Cryptocurrency and the Problem of Intermediation

CAMERON HARWICK

The rise of cryptocurrency in the past decade is more than simply a technological feat; it is a real-world incarnation of a monetary system with numerous features that have existed to date only as thought experiments. As with any unprecedented innovation, bold claims are made for it. The boldest, perhaps, is the claim that cryptocurrency in general or Bitcoin in particular can or will supplant the current international regime of central-bank-issued monies.

The claim has some plausibility. Distributed technologies such as Uber and Airbnb are already rendering obsolete many established regulatory regimes, much to consumers' benefit. Because cryptocurrencies lack a central issuer, the hope is that they, too, will be able to grow outside of established regulatory structures until they become too big to ignore. Of course, the challenger faces a number of daunting hurdles before this goal becomes feasible. Existing regulatory structures are not totally avoidable. Bitcoin, in addition to the opposition it faces and will continue to face from established interests, also must overcome a number of technical and economic hurdles.

Bitcoin's purchasing-power volatility, on the order of history's most severe episodes of hyperinflation, is emblematic of these latter hurdles. In contrast to the narrow focus on stabilization that has characterized much of the literature thus far, this paper considers the institutional prerequisites of purchasing-power stability, economic efficiency, and sustained economic growth—namely, a market for financial intermediation. It is such a market that cryptocurrency entrepreneurs will find most difficult to operate outside existing regulatory regimes.

Cameron Harwick is a Ph.D. student and adjunct professor at George Mason University.

The Independent Review, v. 20, n. 4, Spring 2016, ISSN 1086–1653, Copyright © 2016, pp. 569–588.

After a brief introduction to the mechanism of cryptocurrency, this paper compares its development over the past several years to the development of fractional-reserve banking under a regime of gold redeemability. From there, drawing on the historical experience of gold, it explores the technical, legal, and economic hurdles that cryptocurrencies face in the future, focusing on the unique problems of financial intermediation in these currencies. Although cryptocurrencies have already established a niche for themselves as media of exchange, these hurdles will need to be overcome before cryptocurrencies can be competitive with—much less supplant—central-bank issues.

Finally, the paper evaluates some schemes to stabilize purchasing power by automatically adjusting the quantity of coins and concludes that the future progress of Bitcoin—and of cryptocurrency more generally—depends not only on the achievement of a more or less stable purchasing power, but also on the establishment of financial intermediaries whose cryptocurrency-denominated liabilities circulate as media of exchange. Although stability is certainly necessary to support a modern industrial economy, it is hardly sufficient: to achieve demand elasticity for a currency *outside* of a market of financial intermediaries is no foundation for economic growth and efficiency. Without such a market, Bitcoin remains in a sense "dependent" on other currencies such as the dollar.

What Is Cryptocurrency?

A cryptocurrency is a method of constituting virtual "coins" and providing for their secure ownership and transaction using a cryptographic problem. This problem is designed to be easy to verify but computationally difficult to arrive at a solution. Various cryptocurrencies use different functions for this purpose, the most common being a hash target, by which hashes are calculated so as to come in lower than a certain value.[1] The hash target (i.e., the difficulty of the problem) is adjusted every so often based on the total computing power on the network, which has the advantage of keeping the time between solutions more or less constant. Other protocols, such as Primecoin, provide for the problem by the calculation of large prime numbers. In theory, any hard-to-calculate but easy-to-verify function with easily adjustable difficulty would do.

This computationally intensive "proof of work" is the method by which transactions are verified as unique and trustworthy. To incentivize participation, transactors can include a transaction fee that goes to the first user to successfully verify it. This fee is optional in Bitcoin but mandatory in some others.

1. What follows is a brief account of the proof-of-work paradigm. For the sake of brevity, many technical details are elided. These details are unimportant for the paper's purposes, but they can be found in Nakamoto 2008. The details of the less common proof-of-stake paradigm (King and Nadal 2012) are somewhat different, but the security implications are largely similar. The economic implications are discussed in subsequent sections.

In addition, the network rewards verifiers with a certain number of coins after they have successfully verified a block of transactions. This process, called "mining," is the means by which the supply of coins on a network is expanded, and the adjustable difficulty ensures that computing advances will not affect the rate of expansion. As might be expected, the marginal cost of mining (mainly electricity) tends to equilibrate to the marginal benefit.[2] In Bitcoin's case, the reward for mining halves every 210,000 blocks verified, leading to a supply path over time with a positive first derivative that diminishes discontinuously to zero.[3] A great variety of supply schemes have been implemented by alternative cryptocurrencies, some of which are discussed in subsequent sections.

A coin itself is constituted by its transaction history on the network, going back to the block from which it was mined. Each input into a transaction points to the output of a previous transaction. This history is kept track of by every computer on the network in a continuously updating record called the "blockchain"—literally a chain of transaction blocks to which newly verified blocks are added. Because transaction records are public, anonymity is maintained only by keeping the account owners private. If there are competing blockchains among different users—for example, if two transactions are received in a different order by different users or if someone attempts to forge a transaction—the protocol defines rules by which only one is accepted. This method is quite secure, the more so as the protocol gains wider currency. Bitcoin and its close relatives will prefer the longest blockchain—that is, the one with the most computing power behind it. Thus, to forge a transaction, an attacker would have to make sure that his own blockchain was longer than the legitimate one, requiring him to have at his disposal more computing power than the total of the honest nodes.[4]

2. The marginal benefit of mining will include expectations of the cryptocurrency's future price, so when its value is expected to rise, the electricity costs can exceed the value of the coins mined. That this amount of electricity is very large is illustrated by the police raid of a Canadian Bitcoin miner's home in 2011 because his energy usage was consistent with the energy usage of the high-powered lamps used for growing marijuana ("Bitcoin Miners Busted?" 2011).

3. Starting with a reward of 50 coins per block, the supply path is described by the infinite sum $\sum(210{,}000 \times 50/2^i)$, which comes to 21 million. Because the hash target adjusts to keep the time between verified blocks more or less constant, each period i is about four years.

