CMSC 398F
Week #7
Altcoins, ETH, and Politics/Regulation

...

Announcements

- Project 1 due date extended to Sunday
  - Questions regarding project?
- Join the class Piazza!
  - piazza.com/umd/fall2022/cmsc398f

From Last Week

- Wallets help manage their keys
    - They can send and receive to anyone else on the same network.
- There are different types of wallets
    - Hot wallets
    - Cold wallets
- Recovery Phrases

Altcoins

- “Altcoin” refers to any type of cryptocurrency other than Bitcoin
    - Ethereum is the most popular altcoin
    - People use the full name (Ethereum) when talking about the broader blockchain network but Ether (ETH) to discuss the currency itself.
    - Some other altcoins are Solana, Dogecoin, Uniswap, XRP, Polkadot.
- All altcoins have a different blockchain network than of Bitcoin with varying benefits.
- Altcoins come in various flavors and categories:
    - Payment Token
    - Security Token
    - Meme coins
    - Utility Tokens

Types of Altcoins

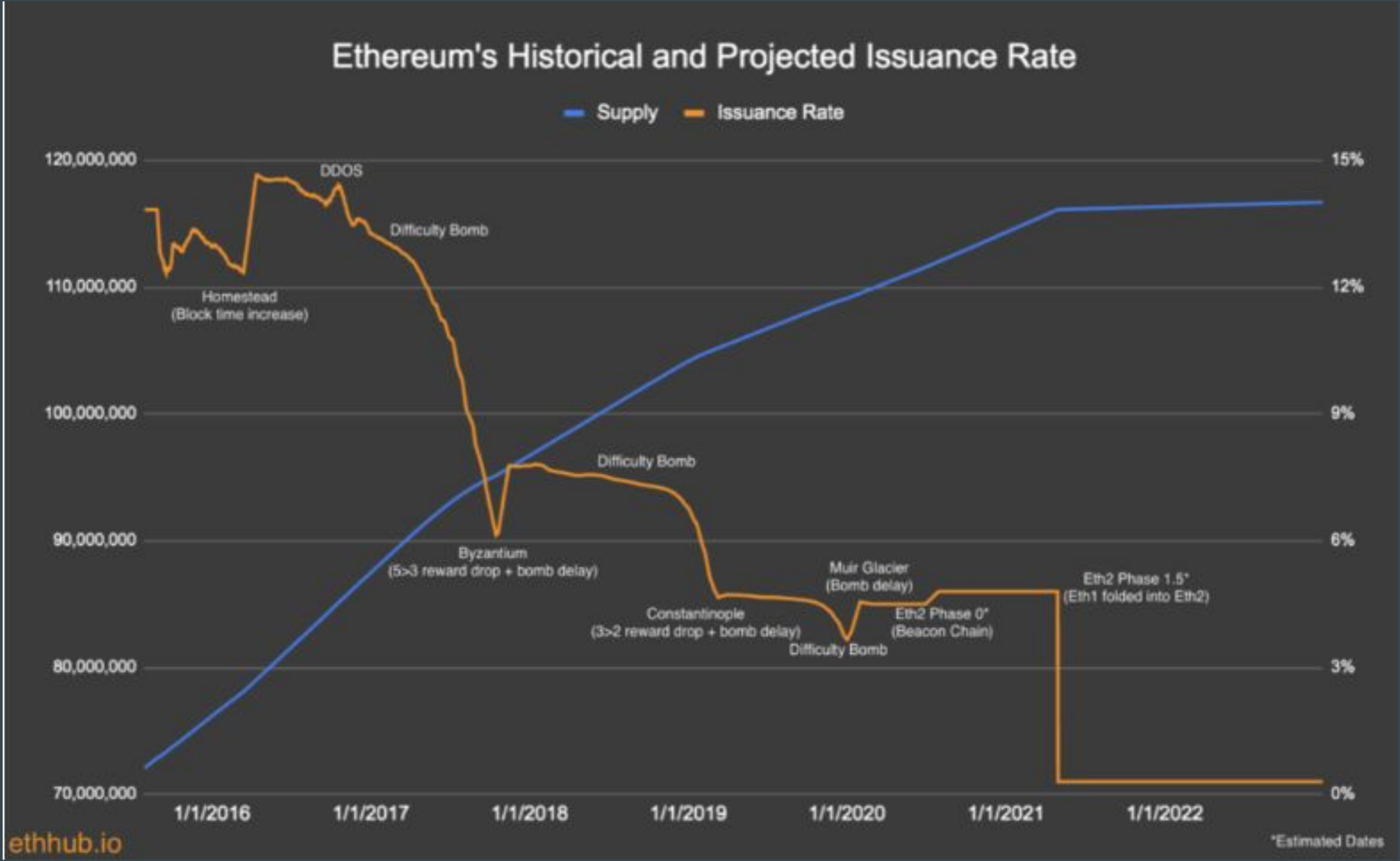
- Payment Token
    - Basically what a cryptocurrency
    - Usually have their own Blockchains
- Security Tokens
    - similar to the traditional securities or stocks sold by publicly traded companies
    - Overseen by a country’s financial regulator
    - Limits them to the same strict regulations has ETF’s, bonds, stocks, etc.
- Meme Coins
    - Type of cryptocurrency
    - Used to make a quick buck but are risky
- Utility Token
    - Provide access to a specific service or product
    - Can be for transactions but are usually used for other things

