BITCOIN: THE GOOD AND THE BAD NEWS ABOUT CRYPTOCURRENCY

NEAL KOBLITZ

1. What Bitcoin Is and How It Works

Until quite recent times the standard method of payment was cash. In many parts of the world cash payments have been largely replaced by electronic payments, usually by credit card. These payment systems are controlled by the big banks, and they are usually carried out in US dollars (or euros or yen).

Bitcoin is a new type of currency, launched in 2009, that is not controlled by any central authority, such as a bank or government. It is managed collectively by the community of users. Its proper functioning is guaranteed by the mathematical properties of certain cryptographic tools.

The two basic tools used in bitcoin are digital signatures, which are implemented using Elliptic Curve Cryptography, and a hash function. A digital signature provides a guarantee, verifiable by anyone, that the payer approved a given transaction. A hash function is a publicly available algorithm whose input is a long sequence of bits that represent transaction data, public cryptographic keys, and other things, and whose output is a random-looking sequence of 256 bits, corresponding to an integer of at most 78 decimal digits.

The hash function is used to create a *blockchain*. The blockchain, by giving a temporal order to the transactions, provides a way for users to verify that no bitcoin was spent twice. (The prevention of double-spending is a central problem for any electronic currency system.) Each block in the chain — consisting of the records of a few hundred or a few thousand transactions that were completed worldwide in roughly a 10-minute period — has to be *verified* when it is added to the chain.

Groups of *miners* (a word that was traditionally used for people who dug gold or silver or copper from the earth) compete for the right to verify a block. The winner is the first person who, in applying the hash function, obtains an output that is below a certain bound (at present this bound is roughly 10^{55}, that is, the first 23 decimal digits must be zero). Achieving such a hash function output is called *proof of work*. The miner's reward consists of two parts: a transfer to the miner's account of a fixed number of newly created bitcoins (this number started at 50, is currently at 12.5,

Date: 5 November 2017.

every 4 years gets reduced by a factor of 2, and will disappear entirely in the year 2140) and the transaction fees for all of the transactions in the block. Bitcoin transactions generally do have fees (for the purpose of giving the miners an incentive to include the transaction in their block), but they are extremely tiny compared to the fees charged to merchants for credit card transactions.

2. Forks

There are two basic ways that the blockchain can *fork*, that is, set out in two different directions. A "soft" fork occurs when two miners successfully verify a block at almost the same moment. Because different miners receive the information at slightly different times, they disagree on who completed the proof of work first. The question is resolved by "majority vote" in the sense that the miners with more computing power are able to build upon their choice of "first block" before the other group. The longer fork then becomes the valid one, and the transactions in the losing fork must be re-verified. In practice, it takes less than an hour to resolve a soft fork. This means that for extra security in a high-value transaction it's best to wait an hour before finally accepting the transaction; otherwise there's a small possibility that the bitcoins were already spent before and the transaction is invalid.

A "hard" fork is more serious. A hard fork occurs when different users have different versions of the bitcoin software. The first hard fork took place in March 2013, when some people were using an updated version of the software that had an unexpected incompatibility with the old version that other people were using. This problem was resolved in less than a day, with little damage done.

The second hard fork occurred in August 2017 when the software engineers who volunteer to maintain the bitcoin network had a dispute about the best way to fix the bitcoin scalability problem, that is, the limitations caused by a 1-megabyte limit on block size in the original software. As a result of this disagreement, a new fork in the bitcoin blockchain was deliberately created and even given a new name: Bitcoin Cash. It is not yet clear whether the original bitcoin or this alternative — or maybe some other cryptocurrency — will ultimately dominate the market.

3. The Good Side of Bitcoin

The slogan imprinted on all U.S. coins and paper currency is "In God We Trust." However, confidence in a global financial system that depends heavily on the dollar requires trusting not so much in God as in the future stability of the U.S. economy and monetary system. After the crisis of 2008, many people believe that both the politicians and bankers in the United States behave irresponsibly much of the time. More recently, political developments in Europe have caused many to have doubts about the future

of the euro as well. As a "peer to peer" digital technology, bitcoin is totally independent of any government monetary system. The slogan of bitcoin — in deliberate mockery of the U.S. slogan — is "In Cryptography We Trust."

