(More than just)

Cryptocurrency

Admin Stuff

- I have written and passed the Series 65 Investment Advisor exam and both levels of Insurance Representative exams. However I have let these lapse so I am currently just a basic schmoe.
- I'm not selling or promoting *anything* except common sense.
- This supposed to be fun.

Legal Stuff Too

- All the images used in this presentation are obtained from three sources:
  - Images photographed or illustrations created by me, the author.
  - Image files downloaded from Wikipedia and covered under a creative commons license
  - Publicly available financial data graphs

Context

- Cryptocurrencies do not exist in a vacuum. Rather they are simply another step in the long evolution of money and how it is used to power the world economy.
- This presentation will attempt to show how cryptocurrency fits into that complex jig-saw puzzle and try to see how it adds value.

Wealth (Briefly)

- In general wealth can take two basic forms:
  - Assets – things that are inherently valuable.
    - Land, Food, Clothing, Cars, Jewellery, Gold Coins
    - Labour, A job, A pension, A generous uncle
    - Stocks, Bonds, RRSP, TFSA, Art, Collectibles
    - Magic the Gathering Trading Cards, Penguins
  - Currency – things that are valuable because they can be used to carry out transactions.
    - Cash, Bank Account Balance, Line of Credit
    - Money Market funds, Certificates of Deposit
    - Cryptocurrency

Transactions: Barter

- For all of human history, people have needed to exchange assets to provide for their needs.
- The most direct way to do this is to exchange assets directly. This is called barter.
  - This approach is inefficient for many reasons.
- Barter still exists today, but only in an informal context or in economies operating at a very primitive level.

Money

- If you can swap something easily and predictably for goods and services, it's money.
- If you can't, it's not.
- So, what is cryptocurrency then? Is it money?
- If so, how is it different from "regular" money?
- To answer this, let's take a closer look at the money we rely on all the time.

Commodities

- One solution to the problems of barter are to choose a suitable commodity and trade that as a proxy for the exchanged asset.
  - The commodity is still valuable in itself so there is confidence in the transaction.

Commodity Backed Currency

- Carrying around sacks of rice to pay for stuff is cumbersome. So instead, people started carrying vouchers for that rice. The bearer of the voucher could exchange it for their rice.

Problems with using Commodities or Commodity Based Currencies

- The supply of the underlying commodity may not match the overall growth in the economy.
  - A shortage of commodity can make money scarce and transactions difficult to carry out.
  - A surplus of commodity can cause prices to rise as excess money "chases" the same assets.
  - Instability in commodity supplies causes instability in the entire economy.

Fiat Currency

- All modern cash falls under the umbrella designation of "fiat" currency.
- Money has value because the government says, by decree (or fiat), that it does and we agree.
- Bits of plastic have no intrinsic value.

