The Market for Cryptocurrencies

Lawrence H. White

Cryptocurrencies like Bitcoin are transferable digital assets, secured by cryptography. To date, all of them have been created by private individuals, organizations, or firms. Unlike bank account balances, they are not anyone's liability. They are not redeemable for any government fiat money such as Federal Reserve Notes or for any commodity money such as silver or gold coins. The cryptocurrency market is thus a market of *competing private irredeemable* monies (or would-be monies). Friedrich A. Hayek (1978a) and other economists over the last 40 years could only imagine how market competition among issuers of private irredeemable monies would work. Today we have an actual market to study. In what follows I will discuss the main economic features of the market. I also discuss whether the market is purely a bubble.

As an introduction to the topic, I offer the following comic verse about the contrast between Bitcoin and the physical gold coins of the past:

> In the past, money's value was judged with our teeth;
> We *bit coins* to confirm they were real.
> Now a Bitcoin's just data, no gold underneath.
> That's okay if it buys you a meal.[1]

Cato Journal, Vol. 35, No. 2 (Spring/Summer 2015).

Lawrence H. White is Professor of Economics at George Mason University, a Senior Fellow with the F. A. Hayek Program for Advanced Study in Philosophy, Politics and Economics at GMU's Mercatus Center, and a Senior Fellow at the Cato Institute's Center for Financial and Monetary Alternatives. He thanks Patrick Newman for research assistance and participants at Cato's 32nd Annual Monetary Conference for comments.

[1]The fourth line is mine. It refers to the news that Washington, D.C. now has a food truck that accepts Bitcoin payments. The first three lines are by Gary Crockett (2014). His original fourth line was: "Bitten bits don't make much of a meal."

The Size and Composition of the Cryptocurrency Market

Bitcoin rightly gets the lion's share of media attention, but it is not alone in the market for cryptocurrencies. The authoritative website CoinMarketCap.com tracks the U.S. dollar price and total "market cap" (price per unit multiplied by number of units outstanding) for each of more than 500 traded cryptocurrencies. Bitcoin is the largest by far. On a recent day (March 9, 2015), the site showed Bitcoin trading at $291 per unit, with a market cap of $4.05 billion. The second and third largest cryptocurrencies, Ripple and Litecoin, had market caps respectively 8.5 percent and 1.8 percent as large. The entire set of non-Bitcoin cryptocurrencies (known as "altcoins") had a market cap of roughly $619 million, or 15 percent of Bitcoin's. Stated differently, Bitcoin had roughly 87 percent of the market, altcoins 13 percent. In percentage terms, altcoins do a higher share of Bitcoin's business than Bitcoin does of the Federal Reserve Note's business (currently $1.35 trillion in circulation). In trading volume the percentage share of altcoins (led by Litecoin and Ripple) has been similar.

The cryptocurrency market has grown about fourfold in market cap over the last 22 months, with altcoins growing faster than Bitcoin. This is seen by comparing recent data to the oldest snapshot of the CoinMarketCap site available via the Internet Archive "Wayback Machine," which reports data for May 9, 2013. On that date, Bitcoin had a price of $112 per unit, and a market cap of $1.2 billion. The two largest altcoins at that time, Litecoin and Peercoin (aka PPCoin), had market caps respectively 4.7 percent and 0.4 percent as large. Only 13 altcoins were listed. Jointly their market cap was about 6 percent of Bitcoin's, giving Bitcoin 95 percent of the market. Since then, the market share of altcoins has doubled, and their market cap has grown ninefold. Trading volumes then were not reported.

At $4.05 billion, the market cap of Bitcoin, as of March 2015, was slightly smaller than the dollar value of the September 2014 monetary bases of the Lithuanian litas ($5.8 billion) and the Guatemalan quetzal ($5.5 billion), but larger than those of the Costa Rican colon ($3.3 billion) and the Serbia dinar ($3.3 billion).[2] The August 2014 figures from the Central Bank of the Bahamas do not provide the

[2]All figures to follow come from official central bank websites, converted to U.S. dollars using the xe.com rates for September 30, 2014.

monetary base, but count Bahamian dollar currency in circulation at $210 million, less than two-thirds of Ripple's recent market cap of around $344 million.

Medium of Exchange, Store of Value, and Medium of Remittance Functions

The retail use of Bitcoin as a medium of exchange for goods and services is small to date, but is growing. In December 2014, Microsoft began accepting bitcoin payments "to buy content such as games and videos on Xbox game consoles, add apps and services to Windows phones or to buy Microsoft software" (BBC 2014). In doing so it joined prominent online retailers Overstock, Dell, Expedia, TigerDirect, and Newegg, and the payment processors Paypal and Square. The list grows weekly. Payments processing firms Bitpay, Coinbase, Coinkite, and others are enabling (and recruiting) brick-and-mortar retail shops to accept Bitcoin from any consumer whose smartphone "Bitcoin wallet" application can display a QR code. On its website Bitpay claims a clientele of "44,000 businesses and organizations"; Coinbase claims 37,000. These processors offer to purchase the consumer's bitcoin as it is spent, paying the equivalent (minus a fee) in dollars or other preferred currency to the merchant. The merchant avoids all exchange rate risk of holding bitcoin. For the retailer on the front end of the transaction, "accepting bitcoin" via these services actually means receiving dollars (or euros, etc.), just like accepting a credit card or debit card does. Bitpay and Coinbase thereby remove the barrier against transacting in cryptocurrency posed by the incumbency advantage of the established domestic currency unit (Luther and White 2014), just as Visa and Mastercard enable merchants to accept credit and debit cards from a customers whose accounts are denominated in a foreign currency.

