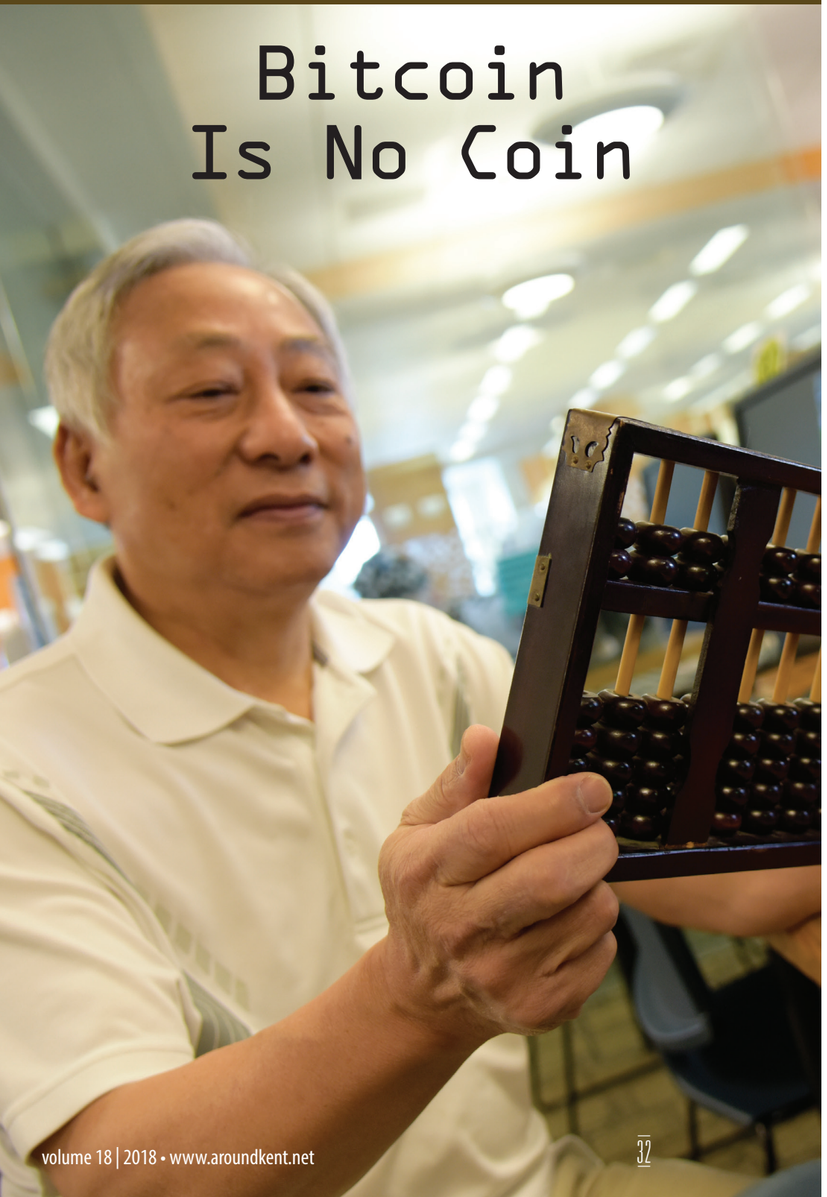
THE SIXTH IN A SERIES OF ARTICLES

Bitcoin Is No Coin



Paul S. Wang

Introduction

The digital revolution has brought many significant and wide-ranging changes to our lives – both positive and negative. Understanding the pros and cons of digital technologies and knowing how best to make use of them are part of *Computational Thinking (CT)*. The widely publicized and curiously fascinating *Bitcoin,* started in January 2009, is a case in point and our focus here.

This article is the 6th in our CT series (previous articles in aroundkent.net Vol. 13 to 17) which aims to sharpen our digital minds and give us a powerful way of thinking through a deeper understanding of modern computing technologies.

Bitcoin Is Not Money

Promoters say Bitcoin is a particular type of *cryptocurrency* – a digital currency using encryption techniques to generate currency units, verify fund transfers, and record transactions. Basic denominations of Bitcoin are *Bitcoin* (BTC) and *Satoshi* (1 BTC equals one hundred million Santoshis). The highly advanced and convoluted nature of its technologies help make Bitcoin fascinating and curiously inviting. However, whatever Bitcoin is, it is not money.

With cash money, you can purchase groceries, meals, and products. You can pay rent and mortgage, make deposits into bank accounts, and all the other things you do with the legal tender, issued by your government, which no one can refuse to accept. In contrast, Bitcoin is accepted by almost no one and there is no legal obligation for anyone to accept it as payment. My advice is neither should you.

