The Blockchain and Increasing Cooperative Efficacy

MALAVIKA NAIR AND DANIEL SUTTER

Bitcoin is a cryptocurrency based on open-source software created by the pseudonymous Satoshi Nakamoto in 2009. The Bitcoin currency has attracted considerable attention, first among computer scientists and later among businesspeople and the general public. It is being accepted by an increasing number of merchants worldwide; the current market price of Bitcoins is now widely available; and thousands of people worldwide used more than 1.46 terawatt hours of electricity in Bitcoin mining in 2015. Economists have noted the potential for Bitcoin or perhaps a rival cryptocurrency to supplement or even displace fiat currencies. Regulators and policy makers have taken note as well, sometimes responding with regulations not well informed by the realities of Bitcoin (Brito and Castillo 2016).

The Bitcoin payment system is based on the blockchain, a permanent record of all transactions maintained on users' computers. The blockchain is a distributed ledger that not only allows the Bitcoin payment system to operate but also opens possibilities for new forms of contracting and cooperation. Tech writers, bloggers, private corporations, government organizations, and economists have begun to notice the economic implications of the blockchain, recognizing that it may far exceed that of Bitcoin itself. As Melanie Swan points out,

Malavika Nair is assistant professor at the Manuel H. Johnson Center of Political Economy, Troy University. **Daniel Sutter** is Interim Director of the Manuel H. Johnson Center of Political Economy, Troy University.

The Independent Review, v. 22, n. 4, Spring 2018, ISSN 1086–1653, Copyright © 2018, pp. 529–550.

> More important, blockchain technology could become the seamless embedded economic layer the Web has never had, serving as the technological underlay for payments, decentralized exchange, token earning and spending, digital asset invocation and transfer, and smart contract issuance and execution. Bitcoin and blockchain technology, as a mode of decentralization, could be the next major disruptive technology and worldwide computing paradigm (following the mainframe, PC, Internet, and social networking/mobile phones), with the potential for reconfiguring all human activity as pervasively as did the Web. (2015, vii)

In this paper, we offer a framework for evaluating and integrating the various different consequences and impacts of the blockchain for the economy. We apply the public-goods argument for government and a comparative institutional approach to assess the government's and the voluntary sector's ability to produce different individual public goods. The public-goods argument holds that government provision (via taxes and regulation) will be frequently chosen given the limitations of voluntary provision—namely, the free-rider problem. In a comparative institutional framework, however, the imperfections of government must be compared against the effectiveness of voluntary mechanisms. People's willingness to contribute voluntarily to public goods and various mechanisms' ability to convert willingness into effective provision have been labeled "cooperative efficacy" (Cowen and Sutter 1999).

We interpret the blockchain as a technological innovation that has the potential to increase cooperative efficacy significantly and consequently to reduce the size and scope of government. Toward this end, we provide examples of already existing and potential applications of the blockchain that illustrate cases of increasing voluntary cooperation outside of government-provided public goods. Specifically, we identify three mechanisms stemming from technological properties of the blockchain that help create trust between potential trading partners by replacing the need for a third-party watcher or enforcer of rules: a publicly verifiable ledger, open entry, and decentralization of power through a widely distributed mining network as well as the open-source nature of the underlying code. The blockchain thus allows the creation of trust without the need for a concrete third-party watcher who has vested authority and impartiality that the potential traders must trust.

We do not discuss the factors affecting whether the scope of governments will actually expand or contract. Blockchain innovations will reduce the need for government to provide certain public goods or types of regulation on behalf of citizens, but this does not mean that the scope of government will immediately shrink. Entrenched interests benefiting from government provision or the regulatory status quo could conceivably block privatization or deregulation regardless of the blockchain's potential. The blockchain does, however, offer significant potential for de facto or unauthorized privatization of current government activities, as perhaps best illustrated by the potential for Bitcoin or another cryptocurrency to serve as a medium of exchange without

government permission. Thus, the blockchain and its applications could also bring about significant disruption of the status quo despite entrenched interests' efforts. We focus, however, primarily on their tremendous potential for voluntary society.

The first section provides a summary of the existing public-goods argument. It is followed by a brief explanation of the blockchain. In the third section, we describe current as well as potential examples of the blockchain in uses that illustrate increasing cooperative efficacy. We close by considering potential problems in the fourth section and then drawing broader conclusions.

Cooperative Efficacy and the Public-Goods Argument

The public-goods argument for government recognizes that many of the core functions of maintaining civilized society, such as enforcing property rights, adjudicating disputes, and protecting against criminals and foreign invaders, have the characteristics of a public good—namely, nonrivalry and nonexcludability. Apprehension and punishment of criminals benefit all citizens in the community, regardless of whether they contribute to law enforcement. Sufficient institutional protection of property to enable people to trade with one another, invest in capital goods, or conserve durable assets and natural resources can lead to spillover prosperity. Voluntary efforts at providing public goods typically fail to provide the efficient level due to free riding, suggesting the use of coercion to increase the supply. The fact that people generally benefit from these goods suggests that the value of coercion can be justified on a consequentialist basis (Taylor 1987; Schmidtz 1991).

Beyond the fundamental functions of government, citizens may choose to have the government supply other goods and services with public-good characteristics, following the distinction between the productive state and the protective state (Buchanan 1975). A citizen evaluating the provision of public goods from a consequentialist perspective may consent to government coercion to collect taxes in order to increase the supply of public goods. The public-goods argument does not require that voluntary cooperation be unable to supply public goods or that government provision be perfectly effective. Citizens make a comparative analysis and direct government to supply the public goods that it more effectively provides.

The term *cooperative efficacy* refers to the joint effectiveness of voluntary mechanisms (Cowen and Sutter 1999). Cooperative efficacy involves a community's or group's ability to engage in collective action. The extent of voluntary cooperation depends on individuals' willingness to contribute to a common cause and to effectively do so by overcoming the free-rider problem as well as by achieving lowered transactions costs. Solving these two problems separately or in some combination of the two may conceivably come about in various ways (as elaborated in Cowen 1988).

Mechanisms for achieving exclusion include creating a club or tying a public good to a private good, defining property rights over previously unowned resources, making technological and entrepreneurial innovations, and making effective emotional appeals

