

HARWOOD

Economic Review

AMERICAN INSTITUTE FOR ECONOMIC RESEARCH

FALL 2017
Volume 1, Issue 1

**Is Blockchain the
Future of Freedom?**
page 4

Harwood Economic Review

AMERICAN INSTITUTE FOR ECONOMIC RESEARCH

- 3** In This Issue
Edward Stringham
- 4** Is Blockchain the Future of Freedom?
Max Gulker
- 8** Prospects for a Digital Gold-Backed Currency
Theodore Cangero
- 12** Decision Time for Bitcoin?
Patrick Coate
- 14** Bitcoin: Decentralized Governance Put to the Test
Max Gulker



In This Issue

Edward Stringham, President

Welcome to the American Institute for Economic Research's new periodical, *Harwood Economic Review*. Colonel E.C. Harwood founded our institute out of MIT in 1933 and was an early contributor to what today is called the Austrian Theory of the Business Cycle and other areas where government was not as scientific as its officials claim." He correctly predicted inflation and economic malaise in the 1930s and 1970s and said those resulted from ill-conceived government policies. As recently as ten years ago, many economists were claiming that government had permanently solved the problem of business cycles, and today many of these same people still claim that we need government to manage the economy moving forward. Yet Harwood's insights were just as relevant now or ten years ago as they were in Harwood's time. We should not be swayed by technocrats who believe they can manage the economy better than the market can.

Harwood's friend F.A. Hayek said those who believe they can centrally manage an economy suffer a pretense of knowledge or a fatal conceit. Yet despite the disastrous failures of socialism in U.S.S.R, Cuba, North Korea, Venezuela, and everywhere it has been tried, the economic lessons are being lost. Today 51 percent of American Millennials say they oppose capitalism. A bad understanding of economics opens the door for politicians to promise everything under the moon from free healthcare, to free college, or even to a no-strings attached "universal basic income" where all people could somehow get away without working for their entire lives.

Economics explains the great mysteries of how the world works, but economists have not been successful at capturing the hearts and minds of the public. Most economists are actually guilty of writing for other academics in a dense and obscure way and ignoring what is important for the everyday person. But it would be a tragedy to give up the great debate and let our country go more in the direction of Greece or the explicitly socialist countries.

In 1950 E.C. Harwood wrote, "The American basic plan established the individual's right to seek life's satisfactions in any way that he desires, provided he does not infringe upon the equal rights of his fellows," but he was worried about negative developments in our country. Yet he stated "that most of the undesirable aspects of social development in the United States are not only remediable: they are traceable to deviations from, rather than defects in, the basic principles of the Nation's social plan."

Despite all of the achievements of our market economy and the massive failures of government interference with it, the progressive narrative that our heritage is fundamentally flawed is becoming increasingly popular. Step foot on a college campus and speak with any humanities professor for evidence.

Those who care about economics and the principles of a free society have our work cut out for us. But as Dwight Eisenhower said: pessimism never won any battle.

In the pages of *Harwood Economic Review* you can expect to read accessible, and relatively jargon-free, articles on economics. E.C. Harwood had a longstanding interest in gold or silver as an alternative to government fiat money. Might it be the case that cryptocurrencies like Bitcoin or Ethereum or technology associated with them (i.e. blockchain) help reintroduce some of the beneficial aspects of the Gold standard? Articles in this issue discuss some of the ways in which financial intermediaries are currently using blockchain technology to come out with new financial instruments.

As the new president of the American Institute for Economic Research, I hope we can build on the research program started by E.C. Harwood 85 years ago. America can continue to go down an anti-market path or it can look toward a system of free markets. E.C. Harwood stated that although "complete freedom" has "not yet been reached, perhaps not even imagined as yet. In the years to come we hope to aid in exploring the possibilities involved."

Edward A. Stringham

Is Blockchain the Future of Freedom?

By Max Gulker

Those who dream of a world with greater economic freedom have traditionally relied on the pen, the ballot box, and sometimes the sword to effect change. But a relatively new technology called blockchain may make the computer a potent tool to achieve greater liberty.

A blockchain is a type of database that is distributed to all users without a centrally managed hub and that stores unalterable digital records. It is most commonly known today as the technology underlying Bitcoin, keeping records of the cryptocurrency's ownership and allowing ownership to be transferred. This may only be the beginning, as some observers predict blockchain will be as important an advance for transactions and record keeping as the internet has been for communication and information.

This article will explain the basic attributes that make blockchain important, discuss some applications both proposed and already in use, and explain why anyone who cares about economic freedom should be very interested in the technology. While a full-on technological revolution may take a long time, many economists, technologists, and computer scientists do see one on the horizon.

What is blockchain?

It's easy to get bogged down in the computing details of blockchain, so this article will focus instead on the attributes that distinguish this technology. As a first approximation, think of blockchain as an unalterable digital "paper trail." Don and Alex Tapscott, authors of "The Blockchain Revolution," provide a good summary: "At its most basic, blockchain is a vast, global distributed ledger or database running on millions of devices and open to anyone, where not just information but anything of value—money, titles, deeds, music, art, scientific discoveries, intellectual property, and even votes—can be moved and stored securely and privately. On the blockchain, trust is established, not by powerful intermediaries like banks, governments and technology companies, but through mass collaboration and clever code. Blockchains ensure integrity and trust between strangers. They make it difficult to cheat." Observers often discuss five key attributes of blockchain:

Universal access A blockchain is a distributed database, meaning that each user, no matter how big or small, has equal access to the entire database and its real-time changes.

Peer-to-peer transmission There is no central storage hub or manager of a blockchain. Changes or transactions (i.e., blocks) get transmitted peer-to-peer, and the constantly updated database is stored in the multitudes of distributed copies rather than in a central home.

Pseudonymity Each user has a unique alphanumeric address of at least 30 characters; users can be anonymous or choose to provide their identity to others.

