CPSC 367: Cryptography and Security

Michael J. Fischer

Slides derived from a lecture by Alice E. Fischer

Lecture 25
April 25, 2019

Applying Critical Thinking Skills

This lecture looks at blockchains, cryptocurrencies, and their effects on society. As we go through the material, I want you to listen and think critically about it. Questions to consider include:

- How does one know what one knows?
- What things should one believe?
- How can one defend oneself against fake news?
- How can one tell the difference between objective truth and group-think?

Trust

We Have to Trust the Institutions Around Us

Multiple organizations are involved in making our monetary system work:

- Banks
- Charge-card services
- PayPal
- The Federal Reserve
- Congress and the treasury department of the U.S.A.

We expect them to respect our privacy and not steal from us.

Cryptocurrency advocates believe we should not trust them because they can regulate things, enforce laws, and manipulate the currency.

We Have Permanent Records

We trust our governments to keep accurate permanent public records of:

- Births and deaths
- Land Sales
- Citizenship and voters registration
- Taxes owed and paid
- Military service and status

These records have been made, preserved, and made accessible for hundreds of years—all without using cryptography.

Do you trust these systems? Why or why not?
Would you trust a blockchain system more? Why or why not?

We Have Business Records

We trust our large companies to keep accurate records of:

- Investments
- Cash in the bank
- Telephone numbers (paper and online)
- Accounts and payments
- Academic records and degrees

These ordinary business services are the foundation of our way of life.

The point is, we cannot live without trusting third parties. Trust is the basis of all civilization.

We Rely on the Internet

In doing so, we rely on governments and big companies.

- ISP's and Internet Exchanges, some operated by the government, others by universities or businesses.
- Infrastructure maintained by big companies and open to spying and government control.
- Domain name servers.
- Internet access points that connect subnets. Many are owned or controlled by governments.

The proper functioning of blockchains assume that the Internet is trustworthy, open, and free from government intervention. Not so!

Some people do not trust anybody.

Libertarians, like many blockchain proponents, distrust authority, state power, and "big business".

One of the claims about blockchain is that it eliminates the need for trusting third parties.

Blockchain does make it more difficult to pursue criminals or regulate shady practices!

The protocols have been designed to replace trusted third parties by collective trust.

Collective trust

In place of trusting a third party (bank, government, business), blockchains are based on collective trust in the large set of people who maintain the blockchain. The requirements for enabling that trust are:

- The parties maintaining the cryptocurrency must be independent, and no party should hold a majority of the power.
- All maintainers must have a stake in the integrity of the blockchain.
- The majority of maintainers will act in their own self interest by following the rules that support the integrity of the blockchain.

Why Trust the Miners?

In both Bitcoin and Ethereum, miners are collectively trusted.

- Miners invest money (electricity, computer hardware, big buildings) in the mining process. They are (eventually, probably) rewarded for solving a puzzle by getting some bitcoin.
- The self-interest of these miners is to maintain the value of that bitcoin.
- These same people commit transactions (and earn fees for it), manage the blockchain, maintain its validity, and store all or part of it.
- The wasteful mining mechanism makes it expensive to be a miner. This helps to prevent a single miner or group from having enough control to corrupt the blockchain.

Why these assumptions may not hold in the real world

- Mining is not really open to an individual any more. It is only large groups (companies, governments) that can succeed often enough to make it worth the investment.
- A large enough party (e.g., China) that is also strictly authoritarian does not have the same motivations as the individual miners.
- In much of the world, individuals have no choice about obeying their government.
- The internet and access to it is controlled by governments and large companies.

Cryptocurrencies do not eliminate third parties

The blockchain only keeps track of the record of all transactions. By itself, that is not enough to support a currency system.

- There must be a reliable way to locate other miners in order to interact with them and stay synchronized.
- There must be a reliable way to locate the full blockchain if you have been offline for a while.
- Converting to and from real currencies requires trusting an exchange.

Trusted third parties within the Bitcoin community are used for all of these purposes.

Waste

Reality: Protocols

The protocols that implement block chain are far from perfect.