4. This possibility of forgery is known as a 51 percent attack. Although no attack has so far ever been successfully executed, the potential—at least for Bitcoin—is a matter of some debate. Kevin Dowd and Martin Hutchinson (2015) argue that Bitcoin's mining algorithm is characterized by significant economies of scale due to the fact that the cryptographic problem can be more efficiently solved by specially optimized computers known as ASICs (Application Specific Integrated Circuits). In addition, because it is common for miners to join a "pool" to decrease the variance of their returns, the argument is that a malicious pool operator would be in a better position to pull off an attack. In 2014, many users abandoned the Ghash.io pool to prevent it from reaching 51 percent of the computing power on the network. Thus, the very publicity of the problem seems to have stymied it. Ghash responded by implementing measures to lower its own share (see its press release at https://ghash.io/ghashio_press_release.pdf). But if a competitive solution is not satisfactory, there are technical solutions as well. Other cryptocurrencies (Litecoin, for example) implement a modified proof-of-work function that significantly diminishes the potential economies of scale to mining. Others, using proof of stake, dispense with arbitrarily intensive computation entirely.

Here we may briefly put to rest several recurring fears surrounding cryptocurrencies. First, the proliferation of copycat currencies (altcoins) cannot be inflationary unless any protocol is a perfect substitute for any other.[5] Whether they are substitutable in some technical sense or not, entrenched network benefits mean that copycat protocols will not displace or rival existing protocols without clear feature advantages. Where physical notes from one bank or another may fit equally well in a wallet (and both of which might even be dollars), holding multiple cryptocurrencies involves the technical inconvenience of operating on multiple disjunct protocols, plus the additional calculational inconvenience that the currencies float against one another in value.[6]

Second, though the protocol is indeed defined arbitrarily in software, it cannot be changed arbitrarily once created. Once a protocol comes into use, the control of its constitution depends entirely on continued trust in the developers. Each user must be persuaded to upgrade. Thus, contra Reuben Grinberg, the fact that "most users would use [a] new version of the software because of their trust in the development team" does *not* make the development team "the de facto central bank of Bitcoin" (2012, 175–76 n. 71). "Bank of issue," in fact, would be a broader category (private, noncentral banks have also issued currency throughout history), a safer claim, and still wrong. The power of a bank of issue consists in its ability to issue new currency indistinguishable from (or in the case of a central bank with the same legal-tender status as) the old and hence to gather seigniorage. The Bitcoin development team has no such power.[7] Given the precedent of open-source cryptocurrency protocols, trust in the developers is reasonably attributed to their continuing trust*worthiness:* a malicious update will be easily spotted and ignored.

The Moneyness of Cryptocurrency

What makes cryptocurrency money? Ludwig von Mises's regression theorem (1996, 408–10) explaining the emergence of money, by which a particular commodity gradually overcomes network hurdles and becomes accepted as money by virtue

5. This is analogous to the discussion in Selgin 1988, 42–47, in which even minimal note-brand discrimination will prevent undue credit expansion by any single competitive note-issuing bank. See also White 2014.

6. Cryptocurrencies could become much closer substitutes to one another if intermediation were to arise with the help of an abstraction layer through which various protocols can be treated similarly by buyers and sellers. This possibility is discussed later in the article.

7. An update that allowed for the issue of new bitcoins beyond the 21 million limit would require changes to what clients consider to be valid blocks. Such backward-incompatible updates (or "hard forks") have in fact been issued several times over the course of Bitcoin's history, though not entirely smoothly. As the 2016 block size controversy shows, hard forks in practice require something close to unanimous consent from the community. Given the importance that existing users attach to a non-inflationary currency, any attempt to fudge the 21 million limit would in all likelihood fail to be adopted on a sufficiently wide scale. For this reason, if competition should indeed select for a more expansionary protocol, it will almost certainly be something other than Bitcoin. Even if the team did succeed in pushing the update, however, it would still be unable to collect seigniorage from the expansion without further changes involving the rewards to mining.

of its increasing liquidity, has lately been taken by some armchair Austrians to imply that cryptocurrency *cannot* be money because it has never been accepted as something useful of its own account. This is a curious argument, considering that Mises saw money as a category of human action. In other words, something is money when people *use it* as money—that is, as a medium of indirect exchange. In this sense, cryptocurrency clearly qualifies as money. The regression theorem begins with the fact of a money and reconstructs the history by which it became such. It cannot be used in the other direction, starting with the observed history of a commodity and passing judgment on its moneyness.

If the theorem is interpreted strictly so as to demand *some* nonmonetary starting point to give it its original positive value, we could say that Bitcoin's innovativeness or antiauthoritarian ethos was a consumption good for its initial adopters (Lawrence White [2014] calls this "affinity demand"). It would be less of a stretch, however, to say that nonmonetary (industrial) use is *a possible* (and so far the most historically significant) starting point, but not the only conceivable one. It would be foolish to try to enumerate an exhaustive list of the ways a commodity, even an inconvertible one, might initially gain wide enough acceptance to function as money. History, in this case, rules out an interpretation that denies to cryptocurrencies the possibility of being money.

As for why cryptocurrencies might be used as money, it is easy to see how they fit the textbook qualities of a useful commodity for indirect exchange:

1. *Portability.* Cryptocurrencies excel here because they have no extension in physical space. They can be exchanged using any device on which you can carry your "wallet file," and it is no more difficult to send an amount across the world than across the street.
2. *Durability.* Though coins can be "lost," they will not get worn out or depreciate.
3. *Divisibility.* Bitcoins are divisible to eight decimal places. In principle, there is no technical limit to the divisibility a protocol might allow.
4. *Security.* As noted earlier, protocol-level theft and counterfeiting are extremely difficult, although—obviously—the protocol has no special way to prevent more traditional types of theft and fraud such as social engineering.

In addition to these "intrinsic" characteristics, money commodities will tend to possess some economic characteristics as well, such as liquidity (ready acceptance), saleability (wide acceptance), and stability of value. It is on these points, rather than the first four, that cryptocurrencies have borne the most criticism.