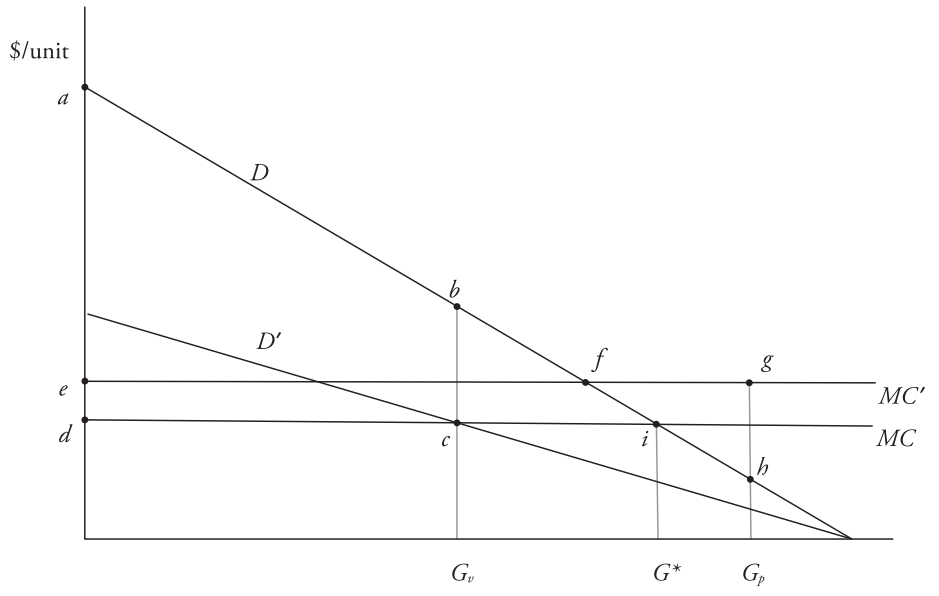
(Cowen 1988). The blockchain, we argue, represents an unprecedented technological and entrepreneurial innovation that lowers transactions costs and overcomes free-riding problems by creating trust, for reasons explained later in this paper. This innovation brings about an increase in cooperative efficacy that manifests itself through different dimensions, depending on the specific application. Regardless, everything else being equal, an increase in cooperative efficacy makes citizens more likely to choose private provision over government provision, and thus cooperative efficacy is related to the optimal size and scope of government.

We illustrate the choice for the specific case of the provision of a public good, but the examples considered later also involve instances of regulation. Figure 1 offers a graphical presentation of a choice by citizens between imperfect alternatives for public-good provision, meaning that neither voluntary provision nor government provision satisfies the Samuelson efficiency condition. Demand or the marginal social value of the good is captured by *D,* and *MC* represents the minimum marginal cost of providing the good. We provide concrete versions of inefficiency for both voluntary and government provision; other varieties of inefficiency can be substituted without affecting the general point. The effective demand falls short of *D* under voluntary provision due to free riding, but provision is efficient given this demand. Let the effective demand be *D′,* the exact location of which depends on the extent of free riding or, alternatively, the amount of cooperative efficacy. The voluntary provision quantity is denoted G_v. Under public provision, we assume that costs are excessively high, *MC′,* due to public-sector inefficiency in production or procurement and that the quantity supplied, G_p, exceeds the efficient level, G^*, due to special-interest rent seeking on the part of the suppliers. Citizens evaluating the institutional choice in instrumental terms compare the net benefits under each form of provision. With voluntary provision, the net benefits would be area *abcd,* and under public provision the net benefits equal area *afe* minus area *fgh*.

We are interested in how an increase in cooperative efficacy alters this choice, which figure 2 illustrates. An increase in cooperative efficacy increases the effective market demand. Initially let the level of cooperative efficacy be such that the effective market demand is *D′* and the level of supply is *G′,* at the intersection with marginal-cost curve *MC*. The increase in cooperative efficacy increases the effective market demand from *D′* to *D″,* increasing the voluntary provision quantity to *G″*. The net benefits of voluntary provision increase by the area *abcd*. The increase in cooperative efficacy, holding the efficiency of government provision constant, makes citizens more likely to choose voluntary provision for this good.

We contend that the blockchain's distributed ledger of actions will increase the efficacy of voluntary cooperation across a wide range of activities. The various applications of the blockchain discussed in the next section involve different elements of cooperative efficacy, in particular entrepreneurial innovations and reduced transactions costs. We see the distributed ledger of the blockchain as fundamentally creating a new way to generate trust. But rather than dwelling on the exact interpretation of each application, we think that the term *cooperative efficacy* keeps the focus on the important point: how the increased potential for voluntary cooperation leads to a wide-ranging

Figure 1
Voluntary versus Government Provision of Public Goods

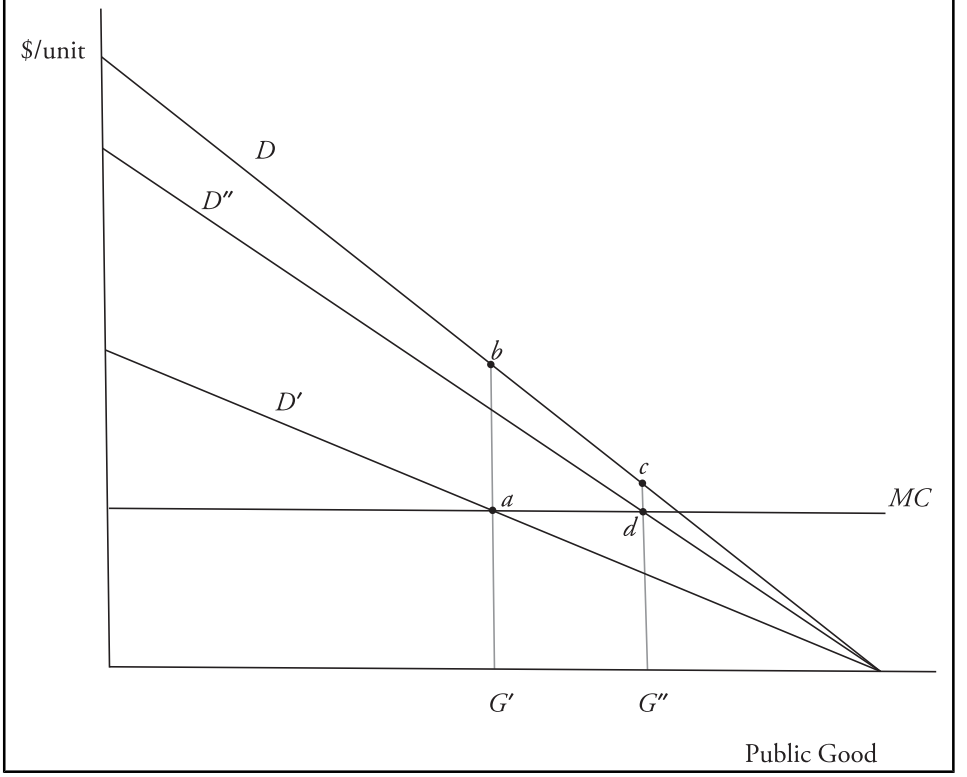


reassessment of the tasks assigned to government. Figure 3 illustrates exactly how an increase in cooperative efficacy affects the choice of institutions for provision or, alternatively, the optimal scope of government. The horizontal axis of figure 3 arrays different public goods (or potential tasks for government, such as regulation), each of which could be provided through either voluntary cooperation or public provision, *PP*. The vertical axis graphs the net benefits possible for each public good through each institution. We order the public goods based on the net difference between net benefits of public provision and net benefits of voluntary provision, with the first public goods on the horizontal axis representing the core functions of government. The optimal number of public goods provided through government is initially *G**, obtained where the net benefits from government provision, curve *GP,* equal the net benefits from voluntary cooperation, curve *VC*. The blockchain increases cooperative efficacy and the net benefits of voluntary cooperation to *VC′*. As a result, the optimal scope of government provision falls to *G***.

