federal court, the starting point for the analysis would be the Federal Rules of Evidence (FRE). (US state courts have rules modeled on the federal rules; thus, the analysis below largely applies there as well.) The federal rules set up two key requirements for the use of blockchain as evidence.

The first is Rule 901, which requires that a party submitting evidence show that it is what the party claims it is and gives examples of how this requirement can be met. One of the ways this can be done is with evidence showing that the process of a DLT "produces an accurate result" [FRE 901(b)(9)]. Another is by using a type of evidence explicitly allowed by federal statute or Supreme Court rule [FRE 901(b)(10)]. Although Rule 901 concerns federal courts, states have similar evidentiary rules, and numerous states have passed statutes that allow entries in blockchain ledgers to be submitted as evidence (e.g., the Illinois Blockchain Technology Act, 12 Vermont Statutes Annotated 1913, and Arizona Electronic Transactions Act).

The second requirement is Rule 801, the hearsay rule. Under this rule, evidence that shows a person made a statement is not admissible as evidence in favor of the statement; the person must make the statement in court. One exception to the hearsay rule is the *Lizarraga-Tirado* test [*United States v. Lizarraga-Tirado* (2015)], which says that if the statement is made not by a human but by a machine, then the evidence of the statement is admissible. For example, if evidence shows that the DLT generated a statement ("B paid A") and B is not a person but a program, then the DLT entry is admissible. Another exception is the business records provision [FRE 803(6)], which allows that records "kept in the course of a regularly conducted activity" of an organization are exempt from the hearsay rule.

Whether and how these rules apply depend on the nature of the fact that one is attempting to prove with a blockchain entry. If the question of fact is whether the entry was made in the blockchain, then the relevant hurdle is Rule 901 and whether the blockchain is immutable. Authenticity can be established by statute or by specific evidence on the immutability of the DLT in question. Neither the best available evidence rule nor the hearsay rule is an issue because the question is not whether B actually sent the message "Pay A" but whether the message is actually on the blockchain.

If the question of fact is whether B made the statement recorded in the DLT entry or whether the DLT entry is a true fact about the world outside the DLT, the answer is more complicated. If B is a person, as opposed to an oracle, then the hearsay rule applies. The business record provision is a narrow exception because it requires that B's statement be a regularly recorded activity. If B is an oracle, then the hearsay rule is not an objection, and the evidence can be admitted. However,

that just pushes back the query from the blockchain to the oracle: Is the oracle itself producing an "accurate result" (Rule 901)?

Of course, the fact that there are circumstances in which a blockchain entry may be admissible evidence in court may not answer the normative question of whether a court should admit evidence. One could question the normative value of existing evidentiary rules and suggest a different rule for blockchain. However, we do not feel there is something special about blockchain that warrants a change in at least the US federal rules. Blockchain is arguably uniquely reliable for validating statements made on the network; e.g., B said to the network, "transfer $1,500 to A." However, it is not uniquely reliable for demonstrating that B indeed transferred $1,500 to A rather than merely telling the network they did. In either case, however, existing federal rules do not seem unreasonable. For the former, evidence of blockchain's reliability under 901(b)(9) or a statutory authorization under 901(b)(10) seems appropriate. For the latter, if the connection between the real-world fact and the blockchain entry is an oracle that meets the definition of a program, then the *Lizarraga-Tirado* exception to the hearsay rule seems appropriate.

3. BLOCKCHAIN AS A NEW CONTRACTING TECHNOLOGY

For blockchain to serve as a contracting technology, we need two things. First, the data being entered should be a true fact about the world. That fact can be either the contract itself, a fact on which the contract is conditioned, or both. Second, conditional on what facts are observed, a promise must be enforced. We addressed the first step in the last section on evidence law. Here we assume that the relevant contract writing and facts are on the blockchain and admissible and address the second step, whether the promise is enforceable.

Enforcing a promise in turn involves two steps: determining what the promise was and then enforcing that promise. The fact that a contract written on the blockchain is admissible as evidence of the promise does not resolve the matter of what the promise was. Just as a court may have a rule that allows for parole evidence—alongside the black letter contract—to inform its judgment about the contract, it may allow parole evidence—alongside a contract written on the blockchain—to influence its interpretation of what the parties promised each other. This may limit the promise of blockchain to practically dictate fully the terms of contracts. A corollary is that public policy will also be able to modify contracts written on the blockchain, insofar as courts have the power to enforce those contracts, a part of which lies on the blockchain.

Turning to enforcement of promises, we consider two scenarios. First, suppose the contract is written and evidenced on a blockchain, but performance is done partly outside the blockchain. This is an easy case. We see no reason that the fact that the contract uses blockchain technology should or will change the law's decision about whether the contract is enforceable. For example, a murder-for-hire contract made on or witnessed by a blockchain is no more enforceable than one made on paper.

Issues become somewhat more complicated in our second scenario, in which contractual performance is done wholly on the blockchain so the contract might be deemed self-enforcing. For example, suppose that a smart contract on the Ethereum blockchain possesses and transmits to B some information from A as soon as the blockchain receives the message "Pay A" from B. If the blockchain has an entry with the information from A, this can be done without any outside involvement of a court. Nor can A easily breach this contract if the smart contract code is also on the blockchain.

