1. What is Cryptocurrency?

Let's Get Started With Crypto!

- **Step #1** -- Claim your FREE Bitcoin: https://www.coursenvy.com/free-bitcoin
- **Step #2** -- Get a wallet to store your cryptocurrency safely offline: https://www.coursenvy.com/ledger
- **Step #3** -- Make passive income from your crypto in an interest-earning account (you can earn up to 8.6%) + get up to $250 in Bitcoin: https://www.coursenvy.com/blockfi
- **Step #4** -- Create a Bitcoin Roth IRA account (get a FREE $100 with our link https://www.coursenvy.com/bitcoin-roth-ira) and learn how to retire early: https://www.coursenvy.com/post/how-to-retire-early
- **Step #5** -- Learn more about making passive income mining Bitcoin: https://www.coursenvy.com/bitcoin-mining

What is Cryptocurrency & Blockchain

Topics Covered:

- What is Bitcoin
- What is blockchain technology
- What are altcoins
- What are tokens
- Tokens versus cryptocurrencies
- Initial Coin Offerings (ICOs)
- Security Token Offerings (STOs)
- State of the cryptocurrencies market cap

The Background of Bitcoin

It all started with **Bitcoin**! Bitcoin was the predecessor to all other cryptocurrencies and its underlying technology has been the foundation for the crypto industry.

The initial bitcoin idea proposed a digital cash. All attempts at digital cash prior to bitcoin had failed and all had one theme in common – they were **centralized**.

Digital cash projects such as ecash, hashcash, and B-Money were all predecessors which failed but Bitcoin incorporated some key elements from each.

Bitcoin's Original Whitepaper: https://bitcoin.org/bitcoin.pdf

How Bitcoin Started

➢The Bitcoin project was born around the time the investment bank Lehman Brothers went bankrupt

➢Project was started by an unknown pseudonymous programmer Satoshi Nakamoto

➢Project proposed a form of digital cash which incorporated elements of previous failed attempts

➢Key difference between bitcoin and previous attempts at digital cash was that bitcoin was decentralized

➢Bitcoin achieved decentralization through blockchain technology

What is a Blockchain?

- Similar to a database but with certain rules attached.
- The database is maintained by a distributed set of computers.
- Transactions are grouped together into blocks (and blocks can only be added).
- Blocks are linked through cryptography. If one of the blocks is changed, all the others after it will be changed. Each block added is linked to the previous one through what is known as a **cryptographic hash function**. If one of the blocks is manipulated, it will change all the others after this.

What is a Blockchain?

- Blocks are added by miners… which are computers that solve mathematical problems to only add valid transactions to the block. Miners are incentivized to add blocks to the Bitcoin blockchain with newly minted Bitcoin.
- Blocks are added approximately every ten minutes to the Bitcoin blockchain. If the blocks are being added faster than ten minutes, the difficulty of mining will increase.
- The network is censorship resistance meaning transactions will not be censored as long as they are valid. As long as a transaction has the funds and the correct digital signature, it will be added.

Blockchain Key Properties

- **Distributed database** – Peer to peer network run by a distributed set of computers as opposed to a centralized network run by Amazon Web Servers or another single server.
- **Append-only** – Data is grouped together into blocks and these blocks can only be added.
- **Immutable** – Once data is added, it cannot be changed. Each block is linked through cryptography. Changing one will change all the others after this.
- **Proof-of-Work** – Computers running the network expend energy to validate transactions. They are incentivized to do this with newly minted bitcoin.
- **Censorship Resistant** – Transactions cannot be censored.

What are the Benefits of Blockchain?

- **No single point of failure –** In a centralized system, there is a single point of failure. In a decentralized system such as Bitcoin, it doesn't matter if one of the computers in the network goes down, as the network is run by a distributed set of computers.
- **Peer-to-peer transactions –** Transactions are processed by the procurers of the network (i.e. the miners). This removes the need for middlemen and intermediaries to process transactions.
- **Censorship resistance –** Transactions will not be censored. A centralized entity such as a bank can easily censor your transactions. While Bitcoins cost to censor or steal is so high, censorship is impossible.
- **Immutable –** Immutability of transactions is one of the key benefits and is achieved through the cryptographic linking of blocks. The further back in the blockchain the transaction is, the more secure it is as there is a greater number of blocks which would be altered if the block the transaction is included in were changed.
- **Security –** There is a large amount of computing power behind the ledger of transactions.

What are the Drawbacks?

- **Scalability –** The Bitcoin network can process around six to seven transactions per second. This is low compared to around 46,000 transactions per second on the Visa network.
- **Energy Consumption –** Because the network is maintained by a distributed computer network, this consumes a vastly greater amount of energy than if it were maintained by a single powerful computer.
- **Potential Attacks –** While there is security benefits to having the ledger backed by a huge amount of computing power, the scope for other potential attacks arises. If one entity were to gain 51% of the computing power mining transactions, this would allow them to conduct double-spend transactions whereby they spend the same cryptocurrency twice. This would be extremely unlikely to take place on the Bitcoin network due to the cost of purchasing the hardware to produce the computing power necessary. However, this type of attack has taken place in smaller cryptocurrency networks.