Irreversibility Records are chronologically linked in a chain and unalterable, due to both the "clever code" mentioned above and the lack of central storage, meaning that even if a hacker succeeded in changing one copy, the overwhelming majority of copies would maintain their accuracy.

Algorithms Users can set up "smart contracts" that automatically transfer assets and clear under specific conditions. For example, such contracts could automatically nullify themselves if assets are not transferred on a certain date or other terms are violated.

What can blockchain do?

Many observers note how long it took for some of the most revolutionary internet-based applications we take for granted today to even be conceptualized. Similarly, they theorize, we are only scratching the surface of what blockchain can do. With that in mind, here are just a few of the technology's current uses:

Currency The TCP/IP protocol that enables the internet involves users sending and receiving copies of data. This system is great for communication and transmission of information, but not for money. The best TCP/IP can do is send orders to transfer money to a central clearinghouse like that bank that provides your credit card. Because of the five attributes discussed above, blockchain can instead transfer digital representations of the real thing, impossible to copy. This is what allowed Bitcoin to be the first cryptocurrency to solve the so-called double-spending problem.

But blockchains can go beyond abstractions such as Bitcoin and enable transactions with actual gold-backed currency. As economist Thorsten Polleit explains, one can purchase gold, get a unique certificate of ownership, and make transactions with a blockchain in a manner essentially the same as Bitcoin. In November, the U.K. Royal Mint announced plans to launch such a blockchain-backed offering.

Record keeping Physical records must be stored and are subject to damage or loss. Anyone who's lost a birth certificate or Social Security card is all too aware of the hoops you have to jump through to replace it. On the other hand, current digital records usually require a centralized location and a good deal of technological infrastructure to protect them from hacking. With blockchain, unique unalterable records can be kept digitally and can even be transferred to another owner. What if the title of your car was safely kept digitally and could be transferred in a sale in real time? Similarly, blockchain offers corporations a more efficient solution to keep and protect records.

Financial services When investors buy stocks, derivatives, or syndicated loans, the transaction may feel like it happens in almost real time. But as "Bloomberg Markets" says, the actual settlement of trades in our current system involves several layers of archaic processes: "When investors buy and sell syndicated loans or derivatives or move money around the world, they must cope with opaque and clunky back-office processes that rely on negotiated contracts between buyers and sellers, lots of phone calls, lots of lawyers, and even the occasional fax. It still takes almost 20 days, on average, to settle syndicated loan trades." With blockchain, actual ownership of a financial asset, rather than a promise of ownership, can be transferred in real time. In addition, blockchain technology may facilitate regulation that is both more effective and less cumbersome, since all transactions are memorialized and market participants can agree (or be required) to turn over data to a regulator.



Blockchain and economic freedom

Core tenets of economic liberty include property rights, lack of reliance on central authorities, privacy, and equality of opportunity. Blockchain can advance each of these principles:

Property rights As discussed above, blockchain can enable the safe digital storage and transfer of titles of ownership of virtually any asset. The permanence of record keeping provides a kind of guarantee that may be completely novel in some parts of the world. In places that are particularly susceptible to government seizure of assets, a blockchain-based record-keeping system leaves the possibility that wrongs can be righted. Imagine a dictator launches a successful coup in a small country, burning the physical records of land ownership, and forcing people off their land and redistributing it to his cronies. If that regime falls, sorting out who owns what could lead to chaos or even war. But if those records had been kept in a blockchain, it would be far easier to go back and return assets to their rightful owners, who would hold their encrypted identities.

Lack of central intermediaries Bitcoin has already provided a tantalizing view of the future for those who favor dismantling the government monopoly on issuing currency. Blockchain technology enables such a private currency to arise without a government or a private central entity to issue notes and establish trust. In fact, blockchain transactions are often called “trustless,” meaning that two parties don’t have to trust each other or a central authority to conduct a transaction. This term is something of a misnomer, however, because trust naturally emerges from the system, bottom-up rather than top-down. Users of a platform could also agree in advance to use a given mediation body to deliberate on more complex contractual disputes.

Privacy Bitcoin has enabled anonymous transactions on the web, the dark side of which has been seen in sales of black-market goods on websites such as Silk Road, the online market best known for traffic in illegal drugs. But in a day and age when the government and corporations can see a staggering amount of data on almost any citizen, blockchain promises a new level of privacy and security. It’s worth noting that infamous bitcoin thefts have not involved any breach of the underlying blockchain, but rather flawed systems built around it by exchanges. Exchanges will need to come up with better technology to address these issues if cryptocurrencies are to become a major player in world markets.

Opportunity Many people in developing nations currently have no access to banking services, due to lack of supply or lack of verifiable identity. Blockchain provides a cheap, easy way to accomplish both from the ground up, with no redistribution of wealth. Putting these people, along with their work and ideas, on the financial map at little cost would only be positive for the global economy.

A revolution, but when?

Observers across many fields believe blockchain is a hugely important technology, but some warn not to expect massive change soon. Writing in the “Harvard Business Review,” Marco Iansiti and Karim Lakhani suggest big changes will take a long time not in spite of but because of the technology’s importance: “True blockchain-led transformation of business and government, we believe, is still many years away. That’s because blockchain is not a ‘disruptive’ technology, which can attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly. Blockchain is a foundational technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure.”

During the dot-com bubble, people went overboard in their predictions of what the internet would change, but the real changes turned out to be massive. It is similarly easy for many to project their hopes and dreams onto blockchain during this early, underdeveloped phase. But given its potential enabling of bottom-up interactions and governance, it may be appropriate to dream a little about its future impact on society.

Alumni News

Recent news from AIER Summer Fellowship alumni



Laurel Mazur (2013 Summer Fellowship program) is a Research Assistant in the Supervision, Regulation and Credit Department of the Federal Reserve Bank of Richmond in Baltimore, MD. Laurel uses the research skills attained at AIER to analyze the regional economy. In September, Laurel starts PhD program in Business Administration at the University of Maryland.