With respect to acceptance (liquidity), although bitcoins cannot yet be spent at the grocery store, a significant and increasing number of online merchants do accept them, and they have already broken into the physical world with the advent of Bitcoin ATM kiosks in various large cities in Canada and the United States. A vibrant and growing niche ensures that bitcoins remain quite liquid. With large

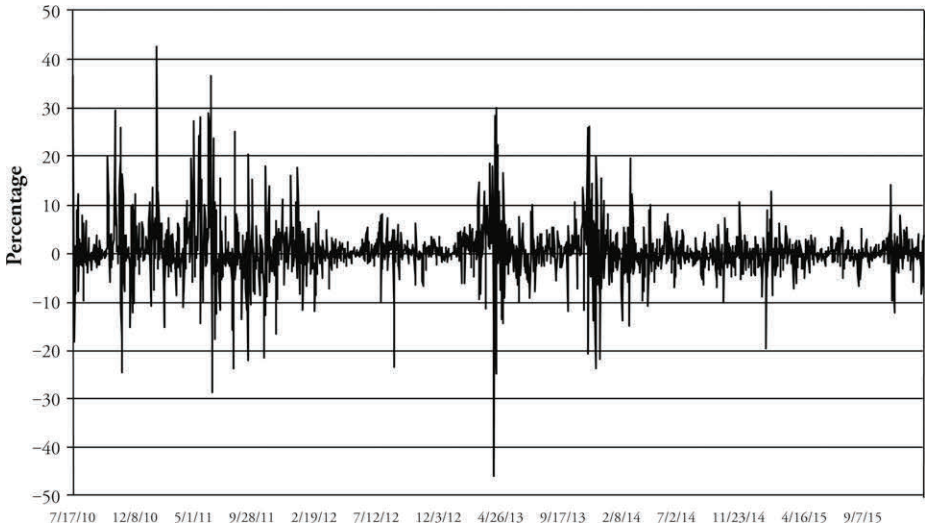
Bitcoin exchanges accessible online, bitcoins can be bought and sold nearly instantly at the market exchange rate from anywhere with Internet access.

On stability of value, however, cryptocurrencies reveal their inadequacy as day-to-day currency. That mass adoption of cryptocurrencies has not been forthcoming cannot be attributed (as William Luther [2015] argues) primarily to network effects. Perhaps this will be a relevant bottleneck in the future. For now, though, the primary impediment is purchasing-power volatility. Bitcoin, for example, despite making up 86 percent of the entire cryptocurrency market (White 2014), has suffered from frequent and severe jumps and crashes since its inception in 2010, as shown in figure 1.

The daily change in the U.S. dollar–bitcoin exchange rate has reached nearly 50 percent in both directions, and regularly exceeds 10 percent. By contrast, the daily change in the U.S. dollar–euro exchange rate over the same period never exceeded 2.5 percent in either direction. This is not simply a problem of scale which can be expected to diminish as the volume of transactions grows: with the exception of its extreme volatility during its time beneath a dollar per bitcoin (roughly the left quarter of figure 1), there is no notable correlation between volatility, price, or volume of transactions following its rise past about $10, even up past $1,000.

Milton Friedman characterized the countercyclical effects of a pure commodity currency (i.e., a system, like the Bitcoin ecosystem currently, in which base money forms the entire money stock) as depending primarily on an elastic supply

Figure 1
Daily Change in the Bitcoin–Dollar Exchange Rate, 2010–2016



Source: Data compiled by the author from the largest bitcoin–dollar exchange at each point in time, so the collapse of one exchange (e.g., Mt. Gox in February 2014) does not introduce spurious volatility.

of the money commodity (1951, 207). The supply of bitcoins, however, is very nearly invariant to anything except time.[8] In terms of the equation of exchange MV = PT,[9] M is perfectly exogenous and predictable. Having no outlet in the money supply, changes in the demand for cash balances, then, must affect nominal spending until prices adjust.

In addition to a secular upward trend as the ecosystem grows (hence the much-lamented "deflationary" aspect of Bitcoin), the demand for bitcoins is also highly volatile. Though difficult to measure, it is well accepted that a very large portion of all Bitcoin transactions are made for speculative purposes—up to 90 percent by some estimates. It is true that investment spending is inherently more volatile than consumption spending, but the more important factor is that without a credible anchor for expectations of the currency's value, *demand shocks will be self-reinforcing.* Jeffrey Frankel and Andrew Rose describe the mechanism: "Expectations can be described as stabilizing when the effect of an appreciation today—relative to some long-run path or mean—is to induce market participants to forecast depreciation in the future. . . . Expectations can be described as destabilizing, on the other hand, when the effect of an appreciation is to induce market participants to forecast more appreciation in the future" (1995, 1710–11). For currencies with a credible price anchor—which does not necessarily imply a fixed exchange rate[10]—speculation will tend to be a stabilizing force, pushing the actual value back toward that target. However, without such an anchor, "the variability of exchanges will tend to multiply [the] magnitude [of short-term movements] and may turn what originally might have been a minor inconvenience into a major disturbance" (Hayek 1937, 64). More prescient words could hardly have been spoken of Bitcoin's current situation.

For this reason, Bitcoin is by no means a unit of account,[11] a situation that bears a striking resemblance to episodes of hyperinflation. Barry Eichengreen, for example, quotes Hjalmar Schacht's (1927) account of the German hyperinflation, which notes that merchants "calculated prices with reference to the exchange rate and converted mark receipts into foreign currency as quickly as possible"

8. The hash target adjusts about every two weeks (more precisely, every 2,016 blocks) based on the time taken since the previous adjustment, so sudden changes in computing power on the network can have transient effects on the rate of coin generation.

9. Discussion at the level of the protocol makes total transactions, T, more appropriate (and, conveniently, more measurable) than sales of final goods and services, *y*. V will then refer to the more expansive transactions velocity, V_T, rather than to income velocity, V_y. P stands for an index of prices denominated in the currency.

10. For currencies on the gold standard, the "gold bands" served as a credible focal point beyond which speculators would not ordinarily let the currency's exchange rate move (Bordo and MacDonald 2012). C. M. Engel and Jeffrey Frankel (1984) also find evidence that the United States was able to take advantage of this sort of speculation during the Federal Reserve's brief stint with money-supply targeting: increases in M1 were actually associated with *appreciation* of the dollar, indicating a consensus expectation of compensating contraction in the future.

11. White (2014), however, notes that Bitcoin *does* serve as a vehicle currency for altcoin exchanges, most of which likely suffer from even more severe volatility than Bitcoin.

(1994, 135). Because prices become nearly perfectly flexible, hyperinflations are remarkable as the most consistent example of short-run purchasing-power parity (Rogoff 1996). Much the same occurs with Bitcoin today and with even less friction. Merchants can convert their dollar prices into bitcoin using up-to-the-second data feeds, and services such as Bitpay allow immediate exchange for local currency following a transaction, minimizing the risk to the merchant of holding a balance of bitcoins (Luther and White 2014).

