

14.27/270 Ecommerce

The Economics of Cryptocurrencies

S. Shang

A step back

What is a currency? The fundamental idea behind an economy is that having everyone be an atomistic subsistence hunter/farmer is an extraordinarily inefficient way to organize ourselves. Much more efficient would be a system where I would focus my efforts on productive tasks where I have an advantage, everyone else would do the same, and we would trade the resulting products so that we'd all have the mix of products that we need and desire. We could barter to obtain that mix, but barter arrangements can be very cumbersome and might entail writing complicated contingent contracts to subdivide units of production, consummate multi-party transactions, or consummate transactions over time. It's so much simpler to have a currency, or medium of exchange, that holds value and can, essentially, do the accounting for us. (We might still have to have contracts, but many, many fewer.)



A step back

What is a currency? The fundamental idea behind an economy is that having everyone be an atomistic subsistence hunter/farmer is an extraordinarily inefficient way to organize ourselves. Much more efficient would be a system where I would focus my efforts on productive tasks where I have an advantage, everyone else would do the same, and we would trade the resulting products so that we'd all have the mix of products that we need and desire. We could barter to obtain that mix, but barter arrangements can be very cumbersome and might entail writing complicated contingent contracts to subdivide units of production, consummate multi-party transactions, or consummate transactions over time. It's so much simpler to have a currency, or medium of exchange, that holds value and can, essentially, do the accounting for us. (We might still have to have contracts, but many, many fewer.)

Hmm, seems like a matching problem---we've seen those before!





Celtic ring money

A step back

The history of currency media used, ranging from precious metals to shells to heavy stones to tiny replicas of the goods traded. While more efficient than barter, these currencies were still cumbersome and vulnerable to theft and counterfeit. Also, unless the medium had significant intrinsic value, a central authority was necessary to validate it. Paper money had many advantages, but a central validating authority was even more important then, as the currency became easier to transport and counterfeit.

Furthermore, governments, as the central validating authority, realized that their decisions regarding the currency---such as how much to validate---could have very significant implications for economic activity. (Governments have, of course, abused this power, but have often used it as a tool for encouraging or stabilizing economic activity. This is called monetary policy.) A government-validated currency is called a fiat currency.

A step back

In addition, governments benefit from creating currency because it costs less to make money than the money is worth. This is called seignorage.

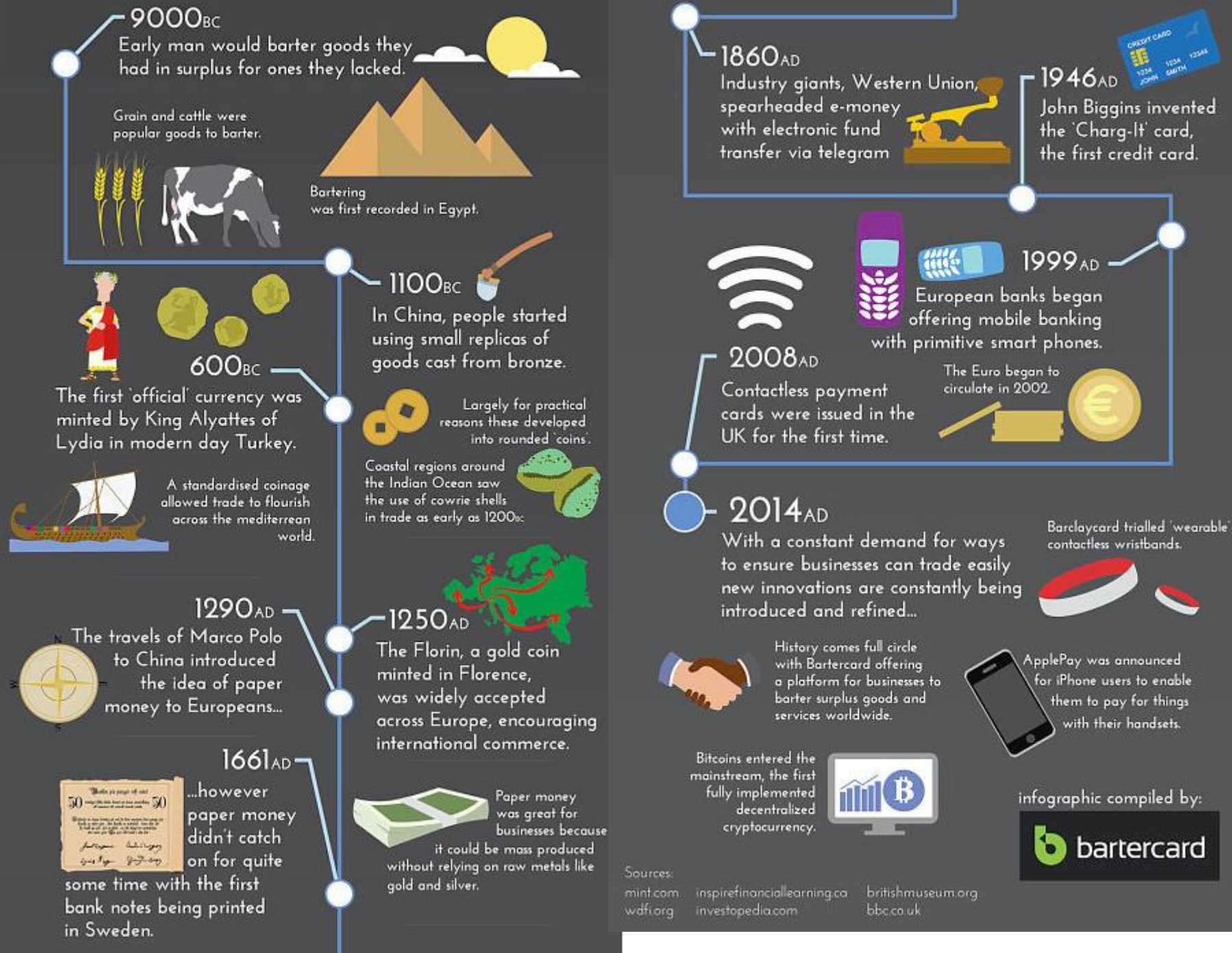
Throughout history, various metals, some of which are considered precious today, appear to have been used as a form of currency. The Bretton Woods system, under which all major currencies were theoretically exchangeable for gold, was abolished in 1971.



