Money, from Cowrie Shells to Bitcoins and the Coming Blockchain Revolution

Robert Bercaw

Presented to the Philosophical Club of Cleveland, December 6, 2016

Abstract

What is bitcoin? It's a currency created in 2008 by an unknown person or persons. It is now used by millions of organizations and people, despite its having no backing of bullion, banks or governments. It raises questions about the fundamental nature of the money we all take for granted. Probably bitcoin's most important contribution is that it introduced an entirely new way of keeping ledgers and other vital records, the blockchain. Records have been traditionally been held in centralized databases maintained by trusted organizations such as governments, banks and credit cards. They have proved to be less than safe, having often been hacked by nefarious people. Blockchain records are publicly distributed on hundreds or thousands of computers, but are kept private by advanced cryptography. Scores of major organizations are now exploring the use of this technology.

Introduction

What would your reaction be if I proposed paying my debt to you in a currency which is not issued by any government or bank and is not backed by gold or silver, say BercawRubles? You're not very enthusiastic. Well, millions of people and organizations are happy to do just that. Not with BercawRubles, but with a currency is called Bitcoin. Most of us have heard of it but haven't used it and see no need to do so. The dollar works perfectly well. Bitcoin is widely used, however, in countries where the national currencies aren't stable. There are several million companies and people who use it. In February 2015, there were over 100,000 merchants who accepted it for goods and services, and by the end of 2015, there were eight million bitcoin transactions a month.

Bitcoin is a most peculiar form of money. More properly, it is a digital asset and payment system that lives on the Internet, but it is not backed by any organization or bullion. It was described in a paper by Satoshi Nakamoto in October 2008 and then the source code for the system was placed on the Internet the next January. Satosh hasn't been heard from since 2011.

There is another problem; Satoshi Nakamoto isn't a known person. It's a pseudonym and no one knows of whom, be it an individual or a group of people. As bitcoin has become popular, a number of people have claimed to be Satoshi, but none of the claims are considered credible.

Bitcoin is open-source software, meaning that like Wikipedia, anyone is free to modify it or add to it. It's then up to the users to either accept or reject the proposed changes.

History of money

I'll go into what makes bitcoin popular, but first it would be useful to review other forms of money and learn something about their natures.

Barter and its problems

When people first discovered that it would be useful to trade things, the obvious solution was barter. If I was good at flint knapping, but not so good at hunting, I might stay well fed by trading flint blades for rabbits. I might also trade them for other things that I need. Bartering works well when there are only a few items to be traded, but it becomes unbearably complicated when there are many different items. To execute a trade, it is first necessary to find someone who has what you want and also wants what you have. Then you have to negotiate an exchange rate. The next time you need something, you have to go through this same process again, probably with a different person. The complexity of this process escalates as the factorial of the number of items that might be exchanged and ultimately makes a market economy impossible.

Bullion and its problems

Yuval Noah Harari in his book Sapiens points out that the concept of money was invented to solve this problem. If there is one item that everyone will take in trade, then the complexity only grows as the number of items, not its factorial. We tend to think of money in terms of dollars, coins, or some other currency, but money can be anything that people will take in trade for most other commodities. People accept it because they share the belief that most other people will also accept it in trade. Money allows people to quickly determine the value of an item or a commodity; e.g., as this is written, wheat is worth $3.15 a bushel. Money also creates an easy way to store or transport wealth.

Over the years, people have adopted many different forms of money, including: barley, cowrie shells, cattle, salt and gold. In parts of Africa, cowrie shells remained in use as money even into the 20th century. The main requirements that a material be useful as money are that it be fairly--but not too--rare, and that a significant effort is needed to acquire more of it. When first refined, aluminum was more valuable than gold. Then the development of the inexpensive Hall-Heroult process quickly dropped the price to current levels. Gold and silver fit the rareness requirement very well and eventually became the dominant media of exchange.

Coinage & money

The next step in the evolution of money was the issuance of coins by kings or other governments. A coin, with its distinctive design, was essentially a guarantee by the king that such a token contained a specific amount of gold, silver or base metal. This greatly facilitated commerce by relieving a seller of the need to weigh and verify the purity of the bullion she was receiving in payment.

Printing money

Eventually the production of coinage couldn't keep up with the increased scope of commerce. One solution was for the government to print paper money and simply guarantee that it would provide the equivalent amount of gold on demand. Such guarantees have frequently been violated, but still paper money has come to be almost universally accepted. Even coins have ceased to be made of precious metal and hence are just IOUs from the government.

Non-cash transactions: Credit cards, checks, etc.