Though Bitcoin is far from hyperinflationary, the safety valves that spare the volume of transactions much of the brunt of fluctuations in the exchange rate evidently come into operation in response to any sufficiently violent and sustained purchasing-power or exchange-rate paroxysms. Should merchants begin to adopt Bitcoin as a unit of account, however (let us suppose there is a long enough quiet period of relative stability for this to happen), prices will not be able to adjust as quickly to changes in nominal spending, and the familiar output effects of monetary disturbances will manifest themselves. The extant crop of cryptocurrencies, then, will hardly be able to supplant the currencies on which they depend as an anchor for the speedy adjustment of prices.

Bitcoin and Gold

Nevertheless, a fixed supply in the face of shifting demand is no death knell for cryptocurrency. It will be illuminating to consider the historical development of another successful money commodity with a mostly exogenous global supply: gold.[12] To answer how Bitcoin and other cryptocurrencies with a rigidly capped nominal supply might overcome the problems associated with it, we should ask, How *did* gold (and other metals) overcome these problems?

Before the explosive economic growth in the West, a pure commodity standard prevailed: the medium of exchange was actual metal coins. The global money supply was therefore more or less fixed in the short run.[13] Without well-integrated international markets, money prices did not vary much from day to day in normal circumstances. Economic growth was slow, and mining was not all that productive, so "natural" inflation and deflation occurred over very long periods when they

12. It is true that fluctuations in the price of gold did sometimes spur prospecting and more intensive output from gold mines, but this effect was both unpredictable and slow. Michael Bordo finds the strongest supply response to deviations from the purchasing-power trend of gold at a lag of sixteen years (1984, 218 n.). Likewise, a jump in the price of bitcoins brings more computing power to bear on the network, but because of the adjustable hash target, this additional power affects only the distribution of coins, not the long-term rate of coin generation. Although these responses move in the equilibrating direction, they are practically useless for the short-term fluctuations with which I am here concerned.

13. Three notes on this point: (1) Metals could be minted from nonmonetary uses, but I consider this to be a medium- to long-run phenomenon. (2) I ignore the problem of debasement except to note that this is an aspect where cryptocurrencies are more resilient to political exigencies than are precious metals. (3) Credit did exist, but private liabilities did not circulate as money prior to the spread of banking institutions and could not therefore contribute to the elasticity of the money supply (White 1999, 12).

occurred at all. Even the so-called Price Revolution, during which prices in Europe more than doubled following the discovery and importation of New World silver and gold, took place over such a long period that the annualized inflation rate stayed in the range of 1 to 1.5 percent, low by modern standards (Kugler and Bernholz 2007). In short, rigidity of the supply of precious metals did not pose a serious problem.

Fortunately, the advent of sustained economic growth starting with the Industrial Revolution was accompanied by a banking revolution as well. Moneylending lost its stigma, and, with financial and actuarial innovations, trade and industry were able to flourish. The observation that financial development generally precedes industrialization can, at least for this era, be explained by the happy circumstance that these financial innovations—fractional-reserve banking in particular—were able to overcome gold's nominal supply problem. As Mises noted of the time period, "The development of the clearing system and of fiduciary media [i.e., circulating bank liabilities] has at least kept pace with the potential increase of the demand for money brought about by the extension of the money economy, so that the tremendous increase in the exchange value of money, which otherwise would have occurred as a consequence of the extension of the use of money, has been completely avoided" (1953, 298). Rather than affecting prices in the long run and the volume of transactions in the meantime, changes in the demand for cash balances, which were for the first time rapidly growing, could be accommodated by changes in the money supply. By using loans and credit to pyramid a larger and variable stock of banknotes and deposits on top of a smaller and fixed supply of physical gold, the money supply was, to varying extents across different countries, able to roughly stabilize nominal spending even in the face of wide variations in the demand for money.[14]

We might expect similar financial innovations to precede an explosion in the use of cryptocurrencies. However, cryptocurrencies face a number of unique hurdles for which the history of gold provides little guidance.

Technical Hurdles

At this point, it will be useful to distinguish the *currency* itself from its *method of exchange*. For most of the world's monetary history, the method of exchange was generally hand to hand. The *currency transition* from gold coins (base money) to bank liabilities (inside money, including paper banknotes and checkable deposits) that marked the advent of fractional-reserve banking was much facilitated by the fact that the same method of exchange that was suitable for one was just as suitable for the other. The two are, of course, wholly different commodities, each entailing

14. See Selgin 1988 for an account of the mechanics of supply adjustment through fractional-reserve banking under a gold standard. Where this process was impeded, periodic crashes were the rule. See also Selgin 2010, 494, for a suggestive graph comparing the responsiveness of U.S. and Canadian money supplies to money demand.

a different sort of claim, even if they are denominated equivalently and exchangeable one for the other at a fixed rate. But besides the usually small risk of bank collapse, accepting and spending gold-backed banknotes had no serious drawbacks compared to gold and required no special investment to begin. Indeed, an important advantage of bank liabilities is that, with the same method of exchange, they were *less* costly (more convenient) to use than gold coins.

The advent of electronic payment, in contrast, marked a transition in the *method of exchange*. Though a similar process had existed for centuries with checks, electronic payment no longer involved the hand to hand transfer of an asset (such as a check). Telephone lines and bank software were now the method of exchange. Even though the *currency* did not change (dollar-denominated deposit balances), the change in method entailed a network hurdle and a fixed cost to join the network because merchants had to install card readers next to their cash registers. Nevertheless, the benefits were clear enough that by now most merchants have joined the network: as of 2011, credit and debit card payments constituted nearly two-thirds of the retail sales volume in the United States (Morrison 2012).

In both cases, the transition was much aided by being limited to one aspect or the other. Those deciding whether to accept a new currency faced no initial cost to joining the network, and those deciding whether to change their method of exchange did not have to worry about whether to accept a new currency. Cryptocurrencies have had the misfortune not only of having to effect both transitions at once but also, on top of that, of being denominated in a different unit of account![15]

Bitcoin's success in spite of this double hurdle is remarkable. But the hurdles are not all behind it: the establishment of bank liabilities redeemable in cryptocurrency will *again* have to make both transitions at once. The necessity of a currency transition is implied in the establishment of fractional-reserve banking in exactly the same way as the original transition from physical coins to bank liabilities. The essential problem here is *trust*. The necessity of a method transition, however, deserves a few more words. Because a cryptocurrency protocol defines both the coinage and exchange of the base money, issuing liabilities on a fractional-reserve basis requires more than simply adding parameters to coins.[16] A bank that wants to vary its issue with demand would need to create its own coinage and exchange mechanism, a new protocol, which would not be compatible with the original even if its processing took place on the same blockchain.[17] Nor would one issuer's liabilities be

15. This means the network effects impeding Bitcoin's adoption described in Luther 2015 are likely understated.

16. Adding parameters to coins would allow at best the establishment of a 100 percent reserve bank, which is somewhat the idea behind Open Transactions' voting pools.