One hard case in this scenario is where the contract is not enforceable, as would be true if the information in the preceding contract was C's social security number and C was not effectively privy to the contract. In this context, the problem is how courts remedy self-enforcing legally

non-enforceable contracts. In practice, courts can award remedies that undo many self-executing contracts on the blockchain. In our social security example, the court can award damages that deter divulging the social security number. This will not stop execution of the blockchain contract at issue but may deter that contract from ever being written. Of course, there will be cases in which monetary remedies are inadequate and an injunction may be appropriate [see *eBay Inc. v. MercExchange, LLC* (2006)]. The challenge with issuing an injunction is that certain self-enforcing actions cannot be undone because code to execute a contract on the blockchain may be immutable, i.e., cannot be changed. Once the blockchain is commanded to reveal the social security number, the command cannot be altered, and the information cannot be unseen. Although we do not think the set of cases that fall in this gap is large, blockchain can blunt the remedial power of courts in these cases. However, these blockchain-related cases are not the only situations in which a court is unable to enjoin harm. Much of criminal law is premised on bad acts that cannot be specifically enjoined. The typical answer is to impose penalties that generally deter illegal action when tort or contract remedies are inadequate. Applying that logic here, the law—from a normative perspective—may want to consider penalties for contractual performance that is self-executing on the blockchain and can be neither compensated adequately via monetary damages nor specifically enjoined.

Another interesting case is where enforceability depends on the facts surrounding the case. A nice example is contract renegotiation. Return to our money-for-information contract example. Assume that the information could be legally exchanged but that, now, there is a second contract that says B will pay a different amount for the same information. This modification is similar to the facts in *Alaska Packers' Assoc. v. Domenico* (1902). The court must decide which contract controls. There are arguments in each direction. Perhaps the new contract was coerced from one party when the other was in a moment of great bargaining power and had no outside options. Alternatively, maybe the new contract efficiently reflected a state of the world different than that anticipated by the parties. Courts have several doctrines that inform their judgment in these cases.

Should the fact that an original contract is self-enforcing on the blockchain change the court's thinking about whether a renegotiated contract is enforceable? We think the answer is, somewhat (Holden & Malani 2021). To start, assume the renegotiated contract is not self-enforcing on the blockchain or that it cannot fully negate the original contract. If the court can nonetheless fully enforce a renegotiation promise with damages or an injunction, then the fact that the original contract is self-enforcing on the blockchain is of no matter. The fact that the contract was written to be self-enforcing on the blockchain is no more informative than a clause in a paper contract stating that the paper contract cannot be renegotiated. If, however, the court cannot fully enforce the renegotiated promise, then the original blockchain-enforced contract constrains the renegotiation. If the parties knew this and chose a blockchain self-enforcing contract over a paper contract with a no-renegotiation clause, the court can infer that the parties really intended to tie their hands, i.e., would have negotiated a different exchange or not traded at all if they could not tie their hands. The court should accept the constraints of the original contract, and perhaps the original contract without even incomplete modification with the renegotiated contract. One might ask why it matters what the court thinks if it cannot fully undo the original contract: The parties have bypassed court enforcement of the renegotiated promise. Although it does not matter to the court, it may matter for a legislature contemplating a statute that penalizes contracts written to be renegotiation proof via the blockchain (or any other technology). So long as the promises made are in and of themselves not illegal, e.g., do not involve murder for hire, there is no reason for the making of an immutable promise to be punished with damages beyond what contract law authorizes.

4. BLOCKCHAIN AND BUSINESS ORGANIZATION

As the example we offered in the introduction shows, blockchain can be seen in part as a new contracting technology that makes some market-based exchanges either more feasible or able to be conducted with lower transaction costs. This has direct implications for the boundary of the firm.

Coase (1937) was the first to ask the fundamental question: If markets are an efficient method of resource allocation, then why do so many transactions take place in firms? The answer Coase himself gave was that there are costs to using the price mechanism: Contracts must be drawn up, bargains must be made, there is haggling and search. Building on this, Williamson (1971, 1975, 1979) made a series of contributions that fleshed out Coase's original observation into what became known as transaction cost economics.

These theories provide an account of the costs, but not the benefits, of vertical or lateral integration. Motivated by this, Grossman & Hart (1986) and Hart & Moore (1990) developed a full-fledged, formal theory of the boundary of the firm that has become known as property rights theory (PRT). A premise of PRT is that contracts are necessarily somewhat incomplete because of either bounded rationality or the inability of the contracting parties to fully describe their arrangement to a third party such as a court. Under PRT, this incompleteness of contracts explains the observed ownership of assets, including ownership of firms. When a contract involving an asset is incomplete, it cannot specify ex ante the uses of that asset in all possible states. It leaves some decisions to the person who owns the asset and thus has discretion over the use of the asset outside the constraints of the contract. Grossman & Hart (1986) argue that this ownership is assigned to the person who will minimize efficiency losses from use of the asset. According to Aghion & Holden (2011, p. 183), "The incomplete contracts/property rights approach produces a theory of ownership and vertical integration. It also directly addresses the question of what is a firm. Grossman and Hart argue that a firm is a collection of assets over which the owner has residual control rights."

