Bitcoin, Blockchain, and the Future of Financial Transactions

Charles G. Cascarilla, CFA
CEO and Co-Founder
itBit
New York and Singapore

Bitcoin is a new financial system that has the potential to have a big impact on the way the world does business. Its open ledger system and distribution network make it a valuable system. Although it is still in its infancy, as bitcoin becomes larger and more sophisticated, it may very well provide solutions to many of the current financial system's problems.

I approach bitcoin from an unusual perspective: I am not a technologist, and I do not know how to program. I covered financial services companies at Goldman Sachs, and I also have run portfolios as an investor on the buy side in public equities, private equity, and venture capital. My business partner and I came across bitcoin about five years ago. We did not really know what to make of it, but we had a framework to understand it because it was a payment system and had, in some respects, a financial system component to it.

What Is Bitcoin?

When we began investigating bitcoin, it had a market cap of $500,000 and was only trading at 5 cents per share. At the time, we were thinking of it as a global transaction network similar to Visa, MasterCard, or certain remittance companies like Western Union or MoneyGram. I decided that it was such a fundamental innovation that we should start a company dedicated to the bitcoin space and digital currencies overall. That is why we started itBit—a digital currency exchange. The biggest challenge, even today, is being able to reliably buy and sell bitcoin for fiat cash.

Bitcoin is open source, which means it is constantly being worked on by developers. About 75% of the code has been rewritten in the six years since it was initially released, so it is a living and breathing code base. That feature allows continuous innovation. The other important feature is that it is open 24 hours a day, 7 days a week. It never stops.

One of the most significant features of bitcoin is that it is an open network, which distinguishes bitcoin from other payment systems. Anyone can see what is happening in the network, not just now but during all periods in the past. It is fully auditable, which is very powerful.

Not only is bitcoin open like the internet, but also it is distributed like the internet. This distribution and decentralization allows it to create both stability and ambiguity. There are between 6,000 and 10,000 computers—very powerful computers—that are processing transactions on a continuous basis. This computing power allows the bitcoin network to constantly update and maintain a distributed ledger. The ledger is distributed in that it is truly person to person; there are no banking institutions, governments, or commercial entities involved with bitcoin.

Marc Andreessen put it well when he said, "For five years, many of the world's best mathematicians and computer scientists have been studying bitcoin and trying to figure out what's wrong with it. They haven't found anything yet."[1]

Why Is Bitcoin Important?

Being open and distributed is what makes bitcoin so important. The financial system, going all the way back to the Italian Renaissance, has been a centralized closed ledger system run by a bank or central bank. Increasing complexity has made it very difficult to know what happens in these bank ledgers. The result has been an increase in auditing and regulatory costs. Part of the problem with the financial crisis was that the ledgers did not necessarily balance because the balancing process takes so long. These ledgers do not balance instantly like the bitcoin network, which is clearing and settling every

This presentation comes from the 68th CFA Institute Annual Conference held in Frankfurt, Germany, on 26–29 April 2015 in partnership with CFA Society Germany.

[1]Anthony Effinger, "Andreessen on Finance: 'We Can Reinvent the Entire Thing'," BloombergBusiness (7 October 2014): www.bloomberg.com/news/articles/2014-10-07/andreessen-on-finance-we-can-reinvent-the-entire-thing-.

10 minutes. The financial system does not work that way. It can take weeks to settle trades and transactions, creating a lot of counterparty risk. Bitcoin thus represents a real fundamental innovation in moving financial value through the system.

Many tend to associate bitcoin with either an open ledger or a "blockchain." The blockchain is the public ledger in which bitcoin transactions are recorded every 10 minutes. So, the ledger is crystallized every 10 minutes in a manner that allows anyone to go back and look at the past. It is a very auditable track record of all the bitcoin transactions that ever occurred. It is possible to find out where every bitcoin has ever been—a very useful tool for the financial system and for regulators.