HISTORY OF MONEY

Over its vast history, money has been central to developing our modern international trade networks. However new research has revealed that history is coming full circle, with 80% of people admitting to bartering with a business rather than using money.

Here's a cute graphic I found on the Telegraph's website, which has some interesting facts and useful dates. (The part about history coming full circle is crazy, though.)



So what do we want and need from a currency?

- **Easy to transport and trade**
- **Durable and storable**
- **Verifiable**
- **Invulnerable to counterfeit and fraud**
- **Flexible (e.g., conditional payments)?**

What's inadequate with the system of fiat currencies that we have?

- **Trading between fiat currencies can be cumbersome and costly, discouraging international trade and rendering micropayments infeasible.**
 - Overseas bank account
 - Payments on peer-to-peer platforms that span countries, e.g., filesharing
- **An integrated international banking system makes hiding and securing funds difficult. (Obviously, one can want to hide and secure funds for entirely benign reasons or for nefarious and criminal reasons.)**
 - Saudi royalty, Russian oligarchs, guy in South Carolina
 - Criminal activity
- **They are vulnerable to mismanagement and manipulation by governments.**
 - Argentina, Turkey

Remember in our discussion of peer-to-peer platforms, we mentioned the distinction between a centralized matching process and a decentralized one. There's an analogy (but not a perfect one) here. Think of a currency as the means to match someone who has produced more than she needs now and has value she wants to store with someone who needs to borrow value against his likely future production. A central authority doesn't need to do the actual matching of those two but rather validates a medium that makes the matching cheap and easy, currency.

The inadequacies in fiat currencies that we discussed on the previous slide could, perhaps, be mitigated by having a *decentralized* system instead of a centralized one. That's where cryptocurrencies come in. In other words, the key distinction between cryptocurrencies and fiat currencies is not their digital nature but rather their decentralized authority. (You can, essentially, conduct all of your business today in dollars without ever seeing a physical bill or coin, after all.)

But how on earth can you create a non-physical medium of exchange that, by its nature, must be agreed by many people to have value, without having a central authority? Here's one way:

- 1. You have every peer participating in the network keep an agreed-upon ledger of all transactions.**
- 2. To consummate a transaction, say Henry giving a coin to Roxy, there is an easy-to-check method to verify that it's legitimate, i.e., that Henry owned the coin and intended to give it to Roxy.**
- 3. That transaction does not get written on the ledger until it is confirmed. Confirmation is not easy---one must solve a very difficult computational problem in order to confirm---but doing so gives the confirmer, or "miner," a transaction fee plus seigniorage (some of the currency). After being confirmed, every peer adds it to his or her ledger---the "blockchain."**
- 4. There is a pre-determined growth in the number of coins, and the tolerance, determining how difficult the confirmation problem is, changes to implement this growth rate. At some point, the maximum number of coins will be reached.**

So maybe the best way to think of a cryptocurrency is as analogous to a bank account, not a currency.