17. A blockchain is essentially a decentralized database, so multiple protocols can operate side by side on the same blockchain if they speak a sufficiently similar language. This ability allows smaller enterprises to take advantage of the volume of mining done on Bitcoin's blockchain. By itself, it does not diminish the hurdle of protocol incompatibility. However, see the discussion on Open Transactions as an abstraction layer.

compatible with another's. Merchants would need to implement the new protocol, facing a similar sort of cost to those merchants installing pads to accept credit cards.

Technical innovations can, however, collapse the two method transitions. Issuers would find it in their interest to provide an abstraction layer that allows the same apparatus to transact in both base money and bank liabilities. Open Transactions (OT) already facilitates secure cross-blockchain exchange of different cryptocurrencies. If the issuer's protocol can be administered on a blockchain, OT can provide a framework for the relatively transparent use of multiple inside monies and base monies and even the issue of liabilities backed by and denominated in a basket of cryptocurrencies.

In fact, such issues could be denominated in any unit at all. Again, credit card networks are an illuminating precedent. These networks perform a similar function to our abstraction layer: merchants do not have to implement separate pads to accept Visa and Master Card because there is a network that transparently routes the transaction to the appropriate firm. Merchants can even choose which cards they are willing to accept (many refuse American Express, for example, which charges the merchant more per transaction to fund its rewards program). And the process is rendered transparent to consumers by being denominationally agnostic: each network routes dollars just as well as euros and even automatically exchanges them based on what the merchant takes.

Nonetheless, though an abstraction layer can lower the network costs of adopting cryptoliabilities, even if the transition can successfully be made, important qualities of the base money are inevitably lost by using bank liabilities as money. OT can minimize the level of trust that users must have in the bank—for example, the possibility of absconding with deposits can be ruled out. But users must still trust the bank

1. To maintain redeemability at par—that is, not to inflate. This possibility is the price of quantity-stabilizing intermediation. There is no recourse against it but market competition, which would be easily subverted by the incautious application of any modern economy's byzantine banking regulations.
2. With their information, which exposes them to hackers or subpoenas. As Ricardo Cavalcanti puts it, "Although anonymity preserves money, it rules out all forms of credit" (2010, 76).

If minimizing the necessity of trust is integral to the ethos of cryptocurrency, the liabilities of a cryptointermediary will succeed in the market only by sacrificing those qualities to which cryptocurrencies owe their initial success.

Institutional Hurdles

In addition to the intrinsic network hurdles, regulatory uncertainty and hostility also constitute an extrinsic hurdle for intermediation in a way that they do not for the protocols themselves. Though governments around the world have targeted

cryptocurrency users (often under money-laundering regulations for individuals and financial regulations for would-be intermediaries), their success has been mixed. The protocols cannot be targeted or shut down; the best that can be done is to pinpoint prominent individual users, a drawn-out and expensive process. This is the reason that Bitcoin has not succumbed to the same fate as the Liberty Dollar (Dowd 2014), and it is precisely the protection that will vanish with the rise of financial intermediation. OT can prevent the seizure of users' assets, but it cannot prevent the forcible closure of any intermediary that becomes large enough to attract attention.

No doubt some degree of intermediation and liability issue can survive anonymously even under the harshest of legal climates. But legal hostility severely limits the scale of such an undertaking, scale being an important factor in the trustworthiness of an intermediary's promise to redeem. This issue highlights another potential economic hurdle, the closest parallel to which might be the "free-banking" era in the United States, where legal restrictions on branch banking limited banks' capitalization and diversification (Dowd 1992). This limitation left banks highly vulnerable to seasonal fluctuations and made the system as a whole notoriously unstable. Should concerted legal hostility lead to a similar market structure of cryptointermediaries, the cryptocurrency market might well become even more unstable than it is at present.

Finally, should a cryptocurrency come to serve primarily as a reserve currency on top of which circulating liabilities are pyramided, the centralization of transactions that would accompany this development increases the risk of protocol fraud. As noted earlier, the protocol's security lies in the assumption that an attacker will never be able to outwork all the honest computers on the network. The use of bank liabilities as media of exchange has the effect of taking people off the original network and putting them on the bank's own services. If the majority of computing power on the base currency's protocol comes to be controlled by a few banks, the generation of a fraudulent blockchain would require only the hijacking of the servers of a few major intermediaries or collusion among them.

A greater worry is that if a bank were to at any point constitute more than 50 percent of the computing power on the network, it might in principle "manage" the currency by a combination of double spending and rejection of legitimate transactions. In response to this fear, two comforts may be offered. First, in historical situations where intermediaries were allowed to compete most freely, "there was no evidence of natural monopoly in [note] issue, nor even of a natural number of firms that could be called 'small'" (White [1984] 1995, 146; cf. Selgin 1988, 150–54). Second, in today's economy there is no evidence of such a tendency in deposit issue. Nevertheless, history also shows that incautious or malevolent regulation, especially if coordinated globally, might easily create a situation in which one reserve bank holds enough power to monopolize the blockchain's computing power. Here, though, the ease with which new protocols can be created works as a safety valve. When the original protocol is attended with such disadvantages as

a rogue reserve bank, dissatisfied users can always flock not only to a new bank but also to a new protocol. And if the rise of intermediation has by this point been accompanied by the development of an abstraction layer, the costs of switching will be very low indeed.

Alternatives to Intermediation

Intermediation will determine the value of base money more than vice versa. Thus, Hayek notes, "it is an erroneous belief that the value of gold or any metallic basis determines directly the value of money. The gold standard is a mechanism which was intended and for a long time did successfully force governments to control the quantity of money in an appropriate manner so as to keep its value equal with that of gold. But there are many historical instances which prove that it is certainly possible, if it is in the self-interest of the issuer, to control the quantity even of a token money in such a manner as to keep its value constant" (1979, 2). When the circulation of liabilities redeemable in base money comes to dwarf the circulation of the base money itself, the day-to-day demand for base money is low and stable compared to that of a pure commodity currency.[18] If the main source of Bitcoin's volatility is volatile demand, we can expect the issue and circulation of bitcoin-redeemable liabilities to stabilize the demand for (and therefore the value of) Bitcoin by allowing fluctuations to be borne by changes in the supply of liabilities rather than by the price level or the volume of transactions. The base money, in contrast, influences the value of the liabilities only so far as redeemability (as, we presume, will be demanded of private intermediaries [see Selgin and White 1994]) disciplines issuers to maintain such a quantity of liabilities that the two values stay roughly on par.