Bitcoin Transactions

One of the great promises of Bitcoin is anonymity because sending and receiving bitcoins do not require actual identification information. Instead *Bitcoin addresses* that belong to actual owners are used. This is similar to using screen names or pseudonyms in certain online applications. The amount of bitcoins belonging to any given address is derived from recorded incoming and outgoing transactions. This way, no self-contained tokens are used to represent bitcoins and therefore eliminating the possibility of creating a counterfeit copy.

All Bitcoin transactions are recorded publicly in online *blockchains.* A blockchain is basically a widely distributed (duplicated) database for a certain activity. A blockchain usually serves as an immutable ledger of transactions shared among participants. New transactions are verified, grouped into a data block, and placed at the end of a chain of such blocks; hence the name. Bitcoin and other cryptocurrencies depend on the blockchain technology. However, the blockchain technology is independent and can be applied in many other areas and situations.

The Bitcoin blockchain lists chronologically all Bitcoin transactions ever made by all users, from the very first to the latest transaction. The Bitcoin blockchain is *transparent* (accessible to the public) and uses cryptography to safeguard its integrity. Each recorded transaction contains the amount to be sent to a receiving electronic Bitcoin address (usually about 30 characters in length) owned anonymously by a particular user. The user holds a corresponding secret key (often 64 characters) to access bitcoins at that address. The Bitcoin address and the secret key form a key-pair in *public-key cryptography.* Without the secret key, access is not possible.

Bitcoin Transactions Are Not Anonymous

All these elaborate arrangements provide a certain degree of protection but can not guarantee transaction anonymity. Using bitcoins involves online activities on the part of the payer and the payee. To make a transaction, a payer must usually login to a Bitcoin exchange to use a *wallet* containing her/his bitcoins. The user must also have interactions with shopping carts and checkout systems online.

These and other required online activities provide multiple chances for tracking and can easily result in linking a Bitcoin address to the identity of its real owner, and consequently to all transactions connected to that Bitcoin address via data in the blockchain. According to an August 23, 2017 MIT *Technology Review* article, "*Bitcoin Transactions Aren't as Anonymous as Everyone Hoped.*"

It is hard to argue that Bitcoin is more anonymous than cold cash.

Bitcoin Is Not Heaven for Criminals

In fact, Bitcoin may be the perfect trap law enforcement agencies can use to catch criminals. As the March 9, 2016 Science article *"Why criminals can't hide behind Bitcoin"* states:

Ross Ulbricht, the 31-year-old American who created Silk Road, a Bitcoin market facilitating the sale of $1 billion in illegal drugs, was sentenced to life in prison in February 2015. In March, the assets of 28-year-old Czech national Tomáš Jiříkovský were seized; he's suspected of laundering $40 million in stolen bitcoins. Two more fell in September 2015: 33-year-old American Trendon Shavers pleaded guilty to running a $150 million Ponzi scheme – the first Bitcoin securities fraud case – and 30-year-old Frenchman Mark Karpelès was arrested and charged with fraud and embezzlement of $390 million from the now shuttered Bitcoin currency exchange Mt. Gox.

The majority of Bitcoin users are law-abiding people motivated by privacy concerns or just curiosity. But Bitcoin's anonymity is also a powerful tool for financing crime: The virtual money can keep shady transactions secret. ***The paradox of cryptocurrency is that its associated data create a forensic trail that can suddenly make your entire financial history public information.***

> ***You must keep your private key safe and remember it. Forget that key and you have lost all your bitcoins. They are gone forever and there is no way to get them back!***

Bitcoin Is Not Convenient

To buy, sell, and use bitcoins online, you usually must pick a Bitcoin exchange, something better than the now defunct Mt. Gox hopefully, and establish an account which usually also gives you an online Bitcoin wallet.

To use bitcoins, you must first get some. You can purchase bitcoins which will be placed into your wallet. Payment can be with credit card, bank transfer (ACH), or debit card (there goes your anonymity).

Continued on page 34

Continued from page 33

You must keep your private key safe and remember it. Forget that key and you have lost all your bitcoins. They are gone forever and there is no way to get them back!

Bitcoin transactions can incur relatively high fees that are calculated according to a complicated formula making the fee amount uncertain for most users. At times, the fee can be ridiculous. "Just imagine, if you bought a $2 coffee with bitcoin, you would have had to pay $57 to make that transaction go through," said Hyun Song Shin head of research, the Bank for International Settlement.