Here is an example of how the bitcoin system works:

- I want to send Ron $5.00 in bitcoins.
- I send the $5.00 worth of bitcoins to Ron's public key or public address (he also has a private address that only he knows).
- The $5.00 goes from my public wallet to Ron's public wallet, and it appears immediately even though the transaction has not yet been confirmed.
- In 10 minutes, the transaction is confirmed within the network.

Everyone can see that an address controlled by Ron has received $5.00 and that the transaction has been confirmed.

So, bitcoin is basically an open, public, distributed ledger. It is working 24 hours a day, and the network protects against fraud. In a normal financial transaction, information is sent to a merchant and moves through an entire system of authentications, during which a breach can occur. Authentication is not necessary with bitcoin. All of the data breaches that have happened at various credit card companies could not happen in the bitcoin world, which could reduce costs in a very significant way.

Just as the internet changed the way information was distributed, bitcoin could change the way that information is authenticated.

What Is the Value of Bitcoin?

A somewhat controversial topic is whether bitcoin has value. Some believe it might be a Ponzi scheme or that governments will not allow other currencies to exist. Bitcoin should not be considered a currency (although currency is one attribute of bitcoin) but an open ledger within which there is value. Historically, currencies have been backed by a tangible asset—for example, gold or even seashells or salt in the very distant past. Alternatively, there have been fiat currencies that are backed by the taxing power of central governments and the credibility of claims that they will stand behind their currency.

Bitcoin resembles a currency in many ways. There will only ever be 21 million bitcoins that will exist in the bitcoin network. Every bitcoin can be divided to eight decimal places, so there are many partial bitcoins that can exist. But it is the bitcoin *network* that gives bitcoins value.

The network is a very powerful ledger system. There are a finite number of bitcoins, just as there is a finite amount of real estate in Manhattan. This network, or ledger, is very valuable and very powerful. The network is arguably why bitcoin has an estimated value of $4 billion, which may or may not be the correct value. I tend to think it should be worth more—not because it is a currency but because of the tremendous amount of resources that have been put into the bitcoin ecosystem. There has been about three-quarters of a billion dollars invested in bitcoin startups and related businesses—a very significant amount of capital. There is probably about the same amount of money that investors are currently seeking to invest in bitcoin companies.

Publicly tradable private ledger systems, such as Visa, MasterCard, and Western Union, have a market capitalization of almost half a trillion dollars. I am not going to say that bitcoin or any open ledger system is as good as those current centralized ledgers. But recall the early days of cellular technology when there was no such thing as a cellphone. There were car phones that were big and had to be plugged in and maybe even bolted into the car. The technology was analog and not that great. If a landline was available instead, it was preferable to use it. Today, many people do not even have landlines.

At least 30,000 developers are working on bitcoin right now, according to estimates within the industry. There are 100,000 merchants that accept bitcoin online. More than 5,000 merchants accept it offline—a number that is growing significantly every month. The computing power of the network has increased massively. There are now more than 6 million wallets, which are how bitcoins are held and used. So, the growth is very apparent. It is not at a mass adoption phase yet; it is still very much in the early adoption phase. But it is an early adoption phase that has a lot of strong underpinnings in the reality of how important the technology is and the capital that is being supplied.

Three "Use" Cases Today

Bitcoin might not be as good as our main financial system, but I want to illustrate how useful it can be through these three examples.

Retail Purchases. Consider retail purchases. There is a great deal of "friction" involved in moving costly financial information. Depending on the size of the merchant, this friction costs between 2.5% and 3.5%, maybe 4%. With bitcoin, the cost is probably around 30–50 bps, making it an order of magnitude cheaper. That is a big difference in terms of dollars—to the economy and to merchants that have very low profit margins. It means having retail margins of 5%–15% to be able to get back 3.5%–4% cost.

Currently, as **Table 1** shows, the bitcoin network has as much volume as PayPal or Discover. Again, it cannot do what Visa and MasterCard are doing. With the growth of the network, the capacity to move transactions in the bitcoin network, and the businesses that are working to solve the issues of speed, bitcoin may be able to compete on this scale in two to three years. It is a functional issue, not a fundamental problem with open ledgering or bitcoin.