Nuoya Li (2014 Summer Fellowship program) has been working for GEODIS (the largest logistics group in France) in Germany as their Asia Economist and Strategist. In September 2017, she will start Columbia University's Master of Arts program in Economics.



Kristopher Cramer (2015 Summer Fellowship program) was recently hired as an Associate Economist 2 in the research division at Moody's Analytics. He is responsible to cover the economics of Utah, Bulgaria, and several U.S. metro areas.



Elena Casanovas (2015 Summer Fellowship program) has worked with the Brookings Institute in Washington, DC and Uruguay and was a Research Associate at Innovations for Poverty Action in Lima, Peru. In September, Elena will remain in NYC and join Nuoya (see above) at Columbia University in the Masters of Arts program in Economics.



Cheikhou Kane (2016 Summer Fellowship program) was recently elected as Vice President of Relations and Financial Affairs at New College, FL where he is majoring in Economics and Applied Mathematics.



Elena Zee (1993 Summer Fellowship program) is President & CEO of the Arizona Council on Economic Education and active member of the National Association of Economic Educators (NAEE). She recently attended the NAEE annual meeting in Arkansas and met AIER's Education Programs Coordinator, Michelle Ryan. Elena is interested in collaborating with AIER to establish Summer Fellowship Alumni weekends and to host an Economics Across the Curriculum workshop in Arizona in the future.

Prospects for a Digital Gold-Backed Currency

Theodore Cangero

The Federal Reserve increased the money supply to a record level during the Great Recession. In the long run, the massive increase will likely cause inflation. Thankfully, though, a new currency may allow people to protect themselves from inflation.

The Fed increased the money supply by purchasing mortgage-backed securities and Treasury securities from financial institutions. Flush with new cash, financial institutions made loans and kept excess cash reserves at the Fed. Excess reserves hit an all-time high in 2014 at \$2.7 trillion. Today, excess reserves remain elevated at \$2.2 trillion.

Banks will make more loans as the economy continues to improve. The private sector keeps growing, having added 16 million jobs since the Great Recession. Improvements in the labor market have helped repair household balance sheets, which will mean more consumers seeking credit. This sets the stage for banks to lend more of their excess reserves. Credit growth will accelerate inflation and reduce purchasing power for all Americans.

Is there any way to protect your wealth from government debasement of fiat money? There will soon be a new way. Thanks to advancements in technology pioneered by Bitcoin, a new, digital gold-backed currency should be available before the end of 2017.

Until recently, progress toward a digital gold-backed currency was slight. Today, momentum is building. The CME Group and the U.K. Royal Mint have teamed up to create a new currency called the RMG, which stands for Royal Mint Gold. The RMG is currently being tested and will be available before the end of the year. The currency will be fully backed by physical gold held by the Royal Mint. The initial rollout will be worth \$1 billion in gold.

People will be able to securely purchase RMGs using blockchain technology. The structure of the RMG blockchain will solve many problems faced by Bitcoin. Miners have disagreed on how to update the blockchain code underlying Bitcoin. The disagreement over updates to the blockchain code threatens to split Bitcoin into two digital currencies. This has scared off potential users. If a change to the RMG blockchain code needs to happen, the CME

Group will be able to make it happen. And potential users might be more likely to adopt the RMG because, unlike Bitcoin, a clear governance structure is in place. While a governance structure can be helpful, it also opens the RMG to problems. Central control of the RMG could lead to interference such as a decision in the future to reduce the percentage of gold backing. Other problems include the possibility of corporate crime and agency problems. Agency problems refer to conflicting incentives with an organization.

Bitcoins are exchanged on a blockchain network, but it and other digital currencies, such as Ethereum, are not backed by a precious metal. Instead, the value of a bitcoin is determined by the supply of and demand for the bitcoin itself. Miners determine the supply of bitcoins, while demand comes from Bitcoin users.

But gold and other precious metals have been used as currencies (by themselves or as backing for bank money) for most of recorded history. The lack of a precious metal backing bitcoins has deterred some potential users of bitcoins, contributing to the push for a digital gold-backed currency. As mentioned, the RMG will be fully backed by physical gold held at the U.K. Royal Mint. There will not be digital miners creating new RMGs. This eliminates the chance that digital miners could unexpectedly inflate the currency, causing volatility in the market. The RMG is disciplined by physical redeemability.

The RMG and other digital currencies are appealing because they are not attached to a central bank and therefore are free from inflation associated with fiat money. Governments will play a role in the future of the gold-backed currency through taxation and regulation. Governments have yet to issue rules for taxing digital gold-backed currencies. To get a sense for how the RMG

will be taxed, it is helpful to look at Bitcoin, other government currencies, and gold-backed exchange-traded funds.