Some have questioned the premise of PRT. They argue that the contracting parties can use a revelation mechanism—that is, agree to play a certain game form—to reveal the information that they know about the state of the world to a third party. Proponents of this view suggest implementation mechanisms such as those pioneered by Moore & Repullo (1988) and Maskin & Tirole (1999a,b). These mechanisms would convert an incomplete contract into a complete contract and obviate the need to use ownership of assets and concomitant decisions within a firm as opposed to contracts and market transactions. The usual answer has been that the mechanisms are too difficult to implement.

Here is where blockchain technology comes in. Blockchain may partially rehabilitate the types of revelation mechanisms advocated by one side of the foundations of the incomplete contracts debate. Holden & Malani (2021) demonstrate in detail how blockchain technology can be used to partially replicate some types of these revelation mechanisms in a way that is robust to the critiques of Hart & Moore (2008) and Aghion et al. (2012).

Yet because blockchain has limitations, especially with the ability to control off-chain assets, it is a partial solution. As a result, there is still an important role for asset ownership, as emphasized by PRT. Put simply, DLT as a new contracting technology can, at least in principle, allow for some transactions that take place inside firms to take place in the market. It is in this sense that the new contracting technology shifts the boundary of the firm but does not eliminate it.

This has implications beyond the boundary of the firm, as PRT has been applied to a range of other economic settings, including international trade, public versus private ownership, and the mixture of debt versus equity that firms use. In each of these settings, the idea of incomplete contracts and residual control rights helps pin down what countries trade or produce at home,

what government services should be paid for by the state and what should be provided directly by the state, and the capital structure of firms. And in each of these settings, the new contracting technology DLT provides suggests that a change in the mixture of all these things is possible, implying that such technology has even more far-reaching implications. Moreover, from an academic perspective, it suggests that fields in the social sciences, such as finance, international trade, and public choice theory, will all need to grapple with the impact of DLT.

5. TOKENIZATION, INITIAL COIN OFFERINGS, AND SECURITIES LAW

Given that blockchain—as a contracting technology—is most effective when it is self-enforcing (i.e., does not require real-world compliance) and that it is capable of being self-enforcing only if the assets exchanged are both digital and on the blockchain, it is not surprising that the earliest uses for blockchain were digital currencies like Bitcoin that existed on the blockchain. This may also explain why blockchain has been more successful at promoting trade in ownership of digital art (via nonfungible tokens, or NFTs) rather than of physical art.

Simple trade in digital assets soon led to more complicated financial contracts over digital assets. The assets remained digital and on the blockchain, but the trades were more complicated mappings of states onto trades than simple one-way transfers. Among the most notable of the complex contracts were ICOs (Catalini & Gans 2020), specifically the use of utility tokens and their presale to finance new firms.

To understand ICOs, one must first understand tokenization. Blockchains are ledgers that keep track of digital assets. The digital asset could be a currency like Bitcoin, or it could be the digital key (i.e., right) to some other asset, including a digital asset. This digital right is sometimes called a token. The digital rights connected to tokens come in different types. One is a utility token, which gives rights to a digital service or product. Another is a security token, which gives rights to profits from (and perhaps voting control over) a blockchain-based firm.

One example of a utility token is Filecoin, a token issued by an eponymous firm. Filecoin the firm issues tokens called Filecoins (abbreviated FIL), which give holders the right to store a certain quantum of data on storage devices connected to its network. An example of security tokens is the DAO, a form (organized by smart contract) on the Ethereum network. The DAO gets its name from the concept of a decentralized autonomous organization, a firm created and governed by code written on a blockchain. The DAO sold security tokens in exchange for Ether, the currency of the Ethereum network. Owners of the DAO tokens had rights to vote on how the DAO would use any capital that it raised and to the stream of profits that might flow from the DAO's investments.

The challenge that firms such as Filecoin often face is that they need upfront capital to produce the widgets they later want to sell. In Filecoin's case, before it could make functional the tokens that conferred storage rights, it needed to build out its network and secure storage. That required an investment.

ICOs build on the idea of initial public offerings (IPOs). In an IPO, a firm whose equity is worth more with additional capital raises that capital by selling some of its equity to third parties. ICOs do something similar. They sell utility tokens to investors before the tokens can be exchanged for a product and use the capital raised to produce that product. Investors can then sell the tokens to future customers to obtain an investment return. (In theory, one could conduct an ICO using a security token. That would look like an IPO on the blockchain. But it appears the bulk of ICOs have sold utility tokens.) Interestingly, the denomination of the capital raised in an ICO is not fiat currency but rather a blockchain currency, usually Ether.

Filecoin used an ICO to raise $257 million in 2017. Many other blockchain-related start-ups followed its example. At one point, the ICO market rivaled the size of the venture capital market in the United States (Davydiuk et al. 2019).

This boom in ICOs led to a rapidly growing literature on a range of related questions, such as, should ICOs be treated as securities for the purpose of securities laws? Should preregistration with the SEC be required? How can that be enforced? What are the implications of this for capital formation and market efficiency?

