
BITCOIN·DIGITAL·DECENTRALIZED·PEER TO PEER
1TROY OZ 999 FINE COPPER
MONETARY METALS

₿ITCOIN

AND THE COMING REVOLUTION IN FINANCIAL TRANSACTIONS

Bitcoin transactions require no banks and no clearing house—plus they execute in real time. What does this mean for the banking industry? Ignore this virtual currency system, and others like it, at your own peril.

BY ERIC HOLMQUIST

We knew Bitcoin was inevitable. The advancement of technology, the mass utilization of the Internet, a generation comfortable with virtualization—combined with a lack of innovation in our current payments infrastructure—helped lead to this global, stateless, digital currency. While numerous attempts have been made in recent years to create a new form of cryptographic currency, Bitcoin was the first to acquire mainstream attention (even if much of that attention focused on it being the currency of choice in the back alleys of Internet commerce).

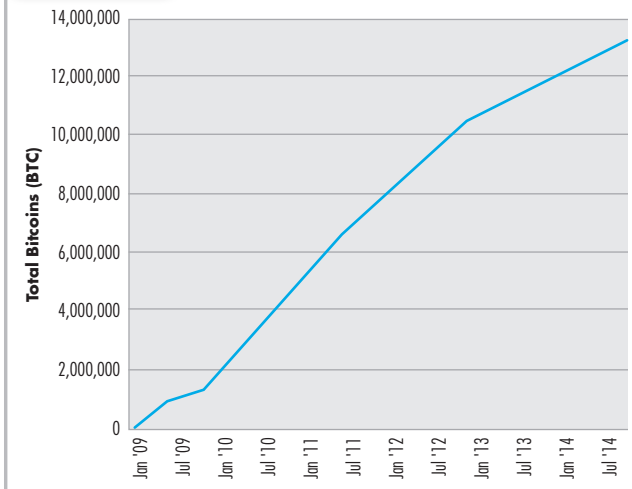
Now, five years after its introduction, Bitcoin is quickly emerging not just as an alternative form of currency but, much more importantly, as a new payments protocol. Time will tell whether Bitcoin itself is viable long term, but there is no question we will look back and see that it was the prototype for a revolution in financial transactions.

In discussions with bankers from a range of institutions, this author has learned that their understanding and perspectives on Bitcoin—and its implications for the banking industry—are highly diverse. All bankers have heard of Bitcoin, but most know very little about it. Some believe it represents a threat to the industry and should be heavily controlled, if not outright banned. Others see it as an opportunity to rethink how payments are processed and currency is exchanged. Regardless of their level of knowledge or perspective, however, they all agree this is something that we ignore at our own peril. And they are right.

Characterizing Bitcoin as simply a grass roots currency designed for drug and porn purchases is like describing the Internet as a convenient way to get sports scores. Bitcoin is, in fact, revolutionary in a number of significant ways, and it is a concept the banking industry needs to study, understand, appreciate, and ultimately embrace.

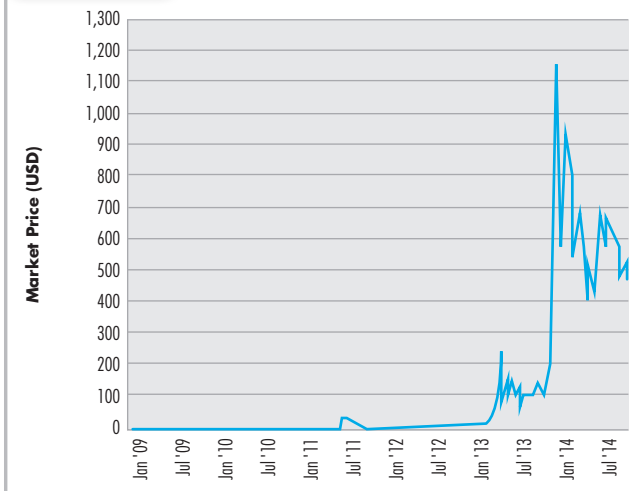
We have known for a long time that our 1970s-era payments infrastructure is woefully outdated. In 2013, the Federal Reserve issued a consultation paper acknowledging gaps in the current payments system and seeking comment on ways to improve its speed, efficiency, and security. The United States is one of the last developed countries still using the Automated Clearing House (ACH) payments protocol, which represents 61% of all payments (followed by checks at 33% and all cards at 6%). In a technology-enabled world, the idea of multiday clearing of transactions is absurd and considered unacceptable to the next generation of customers.