The potential for savings in retail processing (retail, e-commerce, and remittances) is around $200 billion, as indicated in **Table 2**, which shows the market size and transaction fees by market for 2013. That figure is approximately 1.5% of US GDP. Perhaps all these savings cannot happen for various reasons, but it is very credible that this kind of benefit could eventually be brought to society.

Table 1. Average Daily Transaction Volume of Various Payment Networks

Payment Network	Average Daily Transaction Volume ($ millions)
Visa	17,559
MasterCard	9,863
China Union Pay	7,562
American Express	2,434
Discover (Pulse Network)	438
PayPal	397
Discover (Discover Network)	299
Bitcoin	289
Western Union	216
Xoom	15

Note: Bitcoin transaction volume represents a seven-day average as of 3 December 2014. All other volumes are based on latest company filings.

Source: Data are from Coinometrics.

Remittances. The next case deals with remittances. Western Union, MoneyGram, and all the remittance companies move about $550 billion through a remittance network, according to the World Bank, and there is probably about $150 billion to $200 billion that is unreported. The average fee is 10%, maybe a little bit higher when considering all the shadow transactions. Potentially, up to $63 billion could be saved by using the bitcoin remittance system rather than the traditional systems in place because bitcoin can drive the fee down to 1%.

A normal remittance business basically touches a transaction between seven and nine times. "Underbanked" individuals who do not have access to the conventional banking system pay the highest fees, which is unfortunate because they are the people who could use the money the most. Bitcoin could provide a big improvement to society.

Underbanked Market. The last case deals again with the underbanked market. It surprises me that nearly 20% of adults in the United States are underbanked, according to a 2013 survey by the FDIC (Federal Deposit Insurance Corporation).[2] In other countries, the underbanked populations are often an even larger percentage of the population. Because of the growing prevalence of smart phones, many of these individuals can have access to the internet and thus a bitcoin wallet.

[2]Susan Burhouse, Karyen Chu, Ryan Goodstein, Joyce Northwood, Yazmin Osaki, and Dhruv Sharma, "2013 FDIC National Survey of the Unbanked and Underbanked Households," Federal Deposit Insurance Corporation (October 2014): www.fdic.gov/householdsurvey.

Table 2. Market Size and Transaction Fees for Retail, E-Commerce, and Remittances, 2013

	Retail	E-Commerce	Remittances	Total Savings
Market size and fees ($ billions)				
Dollar volume	10,383	609	549	
Prevailing transaction fees	259.6	17.8	48.9	
Bitcoin transaction fees	103.8	6.1	5.5	
Potential savings with bitcoin	155.7	11.8	43.4	210.9
Transaction fees by market				
Prevailing average pricing	2.5%	2.9%	8.9%	
Bitcoin average pricing	1.0%	1.0%	1.0%	

Source: Data are from Goldman Sachs Global Investment Research.

Many large companies accept bitcoin now, and some small businesses accept it. Having a bitcoin wallet removes frictions and limitations for underbanked people or underprivileged people all over the world.

These are examples of what bitcoin can do today.

Bitcoin Tomorrow

What bitcoin can do tomorrow is in some ways even more important. The blockchain can be used for a wide variety of transactions: smart contracts, authentications, micropayments, and so forth. There is an argument that the reason for ads on the internet is that users cannot make micropayments when visiting a webpage. In fact, internet browsers have an error (403 Forbidden) that basically means, "You did not pay me to come to my website."

I do not think that ads will necessarily go away if micropayments become possible, but those ads were developed as a way to monetize the internet because there was not a reliable payment system. But a virtual wallet could easily be used to pay small amounts—amounts so small that they might not even be noticeable because they are fractions of a bitcoin. Think about what this can allow.

Some items can potentially be moved through the blockchain right now. It is not just value that can move but any kind of information—for example, copyrights or ownership. Returning to my previous example, I sent Ron a small fraction of a bitcoin ($5.00). The whole network now knows I sent a fraction of a bitcoin. Ron keeps track of it; it is on the blockchain. I could also attach ownership to a car, a house, a stock, or a bond digitally—almost like stapling it to that small fraction of a bitcoin that was practically worthless. Think about how that changes things. The whole network, essentially the whole world, sees that I have sent, for example, a share of IBM to Ron, and he is now the owner of it. The possibilities are staggering.