It consists of a set of account numbers and a record of the balance in each account.

And cryptographic technologies allow owners to make transfers between accounts and provide records sufficient for recipients to verify transfer in a decentralized manner.

Notes:

\$6500 when I last taught this class

- 1. Bitcoin was the first and remains the largest cryptocurrency. 19 million have been mined and, according to the protocol, only 21 million are left to be mined. A bitcoin is worth about \$45,000 (but fluctuates relative to the dollar a lot).**
- 2. There are now thousands of cryptocurrencies. They do not have identical protocols and, in fact, can vary in important ways. (Most of the foregoing discussion was based on the Bitcoin protocol.)**

Bitcoin, Ethereum, Ripple, and others were originally established to facilitate other business models that necessitated efficient funds transfers.



Here are some ways in which different cryptocurrencies could and do vary:

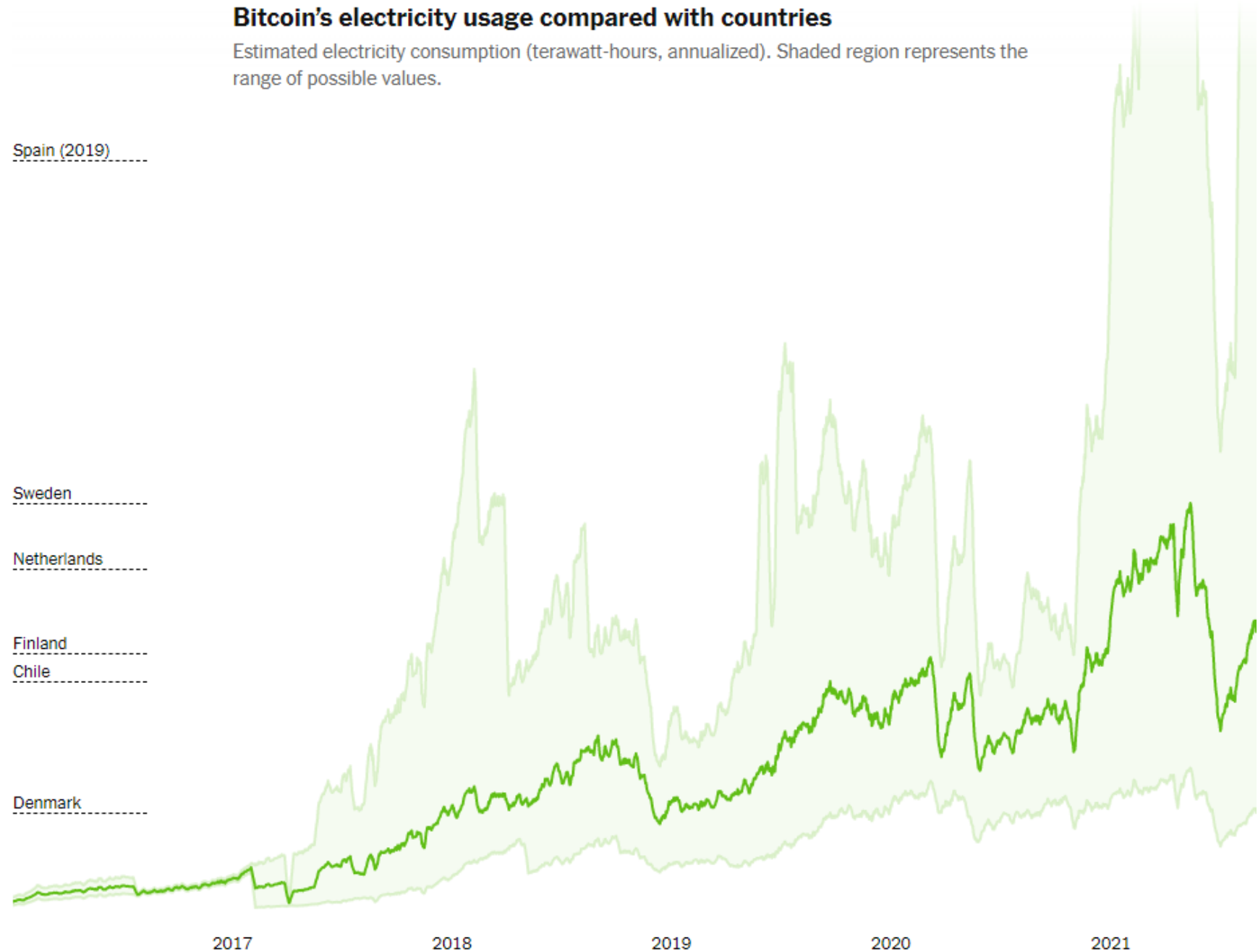
- 1. You might have a fixed “money supply,” or let it grow forever, or let it grow according to something other than a predetermined rate. One could even imagine having the money supply determined by the tolerance which is a function of, say, macroeconomic variables or exchange rates. Creating that dependency would be like automating monetary policy.**
- 2. Bitcoin is a proof-of-work cryptocurrency, which is one where a difficult computational problem needs to be solved to confirm transactions. This type of cryptocurrency has proved disastrous for the environment. Bitcoin mining probably already uses as much electricity as the entire country of Ireland (3.1 GW), and is growing towards Austria’s (8.2 GW) (“Bitcoin’s Growing Energy Problem,” de Vries). One transaction is estimated to take >1000 kWh. Other cryptocurrencies are set up as proof-of-stake. Confirmation is done through an alternative means and is much less wasteful of resources.**