ETH

- Ethereum is a blockchain with a computer embedded in it (Ethereum Virtual Machine)
  - Some state that everyone on the Ethereum network agrees on
  - Everyone who participates in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer.
- Ethereum was created in an attempt to fix the problems with Bitcoin, mainly that Bitcoin’s scripting language is not Turing complete, and so it severely limits the types of applications that can be run on Bitcoin’s network.
- It is the foundation for building apps and organizations in a decentralized, permissionless, censorship-resistant way.

ETH

- Utilizes a blockchain to keep track of its transactions, just like Bitcoin
- Ether (ETH) is a utility token while Ethereum is the network
    - This means that ETH can be used to buy and sell just like Bitcoin
    - It can also be used to build applications that “run” on the Ethereum blockchain
    - It can also be used to make smart contracts
    - More on this next week!
- Ethereum vs. Bitcoin?
    - Ethereum’s network allows for some functionality that Bitcoin does not
        - dApps, smart contracts, etc.
    - processes transactions more quickly
    - No limit to the number of potential ETH tokens in circulation
        - Bitcoin currently has 19.1 million



Ethereum's Historical and Projected Issuance Rate

Proof-Of-Stake

- Proof-of-stake underlies certain consensus mechanisms used by blockchains to achieve distributed consensus. In proof-of-work, miners prove they have capital at risk by expending energy.
- Ethereum uses proof-of-stake, where validators explicitly stake capital in the form of ETH into a smart contract on Ethereum.
- This staked ETH then acts as collateral that can be destroyed if the validator behaves dishonestly or lazily.
- The validator is then responsible for checking that new blocks propagated over the network are valid and occasionally creating and propagating new blocks themselves.

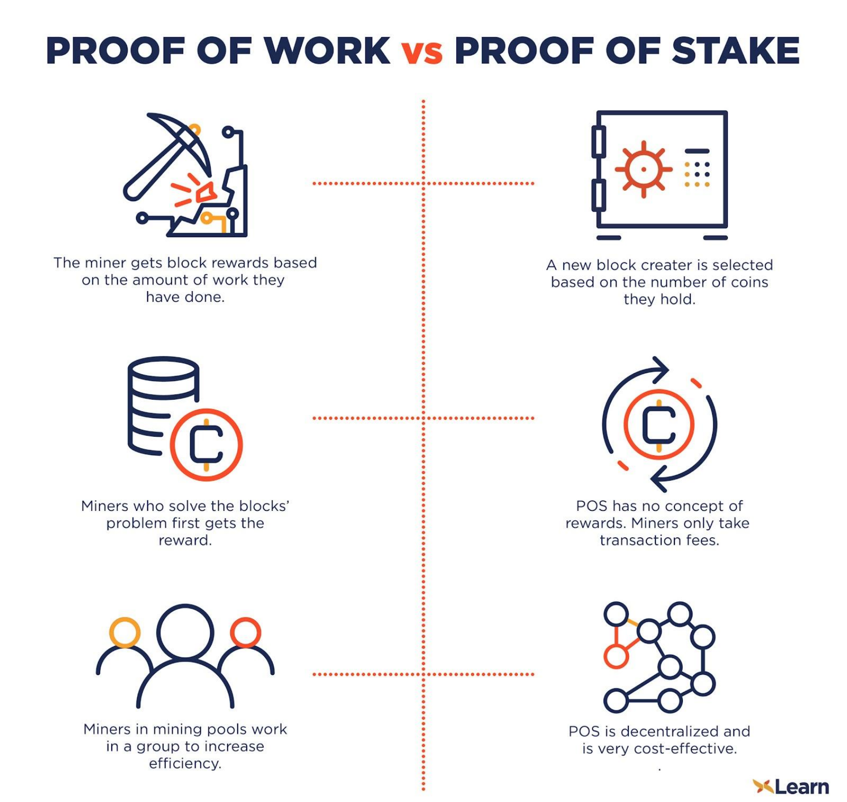
Why POS?