To see why these issues arise, it is important to understand the value of blockchain technology in providing new forms of investment vehicles and hence financing opportunities. New blockchain apps could go down the traditional route of seeking angel investment, then venture capital investment, and then being acquired by a tech giant like Google or having an IPO. But that process is so slow, taking nine years for the median company, even for tech IPOs (Ritter 2021). By contrast, ICOs can be completed in a few short weeks. The problem is that, being a new technology, blockchain attracts naïve investors that are easily convinced to part with their money. The risk of fraud is quite high, evinced by the fact that very few ICOs have produced still-viable firms.

This familiar debate over the appropriate regulation of investment financing misses the bigger picture with ICOs. ICOs offer a glimpse of a whole range of other financial innovations that are possible with tokenization—the process of creating tokens on a blockchain. Tokenization permits the creation of a whole range of financial instruments, some new and some simply better, that have great potential in a range of financial markets.

To see how this works, start with a utility token, like Filecoin's FIL token. Filecoin the firm promised to issue 200 million FIL tokens but no more. It planned to set up a digital data-storage market where people would buy and sell storage, but both buyers and sellers would have to use FIL tokens for transactions. This means the total value of all FIL tokens would be equal to the total revenue in that part of the disk-storage market. The value of a single token is the total revenue divided by the number of tokens issued. If investors buy some tokens, they are making a bet on revenue in the disk-storage market: They can resell them to people who want to buy storage on the network (Holden & Malani 2022). Because only 10% of minted tokens were offered for sale to investors, the fact that Filecoin was able to raise $257 million means investors valued Filecoin's future revenues at $2.57 billion.

Classic equity, by contrast, is a bet on net present value of all future profits: total revenue minus costs. Filecoin did not sell equity, but it could have issued tokens that function like classic equity. It could have put all its equity in a holding company and required that shares in the holding company be bought and sold only with FIL tokens. The value of FIL tokens would then have been equal to the value of Filecoin company shares, i.e., the net present value of its future profits. This small shift—requiring that trade in equity rather than rights to storage be done with tokens—would have caused the value of tokens to be equal to the value of all of Filecoin's equity.

The ability to peg the value of tokens to the item that can be traded with the token opens the door to some interesting possibilities—notably the concept of shadow equity and providing market-based incentives on decentralized measures of performance. For example, tokenization would allow use of tokens to invest or bet on specific components of a company. Take Pfizer as an example. It has a whole portfolio of drugs, and buying stock in Pfizer is a bet on the whole portfolio. But suppose Pfizer issues 1 million Xtandi tokens and says that all future purchases of Xtandi, a prostate cancer drug, will have to be done with those tokens. Then the aggregate value of those tokens is the value of revenue from sales of Xtandi. An investor who buys those tokens will be betting on both Food and Drug Administration approval of and the total market demand for Xtandi. In other words, tokens allow investors to bet on a specific part of Pfizer's portfolio.

This means that it is possible to have publicly traded assets that are tied to a much more granular level of performance within an organization. It obviously does not mean that it is possible to have equity securities in the impact of a single worker—but it is conceivable to have such securities for divisions of companies, or even teams within divisions.

6. RETHINKING TAXATION LAW IN THE CONTEXT OF DISTRIBUTED LEDGER TECHNOLOGY

The anonymity provided by digital currencies that are built on blockchain technology—like Bitcoin or Ether—at least in principle allows for sophisticated yet easily implementable tax-avoidance strategies that could potentially do significant damage to the revenue base of advanced economies. These strategies would not be possible without the anonymity provided by DLT, but they also seem difficult for tax authorities to stop without banning cryptocurrencies altogether.

The underground or black economy is already a significant source of lost tax revenues—even in countries like the United States with strong rule of law and effective institutions. Even there, an estimated 8.4% of gross domestic product (Schneider et al. 2010) is part of this black economy. These are transactions on which sales and income taxes are not paid.

One of the dark sides of blockchain technology is that it could expand this black economy—possibly significantly. Moreover, rather than consisting of people paying wages or service fees in cash under the table for relatively small transactions (for instance, when paying a plumber or babysitter), DLT may well provide the means for tax evasion for large transactions. Indeed, given the costs involved in executing an effective tax avoidance strategy using blockchain, it might be particularly well suited to, and used for, large transactions.

As we pointed out in a 2018 *New York Times* article (Holden & Malani 2018), such a strategy might look like the following: Imagine an individual owns three electronic addresses—we can think of them as Bitcoin accounts. Call them A, B, and C. Now suppose the individual informs the tax authority [say, the US Internal Revenue Service (IRS)] that she owns A. But she does not tell the IRS that she owns B and C. Because of the anonymity inherent in DLT, this may be feasible.

Now consider the following transaction. The individual in question buys one Bitcoin at $15,000 and parks it at electronic address/account A. They expect the price to go up, and let us suppose it does so a few hours later; when a Bitcoin is worth $15,500, they send that Bitcoin to account B and then on to account C.