The Blockchain and Its Mechanisms of Trust

The blockchain was first introduced in a paper published by Satoshi Nakamoto in the context of Bitcoin in 2010. Bitcoin is an online or digital currency utilizing cryptography that is inseparable from the concept of the blockchain. However, the basic

Figure 2
Impact of Increasing Cooperative Efficacy

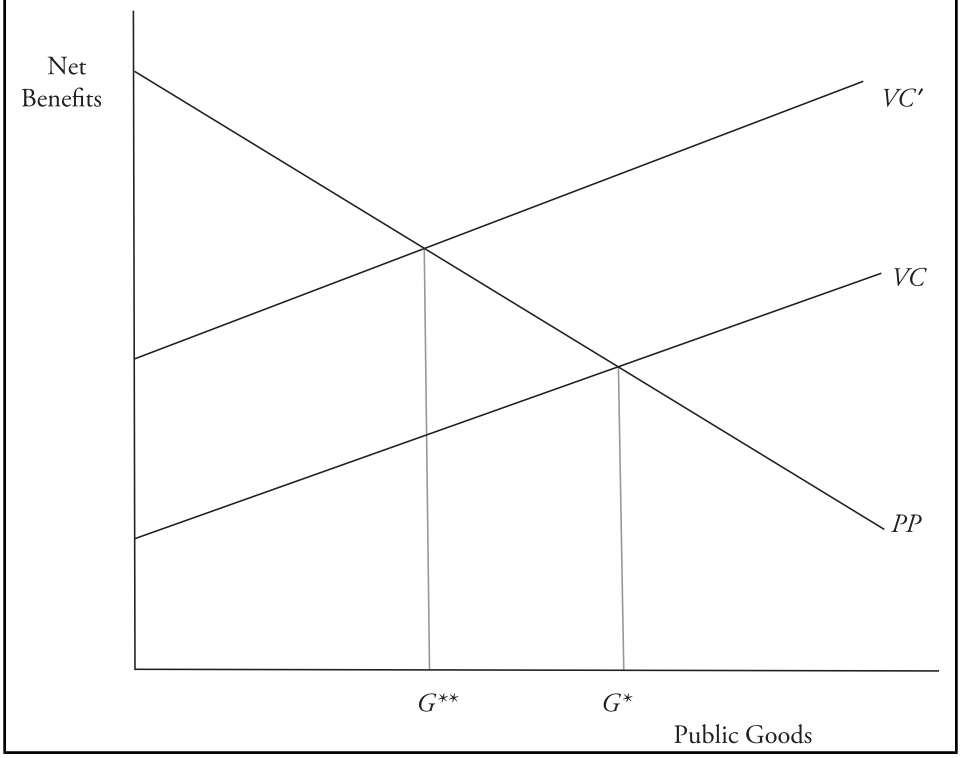


blockchain structure extends past Bitcoin and has been applied to other so-called cryptocurrencies. Although the Bitcoin blockchain is currently the most well developed and widely used blockchain, other systems less widely used today or currently under development may overtake the Bitcoin blockchain in the future.[1]

The blockchain is first and foremost a publicly available ledger of all trades or transfers of Bitcoin among its users anywhere in the world. This complete ledger is maintained by each node or "miner" of Bitcoin on his or her computer. The underlying code rewards miners with newly created Bitcoin for maintaining this ledger and verifying transactions (Antonopoulos 2014). The network of miners takes the place of a third-party account keeper or auditor who would keep a centralized ledger. Anyone is able to look up any transfer or transaction that takes place on the blockchain. A publicly verifiable, distributed ledger of information thus engenders transparency and is a crucial first mechanism that leads to the creation of trust.

1. One such network currently gaining popularity that also happens to be less resource intensive is Ethereum. For the rest of this paper, however, unless otherwise noted, we use the term *blockchain* as synonymous with *Bitcoin blockchain*.

Figure 3
Cooperative Efficacy and Voluntary Cooperation



The second mechanism that leads to the creation of trust is open entry and a decentralized network of miners. The blockchain has very low barriers to entry: anyone in the world can choose to become a Bitcoin "miner" and maintain a copy of the entire ledger. The computing power is thus voluntarily supplied by miners who choose to "mine" Bitcoin, and each miner has the blockchain stored on his or her machine. This feature adds an extra layer of protection from appropriation because becoming a miner is completely voluntary and not limited to any geographical area, which creates trust in the eyes of would-be users. Miners are geographically dispersed, thus making the chance of manipulation or a concerted effort to overtake the blockchain less likely.

The blockchain elicits this voluntary supply of computing power by rewarding miners with newly created Bitcoin. Hence, this system of a public ledger is incentive compatible and self-sustaining as long as there are profits to be made by mining Bitcoin (meaning that the costs of mining stay below the expected Bitcoin price). For the near future, miners will essentially be providing computing power to the blockchain as a voluntary contribution. The blockchain protocol caps the supply of Bitcoin at 21 million and in this way creates scarcity and hence value in the eyes of miners as well as users of Bitcoin, providing the system with a means to compensate the contributors without taxing users.

The third mechanism that leads to the creation of trust relates to the open-source nature of the blockchain code and decision-making process. Although a literature analyzing the economic significance of open-source software already exists, certain unique interactions between the nature of Bitcoin itself and the fact that it is embedded in open-source code have important economic implications. We analyze these interactions in the next section.

Proprietary software or code is naturally under the control of one person or a group of persons. Just like privately provided services, proprietary-software owners earn monetary profits only when people buy their goods. This process, along with competition from other providers, creates an incentive to constantly innovate and provide better-quality services when it comes to most goods. Open-source goods, in contrast, are not under the ownership of any one person or group; rather, they rely on the voluntary contributions of many people to constantly provide improvements to the source code for no monetary gain. The question of what incentives must be present for people to voluntarily provide services for which they receive no payment rather than just to free-ride off the services has received attention from economists (Johnson 2002, 2006; Lerner and Tirole 2002, 2005a, 2005b; Lerner, Pathak, and Tirole 2006; Boldrin and Levine 2009). However, one overlooked advantage of the Bitcoin blockchain's being based in open-source software is that it promotes trust among would-be new users because they don't have to be afraid of appropriation or manipulation of the source code by the proprietor in his or her own favor.

Not only is the source code publicly available and verifiable by anyone, but also any change to the code must be approved via consensus by an existing group of preapproved senior members of the blockchain and is necessarily publicly visible to all users. Although the threat of cheating or manipulation still exists, the potential cost of losing users who simply can stop providing computing power or inputs is large and increases with the number of users. Hence, not only are developers restricted from unilaterally manipulating the code (always a possibility with proprietary code), but the incentive to do so is also minimized unless such manipulation is undertaken as an end-game strategy.[2]

In addition, developers are able to gain monetary profits by building proprietary applications off the open-source code. This ability increases their incentive to ensure that the source code as well as the blockchain in the case of Bitcoin are functioning well, thus further reducing the incentive to manipulate the code secretly.[3] These features help foster trust among new and old users alike, who can rely on the public nature of the code as an ultimate check against manipulation.

2. Hence, two layers of transparency are built into the blockchain—publicly verifiable data as well as publicly visible source code, both of which help increase trust and viability in the eyes of its users. For more on the role of transparency and improving governance mechanisms within government, see Hood and Heald 2006 and Besley 2007.