- They can have, and have had, bugs. They are written, maintained, and managed by true-believers acting in good faith. They have bugs anyway, some disastrous. (See the Bitcoin and Ethereum articles.)
- There are a variety of known attacks on the systems.
- Bitcoin enterprises depend on the internet being reliable, open, and not under anyone's control.
- From an environmental point of view, Bitcoin and Ethereum are irresponsible wastes of energy and resources.

Reality: Environmental Impact

Environmentalists believe in avoiding wasteful use of resources.

- By design, earning a Bitcoin is compute-intensive. The computations are totally useless except for competing for Bitcoins. They do not produce useful goods or knowledge.
- If another miner posts a solution a split second before you do, you lose. Any energy you have used trying to solving that puzzle is totally wasted.
- This is repeated millions of times for every bitcoin mined.
- More miners equals more waste and a higher cost for mining each bitcoin.
- As more mining computers are added to the pool, the rate of waste per bitcoin mined grows.

It's a Really BIG Waste

These statistics involve only Bitcoin. Ethereum and other currencies add to the numbers.

- Whole warehouses of specially designed computers work 24/7 trying to solve these puzzles.
- Currently, worldwide mining uses about 0.5% of the world's electricity. This is more than is used in the entire Czech Republic and almost as much as in Ireland.
- Miners are looking for cheap electricity. Some are investing in renewable energy sources.
- The cheap coal-powered plants in Sichuan and government subsidy of fossil-fuel in Canada make those sites attractive.

Exchange Nightmares

Digital Currency Exchanges

An exchange is a business that allows customers to trade digital currencies for other crypto or conventional currencies.

- An exchange might be a steward for hundreds of thousands of Bitcoins, much like a stock brokerage. The exchange holds customer's Bitcoins and buys/sells them according to the customer's standing orders.
- An exchange typically keeps some part of its funds online, ready to make instant transfers. This is called its hot wallet
- Keeping large sums online is considered a bad security practice.
- The majority of funds are kept offline (cold wallet), and not easily available for transactions or thefts. The keys to unlock these funds are kept on paper or digitally. Both methods are subject to total loss (theft, fire, disk failure).

Major Bitcoin Bloopers

- May 2012, hacking: $91,306
  Zhou Tong, former founder of the exchange Bitcoinica, discovered an entry into Bitcoinica's server through an excessively privileged compromised email address. This caused the theft of the entire "hot wallet" as well as the loss of the main database.
- November 2012, hacker with trojan horse: $38,000
  A trojan horse that doubled as a keylogger stole thousands of BTC between September and November of 2012. BitcoinTalk user "mralbi" lost almost 2600 BTC. The same hacker also stole 200 BTC from Mt. Gox accounts.

Recent Bitcoin Thefts

- December 2017, $77 million
  Slovenian website NiceHash, which lets users buy and sell computer time for mining cryptocurrency, lost about $77 million when its payment system was hacked in a "highly professional" heist.
- Security firm FireEye reported signs of North Korea targeting South Korean cryptocurrency exchanges, but said that, given cryptocurrency's relative anonymity and rapidly rising prices, exchanges are natural targets for hackers.

Recent Cryptocurrency Thefts

Exchanges are, unfortunately, honey pots.

- January, 2018, $530 million
  The exchange, Coincheck, has promised partial refunds to the 260,000 investors affected by this weekend's theft. Coincheck bills itself as "the leading bitcoin and cryptocurrency exchange in Asia",
- This is the biggest such theft on record, eclipsing the ∼$400 million in bitcoin stolen from Mt Gox in 2014.
- The hackers stole customer deposits of NEM, a less well known digital currency.

Bitcoin Gold

May 2018, a known attack: up to $18.6 million.

- A malicious miner used a 51% percent attack to take temporary control of the Bitcoin Gold blockchain and steal funds from exchanges.
- He deposited funds on an exchange and quickly withdraw them again, after which he reversed the deposit transaction. This enabled him to resend the same coins to another wallet under his control.
- Ordinarily, the blockchain would resolve this by including only the first transaction in the block, but the attacker was able to reverse transactions since he had majority control of the network.
- This double-spend attack was at least the third network attack on altcoins that week.