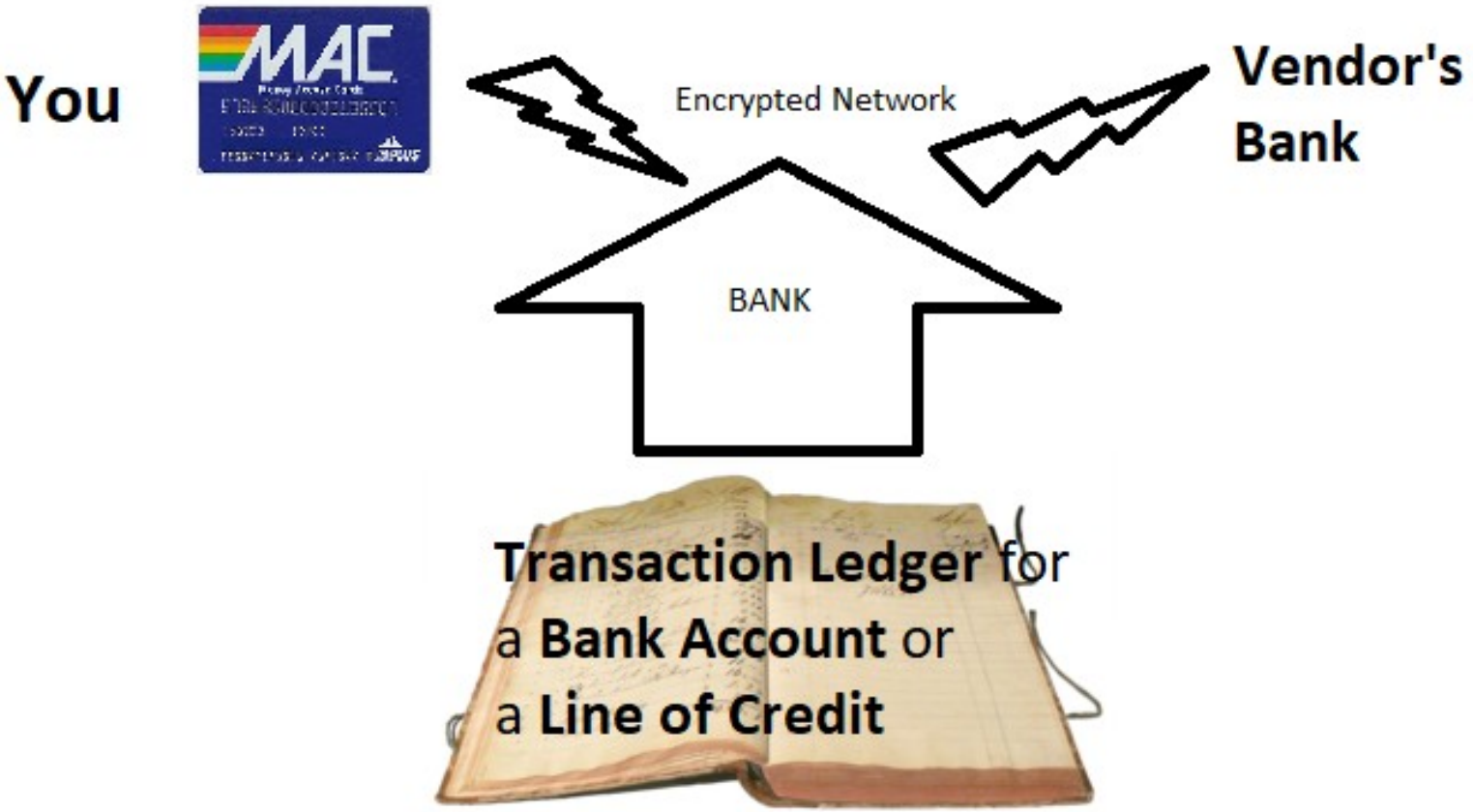
The Money Supply

- To regulate the supply of money, modern economies all have central banks with the authority to print bank notes, mint coins, and electronic transfer vast sums of money.
- In school we were all taught that the value of the dollar reflects the value of the entire Canadian economy. This is not strictly true. Instead, it is more an “aspirational” goal.
- The power wielded by central banks is enormous.

"Modern" Money

- Today, most transactions are not conducted with cash anymore. Rather we all whip out the "plastic" and shop away.
- Our next stepping-stone to cryptocurrency are the debit and credit cards we've all used countless times in our lives.
- Believe or not, this commonplace thing is the progenitor of cryptocurrency.

How does it work?



Key Points

- The bank maintains a database linking the card account number to the person holding the card.
- The bank maintains a record of all transactions of "money" into and out of the account.
- The bank owns (or leases) a secure network to transmit all of these transactions.
- The bank takes a "cut" of each transaction.
- The bank charges interest on the lines of credit or pays (less) interest on the bank account balances.

Cryptocurrency (*Finally!*)

- The creators of cryptocurrency wanted to address several points about modern currency that they did not like:
  - Government control of the money supply meant that individuals were at the mercy of those governments. History is littered with examples of people having their savings wiped out by hyperinflation or by the decree of the “Great Leader”.