Ownership in Today's Financial System

I want to talk a little bit about the current financial system because it can illustrate the possibilities for change. A lot of systemic risk is built into the system, which makes trading and settlement for, say, stocks a three-day process. A stock can be traded in microseconds, but it takes three days to settle that trade. That process is cumbersome and not just for stocks or bonds. It is also the case for moving collateral in general through the financial system.

Consequently, a lot of systemic risk is built up; the "plumbing" in the financial system is insufficient to keep track of the trading. In some ways, the financial system's plumbing is from the 19th century. Every time it rains, the streets flood. That is what happened in 2007–2008. Part of the problem was that it took many, many days to settle. A significant amount of the collateral for Lehman Brothers still cannot be found today. There are accounts that hold bonds, and the bonds are not actually there. There is a representation of the bond and clients get paid as if they own it, but no one knows where the actual bond is. The collateral is floating around through the third-party repo systems.

In 2007–2008, $10 trillion of collateral was moving on a continuous basis through the main financial systems in the United States and Europe. Today, the value is closer to $6 trillion. Nonetheless, a large amount of collateral is moving around in the system, and if someone "fails," the collateral cannot necessarily be found. Hedge funds, investment firms, banks, brokers, and others are all using the collateral. For example, if I want to go short (i.e., borrow) 1,000 shares of IBM stock, I can do it in one microsecond, but I then have to wait for it to settle in three days. The systemic risk that creeps into the system is unbelievable. The solution to the systemic risk is to hold more capital, which creates an inefficient system.

Another example is securitization. The chain of title for a mortgage from homeowner to the eventual trust is very difficult to follow. I am not saying the complexity would go away with an open ledger, but the auditability of this complexity would immediately be addressed. People in the United States do not know who their actual mortgage holder is because the loan has gone through so much processing and has never actually followed chains of authentication. Earlier, authentication was just about payment systems, but I propose that authentication for whole financial systems can be addressed with open ledger technology.

Conclusion

Open ledgers are changing the way information moves in a very fundamental way. Open ledger systems are not necessarily ready to handle what Visa and MasterCard are doing, but the potential to have such a capacity is very significant. Bitcoin is not just a powerful tool to audit things but an innovation that could change our everyday lives. Consider the internet in 1995, when the only option was dial up. Facebook and Netflix were not even ideas yet. Now, think of all the ways the internet has changed people's lives that they could not imagine 20 years ago or even 10 years ago. Bitcoin is a lot like that; it is such a fundamental change that all of the possibilities it represents cannot be conceived.

The key point is that the open ledger technology is very powerful and because it is so powerful, it has value. It might not even be bitcoin that truly takes off. There are about 1,000 alternative cryptocurrencies that exist, but bitcoin is about 90%–95% of the market capitalization of all cryptocurrencies. Bitcoin has not hit the point of inevitability, but it has hit the point at which it has most of the capital and talent working to address its shortcomings and to continue to improve it to be able to handle the many different possible uses for open ledgers.

CE Qualified Activity CFA Institute 0.5 CE credit

Question and Answer Session

Charles G. Cascarilla, CFA

Question: As an open source system, how safe is bitcoin? Can it be hacked, tampered with, or sabotaged?

Cascarilla: That is a very important question. Bitcoin uses very powerful encryption. It is called SHA-256, and it is a very robust encryption technology. Undoubtedly, there is always a battle between cryptographers and hackers. Consequently, at some point, the bitcoin network will need to update its encryption technology. That requirement does not appear to be the case currently.

There are ways to upgrade the cryptology if necessary, but everything on the internet, everything in the whole financial system, works off SHA-256. If someone was able to break the bitcoin network, everything would be breakable. The bitcoin ledger would be the least of the problems. The bigger worries would be about everything from air traffic control to top secret files. It is a very strong encryption system, and it will be upgraded over time as needed.