A potentially vast market for bitcoin and altcoin use is international remittances. For example, workers abroad send an estimated $25 billion per year to the Philippines, where remittances contribute a remarkable 10 percent of national income. The established remittance services Western Union and MoneyGram commonly charge more than 10 percent in fees. Bitcoin remitters, by contrast, are charging only 1 percent. As the CEO of a recently launched bitcoin remittance service remarked to a reporter: "We thought: with

Bitcoin we can do it cheaper." A Filipino working in Singapore or Hong Kong (say) doesn't need to have online access or a Bitcoin wallet. The worker can purchase bitcoins at a BTM (bitcoin teller machine), bring the QR code printout to the local "rebittance" provider's office, and the service delivers Philippine pesos as a direct deposit into a designated recipient's account at a participating bank back home or (for an addition fee but still much less than the legacy firms) as cash (Ferraz 2014, Buenaventura 2014).

Market Competition

The market for cryptocurrencies has always been characterized by free entry. A new development in the past two years is competition from profit-seeking enterprises. Free entry is exhibited by the remarkable growth in the number of altcoins, from the 13 listed in May 2013 to the 500+ listed in March 2015. Profit-seeking by new entrants is especially conspicuous in systems like Ripple (2nd behind Bitcoin in market cap as of March 9, 2015), BitShares (4th), Nxt (6th), and MaidSafeCoin (8th). In each of these systems a substantial share of "pre-mined" coins was initially held by their developer-entrepreneurs. The entrepreneurs hope to profit by raising the coin's market price through efforts to promote wider use of the coin and its associated proprietary payment network or trading platform, such that they can eventually realize a market value for their coin holdings greater than their expenditures on development and promotion.

Bitcoin, by contrast, was launched by a pseudonymous programmer (or set of programmers) apparently as a public-spirited experiment. Revenue from producing ("mining") new coins, the reward for validating peer-to-peer transfers, is open to anyone with the computing power to participate successfully. While Federal Reserve Bank of Chicago economist François Velde (2013) is thus right to contrast the nonprofit Bitcoin system to the profit-seeking firms that Hayek (1978a) foresaw, the contrast does not apply to the new enterprises that are launching altcoins for profit.[3] In these new altcoin enterprises

[3]Velde also writes that Bitcoin does not "truly embody what Hayek and others in the 'Austrian School of Economics' proposed." But I would distinguish Hayek's *proposal*—to allow free choice and private competition in currency—from his *prediction* about what type of money would then dominate the field.

we see a working embodiment of competitive issue of irredeemable money by profit-seeking private firms. It is no longer correct—if it ever was—to say that Bitcoin is not "operating in a competitive environment." Bitcoin competes with altcoins in the same way that the giant nonprofit YMCA competes with smaller nonprofit and for-profit health clubs, or a large nonprofit hospital competes with smaller nonprofit and for-profit immediate-care clinics.

The Novel Implementation of Quantity Commitments

We should not be too surprised that the features of competing irredeemable privately issued currencies are different from what Hayek (and other economists) imagined, for two reasons. First, market competition is a discovery procedure as Hayek (1978b) elsewhere emphasized, in which successful entrepreneurs discover profit in overlooked or unforeseen ways of producing products and reconfiguring product features. Secondly and more specifically, Hayek imagined that the issuer of a successful irredeemable private currency issuer would retain discretion to vary its quantity. The issuer would promise (but not make any contractual commitment) to maintain a stable purchasing power per unit.[4] A naked promise of that sort unfortunately appears to be time-inconsistent (Taub 1985; White 1989: 382–83; White 1999: ch. 12). An issuer whose promise was believed could reap a large one-time payoff by spending a massive batch of new money into circulation until the public caught on. The one-time profit would exceed the normal rate of return from staying in business. By assumption, there would be no legal recourse against the decline of the money's value. Aware of the problem, the public would not believe the promise to begin with, giving the money zero value in equilibrium.

The traditional solution to the problem of giving a privately issued money a reliably positive value is a redemption contract, an enforceable money-back guarantee or *price commitment* (White 1989). Under the gold standard, a banknote was worth $20 when the bank of issue was bound to pay a $20 gold coin for it. Today a

[4]Benjamin Klein (1974), in a more formal model, supposed perfect competition among issuers on "rental price"—that is, the risk-adjusted rate of return to holding money—in an environment of perfect foresight or the equivalent (see White 1999: ch. 12).

bank deposit is worth $100 when the bank is bound to pay $100 in Federal Reserve Notes for it. A suitable medium of redemption has a value that is known and independent of actions by any particular bank of issue.