Figure 1 **Total Bitcoins in Circulation**



Source: blockchain.info

Figure 2 **Market Price USD**



Source: blockchain.info

Ironically, Bitcoin (capital "B" for the system, lower case "b" for the actual currency) solved many of these issues in its simple, imaginative design. Based on a paper published in 2008 by the individual who goes only by the pseudonym Satoshi Nakamoto, the system was first introduced in 2009 as a peer-to-peer electronic cash system.

Since its introduction in 2009, the number of coins in circulation has gone from zero to just over 13 million, with a market capitalization of roughly $7 billion. The software mandates that coins will be produced at a declining rate until 21 million coins are in circulation, at which point no more will be issued. The timeline for the issuance of the final coin ranges from 2110 to 2140.

Don't even bother asking, "Could this go mainstream?" It already has. There are tens of thousands of places where bitcoin can be used to make purchases, including Overstock.com (which, in January, became the first major retailer to accept bitcoin), Expedia, 800Flowers, and Dell Computers. (In fact, Dell customers using bitcoin receive a 10% discount on the Alienware PC line.) In August, New York got the world's first bitcoin ATM. Although it allows only for the purchase of bitcoin with cash, plans are in place to allow cash withdrawals.

Described as cyber currency, cryptocurrency, and digital currency (all true), Bitcoin is changing not only the way we see money, but the way we process and protect payment information. Marc Andreessen, coauthor of Mosaic—the first widely used Web browser—and cofounder of Netscape Communications, said, "I compare [Bitcoin] to the Internet. The Internet was a new way to transmit data. Bitcoin's a new way to transmit money."

Francois Velde, senior economist at the Federal Reserve Bank of Chicago, described it as "an elegant solution to the problem of creating a digital currency." David Andolfatto, vice president at the St. Louis Fed, states that Bitcoin is "a threat to the establishment," which he sees as a positive because it prompts central banks to implement sound policies. And Bank of America Merrill Lynch stated in a 2013 report, "Bitcoin can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers."

How It Works

With Bitcoin, there are no actual "coins." The currency is simply a unit of measure, not unlike a dollar, euro, or yen. (Any use of "coin" from this point on refers to one bitcoin unit.) Unlike traditional currencies, bitcoin exists only in digital form. One bitcoin (or BTC) can be subdivided by eight decimal places into smaller units called "satoshis." (One bitcoin is worth 100 million satoshis.) The Bitcoin protocol (the software behind it all) is based on heavily encrypted information, which is why it is also referred to as cryptocurrency.

Bitcoin is owned by no one. Rather it is a system built completely on consensus. It is supported by a volunteer army of people incented to participate because of the potential reward associated with "mining" new coins, a process described below.

What sets Bitcoin apart is truly fascinating, both in terms of how transactions are processed and how the information is protected. Bitcoin transactions are recorded in what is known as the block chain. Think of this as a general ledger recording all financial transactions regardless of their source or destination. The block chain is

completely public. Anyone can not only see it, but attempt to add to it. It does not exist at any one place: It can be downloaded to any computer, anywhere in the world.

In addition to the block chain, the source code that processes all bitcoin transactions is also completely public (also known as open-source software). While this concept is antithetical to the traditional system of processing payments, the Bitcoin design elegantly solves one of the stickier problems that society wrestles with every day: how to protect information. The Bitcoin protocol has taken the alternative path: Make all the data public, but make it useless.