Today's economy has outstripped the use of both coinage and paper money; the vast majority of transactions take place without their use. Examples include electronic transfers, credit cards, checks and various bank transfers. They are carried out by one or more third parties and include fees of varying amounts, which may be hidden, but are never-the-less real. Banks that provide "free" checking require a substantial minimal balance, which means they have the free use of your money. Credit card companies charge merchants a fee of a few percent of the transaction, which is then buried in the price of the product. International money transfers are significantly more expensive.

Validation by a third party

The main services that are provided by these third parties are guaranteeing the identities of the parties and transferring the agreed upon amount of money between the parties accounts. In order to provide these services, credit card companies and other third-party services require that you provide them with a great deal of personal information: addresses, social security numbers and so on. They are also privy to all your sales and other transaction data. The resulting databases are proprietary and turn out to be quite valuable. The information in them is routinely sold to other organizations, which use them for god only knows what. Even worse, the security of the databases is often poor, resulting in huge amounts of personal data being hacked and sold to criminals and criminal organizations. Examples include Target (70,000,000 accounts), JP Morgan Chase (76,000,000 accounts) and CardSystem Solutions, which is the payment processor for Visa, MasterCard and Discover (40,000,000 accounts).The result is that you have no idea who has access to much of your personal and supposedly private information.

Private transactions

The only way to keep a transaction private is to pay in cash, and indeed many people pay for services in cash to avoid sales and income taxes. The mafia is famous for settling their deals with suitcases full of cash. The US government is onto the potential illegal use of cash. It tries to keep a lid on them by procedures such as requiring banks to report any cash deposits or withdrawals of more than $10,000. Also, a number of governments have withdrawn their large denomination bills from circulation.

Bitcoin

What about bitcoin? It's not a currency in the sense that you can put bitcoin in your wallet or coin purse. It is simply a system for recording transactions between two parties. In this sense, it is similar to PayPal and credit cards. But an important difference is that bitcoin transfers are essentially private. No third party is involved. Transactions are a matter of public record, but they are between addresses, whose ownerships are mostly secret. In effect, only the payer and payee have a record of the transfer. This privacy is likely one of the main reasons for its popularity.

The NY Times ran an article about the use of bitcoin in Argentina where there are a number of brokers who will exchange bitcoin for pesos, euros or dollars. Argentina maintains the peso at an artificial rate that is about 30% higher than the street rate. If you go to a bank to convert your dollars into pesos, you effectively lose 30% of your money; it's the same deal when buying things with a dollar based credit card. If you take cash into Argentina, you can find people who will exchange it at the street rate, but then there are all the risks of carrying cash and limits on the amount you can carry.

Bitcoin provides a solution to these problems. One only has to buy the bitcoin in dollars—there are a number of bitcoin exchanges in the US—and then find a broker in Argentina who will buy them for pesos at the street rate.

This same process is being used to reduce the costs of remittances, that is money sent to relatives in third-world countries. Banks charge 7 to 10 percent to send money overseas. Sometimes banks even refuse to wire money to certain countries. When I was the treasurer of an international non-profit organization, I needed to reimburse a Nigerian speaker his travel expenses. KeyBank refused to send the money. Bitcoin is also much faster than wired transfers, taking minutes, rather than days.

Unfortunately, like cash, the privacy provided by bitcoin makes it a natural for money laundering and other criminal pursuits. The most notorious example is Silk Road, an on-line market that used it to sell several million dollars of illicit drugs.

The other unique aspect of bitcoin is that there is no central bank or repository that holds the transaction records. Instead, the records are held in a distributed, public ledger, called the blockchain. Distributed means that there are identical records on several thousand computers. The bitcoin software keeps all the copies synchronized. If you like, you can download your own copy, but be careful; it is now at 45 gigabytes and growing.

Your account

When you open an account, say by buying some bitcoin from a broker, the software assigns you three very large numbers: a specific address, a public key and a private key. Ownership means you can spend the bitcoin associated with that address. Nothing connects your real name with your address or keys; transactions are strictly between addresses, so nobody can tell who made a given transaction. Oh, and by the way, if you lose the private key, you have lost all your bitcoin, irretrievably. In 2013, one user reported that he lost $7.5 million worth of bitcoin when he accidentally discarded the hard drive that held his private key.