Ronald Coase (1972) identified an alternative solution to the problem—how an issuer is to bind himself not to run down the price of the thing issued—in the context of a monopolist selling a durable good priced above marginal cost. To get customers to pay $200 for an art print when the marginal cost of producing a duplicate copy is $1, the artist must convince them that she will not run off and sell lower-priced duplicates in the future. To commit herself, the artist produces the print in a numbered edition with a stated maximum ("this print is #45/200"), providing an enforceable *quantity commitment* that she will issue no more than a fixed number of prints. Despite discussing this solution years ago (White 1989), I did not foresee that a quantity commitment could be used in practice to launch a successful irredeemable private currency.[5]

It is this second solution that Bitcoin has creatively introduced to the field of private currency. The implementation uses an entirely new technology: the limit on the number of Bitcoin units in the market is not guaranteed by a contractual promise that can (with some probability) be enforced on an issuing firm, but rather by a limit having been *programmed* into the Bitcoin system's observable source code and being continuously verifiable through a public ledger (the "block chain") that is shared among all "miners" who participate in bitcoin transactions processing.[6] Altcoins employ the same basic idea of a programmed quantity commitment verified through a public ledger, though sometimes implemented in a different way.

Altcoin Innovations

In order to compete with the market leader Bitcoin, the developers of altcoins have understandably emulated its best features (decentralized peer-to-peer exchange, quantity commitment embedded in

[5]I believed that redeemable claims to a commodity money would be preferred over any IOU-nothing as a medium of exchange. And perhaps they would be even today, if not for government suppression of the former. For recent examples of suppression, see Dowd (2014: 1–37) and White (2014b).

[6]On the mechanics of the Bitcoin system see King, Williams, and Yanofsky (2013), Velde (2013), and Dowd and Hutchinson (2015).

an open source code, and shared public ledger), while introducing various general improvements and customizations. Most of the emphasis has been on improving speed, robustness, and privacy. A few altcoins aim to serve niche constituencies.[7]

The first generation of altcoins are nonprofit projects like Bitcoin, but tweak the Bitcoin code. Litecoin was introduced in October 2011 to provide faster transaction confirmation times (2.5 minutes versus 10 minutes). Peercoin, launched in August 2012, increases the speed even more by using a newer protocol ("proof of stake" rather than Bitcoin's "proof of work") that is less computationally demanding. This protocol also promises to allow participants to share in the rewards from mining without joining mining pools or buying the expensive specialized equipment that it now takes, as the result of competition, to succeed at Bitcoin mining. Because Peercoin's protocol, unlike Bitcoin's, does not promote the merger of miners into ever-larger pools, it is said to be less vulnerable to a possible collusive attack by 51 percent of miners.[8] Primecoin, a later project from Peercoin's main developer, implements a newer proof-of-work protocol (finding prime numbers) to reduce confirmation times to 1 minute.

Darkcoin, a nonprofit project launched in April 2014, and recently renamed Dash, has introduced payment confirmation "within seconds." Dash alters the Bitcoin code to provide greater anonymity to users. Whereas the Bitcoin ledger puts every transaction and transactor address on public view, Dash transactions are "obfuscated." BlackCoin, supported by an active nonprofit foundation and first listed in February 2014, uses a "proof of stake" protocol for speedy verification. It is connected to a proprietary trading platform, BlackHalo, that promises greater user anonymity than other systems. Blackcoin can now be spent (along with Bitcoin and Litecoin) at participating retail shops using the Coinkite debit card.

[7]While CoinMarketCap.com tracks market caps, the site CoinGecko.com ranks altcoins on a combination of market cap, trading volume, ongoing development activity, and social media buzz. In December 2014 it had Dogecoin at #2 and Darkcoin at #6, each four steps above its market cap ranking, based on their buzz factors. By March 2015 Darkcoin (Dash) had risen to #5 in market cap.

[8]On this problem with the Bitcoin protocol, see Dowd and Hutchinson (2015), who predict that it will bring Bitcoin's demise. Whether or not they are right about that, many altcoin developers have recognized the problem and have made deliberate design changes to avoid what Dowd and Hutchinson call "inherent tendencies toward centralization, takeover, and collapse."

Ripple, first traded in August 2013, is a cryptocurrency issued by the for-profit enterprise Ripple Labs. It does not rely on a mining protocol. A fixed stock of Ripples was "premined," though the developers have not released them all yet. To make the fixity of the Ripple stock credible, the system follows Bitcoin's lead in having a shared public ledger. The Ripple payment network confirms transactions through a "consensus" protocol that works *much* faster than mining protocols (5 seconds versus 1 to 10 minutes), so has a much better prospect of competing with ordinary credit and debit cards for point-of-sale transactions. The coin is only one part of the parent firm's efforts, which include building a wholesale remittance system for "real-time, cross-border payments" between banks, cheaper and faster than the legacy Automated Clearing House system (Liu 2014). Stellar is a non-profit project that emulates Ripple.