3. For example, all the members of the Bitcoin Foundation (development community) are also typically members of the Bitcoin community. In addition, each one owns a proprietary application of Bitcoin.

Another unique feature of open-source software is the decision-making process inherent in it. Unlike private goods or proprietary software, no one person has ultimate decision-making power in the case of open-source software. Although at first glance this very openness may seem to be inefficient or to yield chaotic results, there are definite advantages to it, especially when applied to an application such as Bitcoin and the blockchain. The specific lack of monopolized power as well as the public nature of all decisions made help give legitimacy to the specific product being supplied.[4]

For these reasons, the blockchain promotes the creation of trust and hence leads to increased cooperative efficacy. How exactly the increased cooperative efficacy comes about depends on the particular application and its ability to solve the free-rider problem or to lower transactions costs or some combination of the two.

The Blockchain and Voluntary Alternatives to Government Regulation and Provision of Public Goods

We now offer examples of the potential use of the blockchain to substitute for functions currently performed by government. Some examples are currently functional, and some are applications under development. It is not possible to predict the various ways in which future applications may be developed and enhance cooperative efficacy, but these currently existing applications—even though some are nascent—help shed light on the blockchain's potential.

Digital Currency

The most well-developed application of the blockchain is Bitcoin itself. Bitcoin is a digital currency that allows users to transfer value tokens electronically. The total supply of Bitcoin is capped at 21 million, an arbitrary number that is hardwired into the open-source code. There are currently 16.78 million Bitcoins in circulation.[5] The limitation of the total supply of Bitcoin creates scarcity and helps generate value in the mind of would-be users of Bitcoin. Bitcoins are generated as reward for nodes or users "mining" them, which in turn is how verification of all transactions on the blockchain takes place (Nakamoto 2010; Antonopoulos 2014). This verification process also increases in complexity the more Bitcoins have been generated. In this way, the process of increasing Bitcoin supply mimics the increase in the supply of gold because it increases only at a decreasing rate.

4. An illustration of this property is provided by the recent debate and disagreement that played out in the Bitcoin community regarding a new version of the Bitcoin code named Bitcoin XT. Whereas senior developers were keen for blockchain nodes to switch over to the newly written Bitcoin XT code (which would increase the block size from one megabyte to eight megabytes, thus increasing transaction-processing power in the network), the decentralized mining network did not accept the new code, so it has not been successful despite the senior developers' wishes.

5. As at January 2, 2018. See Blockchain.info/charts/total-bitcoins.

All digital transfers of money suffer from potential double-spending problems because it is virtually costless to copy and reproduce digital files and data. One important role played by financial institutions such as commercial banks and central banks is that they take on the role of third-party watchers over transactions taking place. They thus help create trust in the eyes of users of digital money, who can be reassured that their money is not being appropriated or stolen or spent twice.

This is where the blockchain that powers Bitcoin comes in: it plays a role similar to the one played by third-party financial institutions that maintain ledgers of all financial transactions. The blockchain does the same thing, except on a publicly verifiable ledger that everyone can see; hence, the need for one institution that must be trusted is removed. In the case of money, this property becomes even more significant, for the risk of appropriation or devaluation of currency through creation of new money supply by the centralized issuer is ever present. By taking away the need for a single issuer of money supply, such as central banks, the blockchain increases cooperative efficacy in a large way when it comes to currency.

Further, the fact that Bitcoin is meant primarily to be a currency implies that the existence of trust is especially important for it to be adopted and used. Because currency or money is used primarily as a medium of exchange, its utility is derived from utility in exchange, not through consumption. Thus, the existence of trust becomes crucial, just as in the case of other media of exchange: Why should someone accept or hold Bitcoin if he does not know that someone else will accept it in exchange from him later? With the absence of high-consumption value, being able to trust the currency plays a large role in its adoption.

The use of Bitcoin as a medium of exchange illustrates how cooperative efficacy enabled by the blockchain can change the public perception of the need for government control or regulation. The quantity of any medium of exchange must be controlled, and when an individual or organization has the ability to create the medium, the potential for new or essentially counterfeit issue to debase the value of current holdings exists. Fiat currencies dominate the world today, arguably because governments have recognized and captured the benefits accruing to their position as the supplier of specie. But privately supplied monies would also face this problem, and a lack of public trust in a for-profit bank or supplier of currency may also explain government fiat currencies. Clearly the occasional case of hyperinflation illustrates that control can be greatly abused, but the dominance of government currencies may also reflect public perception that government control provides superior protection against potential opportunism by a for-profit supplier (Taub 1985).

Beyond solving the double-spending problem without creating the need for a trusted ledger keeper, Bitcoin offers several further advantages. First, it allows for safer and more private transfer of information despite the fact that the ledger is publicly available. The safety and privacy are due to the use of cryptography that allows for encoding sensitive private information so that it remains private yet is able to uniquely identify users through a unique public key. Another advantage is significantly lowering

transactions costs by doing away with an intermediary who must keep a record of all transactions. Bitcoin as a payment system offers great promise in allowing inexpensive transfers of value or currency digitally across time and space, integrating millions of persons currently excluded from the global financial system.[6]

The blockchain's cooperative-efficacy innovation with regard to digital payments reduces transactions costs and is a new technological and entrepreneurial means of solving the double-spending problem. The veracity of a payments system can now essentially be crowd-sourced, eliminating the need for a trusted third party to keep the ledger or control the money supply.

Contract Enforcement

All commercial society relies on people's ability to carry out trade in both simple and complex scenarios, one-shot trades as well as repeat dealings. However, trade requires trust in the face of the ever-present threat of cheating and reneging on contracts. Government provision of contract enforcement creates a mechanism to support exchange: the threat of government force applied against a party that breaches the contract. Government's enormous capacity for violence can compel performance even by large economic actors, creating trust among market participants in contract enforcement and contributing to an institutional environment that encourages investment in capital and economic growth. Furthermore, the threat of overwhelming government force may reduce the frequency of conflictual contract enforcement and ensure application of due process in advance of the use of force for contract enforcement.

Although the enforcement of contracts is commonly assumed to lie solely within the state's ambit, there are several well-documented cases of such enforcement being provided voluntarily (Landa 1981, 1994; Greif 1989, 1993; Benson 1990, 2005; Bernstein 1992; Stringham 2002, 2003; Powell and Stringham 2009; Nair 2011). In the case of voluntary provision of governance, the question of how or why potential traders would trust one another enough in the presence of the threat of cheating becomes relevant. Although the mechanisms differ from case to case, there is usually some common ground between trading parties that allows them to build trust and partake in mutually beneficial trade. For example, relying on pre-existing reputations or a common religious, ethnic, or caste background as well as functioning in a small clublike setting where members are in close touch with one another are two common mechanisms used to enforce contracts in the absence of government-provided enforcement.[7]

6. For other recent views on Bitcoin and cryptocurrency in general, see Harwick 2016 and Luther 2016.

7. For more on the role of reputation and reciprocity for contract enforcement, see Fehr, Gächter, and Kirchsteiger 1997; Bohnet, Frey, and Huck 2006; and Macleod 2007.