The fact that redeemability does not determine value except so far as it determines quantity means that we might be able to design a protocol so that the total quantity of coins behaves similarly to a system of competitive and redeemable bank liabilities, without intermediation at all. Bitcoin's periodic halving of the mining reward is arbitrary, and several alternative mining schemes have already been devised. Given the hurdles discussed earlier—at least some of which are likely to be permanently intractable—it will be worth considering alternatives by which the flexibility of intermediation might be baked into the protocol, thereby evading the legal hurdles.

One possibility is linking the proliferation of coins to some macroeconomic variable—for example unemployment or an exchange rate—like a central bank might target these variables. The relative ease with which new cryptocurrencies can be created might suggest a wide scope for experimentation here. However, as Robert

18. Note, on the other hand, the dramatic increase in the volatility of the purchasing power of gold following its final demonetization at the collapse of the Bretton Woods system (Erb and Harvey 2013).

Sams puts it, "the variable will be a fact about the world outside of the system that needs to be represented inside the system via some trust-minimizing mechanism" (2015).[19] So far as this arrangement exposes the money supply to somebody's will or to the interference of hostile or well-intentioned governments, it would not differ essentially from rule-based central banking: the rule can be broken, as it has been in every historical example.

The transactions velocity of money, however—V_T in the equation of exchange—could be calculated endogenously. Coins exchanged per hour, reckoned either as a rolling or a cumulative-decay average, would be very close to the textbook definition and would involve little more than a series of queries on the blockchain. We need not concern ourselves with the Sisyphean econometrics and data collection that central banks find necessary to guide their behavior, and without the financial sophistication we are trying to obviate, there is no worry about different velocities corresponding to M0, M1, and so on.[20] The only problem will be to set the optimal period over which the average is calculated. If the period is too long, the monetary base will be rigid in supply; if it is too short, M will fluctuate chaotically with transient changes in V.

Having a protocol-endogenous value for velocity would allow us to target MV at the protocol level, a money-supply norm with growing support (see, e.g., Selgin 1997; McCallum and Nelson 1998).[21] Though in principle any behavior of the money stock is compatible with monetary equilibrium so long as it is perfectly anticipated and adjusted for in prices (Gilbert 1957), George Selgin argues that an MV target will require the fewest discrete price adjustments and for this reason is best suited to engender monetary equilibrium in a world where price adjustment is piecemeal and discontinuous.

Thus, we set our sights on the elusive goal of a neutral money, one in which changes in the money supply cause no transient relative price changes. The problem

19. The Ethereum white paper makes an interesting proposal (Karapetias 2015) to use a decentralized data feed for this purpose. This feed would guarantee accuracy in a manner similar to a prediction market by rewarding all entries within the twenty-fifth and seventy-fifth percentile—the assumption being that the true value is a natural focal point, and the median entry will be a reliable estimate. This is certainly a more robust solution than simply trusting a single data source. Still (as Sams [2015] notes), skewing the focal point will be much easier than an analogous 51 percent attack on a cryptocurrency's blockchain, especially if the source of the data is a single agency.

20. Off-chain transactions (i.e., Bitcoin derivatives) do exist, which might indicate a rudimentary financial market. Nevertheless, I am not aware of any evidence that such derivatives circulate *as currency,* which is the important aspect for stabilizing the demand for base money.

21. Bennett McCallum and Edward Nelson actually advocate a nominal gross domestic product (NGDP) target, which differs from our MV target only in practical considerations of measurement: (1) using the narrower income velocity, V_y, rather than transactions velocity, V_T, and (2) using the other side of the equation of exchange, Py, as the target. Selgin (2015) suggests the possibility of an NGDP-targeting cryptocurrency but does not go into any technical details. A price-level target (as advocated by Sams [2015], for example) would require the same data-feed apparatus as targeting other external variables: the protocol can calculate the product PT endogenously (because it equals MV), but calculating a value of T to separate out a targetable value of P would require the construction of a price index—a difficult task without an existing taxation apparatus and fraught with the same specification and measurement issues that come with the construction of any other price index.

will be to set the net rate of proliferation of coins (ΔM) to offset changes in velocity. This can be done easily enough by a protocol that provides both for the proliferation and deletion of coins,[22] varying the rates of each to match the ΔM implied by the current measure of velocity in a mechanism similar to the dynamic adjustment of Bitcoin's hash target to computing power on the network.

I omit the details of implementation, however, because the focus on macroeconomic aggregates gets us in fact no closer to a solution. Such a scheme would be form without substance—a macroeconomic cargo cult, lacking the cardinal function of intermediation: the channeling of liquidity to its most valued uses. Intermediation ensures a relatively quick diffusion of new money through the economy; otherwise, we are left with the transmission mechanism of the idiosyncratic spending habits of the miners to whom the new money goes as a reward. This mechanism necessitates spurious and self-reversing price adjustments as miners spend their funds.[23]

Such self-reversing price adjustments, of course, are equivalent with monetary disequilibrium; they vitiate completely the vaunted neutrality of our currency. Historically, equilibrating changes in the quantity of money have propagated through financial intermediaries. A currency that adjusts the quantity *without* intermediation, by contrast, highlights the fact that money approaches neutrality *only* when quantity changes are borne through a loanable funds market and only to the extent of the depth of that market. Where changes in the quantity of money enter *elsewhere* than through a loanable funds market, transitional disequilibria will arise with greater severity, even if the quantity change is in the equilibrating direction.

A loanable-funds market, where intermediaries can take bids from those most willing to bear those monetary changes, is more than a merely automatic act of channeling funds. Even if the protocol should also provide for a central clearinghouse to channel savings to those who might bid for it, individual to individual, the specialization and economies of scale that constitute the chief functional justification of banking as a separate industry are still lost. Individual entrepreneurs would scarcely be able to take on the administrative functions of an intermediary, and still less would miners, who are by no means the same sort of person who would excel as an entrepreneur.