BitShares also promises greater anonymity and ease of use. Like Ripple, it is part of a larger for-profit enterprise funded by venture capital. In this case the larger project, according to the BitShares Wiki (http://wiki.bitshares.org/index.php/BitShares), is an "experiment," based on "a business model similar to existing banks or brokerages," to enable the creation and trading of "BitAssets," digital derivative contracts on "the value of anything from dollars, to gold," to exchange-traded equities, bonds, and commodities. The project exemplifies what two *Wall Street Journal* writers (Vigna and Case 2014) describe as "so-called Bitcoin 2.0 technologies—those bitcoin-inspired software applications that bypass financial middlemen and allow almost any asset to be digitized and traded over a decentralized computer network."

The niche-market strategy of CannabisCoin is to offer a payment service for medical marijuana dispensaries and other cannabis retailers whose access to bank accounts and credit cards is currently being blocked by the federal government even where their business has been legalized at the state level. In October 2014, the coin's promoters were seeking retailers willing to provide a specific type of cannabis to patients at one gram per one CannabisCoin. Whether this will lead to the institution of a new commodity money standard remains to be seen, however, as the number of participating retailers and their supplies were quite limited. The promotional effort appears to have helped the market cap of CannabisCoin to surge ahead of other cannabis-themed

cryptocoins, such as the earlier-launched Potcoin and the more recent MaryJaneCoin.

Auroracoin is an Iceland-only altcoin introduced in February 2014 for the purpose of helping Icelanders evade the country's exchange controls. (The controls, which included a ban on Bitcoin purchases, were imposed during the financial crisis in October 2008 and are still in place.) Scotcoin, launched by an Edinburgh venture capitalist in May 2014, in advance of Scotland's independence referendum, is likewise a nationally specific enterprise. Its backer has expressed the hope (Hern 2014) that "introducing a voluntary cryptocurrency, which may in the future act as a medium of exchange for the Scottish people, can only benefit them should there be major disruption." A recent entry is CzechCrownCoin, launched October 2014, at least half of which is being distributed to Czech citizens. None of these national coins had a March 2015 market cap above $55,000.

But Aren't They All Just Bubbles?

A quantity commitment solves the problem of making a credible commitment not to overissue. But it has a major shortcoming when applied to currency. Unlike a price commitment, it leaves the market price of the currency to vary with demand. This explains how it is possible for the prices of Bitcoin and other cryptocurrencies to be as volatile as they have recently been (Luther and White 2014). And it explains how it was possible for several altcoins, when enthusiasm for them evaporated, to decline to near-zero market cap.

The collapse of several altcoins is readily evident on CoinMarketCap.com. Three of the earliest thirteen altcoins have declined substantially in market cap. Terracoin, which at its peak had a market cap of $7.1 million, is now (March 2015) down to around $23,000, a decline of more than 99 percent. Freicoin, which peaked at $16.1 million, has fallen to around $61,000, also a decline of more than 99 percent. The whimsically named BBQCoin, having peaked at $7 million, now trades around $21,000, another 99+ percent decline. All three had very sharp run-ups to their peaks in early December 2013, mostly reversed by month's end. Megacoin, first listed in July 2013, experienced the same December 2013 pattern, soaring from $1.2 million on

November 23, 2013, to a peak of $47.5 million on December 1, then sliding to around $328,000 today, a decline of more than 99 percent. Later-peaking examples of altcoins suffering 98 percent or greater peak-to-present declines have included Mooncoin, CryptCoin, Scotcoin, Bitgem, and CrtCoin.

Looking only at the market cap charts, the most remarkable case appears to be Auroracoin, which quickly climbed to chart a recorded market cap of $953 million, but is valued today at around $46,000, a drop of more than 99.99 percent. The incredible valuation of nearly $1 billion was, even at the time, a misstatement. The Auroracoin launch plan (Hern 2014) was to jump-start enthusiasm by giving away about 30 premined coins to every Icelandic citizen, for a total of 10 million units. (Such a giveaway is known, in honor of Milton Friedman's famous thought experiment, as a "helicopter drop" or "airdrop.") Dividing the CoinMarketCap.com peak valuation by the price on that day (March 4, 2014) indicates 10 million units in the market, when the number of coins actually available was one-hundredth of that figure (Torpey 2014), the airdrop having yet to be made. Multiplying the price by the actual number of coins, the true market cap was one-hundredth of the reported value, around $9.53 million. A drop from $9.53 million down to the current $46,000, however, is still a 99+ percent drop.

The repeated experience of crashing altcoins, in which the market valuation of a once-popular cryptocurrency all but evaporates, suggests in retrospect that the prices of *those* coins, at least, were simply bubbles. That is, such a coin's demand was unsupported by any price-independent usefulness that would put a floor under its equilibrium market price. (By contrast, industrial and ornamental uses support gold's market value.) To understand the argument, consider again the example of an artist's print. Some print buyers are presumably not just speculators who will put the print in storage and hope for its price to rise, but art-lovers planning to hang it on the wall and enjoy the real aesthetic pleasure it provides. That enjoyment is independent of its price. An irredeemable currency, by contrast, is presumed in standard monetary theory to be held only in order to be later spent or sold. It provides no service that is independent of its market value. People thus presumably have a positive demand price for any irredeemable currency, giving it a positive market value, only to the extent that they expect it to have a future market value. A market

valuation anchored by *nothing* but expectations of market valuation is the definition of a bubble.[9]

Does this logic show that the prices of all cryptocurrencies are pure bubbles? No. We cannot rule out that the flourishing cryptocurrencies have some fundamental support.