Key Properties Coded into the Bitcoin Blockchain

Each blockchain and cryptocurrency has its own properties coded into it. Some of the key bitcoin properties are:

-Supply

-Issuance

-Block size

-Block time

-Network difficulty

Key Properties Coded into the Bitcoin Blockchain

Supply – The maximum supply there can ever be is 21 million Bitcoin.

Issuance – The amount of newly minted Bitcoin rewarded to miners halves approximately every four years.

Block size – The block size limit is currently 1mb meaning that 1mb worth of transactions can be included in each block.

Block time – It takes approximately 10 minutes for each block to be added.

Network difficulty – If blocks are being added faster than 10 minutes, the difficulty to mine increases bringing the block time closer to ten minutes. If it is taking longer than 10 minutes, the network difficulty will decrease. The network difficulty adjusts approximately every 2 weeks.

Can a Blockchain be Changed or Upgraded?

Short Answer...

Yes!

Can a Blockchain be Changed or Upgraded?

Long Answer…

The code for a blockchain can be changed but those who are running the network need to be convinced to upgrade their software.

This can be a long process that results in a lot of debate and discussion among community members. If there is a disagreement, some may upgrade while others don't, resulting in the network forking into two separate blockchains. This can be disastrous for projects as its splits the resources supporting a network.

For example, changing something important as the supply model of Bitcoin would be almost impossible as it would nearly be almost impossible to convince everybody to change this aspect of the code.

The Arrival of Altcoins

Altcoins adopted blockchain technology for different use cases

- Some seeking to improve on the Bitcoin network
- Some seeking to decentralize different business areas
- Some applying a completely different approach
- Each have their own properties coded into the network – e.g. supply and issuance model, mining algorithm, etc.

The Arrival of Altcoins

How are altcoins created?

- Some have forked the code from the Bitcoin blockchain and launched their own blockchain. This is essentially adapting the code and launching a new network.
- Forked the code of an altcoin.
- Others have built their blockchain from scratch.

Top Altcoins

Ethereum – One of the most popular altcoins. Uses a *Turing-complete* programming language which makes it easier for developers to build decentralized applications with.

Litecoin – Forked from Bitcoin with some factors such as supply changed.

Monero – Cryptocurrency focused on privacy.

Bitcoin Cash – Fork of Bitcoin that increased the block size limit.

Dogecoin – Initially started as a joke but found a strong use case as a tipping coin.

https://coinmarketcap.com

Top 100 Cryptocurrencies

Cryptocurrencies ▾ Exchanges ▾ Watchlist

#	Name	Market Cap	Price	Volume (2
1	Bitcoin	$60,110,986,112	$3,433.18	$5,796,511
2	XRP	$11,903,987,655	$0.289188	$448,402
3	Ethereum	$10,982,537,457	$104.97	$2,814,296
4	EOS	$2,054,045,960	$2.27	$803,413
5	Tether	$2,036,880,549	$1.01	$4,148,828
6	Bitcoin Cash	$1,944,083,622	$110.50	$256,443
7	Litecoin	$1,863,251,436	$30.93	$699,454
8	TRON	$1,805,610,641	$0.027086	$265,895
9	Stellar	$1,586,515,825	$0.082771	$154,265
10	Bitcoin SV	$1,117,773,198	$63.54	$85,016
11	Cardano	$985,042,079	$0.037993	$19,712
12	Binance Coin	$782,500,607	$6.06	$48,794

Tokens

- Tokens are another form of digital assets. While cryptocurrencies deal with the functions of a currency on the blockchain, tokens can perform a wide variety of functions and act as a digital good or service.
- Tokens do not necessarily require their own blockchain. They can be issued on another blockchain. Ethereum has over 150,000 tokens issued on its blockchain.
- Tokens often represent a good or service. This good or service can exist in the physical world such as a token representing a barrel of oil. It can also exist in the digital world such as a token representing a unique digital kitten, as in the case of the decentralized application built on the Ethereum blockchain, Cryptokitties.
- Tokens are also used to tether assets which is a token which represents an underlying asset. One of the largest market caps tethered asset tokens is USD tether which is a token that aims to remain pegged in value to the USD by backing the tokens with USD.

Cryptocurrencies vs. Tokens

Cryptocurrencies

- Currency native to a blockchain.
- Can be used as medium of exchange, store of value, unit of account, etc.
- Boils down to being the currency that operates on a blockchain.
- Properties of the cryptocurrency depend on the blockchain it operates on.

Tokens

- Can represent a digital good or service and be much than just a currency.
- Does not require its own blockchain.
- Two broad categories of tokens are utility tokens and security tokens.
- Utility tokens derive their value from their function in a system such as an application built on the blockchain.
- Security tokens derive their value from their representation of ownership in something. For example, a token could represent ownership in a fraction of some real estate.