Suppose the asset (Bitcoin) continues to appreciate in price (this is the only interesting case because losses are not taxable). Imagine that a few months later, the Bitcoin is now worth $25,000, and recall that it is sitting in account C. Now our individual can send it from account C to account A and tell the IRS the following: "I sold a Bitcoin to an anonymous counterparty at B back at $15,500 (a gain of $500) and just now bought a Bitcoin from another anonymous counterparty at C for $25,000." As a result of this set of transactions, the individual owes taxes on capital gains of just $500, rather than the $10,000 they actually made from the rise in the value of Bitcoin from $15,000 to $25,000. As we pointed out,

> The I.R.S. can observe all the transactions between A, B and C on the Bitcoin blockchain, but it cannot disprove that B and C are "arm's length" counterparties (that is, independent and not colluding). Rules in the United States that require financial institutions to verify the identity of address holders do not solve the problem, because as far as the I.R.S. knows, B and C could have been set up by a foreign institution that does not comply with such rules. (Holden & Malani 2018)

Notice that in the example we have used, we imagined that the asset in question was a unit of cryptocurrency itself—and that is not a trivial market. But, in fact, essentially any asset could be

made part of the kind of scheme we outlined. For instance, the same scheme would work perfectly well with equity securities (stocks) or debt securities (bonds). The key is to make sure that the anonymity provided by cryptocurrency is preserved. A straightforward way to do this is through tokenization, of the kind we discussed in Section 4. The assets being traded could be placed in holding companies, a finite number of new tokens could be issued, and trade of the company's equity could be restricted to those with the new token. In short, cryptocurrencies underpinned by blockchain technology make large-scale tax avoidance arguably much easier than it has been in the past, and this obviously presents major challenges for tax authorities around the world.

It is inconceivable that the IRS or any other competent major tax authority in another country would simply stand by and let there be large-scale, widespread tax avoidance in this manner. But what are the possible ways to prevent this from the IRS's point of view?

The most direct attack on the problem is to break anonymity by getting the exchanges through which accounts are held to ex ante via Know Your Customer (KYC) rules or ex post via subpoenas divulge the legal owner of those accounts. Indeed, In November 2017, the IRS persuaded a US federal judge to order Coinbase, a popular Bitcoin exchange, to reveal the identity of the holders of more than 14,000 accounts. Those accounts were responsible for nearly nine million transactions. Whether this kind of approach, especially on foreign exchanges, will continue to work and stand up to legal scrutiny is unclear.

A more brute-force approach would be to try to ban cryptocurrencies, but this would throw out the useful financial (and other) innovations that have come with them and would be a drastic step.

The two most likely routes toward tax compliance on cryptocurrencies are (*a*) some form of international cooperation or (*b*) switching the tax mix away from income taxes and toward value-added or consumption taxes.

The scheme we outlined above, and potential alternative tax avoidance schemes that rely on the anonymity of blockchain technology, involved the possibility that accounts B and C could have been set up by a foreign financial institution that does not comply with KYC rules. Obviously, if all countries were willing to enforce KYC rules, then such schemes would no longer be possible. It may be that some form of international treaty could be negotiated that would lead to this outcome, but one must be rather skeptical of that occurring.

For instance, several jurisdictions, such as the Cayman Islands and the British Virgin Islands, already facilitate regular (i.e., non-DLT-related) tax avoidance, despite international pressure on them not to do so. Even Ireland has served as a low-tax jurisdiction, which has allowed many major companies—Apple might be the most famous example—to dramatically lower their tax burden, although not avoid corporate income taxes altogether. There is currently a push with the Organization for Economic Co-operation and Development to reach an agreement on taxing digital platforms such as Google and Facebook more effectively, and eliminating transfer-pricing arrangements that facilitate tax arbitrage, but to date no such treaty has been agreed to. International cooperation that requires all nations to participate on these matters is not easy.

The second possibility is for countries to shift their own tax mix away from income taxes and toward taxing consumption. The anonymity of blockchain technology effectively allows one to hide income from tax authorities—say, through the kind of scheme we described above. Consumption, in contrast, cannot be hidden in this way (or any other, really). Thus, one response to increased use of income-shielding technologies would be to reduce income taxes and raise value-added taxes (VAT). Indeed, in the United States, where there are no VAT, this might be an appealing option in any event, because economists generally agree that VAT are less distorting than income taxes. In countries like the United Kingdom and many in Europe, where VAT rates are already significant—sometimes around 20%—this pivot from income taxes to VAT is much less feasible. It would be only a partial solution in some jurisdictions.

7. DIGITAL CURRENCIES AND INTERNATIONAL LAW

The rise of cryptocurrencies such as Bitcoin and Ether has, understandably, attracted the attention of many, including more than just speculators. Most notably, this includes large public companies such as Facebook (now Meta), credit card companies such as Visa and Mastercard, and even nation-states that have explored the possibility of issuing their own digital currency (Eichengreen & Viswanath-Natraj 2022). And despite some roadblocks to the establishment of private digital currencies (e.g., by Facebook, a case study we explore below), it is increasingly clear that public digital currencies will emerge, and it is reasonably likely that more private digital currencies will also emerge in coming years.