The blockchain in this case boosts cooperative efficacy through the innovation of enabling the crowd-sourced veracity of the ledger. Most significantly, this innovation eliminates the need to regulate or watch the watcher to ensure the third party's impartiality. A third party keeping the ledger could always collude with one of the transacting parties to manipulate the ledger or manipulate the ledger for his own benefit. Specifically, the blockchain supports the creation of trust among strangers because of the publicly verifiable ledger, which cannot be manipulated by any one party.[8]

Automated Contracts

Most trade and commerce can ultimately be reduced to bilateral and multilateral contracts between trading partners. Some types of trade require simple contracts, whereas others require more complex formulations, especially when the passage of time and space are involved. For example, spot transactions where goods are exchanged for money at the same time and space require simple contracts. Certain types of trade and contracts lend themselves to being digitized and executed completely by automated machines or other programmable devices, rendering them into so-called smart contracts.

The automated vending machine is one such example of a smart contract being executed. The machine is programmed to dispense food items and beverages automatically once the appropriate amount of money has been inserted by the customer. The machine and the simple program substitute for the third-party human being, who would typically have to be present in order to execute the trade and make sure that the correct amount of money has changed hands and that no cheating has taken place. Similarly, the blockchain can be used in conjunction with smart-contract devices, where the transactions taking place require a verifiable or traceable record.

One such example of smart contracts being executed using programmable devices as well as blockchain technology is Slock.it, which is currently developing devices (small computers that attach to physical assets, such as doors of apartments or cars or bicycles) that will allow owners of idle physical assets (such as apartments or cars) to rent them out directly to renters.[9] Websites or services such as Airbnb currently provide a platform for renters and owners to find one another and be able to trade rentable space. The website itself plays the part of a trusted third party and keeps a verifiable record of all transactions taking place. It thus facilitates trades that would not have taken place in its absence. For although it is possible for renters and owners to trade directly with one another, in

8. The arguments in this paper apply only to public blockchains, where decisions are made by true public consensus and anyone can become part of the consensus process according to the code, such as the Bitcoin blockchain. In contrast, in private or consortium blockchains, decision-making power is in the hands of only one or a few predetermined entities.

9. See the Slock.it website at https://Slock.it.

a world of imperfect information and a lack of perfect certainty, it becomes difficult to trust and trade with strangers. With this smart-contract technology, Airbnb helps increase cooperative efficacy by permitting trade to take place through the creation of a safe and trustworthy platform.

A company such as Slock.it that manufactures hardware that directly records trades and payments that are uploaded on the blockchain and are then publicly verifiable by anyone takes this idea one step further. It does away with the need for a third-party neutral platform such as Airbnb by making use of the publicly verifiable and trustworthy blockchain, thus enhancing cooperative efficacy. The company Slock.it profits from providing the hardware and its upkeep, not from verifying and maintaining a ledger of transactions and acting as an enforcer of contracts.

The innovation to cooperative efficacy involved here is probably best seen as a reduction in transactions costs, similar to trusted sharing platforms such as Airbnb. The blockchain also adds the element of distributed or crowd-sourced trust in place of any third-party platform at all.

Regulation of Corporations

The aggregation of resources in a business organization combined with the vesting of decision rights over these resources in management creates a vulnerability to opportunism. The potential for and consequences of opportunism in the modern economy as well as the perceived inadequacy of purely contractual mechanisms for controlling opportunism create a demand for government legal and regulatory control over corporations generally and over financial institutions (banks, investment companies, insurance companies) in particular. The legal oversight we have in mind here involves protections against fraud, such as the provisions governing an initial public offering of stock for a corporation, the release of accounting data and financial statements, and the financial soundness of banks and insurers (backed up by deposit insurance and guarantee funds). Government oversight typically goes well beyond this basic assurance against a complete fraud, but the demand for such oversight provides an important foundation and justification for more extensive controls.

As a consequence, the potential for a distributed ledger through the blockchain would increase the relative performance of voluntary mechanisms significantly. Financial resources can be misappropriated or embezzled by persons with discretionary control. Centralized ledgers contribute significantly to this fraud risk. Manipulating the transactions ledger (e.g., cooking the books) increases the potential for managers to misappropriate these resources and seems critical for large-scale embezzlement. Discretionary control over both the ledger and the assets creates the potential for large-scale fraud. Contractual remedies exist for this problem, such as turning to independent accountants to keep or audit the ledger and having a board of directors approve expenditures. And the remedies could be viewed as a purely private, contractual matter between investors and companies, with investors free to require assurances against fraud

before they invest. The accounting profession and the rules of accounting practice represent ways to maintain a trustworthy third-party ledger, to ensure against manipulation of the transactions ledger to hide embezzlement or misappropriation.

Clearly, the blockchain's distributed ledger reduces the discretion of persons with control over resources in a business. Because all transactions are publicly visible, top management can no longer secretly approve expenditures that benefit themselves at the company's interest. A ready paper trail, publicly available to all in the blockchain, exists to help recover diverted resources. And the potential for collusion between auditors and management is greatly reduced or eliminated altogether. More radically, the blockchain offers the potential for a new form of corporation or business, with much greater effective decision rights (or greater protection of decision rights) being exercised by stockholders as opposed to reliance on boards of directors, which could be coopted by management.

The distributed-ledger innovation in this case eliminates the potential collusion between the keeper of the ledger and the persons with decision rights over resources. Elimination of this otherwise very hard to regulate potential for opportunism ends up increasing cooperative efficacy. The blockchain also reduces the transactions costs of allowing stockholders to make more decisions for the corporations they own.

Assurance Contracts

The contracting possibilities created by the blockchain may make feasible the complicated and extensive contracts for the provision of public goods. The challenge of providing public goods can be broken down into an assurance problem and a prisoner's dilemma problem (Schmidtz 1987, 1991). The assurance problem involves assuring individuals that if they contribute to the provision of a public good, others will as well, and the prisoner's dilemma reflects potential free riding or the small reduction in quantity provided in response to one person withholding her contribution. David Schmidtz (1987) argues that assurance contracts, or a contingent agreement to contribute when a threshold number of people sign the contract, can greatly facilitate the market supply of public goods, especially given the empirical evidence that free riding is not as prevalent as theory predicts (Andreoni 1995). Alex Tabarrok (1998) demonstrates the potential for dominant assurance contracts, where a public-goods entrepreneur can share some of the profit from a provision via a signing bonus, thus giving potential customers an incentive to contribute.

Assurance contracts can potentially involve thousands (or millions) of signees, but transactions costs have limited their practical application. Transactions costs have imposed two hurdles: (1) the need to identify and reach potential contributors and (2) a mechanism to ensure automatic execution of payments when the contributions threshold is reached. The Internet's lower transactions costs have already allowed implementation of large-scale assurance contracts. For example, crowd-funding platforms such as Kickstarter, Indiegogo, and RocketHub use threshold funding for

projects. In these cases, potential funders rely on the trust of the platform to hold their money and automatically make payment if a project's funding target is met.