As several economists have proposed, owning Bitcoin (or other cryptocurrency) may provide a kind of real pleasure to at least some of its holders, say anti-statists who like what it stands for,[10] tech enthusiasts who admire its ingenuity, or its own developers who gladly stake some wealth to help their project succeed (Luther 2013, Murphy 2013, Selgin 2014). For such an individual we can determine his affinity-based demand curve for Bitcoin by positing that he wants to own Bitcoin worth not just any old amount, but rather a specific amount of purchasing power, say 100 real U.S. dollars. (A "real dollar" here means the equivalent in purchasing power to the dollar of a specified base year.) We can plot the individual's demand curve against the real price, i.e. the U.S. dollar price of Bitcoin divided by the dollar price level. The individual's demand curve will be a rectangular hyperbola, a familiar construct in the basic theory of a fiat money's value. The market demand curve sums all the individual demand curves. At a given U.S. dollar price level, if ten thousand individuals want to hold an average of $100 worth of Bitcoin each, just because Bitcoin is cool, then the market cap of Bitcoin must be at least $1 million.

This account does not explain day-to-day variations in the market price of Bitcoin, but it does potentially explain why the price is above zero. In this way real affinity demand provides an answer to economist-blogger Brad DeLong's (2013) rhetorical question: "Placing a floor on the value of bitcoins is . . . what, exactly?" Of course, if Bitcoin were to become completely uncool to *everyone*, the floor would vanish.[11]

[9]The same argument applies to any fiat money, to the extent that its market value exceeds whatever floor value it has due to exclusive tax receivability or other government compulsion. No cryptocurrency has *that* kind of support.

[10]A pseudonymous commenter on the reddit CryptoMarket page (Pogeymanz 2014) writes about Darkcoin: "I have some DRK because I like what it stands for."

[11]DeLong (2013) also writes: "Placing a ceiling on the value of bitcoins is computer technology and the form of the hash function . . . until the limit of 21 million bitcoins is reached." Actually, of course, Bitcoin's source code does not put a ceiling on the market cap or *value* of bitcoins, only a limit on the *quantity*. The conceptual ceiling on *value* is Bitcoin achieving a 100 percent share of the real value of all money balances in the world (Luther and White 2014).

I previously (White 2014a) too hastily rejected this argument as an explanation of how Bitcoin first achieved a positive market price, on the grounds that it "does not deliver what the argument requires, namely, an account of how Bitcoins initially had a positive value *apart from their actual or prospective use as medium of exchange*. The value at every point in this scenario derives entirely from use or prospective use as a medium of exchange (only such use as a dollar competitor is what might [provide aesthetic pleasure], not the existence of untraded digital character strings)." I was mistaken to think that the argument has such a requirement. A positive affinity valuation of a cryptocurrency may well require the *possibility* of its taking off as a nonstate money, but that does not imply a chicken-or-egg problem. Affinity demand and hence market value can be positive before actual medium-of-exchange use begins.

The affinity account has the additional merit of being consistent with the great market cap of Bitcoin, esteemed for being the first mover, the middling market cap of altcoins that embody valuable technical improvements and have active support communities, and the low market cap of me-too altcoins. Five hundred altcoins are not all making a statement or breaking new technical ground. They have positive market caps, but most of them are slight.

A second grounding for fundamental value lies in the real demand for the sorts of payment services offered by a cryptocurrency. Ownership of a particular brand of cryptocurrency units is needed to make use of the brand's payment system, which may offer advantages over other systems (Tucker 2014).

With regard to the "bubble" element in cryptocurrency valuation, economist-blogger Stephen Williamson (2011) reminds us that official fiat money or a commodity money likewise trades well above its fundamental value. In a case where the surplus of a currency asset's market value over its fundamental value results from its solving a medium-of-exchange coordination problem, that surplus is a good thing because it represents value-added:

> Bubbles can be good things, as any asset which is used widely in exchange will trade at a price higher than its "fundamental," and the asset's liquidity premium—the difference between the actual price and the fundamental—is a measure of the asset's social contribution as a medium of exchange.

I would, however, qualify this claim by saying that the difference is a reliable measure of social contribution only insofar as it arises through voluntary trade rather than legal compulsion, and only after we subtract the costs of generating and maintaining the asset in question. It is from by adding such value that Ripple's entrepreneurs hope to profit. Unlike an official fiat currency, no part of Ripple's valuation is based on legal compulsion.

Is There a Problem of Monopoly? Is There Too Much Competition?