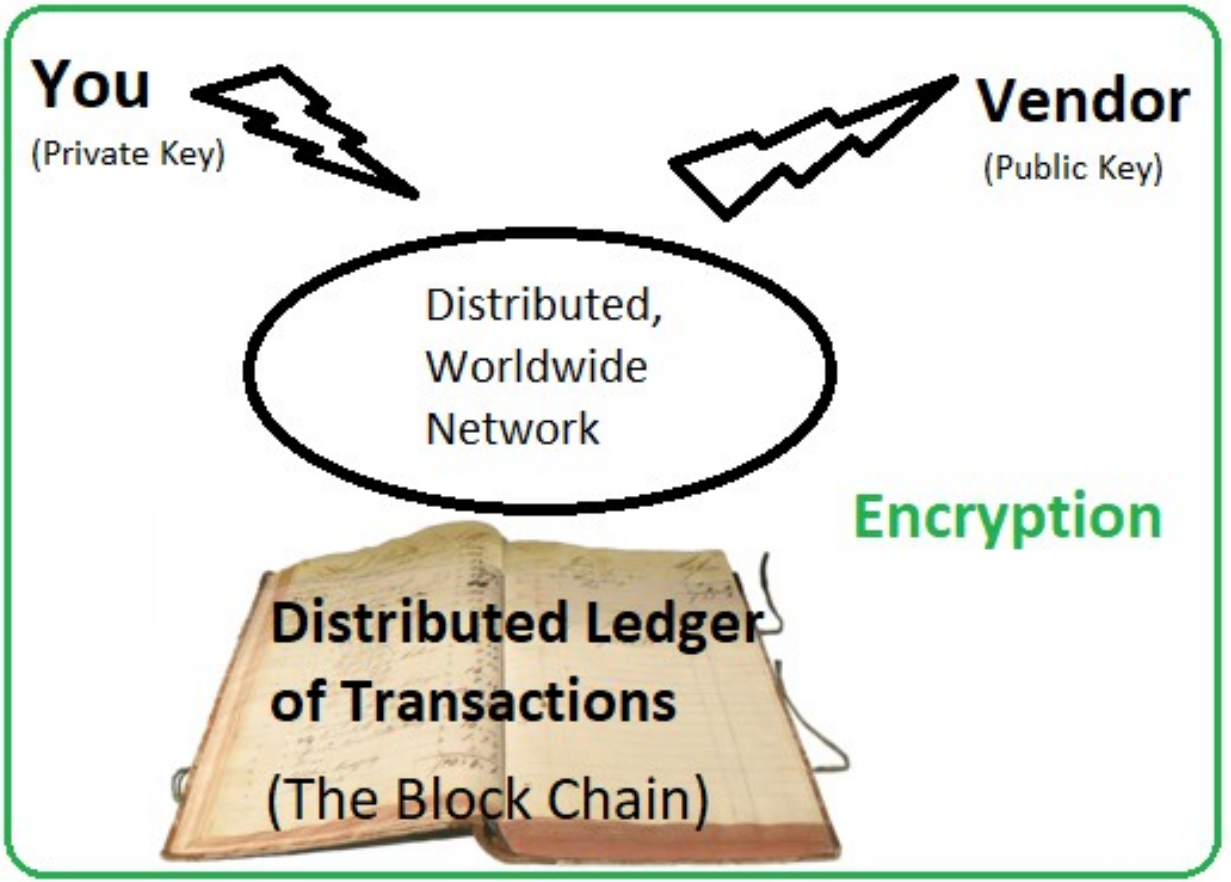
Banks

ii From the previous, the banks hold all the power in terms of record keeping. From an engineering point of view, bank records are a "single point of failure". The designers of cryptocurrency want a more robust system that shared record keeping responsibilities over a large, world-wide network.