QuadrigaCX

February 2019: $190 million USD user funds likely lost.

- QuadrigaCX is a Canadian cryptocurrence exchange, owned and operated by the exchange's founder, Gerald Cotton.
- Cotton reportedly died on a trip to India.
- The company filed for creditor protection on February 5, 2019. A Termination and Bankruptcy Assignment Order was issued by the Supreme Court of Nova Scotia on April 11, 2019.
- Users have been skeptical of the exchange's claims, including whether or not Cotton actually died.
- It seems likely that thousands of users will never be able to recover their funds.

Exchanges come and go.

- March 2014, hacking: $450 million. Mt Gox filed for bankruptcy in Japan after 744,000 bitcoins owned by customers and 100,000 of its own "disappeared". Owners were not compensated. Hackers exploited a weakness in the system for tracking transactions that allowed the currency to be diverted.
- June 2013, Stupidity: $248,088 An unencrypted backup at Bitfloor was mistakenly stored on some servers. It contained the keys to the hot wallet. A hacker gained entry and stole most of both the hot wallet and the cold wallet. Bitfloor's banks shut down the exchange's operation.
- December 2017, South Korean bitcoin exchange Youbit filed for bankruptcy after being targeted by cybercriminals twice in the space of a few months.

Bugs and Attacks

Splitting the Internet

Many countries have a "kill switch" that can isolate the entire country from the internet.

- In these countries, all internet traffic goes through a single exchange point, or a few exchange points, on its way to the rest of the world.
- Turkey, Egypt, India, and the United Kingdom all have authorized kill switches. The US might have one. Russia is reducing the number of exchange points toward that end.
- These countries are also able to selectively let traffic through, and could easily block all of, or selected parts of, incoming or outgoing cryptocurrency transactions.

Internet Outages

If they CAN do it, they probably WILL do it, if motivated.

- It is well known that China censors internet content.
- In Egypt and Cameroon, governments shut down all internet traffic during times of civil unrest.
- Total outages have also been caused by vandalism to cables (under water and on land), cyber attacks on routers, and DNS attacks.

Possibility: Cryptocurrency Warfare

We know that the government of China, is able to control the Chinese internet.

- China has the potential motivation to wreck any western economy.
- It has the resources to start a Bitcoin war by starting up and controlling a large number of miners.
- In an authoritarian state, people do as they are told.
- The state could add miners and command or take over existing miners at will.

How likely? Very, if they had the motivation, they could do it.

A Cyberattack on Bitcoin

Now consider what happens to the Bitcoin economy if large country A decides to use its kill switch to cut its users off from the rest of the world.

1. This will not be evident to any miner, since miners on both sides of the divide still have plenty of available peers.
2. Both sides continue processing transactions, causing the Bitcoin blockchain to fork.
3. But country A has a lot of compute-power. Eventually the A chain will be two or three blocks longer than the other chain.
4. At that point, country A reopens the kill switch and wipes out the other blockchain, causing currency chaos.
5. This ploy can be repeated, at will, to destroy the bitcoin economy.

Reality: Hardware and Infrastructure

The software runs on collections of computers communicating through the internet.

- Computer systems have vulnerabilities. Software has security vulnerabilities. These can be used to attack systems at exchanges, for example.
- The internet infrastructure is vulnerable to attacks such as DNS spoofing.
- Even when it is working properly, we cannot rely on the internet infrastructure to be always available, since governments can shut it down arbitrarily.

These factors add unpredictability to bitcoin transactions, that are already complex.

Software Bugs

Blockchain is implemented by software running on computers.

- Software has bugs. The standard crypto libraries seem free of them, but software is involved in creating and validating a block and in making any transaction.
- Bitcoin software has been created by enthusiastic programmers who believe in themselves and in the wonders of cryptocurrencies. (I have less faith in both!)
- The major blockchain protocols (Bitcoin, Ether) had bugs in them that allowed currency to be stolen or "disappear".
- Tether, which distributes cryptocurrencies tied to the value of the dollar, reported close to $31 million in its coin was stolen. It pushed out updates to its software to freeze the stolen tokens from further transfer.