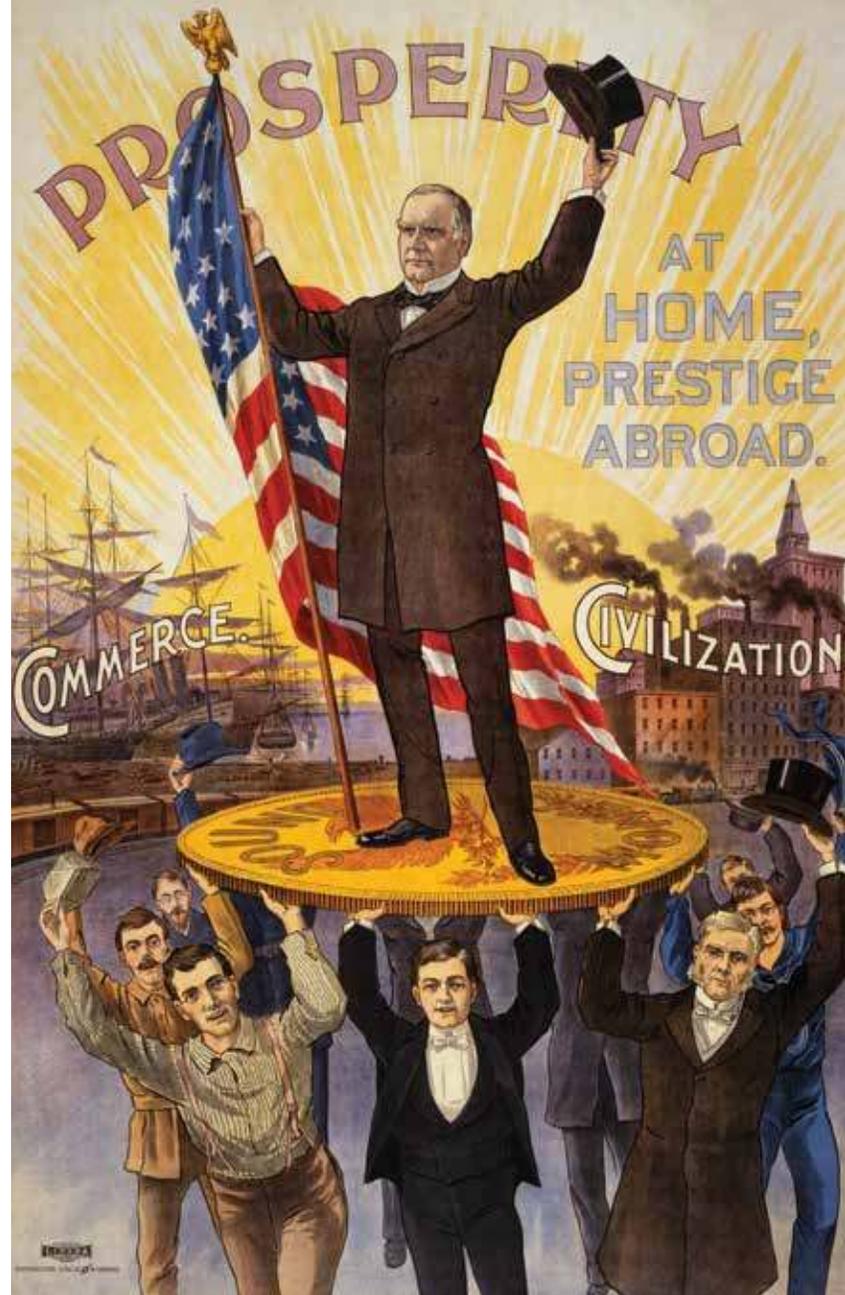
In 2014, the IRS made a critical distinction between property and currency and decided that digital currencies are property. Members of the Bitcoin community applauded the decision. Bitcoin users and miners will be taxed at the capital gains rate as opposed to their income tax rate. Their enthusiasm is shortsighted. By taxing Bitcoin at the capital gains rate, every retail transaction triggers a taxable event. Keeping track of capital gains on every transaction would create burdensome record-keeping requirements. If the RMG were taxed this way, it would be difficult for everyday use.

Instead, it is likely the RMG will be taxed like a gold-backed ETF and thus like a collectible. Capital gains on profits from gold-backed ETFs are taxed as if they were earned on physical gold, which is taxed as a collectible. Collectibles include rare items such as art, antiques, and vintage wine. For tax purposes, collectibles are treated like ordinary income. If you hold a collectible for less than a year, it is taxed as ordinary income, which can be nearly 40 percent. If you hold a collectible for more than a year the maximum tax rate is at 28 percent.

In comparison, the maximum tax rate on capital gains from stocks—and bitcoins—is 20 percent. The government taxes collectibles at a higher rate than other investments for several reasons including that collectibles do not contribute to economic growth nearly as much as business capital formation. So if the RMG is treated like a collectible, it will be free of the record-keeping requirements of bitcoins. However, high-income individuals would face a larger tax burden.

Will there be any fees associated with the RMG? Again, it is instructive to look at gold-backed ETFs. SPDR Gold Shares, the largest gold-backed ETF, has an expense fee of 0.4 percent. CME Group has not released a fee schedule for the RMG, but people should expect to incur fees with the new gold-backed currency. Other products offered by the CME Group come with exchange fees for clearing and trading. Exchanges that currently deal in digital currencies also charge fees. For example, Bitsquare, one of the largest international Bitcoin exchanges, charges fees to transact in bitcoins and mine new bitcoins.

What are the prospects for wider adoption of the digital gold-backed currency? If inflation accelerates, more people will look to it to preserve wealth. Even more people will adopt the RMG when they develop trust in the block-



chain network. History is full of examples of good money backed by precious metals competing successfully with fiat money. Thiers' law says good money will push out the bad if inflation accelerates (in the absence of effective legal tender laws). In the 1980s, Ecuadorians adopted dollars over their inflated national currency. The situation was similar after the collapse of the Soviet Union in the early 1990s. Should excess reserves held at the Fed push inflation higher, watch for more people adopting the new gold-backed currency to preserve their wealth.

Student Fellowship Program

AIER pursues its education mission by creating comprehensive programs for students, teachers, and professionals. The Student Fellowship program was set up by our founder, Col. E.C. Harwood, in 1946. Preserving his legacy, the program has an experiential-learning format where students are actively engaged with staff researchers in research projects pertaining to AIER's research agenda. Through time, the fellowship has grown to encompass three programs that allow students studying economics at undergraduate and graduate levels to practice the art and science of economic analysis.

The **Summer Fellowship** program continues to attract high-caliber students from prestigious colleges and universities across the United States. Students undertake and complete substantive projects, while the program provides diverse educational forums and includes a Berkshire County cultural program. Mrs. Maureen Foulke and The Foulke Foundation are major supporters of this program.

Our **internship program** helps local high school and college students gain practical experience in the economic think tank setting. The students who work with us come from diverse local academic institutions such as Berkshire School, Miss Hall's School, Monument Mountain Regional High School, Bard College at Simon's Rock, and Williams College.



gram

The newly created **Winter Program** continues a semester-long engagement with applied economic-research courses at our partner universities. This year, 12 undergraduates from the University of Sioux Falls and their professor Lorri Halverson came to the AIER campus to continue their immersion in economic research.