Power a
typical
American
home for six
weeks!

Bitcoin's energy consumption over time.

Bitcoin's electricity usage compared with countries

Estimated electricity consumption (terawatt-hours, annualized). Shaded region represents the range of possible values.



Source: [EIA, Cambridge Bitcoin Electricity Consumption Index](#) - Country usage numbers are from 2019. Electricity cost for miners is assumed to average \$0.05 per kilowatt-hour. Upper, lower and best guess trends are estimated using the [research methodology](#) behind the Cambridge Bitcoin Electricity Consumption Index.

Here are some ways in which different cryptocurrencies could and do vary:

3

- 1. Bitcoin allows those wanting to make a transaction to offer a fee of their choice. Those offering higher fees will have transactions that are more attractive to include in a block and, therefore, get confirmed faster. (Confirmers get paid seignorage plus the fee.) There are many alternative ways to set up compensation for the confirmers.**

Also, security, record-keeping capacity, computational capability, stable v. floating value, anonymity, etc.

Questions:

1. How does everyone verify Henry's intention to give Roxy a coin? Well, they just check to make sure that whoever proposed the transaction had Henry's password.
2. Is there any special skill involved in solving the computational problem? No, you mostly have to have a specialized computer and access to cheap electricity.
3. What if two people solve the confirmation problem at essentially the same time? That happens, and forking of the blockchain can occur, so peers typically agree not to carry out the actual exchange until it's clear which fork will be added onto. (The other fork is abandoned, or orphaned, and its transactions are not recognized.)
4. How is anonymity preserved if the ledger is public knowledge? Accounts need not have any traceable connection to a person. Patterns of transactions may hold clues to identity, though. Also, people might be traceable through exchanges.
5. It seems like everyone is playing a repeated (or dynamic) game. Is the intended equilibrium the only one? Probably not.
6. How vulnerable are cryptocurrencies to attacks of various kinds? Work is being done ...

Incentives and multiple equilibria:

The system relies on confirmers being willing to solve these problems, bundle together transactions, and add them to the end of the longest chain in the blockchain. But what guarantees their behavior? Well, we know that they are compensated for solving the problems and bundling the transactions. How about the last part? Biais et al, in “The Blockchain Folk Theorem,” prove that

- 1. There exists a Markov perfect equilibrium where all blocks are added to the longest chain.**
- 2. There are other Markov perfect equilibria. For instance, consider the rule to always add to the end of the longest chain except on any day after the Red Sox win the World Series and then add to the block N blocks back on the longest chain where N is the number of home runs that the Red Sox hit during the World Series.**

Incentives and multiple equilibria:

The system relies on confirmers being willing to solve these problems, bundle together transactions, and add them to the end of the longest chain in the blockchain. But what guarantees their behavior? Well, we know that they are compensated for solving the problems and bundling the transactions. How about the last part? Biais et al, in “The Blockchain Folk Theorem,” prove that