The first thing to note about existing cryptocurrencies is that they are significant in scale. For instance, in December 2018, the market capitalization of all such currencies was US$400 billion, equivalent to 11% of the M1 measure of the US money supply (the most liquid instruments). If a company like Facebook, Alphabet/Google, or Apple launched a more mainstream digital currency, then private currencies would be serious competitors to fiat currencies issued by nation-states. Consumers might be equally happy to use Facebook tokens in lieu of dollars when shopping on Amazon or traveling abroad.

Indeed, in mid-2019, Facebook announced plans to launch its own digital currency called Libra, with several partner companies such as credit card providers being part of the Libra Association—although there have been substantial changes to the scope and membership of the project since that time. On December 1, 2020, it was renamed Diem.

The stated goal of Diem was to "enable a simple global payment system and financial infrastructure that empowers billions of people," with the Diem/Libra (2020) white paper noting that an extraordinary number of people around the world remain unbanked: "1.7 billion adults globally remain outside of the financial system with no access to a traditional bank, even though one billion have a mobile phone and nearly half a billion have internet access" (citing Demirgüç-Kunt et al. 2018).

The original Libra design was for a multicurrency stablecoin, meaning that Libra coins would be bought by individuals exchanging traditional fiat currency for coins. One of Libra's distinguishing features was that all of these funds would be held in reserve (likely invested in government bonds or other low-risk securities), and therefore the coin would be fully backed. This would provide confidence to coin holders that a kind of bank run on the coins was unlikely, and other holders would know that as well. Thus, making solid backing, in the language of game theory, common knowledge would prevent a run on the coins, hence making them stable.

The Diem White Paper notes that "a key concern that was shared was the potential for the multicurrency Libra Coin (≈LBR) to interfere with monetary sovereignty and monetary policy if the network reaches significant scale in a country (i.e., ≈LBR becomes a substitute for domestic currency)." This has led to Diem initially permitting only three single-currency stablecoins (USD, EUR, and GBP), with more currencies possible over time.

We do not think this is the most serious concern with a multicurrency stablecoin, launched by one of the world's most valuable companies (with a network of partners to boot), that has the potential to be widely adopted and account for a nontrivial portion of transactions globally. A more pressing issue is that, although the rules of the Libra Association required full asset backing, they gave discretion to the association as to the composition of currencies in the basket. Imagine, then, that Facebook was unhappy with a regulatory decision of a particular country. It could simply reweight the basket of currencies that back its stablecoin by selling the currency of that particular country and buying the currency of other countries. This would cause a significant devaluation of the currency of the country that offended Facebook. That, in turn, would discourage countries from regulating Facebook.

All of this raises important questions about the interaction between cryptocurrencies or stablecoins and traditional fiat currencies. Does the existence of these alternative means of exchange, if pervasive enough, imply a loss of control over monetary policy for a central bank? What implicit monetary policy arises in equilibrium competition between private and traditional currencies? Should nation-states adopt their own digital currencies as a defense mechanism, and would doing so be effective?

As a useful starting point in thinking about currency competition, Schilling & Uhlig (2019) develop a model of currency competition between traditional fiat currency and a cryptocurrency like Bitcoin. In their model, two types of infinitely lived agents can either produce or consume. In fact, they alternate between the two so that there is no "double-coincidence of wants," and hence a medium of exchange (currency) has value. They assume that there is a cryptocurrency and a fiat currency whose supply is controlled by a central bank.

The authors assume that the central bank follows an inflation-targeting regime for its currency, whereas the cryptocurrency grows deterministically. Schilling & Uhlig's analysis applies to any cryptocurrency but, as they emphasize, does not immediately translate to utility tokens or stablecoins (like Libra/Diem).

They show that when a cryptocurrency and traditional currency coexist as currencies used for exchange, i.e., in a currency equilibrium, it must be that the crypto's expected future price expressed in "dollars" equals its current price, otherwise the cryptocurrency has more value for speculation than for exchange. Perhaps most interesting, there are meaningful implications for the monetary policy of the central bank. If the crypto price in a currency equilibrium changes, e.g., owing to a change in crypto supply, then this necessitates a response from the central bank—potentially requiring it to inject dollars into the money supply to meet its inflation target. In a different scenario, where the inflation target is met, central bank policy can influence the price of the cryptocurrency. The key point is that the two currencies do not simply sit side-by-side as alternatives to one another but interact in important ways.

What the Schilling–Uhlig analysis does not cover is what might be the worst-case scenario for national fiat currencies. That is something like the original Libra design—a multicurrency stablecoin with the prospect of widespread adoption—simply crowding out traditional currency. Given that cryptocurrencies are already, by the measure discussed above, approximately 11% of the US money supply, a compelling stablecoin launched by a company like Amazon that already accounts for a large volume of transactions could push that 11% up significantly. In that case, the United States could plausibly lose its status as the global reserve currency, ending what macroeconomists call the exorbitant privilege (Eichengreen 2011), or the ability to print money without significantly sacrificing its purchasing power, pushing US interest rates significantly higher, and thereby impacting both the private and public sector in a meaningful, negative way.