Milton Friedman (1960: 8) wrote of "the technical monopoly character of a pure fiduciary currency which makes essential the setting of some external limit on its amount." By "pure fiduciary currency" he meant an irredeemable or fiat currency. By "technical monopoly character" he meant that open entry into counterfeiting would drive the value of an irredeemable paper currency note down to the cost of paper and ink,[12] and all the way down to zero if ever-higher denominations could be introduced at no higher cost. Therefore, a single authorized issuer was needed to preserve the currency's value. As Benjamin Klein (1974) pointed out, however, Friedman here conflated monopoly with enforcement of trademarks. To ban the selling of knock-off perfume in bottles bearing a counterfeit Chanel trademark does not imply giving Chanel a monopoly except in the sale of Chanel-branded perfume. It does not require any restriction on the production of competing perfumes under different trademarks. Enforcing a ban on the counterfeiting of Federal Reserve Notes, or in other words having the Secret Service protect the Federal Reserve's trademark, does not require giving the Fed a monopoly on currency issue.

The counterfeiting of bitcoins (also known as the problem of "double spending") is prevented not through police work and legal prosecution by any central authority, but quite elegantly by the decentralized verification process that prevents the transfer of any coin of unattested provenance from being accepted onto the public ledger. With such effective de facto counterfeiting protection, the quantity of bitcoins remains on its programmed path.

[12]For a real-world example of this happening, see Luther (2012).

Velde (2013) states that Bitcoin has "a status of quasi-monopoly in the realm of digital currencies by virtue of its first-mover advantage." By "quasi-monopoly status" he may mean only that Bitcoin has a large market share, derived from its being the first mover into (that is, creating) the market. But such a status is distinct from the usual concept of natural monopoly (or quasi-monopoly) status due to economies of scale, which denotes the ability to serve every (or nearly every) part of the market at lower marginal cost than competitors. The main static danger of a monopoly in the usual sense, whether natural or state-granted, is that the monopolist firm may restrict output to raise price above marginal cost, thwarting efficiency by sacrificing potential gains from trade. Because the quantity of bitcoin is predetermined by a program and not manipulable by a discretionary issuer, it poses no danger of any such monopolistic output restriction.

Competition from new entrants surrounds Bitcoin. The new entrants have the advantage of being able to introduce altcoins with improved features while the Bitcoin code was written five-plus years ago. The Bitcoin community can at most agree to patch the code, not to fundamentally revise it. Bitcoin does have the largest established network, but a dominant proprietary network does not imply monopoly pricing (in this context, transaction fees above marginal cost) when the market is contestable. Ripple, Litecoin, BitShares, and others entrants are vigorously contesting the market. The cryptocurrency market exhibits Schumpeterian competition from new business models rather than only static price competition.

DeLong (2013) raises an issue that is the opposite of monopolistic restriction. He worries that competition from more and more altcoins may expand the total quantity of cryptocoins without limit, and thereby—unless Bitcoin "can somehow successfully differentiate itself from the latecomers"—drive the market value of Bitcoin and all other cryptocurrencies to zero. He writes: "the money supply of BitCoin-like things is infinite because the cost of production of them is infinitesimal." To consider this possibility let us suppose, for the sake of argument, that the cost of introducing a me-too altcoin is indeed infinitesimal. The economic implication is that in a fully arbitraged equilibrium the

marginal altcoin will have an infinitesimal real value (which is an approximate description of the marginal altcoins we do in fact observe). But this is not to say that the value of bitcoins (or of established altcoins) will tend toward zero. Infinitesimally valued altcoins do not eat into Bitcoin's market share in real terms. Only valued altcoins can do that, as they have since May 2013 (reducing Bitcoin's share to 87 percent from 95 percent as noted; but at the same time Bitcoin's market cap in U.S. dollars grew more than three-fold).

In the foreign exchange market for government fiat monies with flexible exchange rates, hyper-expansion in the nominal supply of dollar-like things, say Zimbabwe dollars or Venezuelan bolivars, does not drag down the purchasing power of the U.S. dollar. Likewise, in the existing altcoin market with its completely flexible exchange rates, cheap altcoins simply have low exchange value against Bitcoin and do not drag down Bitcoin's real market value.

Cryptocurrency and Fiat Currency: Comparisons and Contrasts

DeLong likens Bitcoin to government fiat money in the following way: "Bitcoin is like fiat money, and unlike 18th and 19th century Yap stone money, in that its cost of production is zero." In fact, although Bitcoin is similar to a government fiat money (and unlike gold) on the demand side, in that nothing supports its price if transaction and other money-related demand for it goes to zero, it is absolutely *unlike* a government fiat money on the supply side. It does not have an indefinitely expandable supply but the opposite. Just as monopolistic under-supply is ruled out (see above), so too is hyper-expansion. Bitcoin has a verifiably programmed commitment to a pre-specified quantity path.[13] In light of that commitment, the

[13]Blogger Charlie Stross (2014) colorfully comments that Bitcoin "wears a gimp suit and a ball gag, padlocked into permanent deflation and with the rate of issue of new 'notes' governed by the law of algorithmic complexity." That padlocked "gimp suit and ball gag" is Bitcoin's binding quantity commitment. It is a feature, not a bug.

cost of production beyond the scheduled quantity is extremely high, not zero.[14]

Noting that "improvements, bug fixes, and repairs" to the Bitcoin code have been "carried out by the community of bitcoin users, dominated by a small set of programmers," Velde (2013) downplays the prospects for Bitcoin to rival the fiat U.S. dollar:

> Although some of the enthusiasm for bitcoin is driven by a distrust of state-issued currency, it is hard to imagine a world where the main currency is based on an extremely complex code understood by only a few, and controlled by even fewer, without accountability, arbitration, or recourse.