If you'd like to support our educational programs, consider making a donation at www.aier.org.



Decision Time for Bitcoin?

Patrick Coate

A dispute about updating the code underlying Bitcoin has yielded two competing proposals, and might result in the digital currency splitting in two. This possibility is a serious concern for both Bitcoin users and investors.

The current problems are an impressive illustration of both Bitcoin's strengths and weaknesses. Bitcoin's blockchain—the ledger of official records of bitcoin creation and transactions—is continually updated by computers running Bitcoin software. A new block is added every 10 minutes, and “miners” that add these blocks are rewarded with newly created bitcoins and transaction fees. The problem that has been brewing for some time is that the network is designed to add a new block every 10 minutes no matter what the traffic, and each block only contains 1 MB of information. If there are more desired transactions than can be fit onto a new block, users have to pay higher transaction fees or wait. This is in contrast to credit card transactions, for instance, in which Visa or MasterCard can process huge numbers of transactions almost instantaneously. As Bitcoin increases in popularity, demand for transactions continually increases and this problem only becomes more acute. This is a serious bottleneck to any desire for Bitcoin to be used by a wide consumer base.

Two Competing Update Options

Bitcoin users and software developers are in almost unanimous agreement they should update the software to increase the number of transactions that can be processed by the network. They are in sharp disagreement as to how. There are two primary competing proposals. One protocol streamlines the information recorded for each transaction, making it easier to fit more transactions on one block. The other would instead make blocks bigger, allowing Bitcoin users to increase block size indefinitely.

Each side has its merits. The latter proposal, known as Bitcoin Unlimited, is clearly the more flexible solution to the problem of increasing transactions. The former, known as Segregated Witness or SegWit, would double capacity, but both factions of Bitcoin's user base are united in hoping there will someday soon be more than twice as much demand for transactions as there is now. This would only be a temporary solution. The argument for SegWit and its sponsoring group Bitcoin Core is not whether Bitcoin Unlimited would make transactions easier. It's an argument about whether it should.

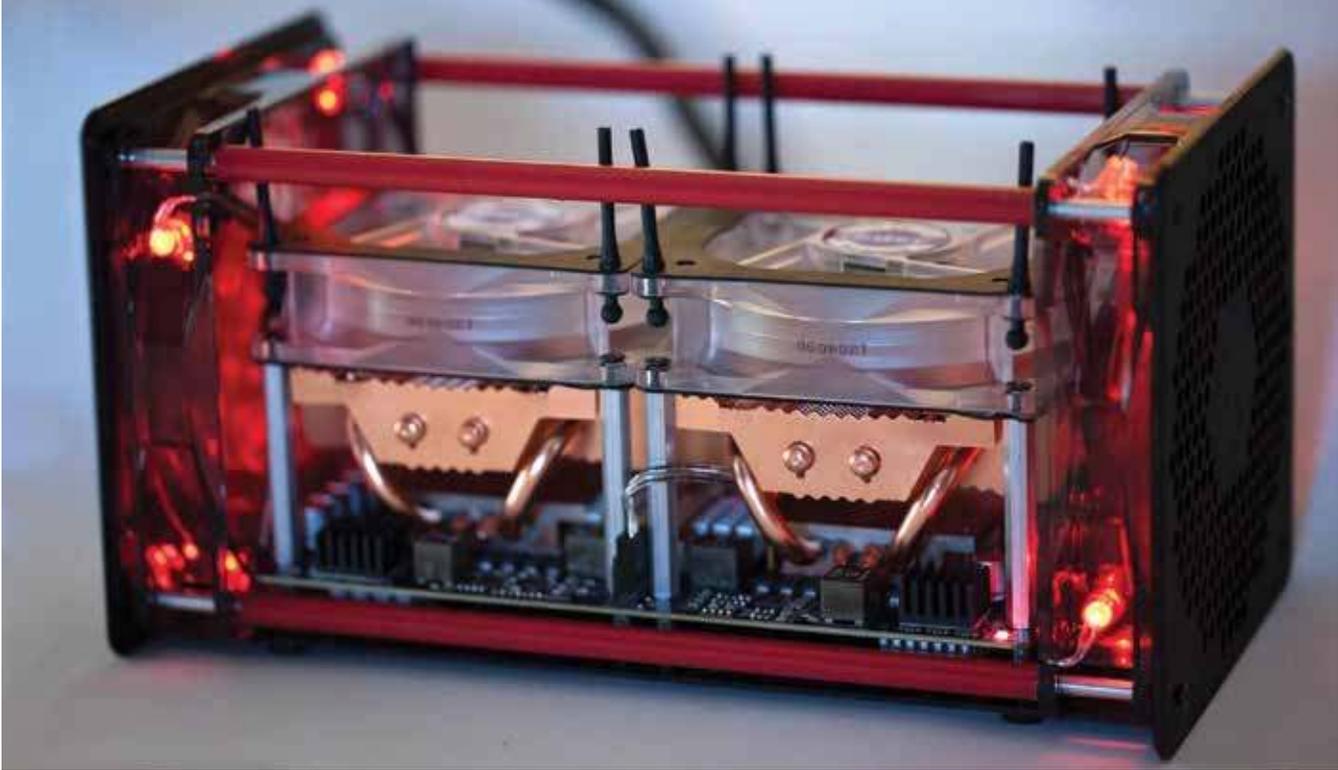
I wrote in a previous piece about the increasing influence of Bitcoin “mining pools,” large operations with many computers running specialized Bitcoin code. These pools create a majority of new blocks (and thus collect most of the associated newly created bitcoins as transaction fees). This concentrates a lot of the power in shaping Bitcoin's future into a few hands, belonging to the leaders of the mining pools. Bitcoin Unlimited allows nodes running Bitcoin software to vote on when and by how much the block size would be increased. In practice, this concentrates mining pools' power further by allowing mining pools—a large percentage of the nodes—more control over the nature of the code itself. This arguably strikes at the decentralized nature of Bitcoin that is one of the tenets of its appeal.