Evidence of value is stored in encrypted strings of information called hashes. All you need to prove ownership of bitcoin is a string of information that is recognized in the ledger as unique. No one else has your exact string. To store bitcoin, a user creates a "wallet," either by downloading software onto a computer or mobile device, or by using one of a number of online wallet services. Once your wallet is created, you can transfer bitcoin into it either by purchasing it directly, through transfer from another user, or by mining new coins. Similarly, value can be transferred from your wallet to someone else's (whether a merchant or another individual) using a simple app with only a few pieces of information.

New Coins and Processing Transactions

Pending transactions are posted publicly to the Bitcoin network, which is visible to anyone who wants to participate. Posting transactions to the block chain requires solving complex mathematical calculations, and the first to find the solution is awarded a block of new bitcoins (a process that is successful roughly every 10 minutes). This process is complex, and while there are hundreds of articles that provide a similar abstract description, they all leave the reader somewhat confused about how it actually works.

Consider the following analogy. There is a pile of neatly folded clothes in the middle of a room (these represent past transactions that have been completed). Throughout the day people drop piles of unfolded clothes (pending transactions) next to it, and the piles are available to everyone. Anyone can grab a handful of clothes and attempt to fold them together and add a pile to the folded pile. If they do so, they will be paid in new bitcoins. However, in order to add to the pile, you need to know the exact number of threads in the last article on top of the folded pile, so you start counting. But by the time you have finished counting the threads, the pile has grown by another 10 articles, or 100 or 1,000, and you are too late.

While this is a crude example, the Bitcoin ledger works somewhat similarly. While pending transactions are visible to everyone, the identities of the sender or receiver are not. Computers worldwide (often working together) race to bundle these transactions into "blocks" and add them to the block chain. But in order to be successful, they must calculate the correct string of characters that picks up information from the last block combined with information in the new block. This process requires remarkable computing power.

Once a block has been successfully added, it is validated by all of the other computers, which agree that the transactions are unique and that they don't represent any transactions that have been previously posted. This is a "consensus"-based model. Transactions are validated when enough nodes "accept" and build on them. Unconfirmed transactions are ignored and ultimately dropped. In this model, majority consensus replaces a central clearing authority.

While this method is, at face value, spectacularly different from traditional payment- processing methods (and may sound dangerous at best and insane at worst), it does solve a number of traditional problems very elegantly:

1. Payments are processed almost in real time. Initial confirmation happens within approximately 10 minutes, and further confirmations are received over the next hour as new transactions occur. For faster confirmation, parties can also pay a small fee that goes to the miner who successfully records the transaction.
2. Transfers are made directly with no third-party clearing entity involved or required.
3. Double payments are effectively impossible. In order for a transaction to be posted to the ledger, the bitcoin value cannot have been previously spent. Because the entire ledger is visible, the history of any given coin is known.
4. Average bitcoin transaction costs are substantially lower than traditional funds-transfer methods, for both sender and receiver. Merchants are therefore highly incented to accept bitcoin because, while there is a small fee associated with converting their bitcoins to U.S. currency, it is significantly less than current interchange fees.
5. Since the data is public, there is nothing to protect. You could attempt to add transactions to the block chain, but the fact is, you're just not fast enough. And because all of the data is encrypted, even though you can see it, there's nothing you will be able to do with it.
6. Transactions are basically anonymous (although the identity of both sender and receiver can be determined).
7. Because the block chain does not exist in any one location, it cannot fail. There are always many copies of it in existence, and the system self-corrects to ensure that it is always accurate despite massive replication.
8. The whole system is self-supporting, self-correcting, self-policing, and remarkably stable.