Substitute the phrase "bureaucratic agency" for the word "code" in this statement, however, and the hard-to-imagine world becomes a fair description of our current world of Federal Reserve currency. This fact completely overturns Velde's argument. If the prospects for Bitcoin against the dollar depended only on the public's choice between trusting an open source code with a public ledger and trusting a byzantine central bank, the prospects would look extremely good.

Bitcoin as a Vehicle Currency and Unit of Account

Finally, Bitcoin has an interesting role that is often overlooked or denied. A recent paper by a team of Bank of England economists (Ali et al. 2014), for example, declares that cryptocurrencies "are not typically used as media of exchange" and "there is little evidence of digital currencies being used as units of account." In fact Bitcoin is the vehicle currency (commonly accepted medium of exchange), and consequently is the unit of account, in most altcoin markets. With a few exceptions (Litecoin against U.S. dollar, Chinese yuan, and euro; Chinese exchanges where altcoins trade against yuan; Peercoin

[14]In light of its programmed production limit, Selgin (2013) calls Bitcoin a "synthetic commodity money." He helpfully likens Bitcoin's quantity commitment to the quantity commitment of an artist who publicly destroys the engraved plates from which a known number of lithographic prints have been made.

against dollar), the vast majority of altcoin exchanges trade and quote prices in bitcoins, not in dollars, euros, or yuan.[15]

The altcoin market is structured this way for the same reason that the U.S. dollar is the vehicle currency for foreign exchange transactions (Kreuger 2012). To trade (say) Australian dollars for British pounds, the standard route is AUD for USD, then USD for GBP. Thicker markets enjoy lower bid-ask spreads. The U.S. dollar currency markets are so much larger than others that for most almost all currency pairs that do not include the U.S. dollar (euro-yen is an exception) the sum of bid-ask spreads is less for indirect exchange via the U.S. dollar than for direct exchange. This pattern is self-reinforcing by bringing more volume to the U.S. dollar markets.[16] Most non-USD to non-USD foreign exchange markets are missing.

The Bitcoin-U.S. dollar market has much more volume and thus much lower spreads than any altcoin-U.S. dollar market. To trade U.S. dollars for an altcoin, often the *only* route in practice is to trade U.S. dollars for Bitcoin, and then Bitcoin for the altcoin. Most altcoin-dollar markets are missing because volume would be too low to have attractive bid-ask spreads. With by far the thickest potential markets against any altcoin, even compared to U.S. dollars, Bitcoin is naturally the vehicle currency and thus the unit of account in altcoin markets.

Policy Implications

The market for cryptocurrencies is still evolving, and (to most economists) is full of surprises. Policymakers should therefore be very humble about the prospects for improving economic welfare by restricting the market. Israel Kirzner's (1985) warning about the perils of regulation strongly applies here: Interventions that block or divert the path of entrepreneurial discovery will prevent the realization of potential breakthroughs such that we will never know what we are missing.

[15]See http://www.cryptocoincharts.info/main/priceBoxes.

[16]The positive network effect that makes the U.S. dollar the common medium for inter-currency exchange echoes the self-reinforcing Mengerian process by which a common medium for inter-commodity exchange (money) emerged out of barter.

References

Ali, R.; Barrdear, J.; Clews, R.; and Southgate, J. (2014) "The Economics of Digital Currencies." Bank of England *Quarterly Bulletin* (Q3): 1–11.

BBC (2014) "Microsoft to Accept Payments made in Bitcoins" (11 December): www.bbc.com/news/technology-30377654.

Buenaventura, L. (2014) "The Rise of Rebittance: Reinventing Money Transfers in the Philippines with Bitcoin." *The Next Web* weblog (28 September): http://thenextweb.com/insider/2014/09/28/rise-rebittance-reinventing-money-transfers-philippines-bitcoin.

Coase, R. (1972) "Durability and Monopoly." *Journal of Law and Economics* 25 (April): 143–49.

Crockett, G. (2014) "Bitcoin Is Seen as an Ephemeral Currency." *Washington Post* Style Invitational Contest, Week 1062: Poems from the headlines (27 April): www.washingtonpost.com/entertainment/style-invitational-week-1069-big-thoughts-little-words-plus-more-from-recent-contests/2014/04/16/f556bf74-c331-11e3-b574-f8748871856a_story.html.

DeLong, B. (2013) "Watching Bitcoin, Dogecoin, Etc." *Equitable Growth* weblog (28 December): http://equitablegrowth.org/2013/12/28/watching-bitcoin-dogecoin-etc.