Question: What are your expectations for the volatility of bitcoin, and do you think it will continue to be volatile?

Cascarilla: Bitcoin is very volatile. I think it averages between 5% and 10% daily volatility, whereas most currencies are averaging 1%–2% daily volatility. But bitcoin's volatility has been trending downward on a daily basis. It is probably at around the same point as some of the more volatile, less liquid currency pairs, but that is not good enough. It needs to go down more.

Why it is so volatile is important. The value is very uncertain. The ledger system is still in its infancy, and the power of it is still not widely understood. Liquidity is also still fairly low. There is no reliable place to buy and sell bitcoins today. At itBit, we are working to solve that problem. Fiduciaries can buy bitcoins, but there is no bank that would want to interact with any of the current bitcoin exchanges or intermediaries.

There is a maturation process in terms of understanding the value of the actual ecosystem, of being able to handle fund flows. Low volatility is not necessary to take advantage of bitcoin's many benefits. Most of the very powerful ways of using bitcoin are not at all tied to its value, which is why an open ledgering system provides value, despite what the volatility does.

Question: What is the biggest obstacle for bitcoin's global acceptance?

Cascarilla: I think the biggest obstacle is that the business models that have been implemented in bitcoin have not been as compliant as they should be. In order to interact with the current financial system, a lot of "know your customer" and anti-money-laundering rules are necessary. Better regulations and better levels of compliance will help bitcoin be able to be more broadly adopted.

Question: How will the blockchain bridge the 10 minute fraud gap—that is, the time before authentication when no party stands behind the transaction?

Cascarilla: That is another important innovation that is in the process of being developed. There are conventionally two main problems with open ledgers and, even more specifically, with bitcoin: a speed issue and a "bloat" issue. As I mentioned, there are 30,000+ developers working for bitcoin-related companies and on changes to the protocol. They are working on very innovative ways to be able, with 99.99% certainty, to have a transaction approved within 5–10 seconds. Bitcoin is not there yet.

The other issue is bloat. Can bitcoin handle enough transactions at one time to increase the speed of the transactions? Can bitcoin operate with a volume of transactions equivalent to Visa or MasterCard? Right now, absolutely not. The network could not handle that amount of transaction volume. But in two to three years, based on the growth of the network and the developments that are in process by programmers, such volume could be possible. This problem is functional and not fundamental.

Question: To what extent should Visa be worried about its business prospects with the advent of bitcoin?

Cascarilla: Visa is a centralized bookkeeper that facilitates value transfer. Ultimately, Visa and MasterCard are taking only 10–15 bps of the 2.5%–3.5% transaction fee. Some of that percentage is from being willing to extend credit, some of it is for authentication and compliance purposes, and some of it is just profit margin. I think that there will be a reduction in the fees, which will add value. So, if such companies as Visa and Mastercard are not providing solutions that have value beyond keeping centralized ledgers, they are going to face significant problems because of the open ledger technology. It is not just a problem for Visa and MasterCard. It is a problem for every centralized ledger-keeping system.

Question: Regarding the prospects for bitcoin as money or currency, how can the amount of currency be controlled to deal with inflation?

Cascarilla: Bitcoin has built-in inflation. We know there will only be 21 million bitcoins ever in circulation. Right now, there are about 14 million. So, it will become more and more difficult to get bitcoins over time. Because the number of bitcoins is fixed, the inflation rate is hardwired in.

Question: How will bitcoin hold up in times of illiquidity and poor buy-side pricing?

Cascarilla: That is a very good question, but I cannot give a great answer. I can only give examples from the past. There have been moments when bitcoin has benefited from volatility in currency systems—for instance, with Cyprus and certainly in Venezuela and Argentina. Bitcoin has some usefulness in that context.

The next thing I would say is that as bitcoin becomes more common and more liquid, it will become more stable in value. Right now, the actual infrastructure for liquidity is about as bad as it can get. The lack of financial infrastructure is pretty amazing compared with how much we talk about it and how important it might become. Once those things are in place, having liquidity brought into an asset class that has a finite amount of supply is more of a possibility.