Because the block chain is basically a history of time- and date-stamped transactions, it can actually be used for much more than just currency exchange. The same protocol could be used to keep a digital record of the existence of legal documents (property deed, contract, will, etc.), proving they existed at a point in time. A recent *American Banker* article revealed, "In theory, Bitcoin could serve as the backbone for a worldwide capital market where companies could issue securities while relying less on intermediaries like clearing houses."

Despite these limitations and risks, the system has provided a working prototype of what a virtually frictionless, stateless, real-time, secure, and efficient payments protocol and universal currency can look like.

Still, Bitcoin isn't without its drawbacks and limitations. It is considered a fiduciary currency—not backed by any government or asset—so it is entirely dependent on the market's perception of its value. Over the last year it has been subject to dramatic price volatility, although this is not uncommon for any early-issue currencies or securities. Here are some other weaknesses:

- Transactions have no recourse. If a trade is made by mistake or through some form of fraudulent means, there are no chargebacks. And while there is some ongoing discussion about creating an "FDIC for Bitcoin," there is currently no insurance for losses due to failed companies holding digital wallets.
- Because transactions are anonymous, they present significant money-laundering risks.
- Buying bitcoin is still complicated and cumbersome, although this situation should improve substantially in the coming year.
- Holding bitcoin can be risky because of price fluctuations. However, a number of intermediaries, including Bitpay and CoinBase, allow people to buy in bitcoin and then immediately convert it to dollars or other currencies, mitigating much of the market risk.
- Governments and regulatory agencies are trying to determine whether regulation of cyber currencies can be managed with existing laws and regulations or whether new ones will need to be written. (Hint: They will.)
- Nakamoto's system design had one key limitation: It is incapable of processing more than seven transactions per second—a very small amount compared to what would be required in order to achieve global usage and acceptance. By comparison, Visa processes almost 480 transactions a second and can handle up to 47,000 a second at peak times.
- While considered extremely unlikely, the system could be attacked. Attackers would need to dominate 51% of the network's processing power. However, the design of the system is such that even if one entity were to somehow harness that much CPU power, their energies would be spent more profitably in supporting the process than they would be in trying to defraud it (unless, of course, their goal was not monetary, but purely disruptive). In practice, given the design of the block chain and its broad distribution, the only thing attackers would likely be able to do is modify one of their own transactions rather than modify the entire chain of transactions.

Despite these limitations and risks, the system has provided a working prototype of what a virtually frictionless, stateless, real-time, secure, and efficient payments protocol and universal currency can look like. And it isn't going anywhere.

More on Security

There are basically two ways one might be able to corrupt the block chain ledger and steal bitcoins: by fraudulently

adding to it or modifying it. The system protects the block chain against both by using a combination of digital signatures identifying the parties involved and encrypted strings called hashes. Its various nodes just aren't going to accept invalid transactions.

An attempt to add fraudulent blocks to the ledger would be possible only if attackers could "outrun" all of the honest nodes. In practical terms, they would, at best, be able to modify their own prior transaction rather than originate new ones. And the longer attackers wait past the posting of the original transaction, the deeper the transaction gets in the block chain and the less likely they could succeed in changing the transaction.

When it comes to privacy, Bitcoin may be getting closer to a balance of security versus privacy than our current payments systems. Transactions are anonymous in that no one can readily tie a transaction to a person. However, there is a complete audit trail of transactions. Therefore, under certain circumstances, the identities could be determined. This is not that dissimilar from how stock exchanges publish trade information, showing the transaction but not the parties involved. It certainly seems possible that a structure could ultimately exist where these transactions remain anonymous while allowing for some form of regulatory oversight to monitor for money laundering and other illegal activities.

The strength and elegance of the protocol are the visibility of the data and the consensus model of processing. The former addresses one of the stickiest challenges for all institutions: protecting confidential data versus making the data meaningless. Can you imagine a system that could make social security numbers public but include controls so that no one could actually do anything with that information?