Bitcoin transactions can be slow to confirm due to the possibility of double spending (spending already-spent bitcoins). They are also irreversible – once made, there is no cancellation of a Bitcoin transaction.

Compared to online payments by debit/credit cards, by Paypal, or by Alipay, Bitcoin is a poor and inconvenient choice at best.

Bitcoin Is Not An Investment

A bitcoin is not a coin which is made of a material that has at least some intrinsic value. Neither is it a currency backed by the full faith and credit of a government or tied to some substance such as gold or silver. It is some digital data contained in blockchains and what value is that?

Unlike commodities or stocks, the value of bitcoins is pure speculation. There is no rational way to estimate its value at all. The January 19, 2018 *Financial Times* article *"I told you investing in bitcoin was a bad idea"* says:

Its value peaked just before Christmas at $19,434 per virtual coin. By this week, it had plunged to more like $9,000. Down more than 50 percent in a month and many, many billions along the way.

The price of one bitcoin was down to around $6,200 in the third week of June 2018. At that time, US regulators opened a price manipulation probe requesting data from several cryptocurrency exchanges. On June 11, 2018, *CNN Money* reported "The price of bitcoin slumped more than 7 percent after South Korea's Coinrail announced that it had been targeted by cyberthieves." Price fixing has been a reported problem and, in late May 2018, the U.S. Justice Department started a new probe into price manipulation in cryptocurrency markets.

Bitcoin transactions can be slow to confirm due to the possibility of double spending (spending already-spent bitcoins). They are also irreversible – once made, there is no cancellation of a Bitcoin transaction.

Thus, investing in bitcoins is gambling at best. In fact, according to *CNN Money,* "Warren Buffett says bitcoin is 'rat poison.'" Stay away if you know what's good for you.

What Is Bitcoin Mining?

Wonder how bitcoins are actually produced? New bitcoins are created through a well-defined and algorithmic process called *mining.* Anyone with the right computing hardware and software (publicly available) can participate, becoming a miner, from anywhere on the Internet.

The mining process, according to *Investopedia,* involves verifying and compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. Verification is straight forward – making sure the source address actually has the funds and the transaction has been signed by the address owner. The first miner who solves the puzzle is the winner and gets to place the next verified block on the block chain. The winner can also claim stipulated rewards. The rewards incentivize mining and include both the transaction fees (paid to the miner in the form of bitcoins) as well as an amount of newly issued bitcoins. The amount was 50 bitcoins in early 2009, when Bitcoin started. The winner reward amount reduces by 50 percent roughly every four years. The rewards are given to the winner in the form of a recorded transaction.

For each new block on the blockchain, there is only one winning miner. ***All other miners are losers and can try their luck on the next block.***

Globally, huge amounts of capital, equipment, and computing power are wasted in this mindless Bitcoin mining effort. It is estimated that Bitcoin mining accounts for about 0.60 percent of the world's total energy consumption. This is hugely wasteful.

A *New York Times* 2018 article *"Is Bitcoin a Waste of Electricity, or Something Worse?"* reports:

It appears that much of our evolving digital infrastructure is devoted to activities, like the proliferation of cybercoins, that are worse than frivolous," said James McAndrews, the former head of research at the Federal Reserve Bank of New York.

It is an understatement to say that Bitcoin mining is a waste of resources and a serious act of pollution. Some countries have banned Bitcoin mining.

Furthermore, there is an upper limit for the number of bitcoins – 21 million. When that number is reached, no more new bitcoins will be issued as incentive for miners. The lack of incentive for solving puzzles and adding new blocks to the blockchain can lead to a drastic reduction in the number of miners and a timebomb for the continued viable operation of Bitcoin.

Is Bitcoin Not A Scam?

Bitcoin is free-for-all to operate and deal. Some people, including former PayPal CEO Bill Harris, say "Bitcoin is a scam." Even if that is not 100 percent true, the entire Bitcoin enterprise is certainly continuously mired in many, many different kinds of frauds and scams all over the world. The situation is so serious that many Bitcoin exchanges publicize warnings about scams in an attempt to show that they themselves are somehow legit.

For example, cointelegraph.com has a *"Bitcoin Scams News"* page listing many instances. Here are some examples:

- In South Africa, a Ponzi scheme involving 28,000 investors has caused losses exceeding 1 billion rand ($80.4 million).
- Australian consumers lost approximately $2.1 million to cryptocurrency scams last year, according to the Australian Competition and Consumer Commission's annual scams report published May 21, 2018.
- Reported recently (May 18, 2018), a Chinese government study detected 421 fake cryptocurrencies.