One defense mechanism against this is for nation-states to develop their own digital currencies, and several countries have explored this—most notably China (where private digital wallets WeChat Pay and Alipay account for an extraordinary volume of domestic transactions) and Singapore, which is a democracy but with an unusual degree of central control. Other countries, like Australia, have begun to consider such a central bank digital currency but have been extremely cautious and do not look poised to act (Pandey 2021).

8. BLOCKCHAIN, VOTING, AND ELECTION LAW

A nascent area where blockchain is being used is in voting. DLT has already begun to be used for security purposes in online voting. Online voting is permitted in 32 US states—with West Virginia becoming the first state to permit mobile voting in a federal election, in 2018 (Fowler 2020).

Although not a focus of this section, DLT is also used for voting in decentralized autonomous organizations (DAOs). DAOs are smart contracts that create a corporation whose charter and rules are codified in code. Just as shareholders in a traditional corporation might vote for directors, owners of the DAO may vote for which projects the DAO will undertake. This voting, in turn, may be conducted and recorded on the DLT.

To assess the potential for using blockchain to improve voting, it is helpful to examine current problems with voting in the real world and then identify those problems that DLT can help address and those it cannot. This exercise identifies the fruitful avenues for research or application of DLT for voting.

One concern with elections is how political boundaries are drawn. Criticisms of gerrymandering concern the gaming of these boundaries by incumbent parties to reduce the voting power of those who support a party's challenger. A second concern is who is allowed to vote in a jurisdiction. Old literacy requirement for voting, the change in voting age during the Vietnam era, and recent questions about whether noncitizen residents can vote belong in this category of concern. Unfortunately, DLT voting cannot address these boundary and eligibility problems. The majority vote getter in an election, even one run on a blockchain, must be seated by a real-world judiciary and executive branch. Just because someone who is not otherwise eligible to vote votes in a DLT-tracked election does not mean these real-world authorities will seat them.

A third concern with voting is low turnout in locations where voting is optional. Turnout in US presidential elections rarely tops 60%; elections for lower offices have even worse turnout (Am. Pres. Proj. 2022). The problem with low turnout is that elections will not truly represent a majority of the voting-eligible population's preferences. Whether DLT-based voting will change that depends on the reason turnout is low. If the problem is that the return to voting is low, e.g., because only the probability of being the marginal voter is low, DLT will make no difference. If the problem is that the cost of voting is high, then online voting without DLT would accomplish what DLT could do. Only if the reason turnout is low is that voters do not trust that their votes will not be ignored or tampered with will DLT increase turnout. If this lack of trust is a material reason for low turnout, DLT could raise turnout—whether or not the voters' concerns were unfounded. This is obviously a salient issue after the 2016 and 2020 US elections.

An opposite concern with voting is too high a turnout, or in simpler terms, ballot stuffing. This could involve dead people voting or unauthorized voting by third parties in the name of actual voters. It might appear that DLT could help address this problem, because blockchains are associated with innovative cryptographic methods to improve security. However, those cryptographic methods can be—and are—used for identity verification outside the blockchain context. Therefore, one does not need to record votes on a blockchain to deploy better digital security to stop fraud.

A fifth concern is that voters vote for the wrong person. There are two flavors of this criticism, though blockchain can help with neither. One is that people vote for people that are not the best choice for them. This logic motivates some to question why low-income populations vote for Republicans. The other flavor worries about voter intimidation or instrumental voting: People might vote for a candidate because votes are not private or because voting allows them to gain favor in their social setting, rather than because they like that candidate based on the voter's internal preferences. Unfortunately, DLT voting likely cannot help with either flavor of criticism. People are as likely to vote for the wrong person or for the wrong reasons (social status) on the blockchain as outside of it. It might appear that the anonymity blockchain provides—the same anonymity that enables tax evasion—would address problems of intimidation. However, many of those benefits can be achieved by creating encrypted identities for traditional electronic voting.

So what substantial value does DLT have for voting? If there is a concern that votes are not counted or counted accurately, blockchain has a unique solution. With DLT voting, a cast vote

cannot be discarded. It cannot be deleted or interpreted differently than cast. This is because DLT records are effectively immutable (and publicly known, even though voters' identities are not). Although one might have thought that this attribute of DLT voting would have value only in elections in low-capacity states where ex post election fraud was rampant, the recent US presidential elections suggest that it may even be a concern there.

9. CONCLUSION

Blockchain technology has in some ways, like the market value of cryptocurrencies such as Bitcoin, been overrated. But the fundamental technology behind DLT—an immutable, trustworthy digital ledger with bleeding-edge encryption—could have far-reaching implications for a range of economic transactions, political processes, and legal doctrines. In this sense, DLT is likely to be an ongoing presence in a range of discussions in the social sciences broadly understood.

DLT's key attribute is immutability, which makes it possible to contract more broadly and in a way that materially limits renegotiation. This expands the range of economic transactions that can be conducted, and conducted outside of firms. It also expands the amount and quality of information available to courts.

The anonymity that is often bundled into DLT creates problems for tax and regulatory compliance. However, changes such as KYC rules that materially impinge on the anonymity offered by blockchain render the technology not useless but with fewer use cases.