However, others argue Bitcoin Core has itself acted as an unofficial legislative body throughout Bitcoin's development and is not representing the preferences of the user base. Many of the developers of Bitcoin Core have been involved in the code since the early days of Bitcoin and have wielded significant influence through their experience and expertise.

What Happens Next?

There is nothing stopping any Bitcoin user from updating their software and implementing either of these solutions right now—except if they do, other nodes that do not change their software won't accept their new blocks as valid. Essentially, any significant bloc of users can enact veto power on changes by refusing to change their software. Any new blocks that are not backwards-compatible create a crisis as to whether their additions to the blockchain are valid. The only ways to make a change are to get a critical mass of users to agree on updates so that the rest have to go along, or to divide into two camps and create mutually incompatible paths, like rival medieval popes excommunicating one another. For now, both sides—and investors—are wary of creating such a “hard fork.”

What will happen if they do? Well, one reason this debate, which has been ongoing for some time, has gained attention recently is because in March 2017 major Bitcoin exchanges released an official statement detailing their contingency plan. The causality of this release to the likelihood of a fork runs in both directions: the exchanges made a statement because of the increasing possibility of a fork, but the statement also inspired further consideration



Bitcoin miners use specially made hardware to verify and record transactions. They are compensated with newly “mined” bitcoins.

of the possibility. In the event of a fork, the exchanges announced their intent to list Bitcoin Core and Bitcoin Unlimited as separate assets.

Observers—surprise!—are divided about the effect that would have, as well as about the likelihood of a split. Some Bitcoin enthusiasts welcome a potential split. It would allow the two competing models to prove themselves in the marketplace. Others are unconvinced both would be simultaneously viable, and partly due to this predict a hard fork will be averted.

Potential Dangers Ahead

One potential concern is that users who hold bitcoins in digital wallets, unless they take preventative action to ensure being on a particular side, would see these bitcoins' path determined by the practices of what service they hold their Bitcoin wallet with. To me, this seems like one of the greatest dangers of the hard fork: the possibility that it will confuse people with a casual interest in the subject and lead them to shy away. Whether Bitcoin intends to circulate as money or whether it is meant to be a financial asset, the Bitcoin community benefits from expanded demand from new users. A hard fork is going to scare some people off.

There is also speculation that each side could “attack” the other’s blockchain in case of a fork. Bitcoin miners could use some of their processing power to create empty blocks on the other blockchain to disrupt its operations

and force a reunification. This could work or else cause the offended branch to drastically change their algorithm. Either case could cause serious reputational harm to one or both sides. A peaceful solution might result if miners choose to run both new protocols and assign relative processing power in a way that their expected return from each branch is equal. This could create an equilibrium in which ideological users could choose their own branch and miners would step into any arbitrage opportunities and balance an exchange rate.

In a twist that may complicate matters further, a group of Bitcoin companies unaffiliated with Bitcoin Core signed an agreement to activate the SegWit proposal once 80 percent of the community signaled approval. While this would appear to be good news for Bitcoin Core and bad news for Bitcoin Unlimited, the Bitcoin Core group has not endorsed it and objects to the specifics of how it would be implemented.

Whatever happens, it is imperative that both sides are gracious in victory or defeat. Bitcoin is backed by the integrity of the blockchain, much in the same way that dollars are backed by the Federal Reserve and were once backed by precious metals. Just as bimetallism was disruptive and divisive to the 19th-century dollar, a “bi-blockchain” Bitcoin running two protocols will create uncertainty and unease among investors and work against Bitcoin’s price and adoption in the global market.

Bitcoin: Decentralized Governance Put to the Test

Max Gulker

Bitcoin's system of radically decentralized governance is facing perhaps the biggest test in the digital currency's history. As we describe in this issue, the code used to run Bitcoin's blockchain database needs to be updated to transmit more information faster. However, there are two major proposals on the table for how to change the code. The controversy has raged for months and may even result in Bitcoin splitting into two currencies.

Many of Bitcoin's greatest strengths come from its decentralized nature, but if there were somebody at the center of its network making decisions, the current problem would look very different. The governing body would choose one path, and those who didn't like it could sell their bitcoins. This structure would resolve the uncertainty much faster, and not result in a split that would likely scare off some potential Bitcoin users.

The decentralized structure of Bitcoin is not, alas, a free lunch. Decentralization is a tradeoff with pros and cons relative to a more traditional structure. This article will consider those pros and cons. But first, let's look at how decisions are currently made in the Bitcoin network, and what a more centralized structure might look like.

Bitcoin vs. Bitcoin Inc.

Decisions like modifying Bitcoin's code currently involve interactions between developers (anyone who wants to write open-source code and propose to the Bitcoin community that it be adopted) and miners (those who run the code behind the blockchain database and are rewarded with new bitcoins). In practice, the blockchain database must "fork," meaning it branches into two blockchains, one with the change and one without. Each miner has control over the code they use. They could in theory make a unilateral change, but that would stop their copy of the database from being linked to all the other "nodes." For a change like the one currently on the table to be adopted, 95 percent of mining nodes must approve and run the new code. (Miners and developers can communicate in online forums.)

But what if these decisions were instead up to a centralized entity that we'll call Bitcoin Inc.? Bitcoin Inc. is a hypothetical private for-profit firm that has some ownership and control

over the network. Assume all code is still open-source and can be written by third party developers, and that the system is still run by open mining (i.e., this is still a public blockchain rather than a private, permissioned one). However, decisions about changes to the code, rules, and dispute settlement lie with Bitcoin Inc. The company could get its revenue by either doing some mining itself or charging a miniscule transaction fee. These alternatives are interesting to consider but don't matter for the exercise. While this system involves more centralized control, it is still private, lacking any government management of the currency.

In what follows, I'll make the case first for Bitcoin Inc., and then for the currently decentralized Bitcoin. Bitcoin's current governance structure prevents undue influence from any single individual or organization, but does so at the expense of not being able to quickly innovate or respond to unforeseen events.