The Six (Technical) Features of a Cryptocurrency

- The system does not require a central authority; its state is maintained through distributed consensus.
- The system keeps an overview of cryptocurrency units and their ownership.
- The system defines whether new cryptocurrency units can be created.
- Ownership of cryptocurrency units can be proved exclusively cryptographically.
- The system allows transactions to be performed in which ownership of the cryptographic units is changed.
- If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

How does it work?



The Keys

- In the diagram, accounts are identified by their RSA (elliptic curve encryption) keys.
  - The source key is the sender's (in this case your) private key.
  - The destination key is the receiver's (in this case the vendor) public key.
- Private keys need to be kept secure.
- Public keys can/should be published in order to receive funds.

The Blockchain

- The blockchain is a ledger of transactions (and other data) maintained across all the servers in the currency network.
- This ledger is open for anybody to read.
- Additions to the ledger are done by the authority of the computing power of the entire currency network.
- Forging fake currency is all but mathematically impossible.

Mining

- As a reward for processing the transactions of the currency system, the participants can receive cryptocurrency
- The computers used in the Bitcoin system represent a vast amount of computing power.
- Processors of transactions can also receive modest fees (also in cryptocurrency) for their work.
- Mining is so lucrative that Intel has just announced the release of new chips that offer double processing power over existing chips.

Some Cryptocurrencies

- There are literally thousands of cryptocurrencies in existence. Most are very small and of limited usefulness.
- Today we look at these:
  - Bitcoin (BTC)
  - Ethereum (ETH)
  - Stablecoins. A sub-group of cryptocurrencies.
- To see more, head over to coinmarketcap.com

Bitcoin (BTC)

- The first, most widely used cryptocurrency
- It laid the foundation of the technology. A system for moving numbers from one encrypted account to another. At first these numbers were just numbers; worthless things called Bitcoins
- The initial network was so small that you could mine a decent number of these worthless coins on any modest personal computer.
- One day that all started to change.

• Bitcoin Pizza Day

- On May 22, 2010, Lazlo Hanyezc exchanged 10,000 bitcoins with a theoretical value of $41 for 2 large pizzas worth $25.
  - For the first time, an equivalence between Bitcoin (BTC) and US Dollars existed.
  - This amount of BTC is worth $418,000,000 USD at today's exchange rate. Still Lazlo has no regrets saying: "It wasn't like Bitcoins had any value back then, so the idea of trading them for a pizza was incredibly cool."
- NYC Mayor Eric Adams to be paid in Bitcoin.

Key Stats

- The value of BTC is about $744 billion.
- The number of BTC is capped at 21 million. To date about 90% have already been mined.
- The cycle time of BTC is 10 minutes. Transactions can take up to an hour to complete making this one of the slowest cryptocurrencies.

Volatility


Bitcoin to USD Chart
Price
Market Cap
TradingView
History
1D
7D
1M
3M
1Y
YTD
ALL
LOG
68.0K
64.0K
60.0K
57.8K
56.0K
52.0K
48.0K
44.0K
40.0K
36.0K
24.0K
USD
Mar
May
Jul
Sep
2
2021
Feb
CoinMarketCap
Daily News Recap

Ethereum (ETH)

- Ethereum is a decentralized, open-source blockchain with “smart” contract functionality
- Ether (ETH) is the native cryptocurrency of the platform.
- Among cryptocurrencies, Ether is second only to Bitcoin in market capitalization

Ethereum Applications

- The addition of “smart” code means that Ethereum can be used to implement financial applications. Some include:
  - Decentralized finance (DeFi)
  - Enterprise software
  - Non-fungible tokens (NFT)
- Visa has also signalled interest in processing NFT and Ethereum transactions.

DeFi

- Decentralized finance (DeFi) applications provide a broad array of financial services without the need for typical financial intermediaries like brokerages, exchanges, or banks, such as allowing cryptocurrency users to borrow against their holdings or lend them out for interest.

NFT

- Ethereum also allows for the creation of unique and indivisible tokens, called non-fungible tokens (NFTs).
- Since tokens of this type are unique, they have been used to represent such things as collectibles, digital art, sports memorabilia, virtual real estate, and items within games.
- Think of these as digital certificates of authenticity.