Major Bitcoin Bloopers

- 50BTC Theft , October 2012: $13,437
  The 50BTC mining pool suffered a hack of the billing software. They were unable to identify the vulnerability and completely rewrote the billing software after the incident.
- February to May, 2013, $230,468
  The support system of a cloud hosting company (Linode) had a vulnerability that was used to obtain administrator access to the servers. Once the Linode servers were compromised, eight accounts dealing with bitcoins were targeted and BTC was transferred.

Ethereum Blooper 1

July, 2017, $32 million. A bug and an exploit.

- Smart-contract coding company, Parity, issued a security alert, warning of a vulnerability in version 1.5 or later of its wallet software. $30 million of ether were reported as stolen.
- At least three ether addresses have been compromised as a result of the bug.
- The issue is the result of a bug in a specific multi-signature contract known as wallet.sol. The issue was mitigated by white hat hackers who took control of other vulnerable wallets.

Ethereum Blooper 2

November 2017, $300 million.

- Parity revealed that, while fixing the multisig bug, it had inadvertently left a second flaw in its systems that allowed one user to become the sole owner of every single multi-signature wallet.
- A user triggered the flaw, apparently by accident.
- When Parity realized what they had done, they rushed to undo the damage by deleting the code which had transferred ownership of the funds.
- Rather than returning the money, that act simply locked all the funds in those multisignature wallets permanently, with no way to access them.
- Parity is asking the Ethereum community to support a "hard fork" to undo those transactions.

Investment

What is Investment?

- People invest in things that have intrinsic value: real estate, art, education, factories, life insurance, children, etc.
- That value should have a high probability of being stable or increasing over decades.
- People expect to be able to sell an investment, now or later, without great loss.
- Many people invest in pension funds and real property in order safeguard their wealth against changing times and conditions.
- Some invest as a way to accumulate wealth and power.

How is Investment like Gambling?

- One should neither invest nor gamble more than he can afford to lose.
- Gambling only provides the possibility of a high reward; there is no promise.
- There are both high- and low-risk investments. High-risk investments often promise high rewards that often fail to materialize.
- Venture capitalists pour money into high-risk enterprises, hoping to invest in a tech startup that will skyrocket in value.
- Many venture capitalists are pouring millions into cryptocurrencies, hoping to get rich fast. However, it is a confusing situation

Cryptocurrency Investment on July 9, 2018

From digitaltrends.com: "It's undeniable that cryptocurrency is the new hotness and all the cool kids are into investing in various virtual currencies."

There are, literally, thousands of cryptocurrencies.

- 1618 species of cryptocash were listed July 9.
- 1405 species traded over a million dollars coin that day.
- 105 more traded between $1000 and $1 million of coin.
- On July 9, 2018, he total market capitalization for all coin species was $272,405,394,136
- The largest-volume app at the apple store was a cryptocoin-trading app.

Bitcoin Speculation

- By the rules of the currency, only a limited amount of Bitcoin can ever exist.
- Speculators bet their real money on the belief that an increasing number of other investors will want to buy the limited number of Bitcoins. Therefore, the value will rise.
- The amount of buy-in dollars cannot continue to grow at the rate it has been growing. Many experts expect the market to collapse.
- Unlike a real commodity (art, gold, tulip bulbs), a cryptocurrency has zero intrinsic value. So when (if) the collapse comes, current Bitcoin owners will lose all.
- Their Bitcoins will suddenly be worth nothing because nobody will be willing to buy them.

Ponzi Schemes

- A Ponzi scheme is a form of fraud in which a "businessman" lures investors and pays profits to earlier investors using funds obtained from newer investors. Investors are led to believe that the high profits are coming from asset-value growth.
- A Ponzi scheme keeps the illusion of a profitability as long as:
  - Most of the investors do not demand full repayment.
  - They are willing to believe in their vaporware assets.
  - There are new investors willing to invest new funds.
- Typically, Ponzi schemes require a large initial investment and promise well-above-average returns.
- It is common for the operator to take advantage of a lack of investor knowledge or competence.