The Case for Bitcoin Inc.

It is impossible for Bitcoin stakeholders to fully plan for every future event. Any coordinated action that these stakeholders currently take is governed by the implicit contracts between them that emerge from the code and the economic incentives it creates. As economist Ronald Coase famously observed, one of the reasons firms exist at all is that in a world of uncertainty, writing enforceable contracts between parties for every possible future state of the world is impossible, and even if it were possible, prohibitively time-consuming. Firms instead put some discretionary power and control in the hands of human beings, who can respond to new information as it arrives and have incentives sufficiently aligned with the firm. In a world with Bitcoin Inc., the firm would make a call on how to change the code, and individuals could decide whether to use the currency, like every product in the market. This system would also be more efficient in deciding whether to reverse allegedly fraudulent transactions. This issue resulted in a split in Ethereum, another cryptocurrency. The inability of these radically decentralized systems to decide whether to reverse a fraudulent transaction is evidence for Coase's observation and suggests just how difficult it is to fully plan for even predictable outcomes.

This difficulty with rapid coordinated action leads to an undeniable inertia in currencies such as Bitcoin. When Bitcoin was first conceived in Satoshi Nakamoto's 2008 paper, it was at the technological cutting edge. Nine years later, many argue that Bitcoin has been eclipsed by other cryptocurrencies as state of the art. Bitcoin cannot readily adopt the open-source innovations of other cryptocurrencies. To do so requires the cumbersome "forking" process described above. This process seems unnecessarily risky and time-consuming, and renders even small changes in the code a big deal. On the other hand, a firm like Bitcoin Inc. would have an R&D department, freely experimenting with new programming innovations evolving from both internal work and other digital currencies. Should management conclude that a change is due, it can simply make the change, and miners or users, just like customers of a restaurant that changes its menu, are free to go elsewhere if they don't like the change.

The event of a fork turning into a full split devalues both new currencies. Currency adoption and use is fueled by network effects: the currency is more valuable when more people use it. In a hypothetical 50/50 split, each new currency would have only half the users it did before. In addition, we are still at a point where most people do not understand or fully trust cryptocurrencies. Such apparent complexity might delay their adoption.

Bitcoin's radically decentralized structure has a clear weakness in being unable to respond to new information in a rapid and coordinated manner. Implementing change is a very complicated process, but is it a worthwhile tradeoff to reap the benefits of decentralization?

The Case for Decentralized Governance

Bitcoin advocates talk about the decentralized system having no single "point of failure." They usually mean that because the blockchain database is distributed rather than having any master copy, a hacker would have to attack



an almost prohibitively large number of network nodes to change the data. This important feature is maintained in the world of Bitcoin Inc., since the database would still be fully distributed. But the point-of-failure concept is also highly relevant for control of a currency and the ability of that control to be coopted. Currently, no one individual or organization has the power to unilaterally change the code or rule on the validity of a transaction. The fact that no individual or organization can unilaterally change Bitcoin's code or rule on the validity of a transaction protects it from government interference, corporate crime, or agency problems stemming from differing individual incentives. More centralized control by Bitcoin Inc., just like any large corporation in a similar situation, would open the system to all these issues.

There are also advantages in Bitcoin's decentralized, bottom-up process for proposing and implementing changes. While slow and unwieldy, the process may allow creative and effective solutions to evolve that Bitcoin Inc. would never think of from scratch. In some ways this is like the free market generating innovations that would elude any central planner. It also illustrates why splits like the one that happened in Ethereum and may happen to Bitcoin aren't necessarily bad. Users are free to choose between the version of the currency with the change and the one without, rather than having a central entity guess which choice is best.

Finally, lack of change itself may be a desirable feature for a cryptocurrency. One of the biggest issues with the fiat currencies widely used today is that their centralized controlling entities, national governments, can manipulate the currency anytime they want. In a system like Bitcoin where change is incremental and not sudden, users can have far clearer expectations about the currency into the future.

Other Governance Models

Bitcoin's current structure and the hypothetical Bitcoin Inc. are only two of many possible systems of governance for a cryptocurrency. In the past several years, the market has produced hundreds of so-called altcoins (non-Bitcoin cryptocurrencies), each with its own characteristics and means of governance.

Ethereum, the largest of the altcoins, has the nonprofit Ethereum Foundation at its center. The foundation does not have the power to unilaterally change code or reverse transactions, but does carry a large amount of influence in the Ethereum community. Ethereum's creator, Vitalik Buterin, and his colleagues on the foundation team constitute a voluntary coordination device for Ethereum's

miners: Buterin can use the influence and trust he engenders as the currency's creator to rally support for changes to Ethereum's code that might take longer for a system like Bitcoin's to implement. When he proposed the "hard fork" to reverse a fraudulent transaction, the intention was for all Ethereum miners to go along with the decision. While 85 percent of Ethereum's miners agreed, the remaining 15 percent did not support the action, resulting in a full split. Ethereum Classic was born, and what was once a single digital currency became two separate currencies running on separate blockchains. Buterin and his foundation's influence goes only so far.

Another solution is to formalize, through code, means for stakeholders to vote on or approve changes short of splitting the currency. Suppose Bitcoin's miners (and potentially also users) could vote to accept or reject a proposed coding change, and if a prespecified percentage of voters approved, the change would automatically go into effect over the entire network. Tezos, developed in 2014, is one example of such a system. Cryptocurrencies could go even further in the direction of a representative democracy, electing members of the community to serve limited terms in which they would have some decision-making power over the code and transactions.

Ready for Prime Time?

Suppose a global crisis of confidence in fiat currencies erupted tomorrow. Would Bitcoin as currently constituted be able to fill the vacuum and become a global currency? The answer is almost certainly no. The current controversy that may lead to a split is about scalability on a much smaller level than would be required to replace the dollar. And scaling up, especially against the backdrop of an economic crisis, would require exactly the rapid change and innovation with which Bitcoin struggles.