Legal and Regulatory Control

The legal and regulatory issues associated with cyber currency (bitcoin or otherwise) are complex and unclear. For starters, is bitcoin a true "currency"? To qualify as "money," something must be 1) a store of value, 2) a medium of exchange, and 3) a unit of account.

There has been debate about whether bitcoin meets these criteria, and proponents and opponents can both be convincing in their arguments. To some extent, this point has proven somewhat academic now that bitcoin seems to have achieved critical mass. The U.S. Treasury has classified bitcoin as "decentralized virtual currency," a view that has been supported by other agencies.

Earlier this year, the IRS issued guidance that established virtual currency as property for U.S. tax purposes, which is slowing bitcoin's acceptance. Bitcoin users must report gains or losses associated with all acquisitions and uses. For someone conducting large quantities of transactions, this could make for a very burdensome reporting requirement. However, certain entities can provide users with a complete history of their bitcoin activity to speed the reporting process. Accordingly, while this requirement in no way kills the use of bitcoin, it creates some friction and buys the government time to figure out how to deal with it.

Compared to some other countries, the United States is considered bitcoin-friendly. The European Central Bank has indicated that traditional financial-sector regulation is not applicable, mainly because Bitcoin does not involve traditional financial actors.

The U.S. Treasury Department's Financial Crimes Enforcement Network (FINCEN) has issued several new guidance documents, largely to provide a definition as to when an entity is considered a money service business. In general, this would apply only to companies that serve as an exchange—not merchants or individuals exchanging bitcoin. Bitcoin miners and escrow services are also exempt, although miners may be subject to a self-employment tax.

The strength and elegance of the protocol are the visibility of the data and the consensus model of processing.

All bitcoin exchanges must register with FINCEN. New York State's Department of Financial Services recently issued draft guidance for establishing a BitLicense, which would be required for anyone conducting "virtual currency business activity." Like the FINCEN guidance, merchants and customers who use virtual currencies exclusively for the transactions of goods and services would be exempt. Alternatively, North Carolina's Office of the Commissioner of Banks recently concluded that it can effectively regulate virtual currency exchanges under the state's Money Transmitters Act with only minor additions.

Could bitcoin or any other form of cyber currency be declared illegal if it is determined that it presents too many risks or that it can't be properly controlled for the benefit of society? This author doesn't believe so, nor would this be a practical solution. Governments are much better off learning from the innovations presented by cyber currency and evolving their own legal and regulatory environment to adapt to this new payments infrastructure.

Governing and regulating virtual currency is going to be a daunting task. There is no central control point, transactions are largely anonymous, there is no clearing entity through which transactions can be monitored or controlled, and it is unclear how much jurisdiction any given government has over a currency that was born—and lives—only on the Internet. Existing regulations are marginal at best in providing oversight, and both the pace of technology and

INNOVATION DOESN'T HAVE TO BE VIABLE TO BE DISRUPTIVE; IT JUST HAS TO CATCH ON.

speed of adoption are unprecedented in banking. Overseeing a currency that is not issued, owned, backed, processed, or guaranteed by any sovereign entity will be a monumental challenge for legal and regulatory bodies.

How Does This Affect Banking?

So what does all of this mean for the banking industry? Does Bitcoin pose a threat to U.S. currency or to the existing payments infrastructure? Will competition force banks to support products and services based on bitcoins? Is Bitcoin an opportunity for early adopters, particularly tech-savvy institutions that can accommodate alternative products while mitigating the inherent risks?

Bankers have mixed emotions, in part because there is so much that we simply don't know. Here's what Susan Moore, vice president for risk management with Iowa-based Hills Bank and Trust, had to say:

We conducted a risk assessment of Bitcoin which was then discussed at our officers risk committee. It seemed apparent that this could not only impact our customers but our industry, although the implications of it are still unclear. What we concluded was that while Bitcoin didn't appear to present any immediate threat, neither did we see it as a significant opportunity just yet. While we haven't adopted any policies that would specifically prohibit us from banking customers that deal in bitcoin, we're not currently pursuing them either. This is definitely something we are keeping our eye on and will re-evaluate as we move forward both in terms of any potential threat to the bank as well as opportunity.