Key Stats

- The value of ETH is about $311 billion.
- The number of ETH is not capped but continues to grow as transactions are processed.
- The cycle time of ETH is 12 seconds. Ethereum programs can only be created by users with a stake in ETH.

Stablecoins

- Stablecoins are a category of cryptocurrencies that are tied to a fiat currency, a commodity, or another cryptocurrency.
- They eliminate the wild fluctuations in the value, often seen as a risk.
- For example the USD Coin cryptocurrency tracks the US dollar with one USDC valued at $0.9995 USD.

Cryptocurrency Uses

- At some point, all of this technology needs to have a use. Let us examine some of the most popular applications:
  - Transferring funds
  - Buying things
  - Investment (Currency Speculation)
  - Curiosity
  - Mining

• Transferring funds

- One of the best uses of cryptocurrency is transferring funds.
  - Sending money to your grandmum in Mexico
- Cryptocurrency fees are much lower than wire transfers
- Fees for currency exchange are avoided

Buying things

- Like other currencies, cryptocurrencies can be used to buy stuff. Stuff like:
  - Gift Cards
  - Cars, most famously Tesla
  - Travel tickets and accommodations
- https://coindoo.com/things-you-can-buy-with-cryptocurrency

Investing

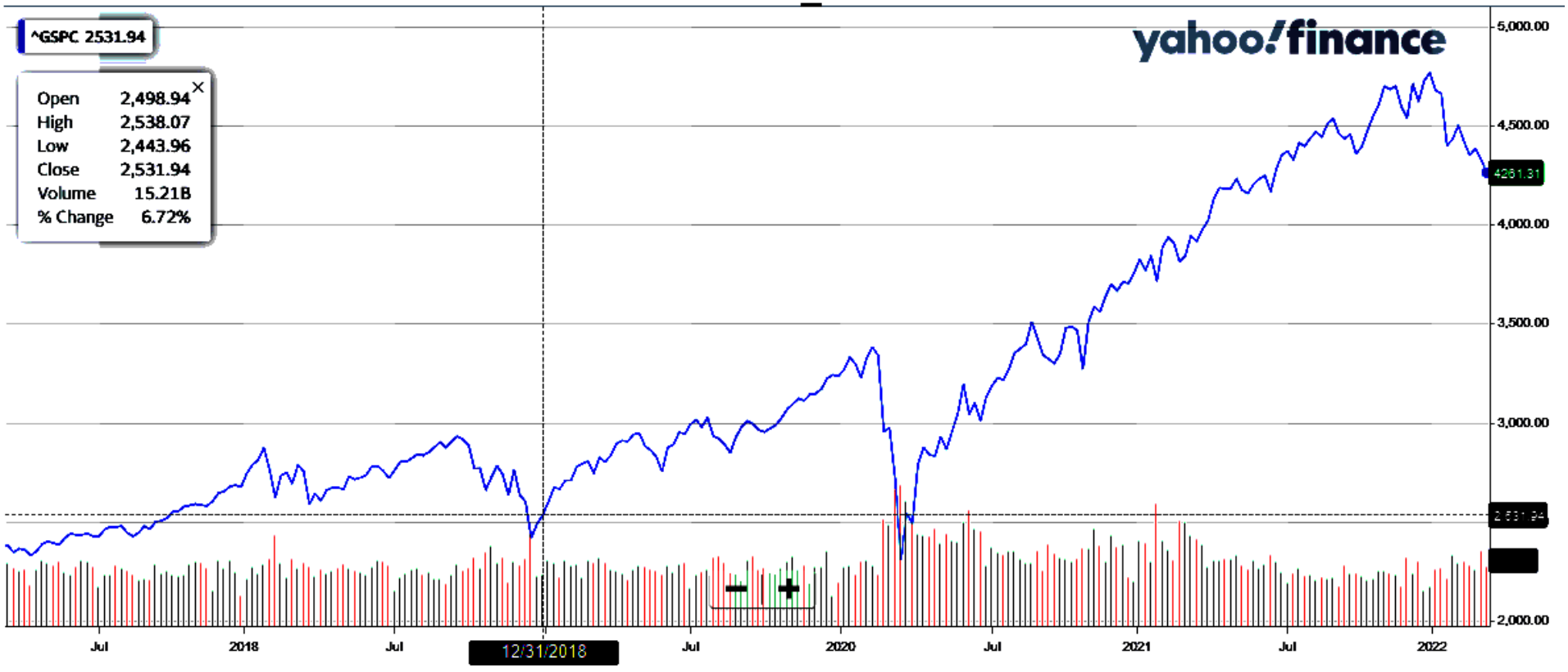
- Currency speculation is making bets on the future relative strengths of various currencies.
- When people say they “invested” in Bitcoin, this is what they are doing.
- Now just as national economies can make their cash risky, market forces come into play here too. We see how volatile the price of Bitcoin is.
- Note though that because the coin supply is not left to political whim, in the long run cryptocurrencies *may* end up being more stable than fiat currencies.