- 1. There exists a Markov perfect equilibrium where all blocks are added to the longest chain.**
- 2. There are other Markov perfect equilibria. For instance, consider the rule to always add to the end of the longest chain except on any day after the Red Sox win the World Series and then add to the block N blocks back on the longest chain where N is the number of home runs that the Red Sox hit during the World Series.**

Somewhat concerning

Attacks and vulnerabilities:

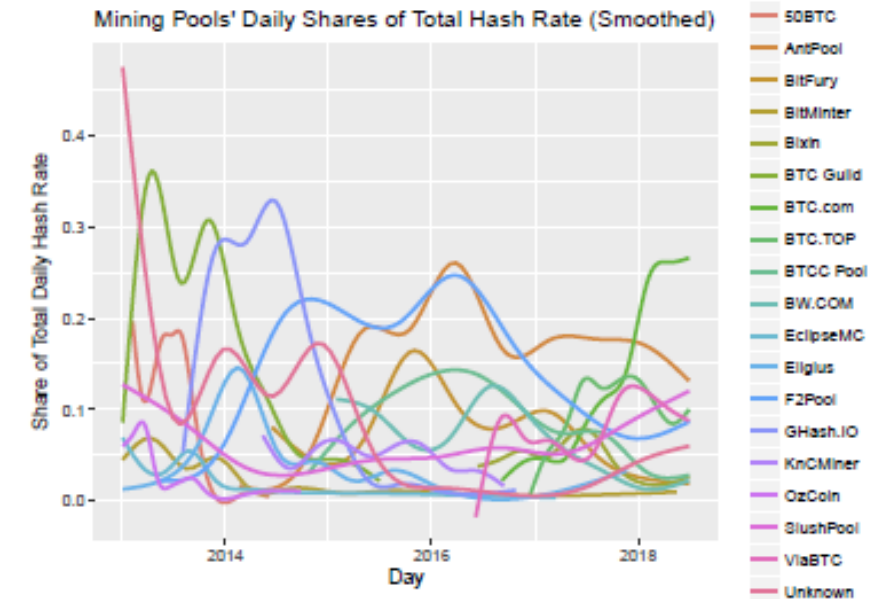
To understand the types of attacks that can occur to cryptocurrencies, it is useful to understand the notion of a mining pool. This is a group of miners all working to solve the confirmation problems and essentially providing insurance for its members against the stochastic nature of mining. So if someone in your mining pool solves the problem and adds to the blockchain, his or her proceeds get divided up by the pool.

There are interesting incentive and verification issues that arise when creating these pools, analogous to the adverse selection and moral hazard issues that insurance companies always have to deal with. But we won't get into those.

Here's a graph looking at how different mining pools' computing power has varied over time.

Mining Pool Market Share by Hash Rate

The plot below shows the (smoothed) shares of hash power for any mining pool that has controlled at least 5% of daily hash power for at least 120 days.



Attacks and vulnerabilities:

Attacks, such as creating orphaned branches which can compromise the integrity of the entire currency, start to become more likely with the existence of concentrated mining capacity, as exists in mining pools.

Theorists in computer science and economics have shown that, for instance, the possibility of majority attacks can effectively limit the number of transactions that can occur, or that conditions exist where it's optimal for large miners to withhold blocks.

Crypto and crime:

One major concern that regulatory authorities (and most people, in fact) have with cryptocurrencies is their potential for facilitating crimes.

tax evasion

ransom attacks

smuggling, trafficking, etc.

illegal gambling

Crypto and crime:

Makarov and Schoar (2021) use the fact that the Bitcoin ledger is public to examine this and other questions about Bitcoin usage and transactions. (Users can make a separate account to hold the proceeds of each transaction, but often store proceeds of multiple transactions in the same account and/or spend money from two or more accounts in a transaction. This makes it feasible to infer identities of some account holders.)

-Naive estimates of Bitcoin volume overstate by a factor of 10---most volume is change retained by the sender.

-About 80% of true volume is transfers to, from, or between exchanges. Illegal transactions, scams, and gambling account for about 3% (e.g., \$1.6b to dark net goods, \$500m to scams, \$16m to ransom payments).

-Mining concentration is highly negatively correlated with Bitcoin value. (As value goes up, miners without access to the cheapest electricity enter, bringing concentration down.)