But what if the timetable to replace fiat currencies was 50 years rather than overnight? In this scenario, the ultimate winners among cryptocurrencies have probably not yet been invented, and the messy process of trial and error inherent in Bitcoin's current system may be desirable. If no single cryptocurrency needs to be ready for prime time anytime soon, one or more splits in Bitcoin could yield the type of market-based evolutionary innovation discussed above. Governance of Bitcoin and other cryptocurrencies is still very much a work in progress.



Viviana Ehrenzeller

AIER Summer Fellow 2010, 2011

For me, AIER's summer fellowship was like an "economics camp" which helped me digest concepts learned throughout the academic year and apply them in arguments. It was a privilege to have my own ideas challenged by staff and visiting researchers. The research skills and the refined ability to construct a persuasive argument are the main takeaways that helped me succeed in my career following the summer at AIER.

After having worked in UBS and Group Treasury in Switzerland for the past six years, I look back with nostalgia to the days I spent at AIER. I realized that I never again will have the opportunity to sit down, research, write, and discuss complex economic questions the way I did in Great Barrington.

The work that truly helps society to advance is analyzing economic paradigms, challenging them, putting them in today's context, and trying to come up with new ones. This is what I learned to do at AIER, and I am grateful for that.

AIER Events

Teach-the-Teachers Initiative Economics Across the Curriculum

June 20–22, 2017 St. Louis, MO

June 28–30, 2017 Miami, FL

July 11–13, 2017 Omaha, NE

Summer Fellowship Program

June 26–August 2, 2017 AIER, Great Barrington, MA

Summer Program Seminar Series AIER, Great Barrington, MA

- July 17, 2017 **Dr. Daniel Neilson**, Bard College at Simon's Rock
From Tulips to Mortgages: a Minskian Perspective on Financial Crises.
- July 19, 2017 **Dr. Max Gulker**, AIER
The Economics of Bitcoin and Blockchain.
- July 24, 2017 **Dr. Jay Liebowitz**, Harrisburg University
Ms. Janet Zeide, Montgomery College
Oral and Written Communication Skills: How to Communicate Effectively in the Classroom and Workplace.
- July 26, 2017 **Mr. Bob Hughes**, AIER
A Review of the Harwood Philosophy on Business Cycles and Personal Investment Plans.
- July 31, 2017 **Dr. George Vachadze**, College of Staten Island and
the Graduate Center of the City University of New York
Credit Market and the Aggregate Savings Rate: Evidence from OECD Countries.

Sound Money, Free Banking, and Private Governance Conference

August 4–11, 2017, AIER, Great Barrington, MA

Discover the Benefits of Planned Giving

Many of AIER's supporters have discovered how giving to AIER through our planned giving programs supports AIER's mission and provides numerous benefits for them and their loved ones.



A good plan will provide for your family or loved ones, protect what you have worked so hard to acquire, and leave you feeling safe and secure.

Certain plans allow you to guarantee income for up to three generations of beneficiaries, so you can put a plan in place for any of the important people, or even organizations, in your life.

In addition to supporting the mission of AIER, a planned gift can provide to you substantial tax advantages, especially on gifts of stocks and real estate. The total income, estate, and capital gains tax savings and the probate expense savings can come close to the amount of your planned gift. The benefits include:

- Income for Life**
- Income Tax Deductions**
- Reduced Capital Gains Taxes**
- Reduced Estate Tax**

Simply by taking advantage of incentives the IRS provides, you and your advisor can craft a gift that fits your needs. A planned gift makes it possible for you, your loved ones, and AIER to all benefit.

Use our online calculator to create unique opportunities to meet your financial goals and support AIER.

<http://plannedgiving.aier.org/calculator>

Interested in learning more?
Contact Kelly Fox 888.528.1216 x3102

SUPPORT AIER

and help us teach Americans the importance of sound money



I followed Colonel Harwood for many years and one thing that came through in all of his writing was that he was a great patriot and a strong believer in an honest currency. Having been in the investment business for 48 years, I think Colonel Harwood's teaching is needed even more now than it has ever been. He had a great impact on my thinking.

—Arnold Van Den Berg, Longtime AIER Member

AIER Members understand the importance of AIER's mission and want others to understand too.

Annual Sustaining Membership dues and donations to our programs help AIER provide the information, tools, and analysis that Americans need to make decisions to advance peace, prosperity and human progress. We promote personal freedom, free enterprise, property rights, limited government and sound money.

The people that value these principles the most are members of the American Institute for Economic Research. Donations to AIER are tax-deductible.

Please donate to AIER today to support our ongoing research into business cycle dynamics, inflation, government in the economy, and investment economics. Call us at 888-528-1216, visit www.aier.org/donate, or mail in the coupon below.

YES! I WANT TO SUPPORT AIER TODAY.

- \$50 Reader Circle Membership \$250 Investor Circle Membership
 \$100 Research Circle Membership \$500 Scholar Circle Membership
 Enclosed is my additional tax-deductible donation of \$ _____

NAME _____

STREET _____

CITY _____ STATE _____ ZIP _____

EMAIL _____

PAYMENT METHOD

- Personal Check or Money Order payable to "AIER"
 MasterCard American Express
 Visa Discover

CREDIT CARD NUMBER: _____

EXPIRATION (month/year) _____

TELEPHONE () _____

SIGNATURE _____

ORDER ONLINE aier.org or CALL TOLL-FREE 888.528.1216

We do not share or sell your personal information under any circumstance.

Mail to: AIER PO Box 1000 Great Barrington, MA 01230-1000

American Institute for Economic Research
250 Division Street
Great Barrington, MA 01230

FROM THE ARCHIVES



Col. E.C. Harwood and Helen Harwood attend the Mt. Pelerin Society meeting in Montreux, November 1972.

In this photograph (l-r):
Helen Harwood, Frances Kanes
Hazlitt, and Henry Hazlitt

Photo courtesy of Fred Harwood