Many civil liberties and human rights advocates have other reasons to mistrust any currency system that's controlled by a central governmental authority. What if a powerful government that has a dismal record on human rights were to pressure the banks into barring electronic transactions with an organization that was exposing the misdeeds of that government?

In 2010 this concern went from a theoretical possibility to reality when the U.S. government blatantly violated the political neutrality of the banking system in its attempt to destroy WikiLeaks. As described in a column in the American business magazine *Forbes* online: "Following a massive release of secret U.S. diplomatic cables in November 2010, donations to WikiLeaks were blocked by Bank of America, VISA, MasterCard, PayPal and Western Union on December 7th, 2010.... It was coordinated pressure exerted in a politicized climate by the U.S. government..." A few months earlier, WikiLeaks had released secret files and videos documenting U.S. atrocities in Iraq and Afghanistan, including the widely viewed "collateral murder" video that showed the cold-blooded killing of an Iraqi journalist by U.S. troops. The U.S. government perceived WikiLeaks as a threat to its interests. In contrast, many human rights advocates saw WikiLeaks as a valuable democratic institution. Supporters of WikiLeaks responded to the U.S. government's politicization of the banking system by turning to cryptocurrency. In 2011, donations started pouring in to WikiLeaks not by credit card, but through bitcoin.

One of the dangerous features of current payment systems is that the banks and other large corporations acquire a tremendous amount of information about our buying habits that can sometimes be used to harm us. Here is an example of how this might occur. Credit card and other payment companies keep records giving payer, payee, date, and amount. Suppose that a payment company sells these records to the SmartAd Company (an imaginary name) that gathers this information in order to help advertisers send out targeted advertising. The SmartAd Company also uses this information to help companies decide whom to hire, and those companies pay SmartAd a lot for that help.

Now suppose that Minh wants a job at a large multinational company that pays SmartAd to give it information on job applicants. Minh has made donations by credit card to a project of the Vietnam Women's Union and to a non-governmental organization (NGO) that campaigns to prevent ecological damage to sites such as the Pù Mát forest. SmartAd software then labels Minh an "anti-corporate activist" and gives this information to the multinational company. That company decides not to hire Minh because Minh will be likely to make complaints if the company is mistreating women or the environment.

Minh would have been protected from this type of corporate abuse of power if he had made his donations in bitcoin, using a different bitcoin "wallet" from the one used for most of his purchases. Note that a bitcoin wallet is just a set of transactions that were signed using a particular cryptographic key. A basic difference between a digital signature and a handwritten signature is that a single person can have many different types of signatures all using different keys. The use of multiple sets of keys makes it much harder for anyone to link a purchase to a particular person.

Aside from issues of human rights and freedom from abuse, there are several practical advantages of bitcoin. For the many "unbanked" people who are too poor to afford high banking fees, bitcoin could liberate them from those fees and allow them at very low cost to have some of the same conveniences as wealthy people. For example, immigrant workers — such as Mexican workers in the United States or Filipino workers in the United Arab Emirates — who want to send remittances home to their family could do so in bitcoin almost free of charge.

For merchants there are two major attractions of bitcoin. In the first place, the transaction fees are very small, and in any case are paid by the buyer, not by the merchant. With credit cards, the fees borne by the merchants are burdensome, especially to small shopowners, and cause them to raise prices. In the second place, transactions are irreversible. Just as with cash, there is no way to cancel payment later. One of the great banes of merchants is that a customer who paid by credit card can easily dispute and reverse the charge (this is called a "chargeback") with little need for convincing justification.