Dowd, K. (2014) *New Private Monies: A Bit-Part Player?* London: Institute of Economic Affairs.

Dowd, K., and Hutchinson, M. (2015) "Bitcoin Will Bite the Dust." *Cato Journal* 35 (2): 357–382.

Ferraz, E. (2014) "Send Home Your Wages Using Bitcoin and Avoid Hefty Money Transfer Fees? That's Now a Reality." *Tech in Asia* (3 July): www.techinasia.com/send-home-wages-bitcoin-avoid-hefty-money-transfer-fees-reality.

Friedman, M. (1960) *A Program for Monetary Stability*. New York: Fordham University Press.

Hayek, F. A. (1978a) *The Denationalisation of Money*, 2nd ed. London: Institute of Economic Affairs.

_____ (1978b) "Competition as a Discovery Procedure." In Hayek, *New Studies in Philosophy, Politics, Economics, and the History of Ideas*. London: Routledge.

Hern, A. (2014) "Bitcoin Goes National with Scotcoin and Auroracoin." *The Guardian* (25 March): www.theguardian.com

/technology/2014/mar/25/bitcoin-goes-national-with-scotcoin-auroracoin.

King, R. S.; Williams, S.; and Yanofsky, D. (2013) "By Reading This Article, You're Mining Bitcoins." *Quartz* webzine (17 December); http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins.

Kirzner, I. M. (1985) "The Perils of Regulation: A Market-Process Approach." In Kirzner, *Discovery and the Capitalist Process*, 119–49. Chicago: University of Chicago Press.

Klein, B. (1974) "The Competitive Supply of Money." *Journal of Money, Credit, and Banking* 6 (November): 423–53.

Krueger, M. (2012) "Money: A Market Microstructure Approach." *Journal of Money, Credit and Banking* 44 (September): 1245–58.

Liu, A. (2014) "Ripple Labs Signs First Two US Banks." *Rippleblog* weblog (24 September): https://ripple.com/blog/ripple-labs-signs-first-two-us-banks.

Luther, W. J. (2012) "The Monetary Mechanism of Stateless Somalia." Kenyon College Working Paper, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2047494.

_____ (2013) "Cryptocurrencies, Network Effects, and Switching Costs." Mercatus Center Working Paper No. 13–17, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134.

Luther, W. J., and White, L. H. (2014) "Can Bitcoin Become a Major Currency?" *Cayman Financial Review* (August): www.compass-cayman.com/cfr/2014/08/08/Can-bitcoin-become-a-major-currency.

Murphy, R. P. (2013) "The Economics of Bitcoin." *Library of Economics and Liberty* (3 June): www.econlib.org/library/Columns/y2013/Murphybitcoin.html.

Pogeymanz (2014) Comment in the Thread "Darkcoin Is Going to Be a Behemoth," www.reddit.com/r/CryptoMarkets/comments/20t9nc/darkcoin_is_going_to_be_a_behemoth.

Selgin, G. (2013) "Synthetic Commodity Money." University of Georgia Working Paper, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.

_____ (2014) "Mises Was Lukewarm on Free Banking." *Liberty Matters* (January): http://oll.libertyfund.org/pages/misestmc.

Stross, C. (2014) "Schadenfreude." *Charlie's Diary* weblog (25 February): http://www.antipope.org/charlie/blog-static/2014/02/schadenfreude-1.html.

Taub, B. (1985) "Private Fiat Money with Many Suppliers." *Journal of Monetary Economics* 16 (September): 195–208.

Torpey, K. (2014) "Auroracoin's Market Cap Is Highly Inflated." *Cryptocoins News* (4 March): www.cryptocoinsnews.com/auroracoins-market-cap-highly-inflated.

Tucker, J. (2014) "What Gave Bitcoin Its Value?" *The Freeman* (27 August): http://fee.org/the_freeman/detail/what-gave-bitcoin-its-value.

Velde, F. R. (2013) "Bitcoin: A Primer." *Chicago Fed Letter* 317 (December): www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf.

Vigna, P., and Case, M. J. (2014) "BitBeat: Ratings Firm Coinist Tackles Trust Problem with Bitcoin 2.0 Projects." *Wall Street Journal MoneyBeat* weblog (12 August): http://blogs.wsj.com/moneybeat/2014/08/12/bitbeat-ratings-firm-coinist-tackles-trust-problem-with-bitcoin-2-0-projects.

White, L. H. (1989) "What Kinds of Monetary Institutions Would a Free Market Deliver?" *Cato Journal* 9 (Fall): 367–91.

_____ (1999) *The Theory of Monetary Institutions*. Oxford: Basil Blackwell.

_____ (2014a) "Ludwig von Mises's The Theory of Money and Credit at 101." *Liberty Matters* (January): http://oll.libertyfund.org/pages/misestmc.

_____ (2014b) "The Troubling Suppression of Competition from Alternative Monies." *Cato Journal* 34 (Spring/Summer): 181–201.

Williamson, S. (2011) "Bitcoin." *New Monetarist Economics* weblog (24 June): http://newmonetarism.blogspot.com/2011/06/bitcoin.html.