A different banker told me of a policy that prohibits banking any company that primarily deals in virtual currency "until we have clearer guidance."

The threat question is one of the more important issues to consider. At the end of the day, banks' purpose can be summed up in one word: trust. They are trusted to receive deposits from customers in return for safeguarding those funds and providing a reasonable rate of return. They are a trusted source of financing for homes, cars, businesses, personal loans, and so on. And they are trusted to facilitate the exchange of funds between two parties.

In the first two cases, we have to accept the reality that banks have already been heavily dis-intermediated. Checking accounts, savings accounts, personal loans, and home mortgages can be obtained from any number of sources, all of which provide similar support, infrastructure, and, in some cases, better rates. It is the third part of this equation where cyber currency truly creates a potential threat. The banking system exists because society needs a trusted element, specifically a mediator, to facilitate the secure transfer of funds. People use banks because they trust banks. But in a consensus-driven, peer-to-peer, real-time payments infrastructure—such as Bitcoin—trust in an institution is replaced with trust in technology.

If an institution is no longer needed to provide that trust, what is it needed for? We are going to have to accept the reality that the technology community created both a currency and a payments infrastructure that is, in many ways, superior to the one we use today—one that is simple, elegant, fantastically complex, anonymous, secure, adaptable, and extremely low cost, but one that is also unregulated, uncontrolled, uncertain, potentially un-scalable, and highly volatile. You have no recourse and no mediator. There is, by design, no "man in the middle" to arbitrate disputes.

Now that it's here, what are we going to do about it? At a minimum, banks should do their homework so that they fully understand how this protocol works and how people are using it. They should talk about this in their risk committees, or other governance forums, so that the board and senior management are fully educated on the risks, opportunities, and trends.

Banks should be ready to talk to their commercial customers, particularly merchants, to understand whether

those customers are accepting alternative forms of payment. The spendbitcoins.com website lists merchants that accept bitcoin. Ask them how Bitcoin works. Banks also need to be prepared to address whether they will serve companies that are part of the virtual currency marketplace. And finally, banks need to be monitoring this area to see how it evolves, and how state and federal laws and regulations will affect individuals and companies dealing in virtual currency.

Believe it or not, the next generation of virtual payments protocols is already being developed. A company based in San Francisco called Ripple Labs is developing the Ripple protocol, which would allow any person or company, anywhere in the world, to seamlessly execute cross-currency transactions between dollars, yen, euros, bitcoin, and even loyalty points. Third parties are emerging at an astonishing rate to support this new payment protocol and take advantage of its opportunities.

It remains to be seen whether Bitcoin or some other platform ultimately dominates, but the idea of a digital currency is something we must learn to live with. Innovation doesn't have to be viable to be disruptive; it just has to catch on. Will bitcoin replace dollars? Probably not, at least not within any reasonable time horizon. Could bitcoin become a global super-currency? Again, it's unlikely. But could it be the crude and earliest of foundations for a world currency at some point in the future? Possibly. From a more practical standpoint, could we as a society learn to live with dual payment systems—one where trust is based on mediation, and one where it's based on technology—that allow people to choose which one works best for them? Honestly, we're already there. But is that a bad thing?

History tells us that disruptive change is both inevitable and necessary within any given society or industry. The irony here is that while the financial services industry laments the current use of outdated methods and tools and the need to simply adapt, the cyber community seems to have given us a very clear picture of what one alternative model looks like. Now it's up to us to decide how we respond. Either way, we don't know what the true "next generation" payments infrastructure will look like. But what we do know is that it will be very different. ❖

Eric Holmquist *is managing director of enterprise risk with Accume Partners. He can be reached at* eholmquist@accumepartners.com.