4. The Dark Side of Bitcoin

One fact about bitcoin that has caused many people to doubt its future reliability is that the exchange value of a bitcoin has fluctuated wildly. At present the value is at a historic high, but there have also been dramatic declines in the value of a bitcoin. Reasons for the volatility include the relatively small volume of users and transactions (compared to the dollar), the influence of speculators, and the effects of rumors and news items. If an important political authority announces plans to restrict or regulate bitcoin transactions, confidence in the cryptocurrency might drop. If a major retailer announces plans to accept bitcoin, its value could suddenly rise.

Most merchants who accept bitcoin do not actually keep bitcoin wallets. Rather, they pay an intermediary such as the company BitPay to immediately convert a buyer's bitcoin payment into dollars or another standard currency. Most of the bitcoins that are held and not immediately spent are being kept for the purpose of speculation.

Another problem is that, even though the bitcoin network itself seems to have been well designed, in its relations with the rest of the financial world

it has to rely on enterprises and organizations that are outside the network and may turn out to be unreliable. For example, in 2013 the largest exchange company was Mt. Gox. Based in Tokyo and headed by a Frenchman named Mark Karpelès, who ran it poorly, the company lost 744,408 customer bitcoins (worth about $400 million at the time) shortly before declaring bankruptcy in February 2014.

People who value anonymity and untraceability of bitcoin transactions should know that these features are not guaranteed. Although nothing in the blockchain record directly indicates a user's real-world identity, the blockchain is a public ledger giving the history of all transactions, and from all that information it might be possible to deduce a user's actual identity. Anyone who wants to be completely anonymous must hope that all of her business associates (that is, users whom she pays or who pay her) similarly want to keep their real-world identity private. Otherwise, an investigator can examine her transactions to determine whom she has done business with. Knowing someone's friends or business associates is often enough to make an educated guess about the person's identity. As mentioned before, a reasonable degree of anonymity can probably be ensured by using different bitcoin wallets for different sets of purchases.

Another criticism of bitcoin is that the proof of work — finding many billions of billions of values of a hash function — wastes vast amounts of electricity and computer resources that might otherwise be used for projects that have social or scientific value.

Perhaps the most powerful objection to bitcoin comes from police and national security agencies, who point out that a large proportion of bitcoin users are criminals involved in drug trafficking, child pornography, terrorism, illegal movement of money, and extortion. For example, a type of cybercrime that has recently become prevalent is *ransomware*. A hacker gets into (for example) a hospital's records, encrypts all the records, and then informs the hospital that they will get the decryption key to recover their records provided they make a certain large deposit of bitcoins in the criminal's account.

For a time one of the most active users of bitcoin was a website called Silk Road, which specialized in Internet sale of illegal drugs. In October 2013 it was shut down by U.S. authorities, and its mastermind, Ross Ulbricht, was arrested and charged with narcotics trafficking, computer hacking, fraud, money-laundering, and other crimes. In May 2015 Ulbricht was convicted and sentenced to life imprisonment without the possibility of parole.

One of the most useful strategies in law enforcement is to "follow the money trail." Large amounts of cash cannot be easily moved around the world, so most large-scale criminal organizations prefer other methods, such as complex systems of bank accounts. Such systems are relatively easy to analyze, and banks are required by law to cooperate with investigators. However, following a bitcoin trail is much harder — but not impossible if

law enforcement or national security agencies have a reasonable amount of intelligence from other sources.

5. What Is To Be Done?

Faced with a bewildering array of positive and negative features, what should be done? Bitcoin and other cryptocurrencies, such as Ethereum's, are a new type of technology. Although their technical features are well understood, the many forms of their impact on society are not. There has not yet been much effort put into finding ways to maximize the benefits and reduce the dangers. My own view is that governments should not react with fear and absolute prohibition. Rather, they should encourage further study, including the study of bitcoin forensics (used to trace criminal activity), and gradually consider introducing regulations that are realistic (that is, regulations that can be enforced) and that help encourage the use of bitcoin for legitimate purposes.

Department of Mathematics, Box 354350, University of Washington, Seattle, WA 98195 U.S.A.

E-mail address: koblitz@uw.edu