In the US, the Securities and Exchange Commission (SEC) has created howeycoins.com to demonstrate how easy it is to sell a fake cryptocurrency. Why not pay the site a visit?

The bitcoin.com site has a *"Guide to Avoiding Bitcoin Fraud"* that warns against:

- Fake Bitcoin exchanges and wallets
- Phishing scams, Ponzi schemes, and cloud mining scams

And these are just some of the dangers one must face and avoid, every step of the way, when dealing with a cryptocurrency such as Bitcoin.

Bitcoin Can Be Illegal

Due to lack of government supervision, regulation, or control, Bitcoin as well as other similar cryptocurrencies, can be a destabilizing factor for many economies and financial markets. The potential for tax evasion, money laundering, ransomware, illegal drug and arms trade, and even terrorism can be a serious concern.

Therefore, many countries have banned or put restrictions on cryptocurrencies such as Bitcoin. These countries include China, India, Russia, Sweden, and Thailand, among others. The list is growing.

Even people who want to use Bitcoin just for fun or privacy should be concerned. A recent article (March 21, 2018) on the *New York Post* entitled *"Blockchain for bitcoin is infected with child porn"* indicated:

According to a recent bombshell report, the underlying blockchain ledger that's used to record bitcoin transactions – a massive online database that grows each time a bitcoin changes hands – contains files that are tainted with hundreds of links to child pornography sites.

The bombshell report has been published by scholars from Germany's RWTH Aachen University. Because the Bitcoin blockchain cannot be altered, the implication is serious indeed. It means those Bitcoin participants who store a copy of the blockchain can be in violation of child pornography laws. There is no telling what other illegal materials can/will be introduced into the blockchain, by whoever from wherever. Remember, Bitcoin allows public access and manipulation.

All That Glitters Is Not Gold

Bitcoin, as well as cryptocurrencies like it, is a new shiny digital object. It glitters for sure but it is not digital gold. It is hard to pin down exactly what Bitcoin is. It is not money because it is neither legal tender nor accepted in most places. It tries to provide anonymity but instead lays a perfect trap that can reveal all transactions of a user.

Continued on page 36

Continued from page 35

Bitcoin is digital and ought to be safe and convenient online but it is not. Safety and reliability is the foremost concern for online transactions. A well-trusted payment platform that provides guarantee for goods/services delivered and payments made is essential. Banks, credit cards, Paypal, and Alipay are such platforms. Do we have similar platforms for Bitcoin?

Real estate, mutual funds, stocks, bonds, precious metals, and other well-established investments have intrinsic value and/or are well regulated to protect investors. They also provide a reasonable expectation of returns. Can a cryptocurrency which can be started by almost anyone with minimal effort be a good investment? The former US Federal Reserve Chair Janet Yellen said Bitcoin was "highly speculative."

Furthermore, something is hardly harmful if it simply glitters. But, Bitcoin is actually illegal in many parts of the world. The fact that criminals use Bitcoin for tax evasion, money laundering, illegal drugs, and ransom payments, among other things, should at least give us pause.

Applying CT, we should ask

- What purpose am I trying to achieve?
- Is using Bitcoin a means to that end?
- Is it worth the trouble or risk?
- Are there other/better alternatives?

Of course, this is generally good thinking.

Nasdaq, a well-established security exchange, recently became interested and said it might develop a cryptocurrency exchange platform sometime in the future, according to a May 25, 2018 *Investopedia* article. For Nasdaq, The potential for additional commissions is certainly tempting. But, even if such exchanges come to pass, they can't be taken as endorsing investment in certain cryptocurrencies. Remember, major exchanges also dealt with securities that caused the subprime mortgage crisis and the 2007-2008 financial crisis in the USA. It is common sense that the quality of the goods has little to no connection to the market itself.

The fact that criminals use Bitcoin for tax evasion, money laundering, illegal drugs, and ransom payments, among other things, should at l east give us pause.

However, if a government considers digital versions of its currency or a bank looks into blockchains as a way to make its operations more secure and robust, I am all for it. For official digital currencies, there are many technical, societal, and legal problems to address along the way and we will see what the future brings. Meantime, keep your cash and don't throw away your credit/debit cards.

I hope you find this article useful and please feel free to email your feedback to me at pwang@cs.kent.edu.

*A Ph.D. and faculty member from MIT, **Paul Wang** became a Computer Science professor (Kent State University) in 1981, and served as a Director at the Institute for Computational Mathematics at Kent from 1986 to 2011. He retired in 2012 and is now professor emeritus at Kent State University.*