The blockchain's contracting potential will only further facilitate the operationalization of assurance contracts. Contributions to a public good can be held in escrow via the blockchain, thus substantially reducing fees charged by third-party platforms. Bitcoin platforms Lighthouse and Truthcoin are experimenting with implementing both assurance contracts and dominant assurance contracts (Torpey 2015). Cooperative efficacy is enhanced here through a reduction of transaction costs for large-scale assurance contracts and through the innovation of allowing automatic payments without relying on a trusted escrow party when the contract condition is met.

Dispute Resolution

The examples discussed so far relate to how the blockchain increases cooperative efficacy when it comes to specific types of contracts or commercial applications. However, the blockchain can also be directly extended to applications that deal with dispute resolution, thus helping create trust between potential trading partners in a way that can be applied to myriad types of contracts or goods.

One such application, Bitrated, allows two trading partners to hire mutually agreed-upon "trust agents" who act as arbitrators over the contract between them.[10] A contract that requires a payment to be made once a good or service has been delivered requires that the two parties trust each other, especially when the trade is taking place between strangers or across geographical distance. Bitrated allows the payment to be deposited into an escrow account, which releases funds only once the good has been received. Because the escrow is recorded on the blockchain, it is publicly visible and cannot be appropriated by anybody until the buyer himself releases the funds. In case of a dispute, the trust agent is asked to intervene and must come up with a decision about who must get the funds. However, the trust agent does not have full control of the escrow account and the money in it; releasing the funds requires both his signature and the signature of one other trader (buyer or seller) subject to the contract. The blockchain allows the creation of such a multiple-signature escrow account that is publicly visible, hence eliminating the risk of appropriation by the trust agent.

The trust agents, in turn, are rated on a trust scale, and traders get to choose among different trust agents based on their scores. Anyone is free to become a trust agent, and traders can choose any trust agent they wish to hire as long as their trading partner agrees on the person as well. In this way, a marketplace for reputation and trustworthiness is created. Only those trust agents who have a reputation for being fair and trustworthy when it comes to arbitration and dispute resolution will get hired again and again. Those trust agents who gain poor reputations for arbitration will be weeded out of the system. The blockchain technology allows for the creation of trust through

10. See the Bitrated website at http://www.Bitrated.com.

the elimination of the possibility that the arbitrator is able to cheat and appropriate the funds for himself.

The trust agents are free to set their own fees and can compete with one another not just on the basis of reputation but also on the basis of fees charged. A current look at the Bitrated website statistics reveals more than 1,300 registered trust agents and more than 9,000 registered traders.

Property-Title Registry

The blockchain can be used to record and store various kinds of information and data. One such application is the storage of property deeds or who owns what. For instance, the blockchain can be used to create a land-title registry for different countries or jurisdictions. The country of Honduras, among others, is currently testing this application.[11] The advantages of such an effort are huge, especially in developing countries, where the formal property-titling system is often inefficient or corrupt or both.

In the absence of strong property rights and the ability to easily establish who owns what, the potential for trade and commerce using that property greatly diminishes. The ability to easily trade and invest in property leads to economic growth, the lack of which is still a widely prevalent problem in developing countries (De Soto 2003). The blockchain offers a way around this problem because land titles can be easily digitized and uploaded onto the blockchain. Thus, the ownership or property right is established and publicly verifiable by anyone who wishes to buy, sell, or invest in that land in the future. This verifiability would help create trust in existing titles and promote economic activity through enhanced cooperative efficacy even though the formal titling system in the country may be susceptible to corruption and appropriation of property.

Potential for Problems

The great potential for Bitcoin and the blockchain arises from the seeming impossibility of hacking the system and consequently from their innovative way of generating trust via a distributed ledger. But the protocol may potentially be compromised in different ways. We do not take a position on the technical claims we describe, which are beyond our area of expertise, but simply discuss the potential for Bitcoin to be vulnerable to different types of attacks and the extent to which such attacks compromise the potential for the blockchain to produce a significant increase in cooperative efficacy. We believe that forms of social cooperation enabled by the blockchain should prove more robust to some of the pitfalls of a cryptocurrency or payments system. Further, the open-source nature of the code and the consensus process involved in changing the code further insulate the system from potential predation.

11. See, for example, Higgins 2015 and Shin 2016.

The consensus-based nature of the blockchain protocol would require a majority of nodes within the system to accept new blocks. Open entry and thousands of miners across the world initially made the prospect that any individual, group, or organization would attain control over 51 percent of the nodes an impossibility (Dowd and Hutchinson 2015). However, the remuneration of Bitcoin miners favors the assembly of coalitions of miners, and one such coalition has in fact at least temporarily surpassed the 51 percent threshold (Dowd and Hutchinson 2015). A 51 percent attack is one example of a potential problem with the protocol.

Large mining coalitions threaten Bitcoin in other ways. Itay Eyal and Emin Gun Sirer (2014) contend that a number of threats can emerge even at less than the 51 percent control level. For instance, a miners' coalition with less than 51 percent of the computing power could engage in predatory practices against other miners. Further, a 51 percent coalition could exercise its power in ways other than double-spend attacks, which would destroy trust in the system and be self-defeating by debasing the value of Bitcoins possessed by the coalition. This destruction of trust is significant: some Bitcoin proponents argue that a 51 percent attack will not occur because it would not be in the self-interest of miners so heavily invested in Bitcoin to destroy trust in the system. Eyal and Sirer (2014) argue, however, that a mining coalition could essentially engage in price discrimination, imposing differential transactions fees for certain users, which may not destroy trust in the system.

Probably the most sure and significant consequence of a dominant mining coalition is the loss of trust promised by the distributed-ledger system. Even if a dominant mining group behaves, Bitcoin users could do nothing more than simply hope that the group will not use its position in an antisocial manner. Existing national fiat currencies are already dependent on trust in central banks. Economists can make arguments about why central banks should not debase national currencies, and yet episodes of hyperinflation still happen. Much of the interest in Bitcoin is due to the existence of a currency that no central bank or other entity can compromise.

We do not believe that these threats will do more than delay briefly the increase in cooperative efficacy from the blockchain, mainly because of the temporary and transitory nature of mining coalitions and the limited duration of a possible 51 percent attack. Although Kevin Dowd and Martin Hutchinson (2015) contend that Bitcoin is a natural monopoly, large-scale mining coalitions are not more productive than small-scale operations in terms of returns per unit of computing power. Coalitions are formed merely to reduce the variance of the return for risk-averse miners. But mining pools are voluntary, and the central-processing-unit power is not physically controlled by the coalition. As a consequence, a mining pool can dissolve as rapidly as it forms. Presumably, many miners join a pool to reduce the variance of returns to mining and will exit if the pool attempts double-spend attacks and undermines trust in and the value of Bitcoin. Thus, the duration of attacks is likely to be finite and in practice relatively short.

The inherent instability of a mining coalition and the short duration of an attack also limit the extent of harm to the blockchain, particularly in social cooperation

applications. In essence, a double-spend attack would merely result in a fork in the blockchain and not overwrite the history of transactions to date; moreover, the date and time of the initiation of the attack will be observable. The fork from the attack could easily be overwritten by the senior developers to exclude that part of the blockchain, effectively isolating and disconnecting it from the rest of the blockchain. An attack could last only as long as the attackers are able to hide their takeover or fool the rest of the network. However, once again the public nature of the code ensures that such an attack cannot be kept secret for very long, certainly not for a sustained period of time. Hence, the incentives attracting attackers to potential private gain from long-term manipulation are minimized, so such manipulation would make sense only if undertaken as an end-game strategy. If thousands or millions of persons enter into an assurance contract to provide a public good, these records would not be lost or rewritten; the contract would still be available on the blockchain.