Intermediation, then—in particular intermediation carried out by large-scale specialists—is not merely a means to achieve MV stability in pursuit of monetary equilibrium. Rather, intermediation appears to be necessary to take advantage of any benefits that MV stability ostensibly offers.

22. Peercoin, for example, takes Bitcoin's variable transaction fee and makes it a mandatory, fixed amount, which is then destroyed rather than going to the miner. Alternatively, a rate of nominal depreciation could be built into the protocol, amounting to something like a continuously stamped Gesell currency, as discussed in Keynes 1936, chap. 23, §VI.

23. This argument is developed at length in Harwick 2015.

Decentral Banking?

Perhaps then, rather than mimicking the supply effects of intermediation at the protocol level, we could mimic intermediation *itself* at the protocol level—a "decentral bank" that oversees the distribution of ΔM to its most highly valued uses.

The first difficulty in replicating banking at the protocol level is that an automated system lacks the ability to evaluate the profitability of projects for which loans are to be made. There accordingly exists a trade-off between usefulness and vulnerability: the more impossible default is, the less useful intermediation is. The decentral bank can take measures to ensure repayment using auxiliary smart contracts or (because the bank constitutes the protocol) to enforce payment absolutely. But because risk is an inextricable part of any intertemporal transaction, it is unclear that automated intertemporal trade, in conjunction with freedom of account creation, could exist at all without commensurate vulnerability to exploitation. Control of balances can eliminate default risk *to the bank,* but beyond some margin it can do this only by shifting the risk onto some other party—for example, the recipients of borrowed funds—or to currency holders as a whole.[24]

A more sophisticated scheme for the constitution of a decentral bank is what Sams (2015) calls "seigniorage shares." In this scheme, the bank issues two distinct assets, coins and shares. The value of the coin is stabilized, and the value of the share floats. The protocol achieves its target ΔM by buying and issuing shares—something like automated open-market operations. Shareholders broadcast the price at which they are willing to buy and sell shares, and the bank buys or issues a sufficient quantity to achieve the target ΔM.

The question becomes, then, Is this distribution sufficient to direct liquidity to its most valued uses in the same way as a banking system might? The seigniorage shares scheme has obvious parallels with the structure of a private banking system. In the latter, a change in the demand for money registers directly to the issuing intermediaries as a drop in the gross volume of clearings, indicating that (for a given risk preference) the volume of loans and therefore of issues may be safely expanded. The bank distributes these new issues by lowering its interest rates, allowing marginal borrowers to take advantage of the new savings. Seigniorage shares in conjunction with endogenous MV stabilization would work similarly: a drop in the gross economy-wide volume of clearings signals the decentral bank to expand the volume of coins by some amount. The protocol buys shares, driving their value up (i.e., driving their expected yield down).

If we take shareholders to be the same as borrowers, the problem is solved, and there is no obstacle in principle to the wholesale displacement of fiat currencies

24. Derivatives such as futures contracts do exist as smart contracts or multisignature transactions, but (as noted earlier) they do not circulate as currency, and they do not entail any default risk: the coins at stake are held in escrow until a trusted party verifies the state of the world specified in the futures contract. The protocol itself, of course, should ideally be trustless. It is no more capable of verifying the trustworthiness of third-party adjudicators than it is capable of verifying the trustworthiness of the original borrower.

by stable cryptocurrencies. However, this assumption is dubious for several reasons. First of all, the establishment of firms in modern economies—especially highly innovative and highly risky ventures—are predicated on a division of labor between entrepreneurs (who borrow and allocate productive resources) and capitalists (who lend and bear risk). To equate the selling of shares with entrepreneurial borrowing is to merge the entrepreneur with the capitalist, for in order to "borrow," the entrepreneur must already have shares to sell—that is, capital funds—a significant impediment to the establishment of new enterprises. The entrepreneur may of course borrow funds to acquire shares, but this action presupposes an existing financial market, which (if denominated in the cryptocurrency) obviates the whole project of endogenous stabilization or (if denominated in another currency) does not minimize the dependence of the cryptocurrency on other, more established fiat currencies.

The relevance of this friction to the cryptocurrency's volatility is an open question. If entrepreneurs are in fact little impeded by the necessity of being capitalists also, the solution is viable, and such a cryptocurrency faces only a network hurdle in displacing existing currencies. If the friction is a severe impediment to entrepreneurship, the savings implicit in increases in the demand for money (and vice versa) will tend to be maldistributed, necessitating self-reversing relative price changes and a loss of efficiency.

In the end, the same problem rears itself in both schemes: gratuitous or ad hoc credit creation is an irreducibly discretionary act, and on this act depend economic growth and the economical distribution of loanable funds. The volatility of today's cryptocurrencies is merely symptomatic of their lack of credit institutions: creative solutions to the volatility problem that do not address the institutional hindrances to ad hoc credit creation will not allow them to sustain economic growth without relying on markets denominated in other currencies. Until such markets denominated in a cryptocurrency are established, the goal of displacing fiat currencies seems chimerical.

Conclusion

The very existence of cryptocurrency militates against any a priori declaration of a problem's impossibility. Anonymous and trustless financial intermediation may turn out after all to be a technical problem with a clever solution. Nevertheless, so far as borrowing and lending entail risk—and thus moral hazard—that risk cannot be mitigated without personal judgment. Such judgment is difficult, if not impossible, to provide either in an anonymous and trustless environment or automatically by a computer algorithm. Risk in this case is the obverse of trust, and a trustless protocol will be severely limited in dealing with it. This fact appears to put an upper limit on the financial sophistication a cryptocurrency can support without a supportive legal climate. As it is, true intermediation on a scale sufficient to stabilize the value of

the currency will have to fight not only in the marketplace for general acceptance separately from the base money but also in the political realm for the privilege of operating unmolested.

Of course, any opportunity for a cryptocurrency to suddenly supplant a national currency will likely coincide with the relaxation of restrictive regulations. In a political economy sense, it may be valuable to have a cryptocurrency with a stable purchasing power to allay fears of adoption, even if the currency would nevertheless not sustain widespread growth until the regulations preventing intermediation are relaxed. Nevertheless, as it stands now, though it would be an utterly quixotic task for governments to try to stamp out cryptocurrencies, they are well positioned to prevent the emergence of stabilizing financial institutions around cryptocurrency ecosystems. Without these institutions, the hurdles cryptocurrencies face to supplanting more legally privileged and centrally issued currencies appear to be insurmountable.