- Ethereum switched on its proof-of-stake mechanism in 2022 because it is more secure, less energy-intensive, and better for implementing new scaling solutions
- Staking makes it easier for individuals to participate in securing the network, promoting decentralization. validator node can be run on a normal laptop.
- Staking pools allow users to stake without having 32 ETH.
- The threat of a 51% attack still exists on proof-of-stake as it does on proof-of-work, but it's even riskier for the attackers. An attacker would need 51% of the staked ETH.

Other POS networks

- Solana: Solana runs on an innovative hybrid consensus model comprising proof-of-stake (PoS) and proof-of-history (PoH), a proof for verifying order and passage of time between events. Due to this unique protocol design, Solana can handle up to 3,000 transactions per second.
- Cardano:
- Avalanche:Avalanche can handle a whopping 4,500 transactions per second, thereby positioning itself as a serious rival to Ethereum.Avalanche is built around a system of three interoperable blockchains: Exchange Chain (X-Chain), Platform Chain (P-Chain) and Contract Chain (C-Chain).

PoS vs PoW



PROOF OF WORK vs PROOF OF STAKE

The miner gets block rewards based on the amount of work they have done.

A new block creater is selected based on the number of coins they hold.

Miners who solve the blocks' problem first gets the reward.

POS has no concept of rewards. Miners only take transaction fees.

Miners in mining pools work in a group to increase efficiency.

POS is decentralized and is very cost-effective.

Cryptocurrency and Governments

- Anyone can own cryptocurrency
- Some governments, like El Salvador, have already adopted cryptocurrency.
  - Bitcoin is legal tender in El Salvador
- Other governments, such as the United States, refuse to recognize it as legal tender.
  - Cannot be regulated
  - It is used by criminals (money laundering, black market, etc.)
  - Can help people circumvent capital controls
  - Billions of dollars are locked up in Crypto, can effect the economy

Why are governments wary of Cryptocurrency?

- Fiat currencies play an important role in a country's economy. It is backed the full faith and credit of a government.
  - The cycle of transactions in the economy - borrowers, lenders, consumers - relies on a chain of trust between transacting parties. The Federal Reserve is the final leg of that chain.
  - For example, if your house burns down and it has $10,000 in it, the U.S Mint will give you back that $10,000. Or if you are scammed when making a purchase, your bank will refund your money. FDIC even insures up to $250,000 in your bank account.
  - If you lose your crypto wallet, no one can help you recover that money.
  - Many crypto supporters say that by manipulating the money supply, the US government also manufactures asset bubbles and crises.
  - If the citizens use cryptocurrency, the government no longer has control over the money supply, and money policy

Ties to Illegal Activity

- The ability for crypto to bypass existing financial infrastructure for a country is a blessing in disguise for criminals because it enables them to camouflage their involvement in such activities
  - Users on a network are identified by their addresses, which cannot be traced back to their original identities
- The most famous example of a crime involving Bitcoin was the Silk Road case.
  - Silk Road was an online marketplace (Tor hidden service) for guns and illegal drugs, among other things
  - It was very hard to crack by the FBI at first, but eventually they took it down at seized about 174,000 BTC.

Cryptocurrency and Businesses

- In the United States, cryptocurrency is considered property.
    - Cryptocurrency trades you make via exchanges such as Coinbase are taxable. You can use these exchanges to convert between USD and Crypto.
- Since it is taxes differently than income, businesses can leverage this to avoid certain taxes
    - Can also get around reporting rules when it comes to transactions.
    - Normally transactions between a business and its customers need to be recorded.
- Accessibility
    - Allows them to easily accept payment from international customers (no fiat conversions)
    - Wider range of payments
- Speed: cryptocurrency is faster than many standard banks

Regulation in US

- The IRS classifies crypto as a type of property, rather than a currency.
- If you receive Bitcoin as payment, you have to pay income taxes on its current value. If you sell a cryptocurrency for a profit, you're taxed on the difference between your purchase price and the proceeds of the sale.
- SEC has been trying to regulate the digital currency sector, and has recently been targeting exchanges like Coinbase and Binance over their crypto products.
- Government is also actively trying to find ways to tackle illegal activity.

Regulation in Other Countries

- As cryptocurrency has become a more significant factor in the global investment landscape, countries have taken different approaches to regulating the asset class.
- China
  - The PBOC has banned exchanges from operating in the country, stating that facilitate public financing without approval
  - In May 2021, they banned Bitcoin mining, and then in September 2021 they banned all cryptocurrency
  - They are developing the digital Yuan, and as of August 2022, they started rolling some out
- Canada
  - Not considered legal tender
  - first country to approve a Bitcoin exchange-traded fund (ETF), with several of them now trading on the Toronto Stock Exchange
- Japan
  - takes a progressive approach to crypto regulations, recognizing cryptocurrencies as legal property under the Payment Services Act (PSA).
  - treats trading gains generated from cryptocurrency as “miscellaneous income” and taxes investors accordingly.
- El Salvador
  - First country to make Bitcoin a legal tender