A variety of apps have been developed to help you keep track of your bitcoin account and facilitate spending your bitcoin. Because they hold your bitcoin money, they are generally known as wallets. And like a physical wallet, if it is stolen, your money is stolen with it. When your wallet is kept on your computer, it is easy to buy things on-line, but if someone is able to hack your computer, he can make off with your bitcoin. Many people keep their wallets on a thumb drive or on a computer that is not connected to the Internet. Some even write the private key on a piece of paper. There are also wallets that run on a smart phone that can automatically be debited when you make a purchase from a merchant that accepts bitcoin. This is done by holding your phone up to a display provided by the merchant that presents a QR-code that encodes the cost and other details of the purchase. A QR-code is a two dimensional bar code. You may have seen one on your boarding pass at the airport.

How does it work?

Bitcoin is one of a new type of currency known as cryptocurrencies. Its public and private keys are an implementation of the public-key cryptography system. The public key is a number which is used to encrypt a message, but cannot be used to de-encrypt it. The message can only be de-encrypted by using the private key. You give out your public key to everyone that you might like to get a message from. Of course, anyone else who gets ahold of your public key can send you messages. If this seems odd, just think of your mail box and the U.S. mail. Anyone who has the address your mail box can send you mail, but only you or someone with your key can open the box and read the mail.

Bitcoins are spent simply by sending a suitable message, which the payer digitally signs with her private key. The software deducts the specified amount of bitcoins from the payer's address and adds it to the payee's address. The transaction doesn't become official, however, until all the details are validated and the transaction is added to the blockchain. This process is called mining.

Miners are people or groups of with very fast computers, who compete to provide this record keeping service, verifying newly published transactions and combining them into a new group called a block. The block is then added to the blockchain with an encrypted link to the previous block. Hence the name "block chain." Miners are called that because they are rewarded with a few bitcoin for providing this service. They compete by having to solve a mathematical problem, which is difficult to solve, but whose answer is easy to verify. Thus everyone can agree on who the winner is.

Remember that I said that anything that qualifies as money must be reasonably difficult to create. With bitcoin, it's all the computation that the miners have to make and the electricity needed to make them.. The Economist estimates that in 2015, bitcoin transactions burned enough electricity to power 135,000 American homes. And this will go up even if the number of transactions doesn't increase.

I don't want to get into too many details, but it should be noted that the rewards to the miners are cut in half approximately every four years and eventually will decrease to zero. At that point, there will be 21 million bitcoin in circulation. Miners will then be paid only from fees offered in the transactions. Payment of fees is optional; you specify what fee you will pay when you make a transaction. But, miners are not obligated to process all transactions, so people offer fees to insure that their transactions are processed—more or less depending on how fast they need to complete the transaction. Currently, it is 1/2 to 2%, but that is cheaper than credit cards which charge 2-3%.

A huge advantage of the system is that the blockchain records of the transactions are extremely secure. Like the Internet, there is great redundancy; the loss of records on any computer—or even many—is inconsequential. It is essentially impossible to forge transactions. Changing a block involves a huge computational load and the chaining means that all subsequent blocks must also be changed to make them consistent. Having done all that, the changed copy would simply be thrown out by the software that maintains the consistency of all the blockchain copies. The only way to make a forgery stick is to make the same forgery on 51% of the thousands of blockchain copies.

The Blockchain

It's hard to predict what the future of bitcoin will be; some people even call it a Ponzi scheme. That's a bit harsh, but it has a number of problems that limit its use as a general currency. Its price is not very stable; since 2013, a bitcoin has ranged in price from $100 to $1,100. There are the large power requirements needed to do the proof of work calculations and its small block size—about 1400 transactions—limits it to seven transactions a second. By comparison, Visa processes over 1,700 transactions a second.

Distributed Ledgers

Satoshi Nakamoto's most important contribution is that he introduced the concept of and developed the supporting math for the distributed ledger used by bitcoin, generally known as the blockchain. This is a revolutionary development because it is both more reliable and more secure than the traditional, centralized databases.

Bitcoin is only one implementation of a blockchain. Because blockchain can be used to track the transfer of any type of asset, such as stocks, bonds and precious metals, a host of banks and other companies are racing to determine how take advantage of it. Examples include the NASDAC, which is currently working on such a system to record trading of securities of privately held companies. Another is the consortium of 42 banks, including UBS, Goldman Sachs and JP Morgan, that has been established to develop common standards for interbank transactions. It has been estimated that the technology could save banks $20B a year by 2022.

Blockchain can also be used to replace the centralized records and databases at banks, governments and other institutions that have turned out to be less than trustworthy. These can be records of anything of value, such as land titles, contracts and birth certificates.

Essentially, blockchain is to record keeping as the Internet is to communication. They both replace centralized, proprietary systems with public, distributed ones. The two technologies complement each other and it's expected that the impact of blockchain will be similar to that of the internet.