Crypto and crime:

Makarov and Schoar (2021) use the fact that the Bitcoin ledger is public to examine this and other questions about Bitcoin usage and transactions. (Users can make a separate account to hold the proceeds of each transaction, but often store proceeds of multiple transactions in the same account and/or spend money from two or more accounts in a transaction. This makes it feasible to infer identities of some account holders.)

-Naive estimates of Bitcoin volume overstate by a factor of 10---most volume is change retained by the sender.

-About 80% of true volume is transfers to, from, or between exchanges. Illegal transactions, scams, and gambling account for about 3% (e.g., \$1.6b to dark net goods, \$500m to scams, \$16m to ransom payments).

-Mining concentration is highly negatively correlated with Bitcoin value. (As value goes up, miners without access to the cheapest electricity enter, bringing concentration down.)

Can't say much about tax evasion...

Crypto-related businesses:

1. Coin creation

- **These were the earliest successful crypto businesses. Litecoin launched in 2011. Then XRP, Dogecoin, etc., by 2013. 500 entrants in 2014. Now over 10,000 coins.**
- **The developer earns seignorage returns.**

















2. Mining

- **Miners are paid for their role in recording transactions with newly-minted coins and/or transaction fees.**
- **Most miners join pools, reducing their idiosyncratic risk. Pools take 2-4% of revenue.**
- **Most pools were based in China prior to 2021 crackdown. Capacity has moved to US, Kazakhstan, Russia, and Canada. Some of the largest pools are publicly traded.**

3. Exchanges

- **Highly profitable businesses, combining the traditional roles of brokers and exchanges.**
- **Mostly located off-shore.**
- **Offer trading in coins, futures, derivatives, fiat currencies, etc.**

Current exchange volume, characteristics

Name	Exchange Score i	Volume(24h)	Avg. Liquidity	Weekly Visits i	# Markets	# Coins	Fiat Supported	Volume Graph
 Binance	9.9	\$13,310,533,877 ▲ 34.31%	803	24,448,014	1647	395	AED, ARS, AUD and +43 more i	
 Coinbase Exchange	8.3	\$1,701,847,301 ▼ 4.18%	710	2,952,564	503	169	USD, EUR, GBP	
 FTX	8.2	\$1,057,504,852 ▲ 26.46%	748	4,294,539	458	321	USD, EUR, GBP and +7 more i	
 Kraken	7.7	\$402,210,196 ▼ 1.16%	713	1,851,046	472	133	USD, EUR, GBP and +4 more i	
 KuCoin	7.4	\$1,330,827,709 ▲ 22.82%	541	2,594,694	1198	623	USD, AED, ARS and +45 more i	
 Huobi Global	7.2	\$1,322,108,373 ▲ 35.01%	529	1,682,804	1063	475	ALL, AUD, BRL and +47 more i	
 Gate.io	7.2	\$1,534,502,102 ▲ 19.64%	475	3,859,061	2324	1349	KRW, EUR	
 Bitfinex	7.2	\$293,782,930 ▲ 37.41%	616	795,460	394	177	USD, EUR, GBP and +1 more i	



Economic thoughts:

- 1. As cryptocurrencies become more popular, they make the monetary policy of nations increasingly impotent. As we noted before, a tremendous amount of harm has been done in the past with irresponsible monetary policy. What we haven't said yet is that a tremendous amount of benefit has come out of responsible monetary policy. I am no macroeconomist, but I am very happy to live in a country with a competent and (mostly) independent monetary authority that can react to economic downturns, financial crises, and inflation in well-informed and constructive ways.**
- 2. As cryptocurrencies become more popular, they make tax collection less effective and fair. (Honest people can always report their cryptocurrency holdings and remit taxes, but we probably don't want a tax system that relies on unverifiable honesty.) Ineffective and unfair tax systems can cripple governments and endanger basic government services.**
- 3. Furthermore, a country with an ineffective and unfair system of taxation could end up with extreme income and wealth distributions, which could have its own consequences.**

Economic thoughts:

- 4. Little work has been done about the competition between cryptocurrencies. The competition could end up looking quite different from the competition between other types of peer-to-peer networks (such as online auctions), in part because of potential benefits of transacting in multiple cryptocurrencies simultaneously. If any particular cryptocurrency is vulnerable**
- 5 to attack, one might want a diversified portfolio of them.**
- 6. Finally, people trade cryptocurrencies just like one might trade currencies or equities (hence the success of exchanges). The arbitrage opportunities are vast, but the regulatory framework protecting investors has not caught up.**