As with any new technology, from the steam engine to genetic engineering, there are benefits and costs. The nature and timing of regulation can affect the net benefit and thus transformative potential of the new technology. This process is just beginning with blockchain, which has not even hit its teenage years.

DISCLOSURE STATEMENT

The authors are not aware of any affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

LITERATURE CITED

Aghion P, Fudenberg D, Holden R, Kunimoto T, Tercieux O. 2012. Subgame-perfect implementation under information perturbations. *Q. J. Econ.* 127(4):1843–81

Aghion P, Holden R. 2011. Incomplete contracts and the theory of the firm: What have we learned over the past 25 years? *J. Econ. Perspect.* 25(2):181–97

Alaska Packers' Assoc. v. Domenico, 117 F. 99 (9th Cir. 1902)

Am. Pres. Proj. 2022. *Voter turnout in presidential elections*. Accessed Jan. 31, 2022. **https://www.presidency.ucsb.edu/statistics/data/voter-turnout-in-presidential-elections**

Antonopolous AM. 2017. *Mastering Bitcoin: Programming The Open Blockchain*. Newton, MA: O'Reilly Media. 2nd ed.

Catalini C, Gans JS. 2020. Some simple economics of the blockchain. *Commun. ACM* 63(7):80–90

Coase R. 1937. The nature of the firm. *Economica* 4(16):386–405

Davydiuk T, Gupta D, Rosen S. 2019. *De-crypto-ing signals in initial coin offerings: evidence of rational token retention*. Work. Pap., Carnegie Mellon Univ., Pittsburgh, PA

Demirgüç-Kunt LK, Singer D, Ansar S, Hess J. 2018. *The Global Findex Database 2017: measuring financial inclusion and the fintech revolution*. Rep., World Bank Group, Washington, DC. **https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20full%20report_0.pdf**

Diem/Libra. 2020. *White paper v2.0*. Accessed April 6, 2022. **https://diem-developers-components.netlify.app/papers/the-diem-blockchain/2020-05-26.pdf**

eBay Inc. v. MercExchange, LLC, 547 U.S. 388 (2006)

Eichengreen B. 2011. *Exorbitant Privilege: The Rise and Fall of the Dollar and the Future of the International Monetary System*. Oxford, UK: Oxford Univ. Press
Eichengreen B, Viswanath-Natraj G. 2022. Stablecoins and Central Bank digital currencies: policy and regulatory challenges. *Asian Econ. Pap.* 21:29–46
Fowler A. 2020. Promises and perils of mobile voting. *Election Law J.* 19(3):418–31
Grossman SJ, Hart OD. 1986. The costs and benefits of ownership: a theory of vertical and lateral integration. *J. Political Econ.* 94(4):691–719
Hart O, Moore J. 1990. Property rights and the nature of the firm. *J. Political Econ.* 98(6):1119–58
Hart O, Moore J. 2008. Contracts as reference points. *Q. J. Econ.* 123(1):1–48
Holden R, Malani A. 2018. Why the I.R.S. fears Bitcoin. *New York Times*, Jan. 22. **https://www.nytimes.com/2018/01/22/opinion/irs-bitcoin-fear.html?smid=pl-share**
Holden R, Malani A. 2021. *Can Blockchain Solve the Hold-Up Problem in Contracts?* Cambridge Elements Law Econ. Politics. Cambridge, UK: Cambridge Univ. Press
Holden R, Malani A. 2022. An examination of velocity and initial coin offerings. *Manag. Sci.* **https://doi.org/10.1287/mnsc.2022.4314**
Maskin E, Tirole J. 1999a. Two remarks on the property-rights literature. *Rev. Econ. Stud.* 66(1):139–49
Maskin E, Tirole J. 1999b. Unforeseen contingencies and incomplete contracts. *Rev. Econ. Stud.* 66(1):83–114
Moore JR, Repullo R. 1988. Subgame perfect implementation. *Econometrica* 56(5):1191–220
Nakamoto S. 2008. *Bitcoin: a peer-to-peer electronic cash system*. **https://bitcoin.org/bitcoin.pdf**
Pandey S. 2021. Australia weighs Central Bank digital currency, crypto rules. *Bloomberg*, Dec. 7. **https://www.bloomberg.com/news/articles/2021-12-07/australia-weighs-central-bank-digital-currency-crypto-reforms**
Ritter JR. 2021. *Initial public offerings: median age of IPOs through 2020*. Work. Pap., Univ. Fla., Gainesville
Schilling L, Uhlig H. 2019. Some simple Bitcoin economics. *J. Monet. Econ.* 106:16–26
Schneider F, Buehn A, Montenegro CE. 2010. *Shadow economies all over the world: new estimates for 162 countries from 1999 to 2007*. Policy Res. Work. Pap. 5356, World Bank, Washington, DC
United States v. Lizarraga-Tirado, 789 F.3d 1107 (9th Cir. 2015)
Williamson OE. 1971. The vertical integration of production: market failure considerations. *Am. Econ. Rev.* 61(2):112–23
Williamson OE. 1975. *Markets and Hierarchies: Analysis and Antitrust Implications*. New York: Free
Williamson OE. 1979. Transaction-cost economics: the governance of contractual relations. *J. Law Econ.* 22(2):233–61