The open-source code at the basis of the blockchain also affects the vulnerability of social cooperation. The Bitcoin Foundation provides governance of the open-source code. Thus, the blockchain actually combines two layers of protection against centralized attack: the distributed ledger and the open-source code. Open source protects users in two ways—from a designed flaw and from later manipulation. The developer of a proprietary blockchain might hide a Trojan horse deep in the program to allow centralized attack or to overwrite the blockchain to date—say, reassigning title to properties registered on the blockchain. Or the proprietor might manipulate the source code in his favor once the system is adopted and in use. With open source and distributed governance, however, these problems disappear.

The ability of any one contributor to the open-source code to slip in a Trojan horse is low—no developer can unilaterally change the code, and senior members of the Bitcoin Foundation must approve the change and would also have to be duped. As a consequence, the incentive for developers to try slipping in a Trojan horse—rather than building proprietary applications off the open-source code to make money—is diminished as well. With open-source code, users can recognize emerging problems with the blockchain and can collectively make changes to prevent the problem. For instance, whereas Dowd and Hutchinson (2015) contend that Bitcoin mining is a natural monopoly and that this monopoly will inevitably lead to concentration of computing power in coalitions that can execute a 51 percent attack, Eyal and Sirer (2014) claim that an adjustment of the code would eliminate the financial incentive for mining coalitions to form. If the code were proprietary and contained a flaw or an intentional feature that could lead to centralized control, correcting the problem would pose a more difficult challenge.

Finally, the threats to Bitcoin and the blockchain seem to target cryptocurrency and payments applications more than social cooperation applications. A 51 percent attack can be recognized when it occurs and is likely to be short-lived, and the blockchain up to the time of the attack will be preserved. Entirely virtual manipulations will be able to be reversed. For instance, suppose A manages to transfer all of B's

Bitcoins to his account. A's ability to benefit from this attack depends on his ability to exchange the Bitcoins for real goods and services before the attack ends. The speed of the real transactions is relevant to the ability to benefit from an attack. Consider in this regard some of the social cooperation applications. The ledger of a business or registry of land titles prior to the attack will still exist. It will take more time to sell land or extract resources from a business. Suppose A gets the title to B's home transferred during an attack. The attack would have to end before A can contact the local authorities and have B removed from the property based on the bogus title. As a consequence, the gain from mounting a 51 percent attack against social cooperation applications of the blockchain would appear to be significantly limited relative to the gains from attacking a cryptocurrency.

Conclusions

The blockchain has emerged simultaneously with the cryptocurrency Bitcoin and at the same time as many other innovations in social cooperation through the Internet, smart phone apps, and social media. Technological innovations threaten to overwhelm economic understanding. We have offered an integrating perspective on the ongoing innovations. We are witnessing a remarkable increase in cooperative efficacy, or the ability to solve problems of social cooperation through voluntary mechanisms. The distributed ledger of the blockchain is a huge component of this innovation. The exact details of the shock to cooperative efficacy are still being worked out, with many innovations occurring simultaneously. But an increase in cooperative efficacy, ceteris paribus, increases the attractiveness of voluntary means of providing public goods and regulation relative to government provision.

The Bitcoin blockchain protocol represents a first attempt at a distributed, collaborative system of this nature. Even should fatal flaws in the protocol emerge and cause Bitcoin to fail, as Dowd and Hutchinson (2015) fear, the problems will represent an opportunity to learn and avoid flaws in a future system. Learning would allow the creation of an improved distributed ledger. The long-run conclusion that a distributed ledger promises to significantly reshape the optimal scope of government seems justified, even if there may be a few missteps on the journey.

Good government is itself a public good. Monitoring government programs for waste, blocking rent-seeking legislation that benefits some at the expense of the rights and wealth of others, and even becoming informed about political and economic issues provide benefits to all citizens as a group. That good government is a public good generates a paradox for the public-goods argument: government is needed because voluntary cooperation is inadequate to supply a sufficient quantity of public goods, and yet government is unlikely to deliver as intended if voluntary cooperation is inadequate and fails to produce good government as well (Lee 1989).

The increase in cooperative efficacy due to the blockchain might also enhance the private supply of constraint of government, in what Melanie Swan (2015) calls

"Blockchain 3.0." For example, distributed ledgers might help document and detail actions taken by elected representatives and bureaucrats, making the granting of crony favors much easier to discover and penalize politically. Whether the blockchain reduces the optimal size of government would depend on the relative impact of cooperative efficacy on the voluntary provision of good government versus the provision of traditional public goods.

References

Andreoni, James. 1995. Cooperation in Public-Goods Experiments: Kindness or Confusion? *American Economic Review* 85, no. 4: 891–904.

Antonopolous, Andreas M. 2014. *Mastering Bitcoin*. Sebastopol, Calif.: O'Reilly Media.

Benson, Bruce L. 2011 [1990]. *The Enterprise of Law*. Oakland: Independent Institute.

———. 2005. The Spontaneous Evolution of Cyber Law: Norms, Property Rights, Contracting, Dispute Resolution, and Enforcement without the State. *Journal of Law, Economics, and Policy* 1, no. 2: 269–348.

Bernstein, Lisa. 1992. Opting out of the Legal System: Extralegal Contractual Relations in the Diamond Industry. *Journal of Legal Studies* 21, no. 1: 115–57.

Besley, Tim. 2007. *Principled Agents? The Political Economy of Good Government*. Oxford: Oxford University Press.

Bohnet, Iris, Bruno S. Frey, and Steffen Huck. 2001. More Order with Less Law: On Contract Enforcement, Trust, and Crowding. *American Political Science Review* 95, no. 1: 131–44.

Boldrin, Michele, and David Levine. 2009. Market Structure and Property Rights in Open Source. *Washington University Journal of Law and Policy* 30:325–63.

Brito, Jerry, and Andrea Castillo. 2016. *Bitcoin: A Primer for Policymakers*. 2nd ed. Arlington, Va.: Mercatus Center.

Buchanan, James M. 1975. *The Limits of Liberty*. Chicago: University of Chicago Press.

Cowen, Tyler. 1988. Public Goods and Externalities: Old and New Perspectives. In *The Theory of Market Failure: A Critical Examination,* ed. Tyler Cowen, 1–26. Fairfax, Va.: George Mason University Press.

Cowen, Tyler, and Daniel Sutter. 1999. The Costs of Cooperation. *Review of Austrian Economics* 12:161–73.

De Soto, Hernando. 2003. *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere Else*. New York: Basic Books.

Dowd, Kevin, and Martin Hutchinson. 2015. Bitcoin Will Bite the Dust. *Cato Journal* 35, no. 2: 357–82.

Dwyer, Gerald P. 2015. The Economics of Bitcoin and Similar Private Digital Currencies. *Journal of Financial Stability* 17:81–91.