ICO = Initial Coin Offering

Initial Coin Offering (ICO's) are a process by where tokens are issued in exchange for funds. The funds are typically contributed towards the development of a project which the token in most cases plays a role. The underlying idea is that investors will want to purchase the token because of the future value it will have in the developed project.

In 2017 alone, over $5 billion was raised for ICOs and over $6 billion raised in 2018. This has resulted in a huge expansion of the cryptocurrency market but many of these projects are unlikely to survive. We look later into the key factors to take into consideration when analyzing a cryptocurrency project or token to decide what chance it has of surviving.

- ICO Token Sales History: **https://elementus.io/token-sales-history**

Key ICO Components

A project that wishes to raise funds through an ICO will typically have the following:

- **Whitepaper –** This is a document that explains all of the ins and outs of a project. Any ICO worth its weight will have one of these.
- **Website –** This will contain the key parts of the project.
- **Team –** Successful ICO's generally have a team that have the professional experience in the area which is being addressed.
- **Partners & Advisors –** Partners and advisors are also added to the team to add expertise in the areas that the team may be lacking.
- **Roadmap –** This is the plan and dates for how the project will be rolled out.
- **Social Media –** ICO's will typically have a number of social media channels. Some of the main ones include having a Twitter and Telegram channel.

Security Token Offerings (STO's)

Security token offerings (STOs) have begun increasing in popularity over the past year, especially with a large number of investors who lost their money by investing in ICOs which turned out to be scams or poor projects. 86% of tokens issued are now priced lower than their issuing price. STOs offer increased protection to investors as they register the token as a security.

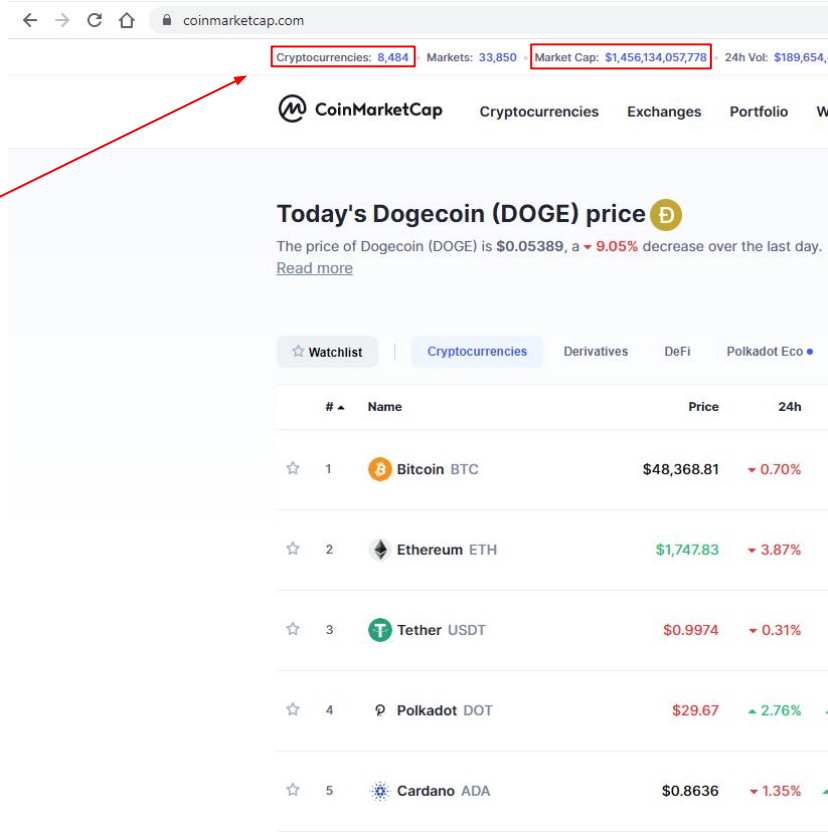
By registering the token as a security, this means that the token complies with security regulations which provide protection to investors.

Registering as a security token will be more costly to the team running the project as they have to cover the costs of registering as a security and hiring legal expertise prior to raising funds. However, this type of offering is becoming more popular.

State of the Cryptocurrency Market

- CoinMarketCap.com is one of the most popular price checkers and data providers. There are currently over 8,000 cryptocurrencies and tokens listed and the market cap is around $1.5 trillion.

- In comparison, the gold market is around $7.7 trillion and the global stock market is around $73 trillion



Section 1 Recap

- Bitcoin was the first technology to use blockchain technology.
- Blockchain technology is a distributed database with certain rules on how data can be added.
- Blockchain technology has a number of benefits and a number of drawbacks.
- Cryptocurrencies have their own blockchain network. Bitcoin was the first but altcoins have been created by either forking an existing blockchain or building the code from scratch.
- Tokens are another form of digital asset. They don't necessarily need to have their own blockchain although some do have their own blockchain.
- Tokens can be used for a wide variety of functions. They can be a digital good or service tied to the real world or even tied to a digital ecosystem.
- ICO's gained popularity as projects issued tokens to raise funds to build a project.
- STO's have been gaining more popularity recently after a lot of ICO's turned out to be poor investments. STO's register their tokens as securities and comply with securities regulation.