The Projects

- An investment in cryptocurrency is also an investment in the team behind the software.
- A good team will provide a stable environment and timely, well tested software updates.
- The community has an acronym: D.Y.O.R. for Do Your Own Research!
- Sorry but “The line goes up!” is *not* research!

The Long View

S&P 500


^GSPC 2531.94
Open 2,498.94
High 2,538.07
Low 2,443.96
Close 2,531.94
Volume 15.21B
% Change 6.72%
yahoo!finance
5,000.00
4,500.00
4,261.31
4,000.00
3,500.00
3,000.00
2,531.94
2,000.00
Jul
2018
Jul
12/31/2018
Jul
2020
Jul
2021
Jul
2022

Curiosity & Mining

- Setting up an account and putting a little money in it is a mostly harmless way of experimenting with cryptocurrency
- Mortgaging the farm and betting it all; Not so much.
- The mining of major cryptocurrencies is now way beyond the means of most
- Some lesser currencies can still be mined on a hobbyist level.

Anonymous?

- A common myth is that cryptocurrency is anonymous and untraceable

  New York (CNN Business)

  A New York couple has been arrested and charged with conspiring to launder $4.5 billion in stolen cryptocurrency funds. Law enforcement officials have seized $3.6 billion of those funds in what US Deputy Attorney General Lisa Monaco called "the department's largest financial seizure ever."

- If you steal enough, the police will eventually get around to finding you
- The only really anonymous currency is cash. Unless your fingerprints are on it.

Scams

- Cryptocurrencies are often seen as scam bait
  - For example, the Squid Game scam misled people into thinking they were investing in a coin linked to a popular show.
  - By configuring the software to not allow sales of coins, the price seemed to always go up.
  - Then the criminals just took the money and ran.

What to do?

- The truth is, scams are *everywhere* with every type of asset and currency ever invented.
- Only deal with reputable, well know dealers and companies.
- Avoid fads and gimmicks
- D.Y.O.R.
- If it seems to good to be true, it probably is

Further Info

- A live view of BTC activity:
  - https://www.bitcoinmonitor.com/
- Bitcoin (BTC) - statistics & facts:
  - https://www.statista.com/topics/2308/bitcoin/#topicHeader__wrapper
- Things You Can Buy With Cryptocurrency:
  - https://coindoo.com/things-you-can-buy-with-cryptocurrency/
- 5 Things You Can Buy Using Cryptocurrency
  - https://www.techdee.com/buy-things-using-crypto/

Wikipedia

- Cryptocurrency
  - https://en.wikipedia.org/wiki/Cryptocurrency
- Bitcoin
  - https://en.wikipedia.org/wiki/Bitcoin
- Ethereum:
  - https://en.wikipedia.org/wiki/Ethereum
- Stablecoins:
  - https://en.wikipedia.org/wiki/Stablecoin

The End

- Any further questions?