References

Bitcoin Miners Busted? Police Confuse Bitcoin Power Usage for Pot Farm. 2011. *Computerworld,* May 23.

Bordo, Michael D. 1984. The Gold Standard: Myths and Realities. In *Money in Crisis: The Federal Reserve, the Economy, and Monetary Reform,* edited by Barry Siegel, 197–237. Cambridge, Mass.: Ballinger.

Bordo, Michael D., and Ronald MacDonald. 2012. Interest Rate Interactions in the Classical Gold Standard, 1880–1914: Was There Any Monetary Independence? *Journal of Monetary Economics* 52, no. 2: 307–27.

Cavalcanti, Ricardo de O. 2010. Inside-Money Theory after Diamond and Dybvig. *Economic Quarterly* 96, no. 1: 59–82.

Dowd, Kevin. 1992. U.S. Banking in the "Free Banking" Period. In *The Experience of Free Banking,* edited by Kevin Dowd, 206–35. New York: Routledge.

———. 2014. *New Private Monies: A Bit-Part Player?* London: Institute of Economic Affairs.

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

Eichengreen, Barry. 1994. *Golden Fetters: The Gold Standard and the Great Depression 1919–1939*. New York: Oxford University Press.

Engel, C. M., and Jeffrey Frankel. 1984. Why Interest Rates React to Money Announcements: An Answer from the Foreign Exchange Market. *Journal of Monetary Economics* 13:31–39.

Erb, Claude B., and Campbell R. Harvey. 2013. The Golden Dilemma. *Financial Analysts Journal* 69, no. 4: 10–42.

Frankel, Jeffrey, and Andrew Rose. 1995. Empirical Research on Nominal Exchange Rates. In *Handbook of International Economics,* vol. 3, edited by Gene Grossman and Kenneth Rogoff, 1689–729. Amsterdam: Elsevier.

Friedman, Milton. 1951. Commodity-Reserve Currency. *Journal of Political Economy* 59, no. 3: 203–32.

Gilbert, J. C. 1957. The Compatibility of Any Behavior of the Price Level with Equilibrium. *Review of Economic Studies* 24, no. 3: 177–84.

Grinberg, Reuben. 2012. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science and Technology Law Journal* 4, no. 1: 159–208.

Harwick, Cameron. 2015. On the Microfoundations of Money Supply Adjustments: An Essay in Loanable Fundamentalism. Working paper. At http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2545488.

Hayek, F. A. 1937. *Monetary Nationalism and International Stability.* Fairfield, N.J.: Kelley.

————. 1979. Toward a Free-Market Monetary System. *Journal of Libertarian Studies* 3, no. 1: 1–8.

Karapetias, Lefteris, ed. 2015. *A Next-Generation Smart Contract and Decentralized Application Platform.* November 21. At https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper.

Keynes, John Maynard. 1936. *The General Theory of Employment, Interest, and Money.* Basingstoke, U.K.: Palgrave Macmillan.

King, Sunny, and Scott Nadal. 2012. PPCoin: Peer-to-Peer Cryptocurrency with Proof-of-Stake. White paper. At https://peercoin.net/whitepaper.

Kugler, Peter, and Peter Bernholz. 2007. The Price Revolution in the 16th Century: Empirical Results from a Structural Vectorautoregression Model. Wirtschaftswissenschaftliches Zentrum Working Paper. At https://wwz.unibas.ch/uploads/tx_x4epublication/12_07.pdf.

Luther, William J. 2015. Cryptocurrencies, Network Effects, and Switching Costs. *Contemporary Economic Policy* 34, no. 1: 1–19.

Luther, William, and Lawrence H. White. 2014. Can Bitcoin Become a Major Currency? *Cayman Financial Review* 36 (August 8).

McCallum, Bennett, and Edward Nelson. 1998. Nominal Income Targeting in an Open-Economy Optimizing Model. Institute for International Economic Studies, Seminar Paper no. 644.

Mises, Ludwig von. 1953. *The Theory of Money and Credit.* New Haven, Conn.: Yale University Press.

————. 1996. *Human Action: A Treatise on Economics.* 4th ed. Little Rock, Ark.: Fox & Wilkes.

Morrison, David. 2012. Credit, Debit Cards Gang Up to Dethrone Cash. *Credit Union Times,* June 13. At http://www.cutimes.com/2012/06/11/credit-debit-cards-gang-up-to-dethrone-cash.

Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. White paper.

Rogoff, Kenneth. 1996. The Purchasing Power Parity Puzzle. *Journal of Economic Literature* 34:647–68.

Sams, Robert. 2015. A Note on Cryptocurrency Stabilisation: Seigniorage Shares. Working paper.

Schacht, Hjalmar. 1927. *The Stabilization of the Mark*. New York: Adelphi.

Selgin, George. 1988. *The Theory of Free Banking: Money Supply under Competitive Note Issue*. Lanham, Md.: Rowman & Littlefield.

———. 1997. *Less Than Zero: The Case for a Falling Price Level in a Growing Economy*. London: Institute of Economic Affairs.

———. 2010. Central Banks as Sources of Financial Instability. *The Independent Review* 14, no. 4 (Spring): 485–96.

———. 2015. Synthetic Commodity Money. *Journal of Financial Stability* 17:92–99.

Selgin, George, and Lawrence H. White. 1994. How Would the Invisible Hand Handle Money? *Journal of Economic Literature* 32, no. 4: 1718–49.

White, Lawrence H. [1984] 1995. *Free Banking in Britain: Theory, Experience, and Debate, 1800–1845*. London: Institute of Economic Affairs.

———. 1999. *The Theory of Monetary Institutions*. Malden, Mass.: Blackwell.

———. 2014. The Market for Cryptocurrencies. *Cato Journal* 35, no. 2: 383–402.

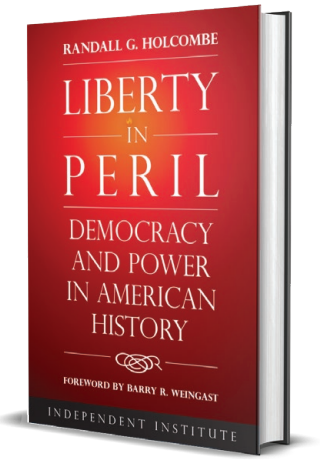
Acknowledgments: I am grateful for helpful comments from Raymond Niles, Andrea Castillo, and two anonymous reviewers. Errors and ill-conceived ideas are my own.

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