Eyal, Itay, and Emin Gun Sirer. 2014. Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *18th International Conference on Financial Cryptography and Data Security*, ed. Nicolas Christin and Reihaneh Safavi-Naini, 436–54. New York: Springer.

Fehr, Ernst, Simon Gächter, and Georg Kirchsteiger. 1997. Reciprocity as a Contract Enforcement Device: Experimental Evidence. *Econometrica* 65, no. 4: 833–60.

Greif, Avner. 1989. Reputation and Coalitions in Medieval Trade: Evidence on the Maghribi Traders. *Journal of Economic History* 49, no. 4: 857–82.

———. 1993. Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders' Coalition. *American Economic Review* 83, no. 3: 525–48.

Harwick, Cameron. 2016. Cryptocurrency and the Problem of Intermediation. *The Independent Review* 20, no. 4 (Spring): 569–88.

Heckman, Robert, Kevin Crowston, U. Yeliz Eseryel, James Howison, Eileen Allen, and Qing Li. 2007. Emergent Decision-Making Practices in Free/Libre Open Source Software (FLOSS) Development Teams. In *Open Source Development, Adoption, and Innovation*, ed. Joseph Feller, Brian Fitzgerald, Walt Scacchi and Alberto Stillitti, 71–84. New York: Springer.

Higgins, Stan. 2015. Factom Partners with Honduras Government on Blockchain Tech Trial. *Coindesk,* May 15. At http://www.coindesk.com/factom-land-registry-deal-honduran-government/.

Hood, Christopher, and David Heald, eds. 2006. *Transparency: The Key to Better Governance?* Oxford: Oxford University Press.

Johnson, Justin. 2002. Open Source Software: Private Provision of a Public Good. *Journal of Economics and Management Strategy* 11:637–62.

———. 2006. Collaboration, Peer Review, and Open Source Software. *Information Economics and Policy* 18:477–97.

Landa, Janet. 1981. A Theory of Ethnically Homogeneous Middleman Group: An Institutional Alternative to Contract Law. *Journal of Legal Studies* 10:349–62.

———. 1994. *Trust, Ethnicity, and Identity: Beyond the New Institutional Economics of Ethnic Trading Networks, Contract Law, and Gift-Exchange*. Ann Arbor: University of Michigan Press.

Lee, Dwight R. 1989. The Impossibility of a Desirable Minimal State. *Public Choice* 61, no. 2: 277–84.

Lerner, Josh, Parag Pathak, and Jean Tirole. 2006. The Dynamics of Open-Source Contributors. *American Economic Review Papers and Proceedings* 96:114–18.

Lerner, Josh, and Jean Tirole. 2002. Some Simple Economics of Open Source. *Journal of Industrial Economics* 52:197–234.

———. 2005a. The Economics of Technology Sharing: Open Source and Beyond. *Journal of Economic Perspectives* 19:99–120.

———. 2005b. The Scope of Open Source Licensing. *Journal of Law, Economics, and Organization* 21:20–56.

Luther, Will J. 2016. Bitcoin and the Future of Digital Payments. *The Independent Review* 20, no. 3 (Winter): 397–404.

Macleod, Bentley. 2007. Reputations, Relationships, and Contract Enforcement. *Journal of Economic Literature* 45, no. 33: 595–628.

Nair, Malavika. 2011. Enforcement of Nineteenth Century Banking Contracts Using a Marriage Rule. *Quarterly Review of Economics and Finance* 51, no. 4: 360–67.

Nakamoto, Satoshi. 2010. Bitcoin: A Peer-to-Peer Electronic Cash System. At https://bitcoin.org/bitcoin.pdf.

Powell, Benjamin, and Edward P. Stringham. 2009. Public Choice and the Economic Analysis of Anarchy: A Survey. *Public Choice* 140, nos. 3–4: 503–38.

Schmidtz, David. 1987. Contracts and Public Goods. *Harvard Journal of Law and Public Policy* 10:475–503.

———. 1991. *The Limits of Government: An Essay on the Public Goods Argument*. Boulder, Colo.: Westview Press.

Shin, Laura. 2016. Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto. *Forbes,* April 21. At http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#65db8bad6550.

Stringham, Edward P. 2002. The Emergence of the London Stock Exchange as a Self-Policing Club. *Journal of Private Enterprise* 17, no. 2: 1–19.

———. 2003. The Extralegal Development of Securities Trading in Seventeenth Century Amsterdam. *Quarterly Review of Economics and Finance* 43, no. 2: 321–44.

Swan, Melanie. 2015. *Blockchain: Blueprint for a New Economy*. Sebastopol, Calif.: O'Reilly Media.

Tabarrok, Alex. 1998. The Private Provision of Public Goods via Dominant Assurance Contracts. *Public Choice* 96, nos. 3–4: 345–62.

Taub, Bart. 1985. Private Fiat Money with Many Suppliers. *Journal of Monetary Economics* 16, no. 2: 195–208.

Taylor, Michael. 1987. *The Possibility of Cooperation*. Cambridge: Cambridge University Press.

Torpey, Kyle. 2015. Crowdfunding Public Goods with the Blockchain instead of the Government. At http://insidebitcoins.com/news/crowdfunding-public-goods-with-the-blockchain-instead-of-the-government/28904.

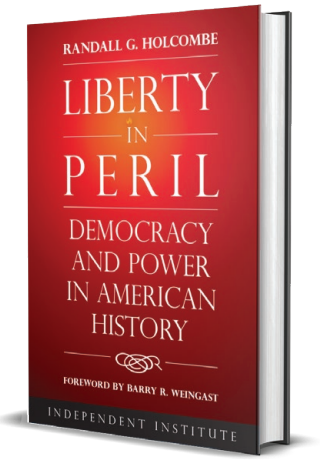
White, Lawrence H. 2013. Anti-fragile Banking and Monetary Systems. *Cato Journal* 33, no. 3: 471–84.

SUBSCRIBE NOW AND RECEIVE A FREE BOOK!

"***The Independent Review*** does not accept pronouncements of government officials nor the conventional wisdom at face value."
—**JOHN R. MACARTHUR**, Publisher, *Harper's*

"***The Independent Review*** is excellent."
—**GARY BECKER**, Nobel Laureate in Economic Sciences

Subscribe to ***The Independent Review*** and receive a free book of your choice such as ***Liberty in Peril: Democracy and Power in American History***, by Randall G. Holcombe.



Thought-provoking and educational, ***The Independent Review*** is blazing the way toward informed debate. This quarterly journal offers leading-edge insights on today's most critical issues in economics, healthcare, education, the environment, energy, defense, law, history, political science, philosophy, and sociology.

Student? Educator? Journalist? Business or civic leader? Engaged citizen? This journal is for YOU!

Order today for more *FREE* book options

SUBSCRIBE

The Independent Review is now available digitally on mobile devices and tablets via the Apple/Android App Stores and Magzter. Subscriptions and single issues start at $2.99. **Learn More.**

Download on the App Store | GET IT ON Google Play | Available on MAGZTER

INDEPENDENT INSTITUTE, 100 SWAN WAY, OAKLAND, CA 94621 • 1 (800) 927-8733 • ORDERS@INDEPENDENT.ORG