Named after Charles Ponzi, notorious for using it in the 1920s

Is Bitcoin a Ponzi Scheme?

When and if Bitcoin crashes, the current holders will lose all. In that sense, it is a fraud. Currently, it maintains the illusion of profitability:

- If many owners start cashing out, the value will start falling and others will also cash out. This is how markets collapse.
- Current investors, miners, and users seem to believe in the enterprise, almost religiously.
- Some investment advisers are actively advocating investment. They promise large returns.
- Some advisers advocate buying Bitcoin, wait for the price to rise, then cash out. This is called pump-and-dump.
- Venture capitalists with no understanding of the computing, cryptography, and network security issues have invested billions in cryptocurrencies.

Bitcoin Psychology

The market value of Bitcoin varies up and down constantly.

- A merchant wants to be paid fairly for his product. If the payment is in Bitcoin, he may get much more or much less than he expected because of the half-hour delay. This is unpopular with sellers.
- To ameliorate that, one service is willing to guarantee a price for 20 minutes. By then, 80% of attempted Bitcoin transactions have been committed.
- Because, overall, the market value is rising, there is a dis-incentive to sell Bitcoin, or to use it for purchases. What if you paid today for a $20. pizza and found out tomorrow that the bitcoin was really worth $30? A week later it is worth $50, and you kick yourself.

Currency

What is a Currency?

To be useful, a currency must:

1. Be easy to use and carry around, like paper money and checkbooks.
2. Be difficult or impossible for individuals to forge.
3. Be convertible to other world currencies.
4. Be widely accepted for purchasing all kinds of ordinary goods.
5. Have a largely-stable value.
6. Be difficult to steal and possible to recover if stolen.

Bitcoin is (1) easy to carry around, (2) difficult to forge and (3) Bitcoin exchanges will convert it to and from world currencies. It sounds good so far.

Weaknesses of Bitcoins

But properties 4, 5, and 6 are lacking:

4. Bitcoin has a highly volatile value, changing constantly. On July 8, its value was $6742. On July 12 it hit $6155 and on July 15 it was $6246.
5. At this time, it is not easy to buy daily needs using Bitcoin.
6. There is no backing by a reputable authority. (FDIC backs bank deposits, Congress regulates banks.)
6. The Bitcoin exchanges are hacker targets.
7. If you lose your wallet or the crypto keys, you lose. About %25 of all bitcoins have been lost permanently.
7. If the money is stolen, you lose. Exchanges often are unable to repay the losses.

. . . and what happens if your private signing key gets compromised?

Summary

Who uses Cryptocurrencies?

They are used for illicit transactions including ransomware and drug deals.

They are used by ordinary people who believe in the cryptocurrency and its bright future, and who praise the "convenience" of using an electronic form of money.

They are purchased by speculators who believe their value will keep rising. These investors are betting that merchants will begin accepting payments in Bitcoins, that cryptocurrencies will gain general acceptance in the future, and that their value will stabilize or rise when that happens.

What is wrong in this picture?

Four sources of major risk:

- If you lose your bitcoin wallet, you lose. There is no way to prove you had $$.
- If a hacker or exchange steals you money, you lose.
- To trust the cryptocurrency, you have to trust all the software and all the people who wrote it. Experience has shown that both authors and software are untrustworthy.
- International groups can and might attack the cryptocoin systems.

The only compelling reason to use bitcoin is illegal activities that need to remain anonymous.

Contrary to popular belief:

- Bitcoin is not free of the need to trust third parties, including governments.
- It is not widely accepted for purchasing goods because, for a merchant, it is unreliable.
- It IS possible to steal, and massive thefts have happened,
- A transaction is not fully anonymous or untraceable, and some have been traced.
- It IS possible to corrupt a chain: it can happen if enough maintainers agree to corrupt it.
- The lack of government oversight and backing is NOT an advantage.

The biggest problem is that, when you get in bed with thieves ... you are in bed with thieves!