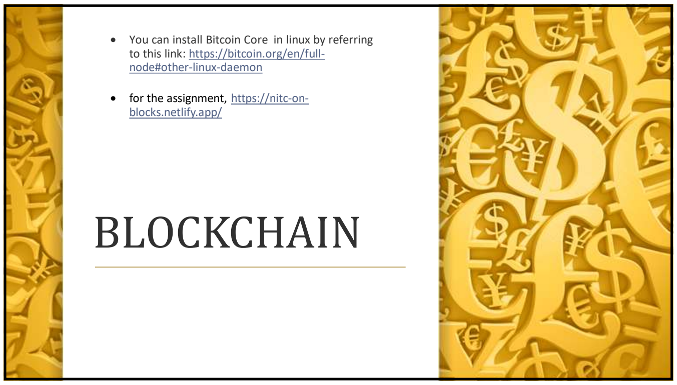
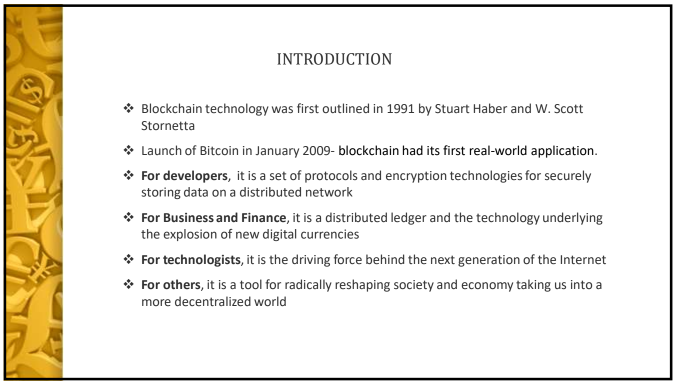


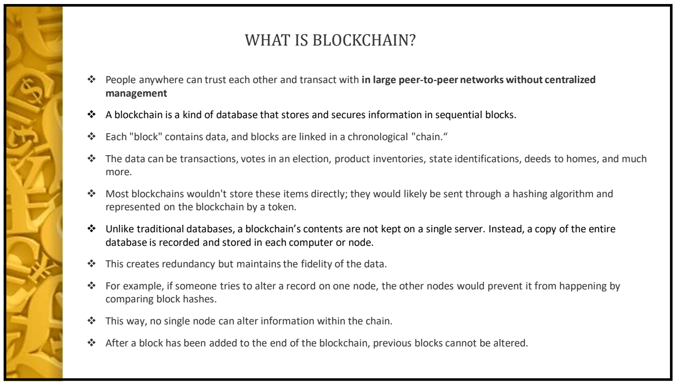
- You can install Bitcoin Core in linux by referring to this link: https://bitcoin.org/en/full-node#other-linux-daemon
- for the assignment, https://nitc-on-blocks.netlify.app/

BLOCKCHAIN



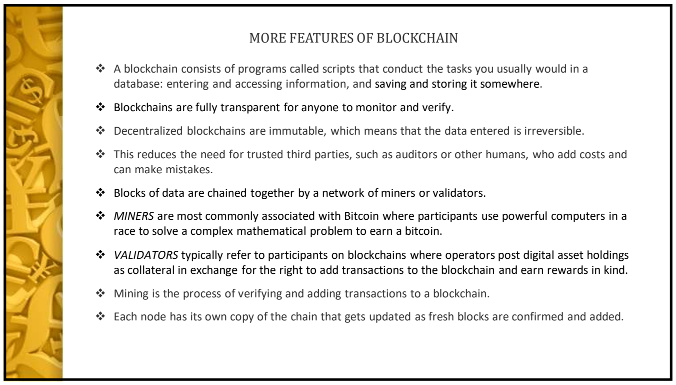
INTRODUCTION

- Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta
- Launch of Bitcoin in January 2009- blockchain had its first real-world application.
- **For developers**, it is a set of protocols and encryption technologies for securely storing data on a distributed network
- **For Business and Finance**, it is a distributed ledger and the technology underlying the explosion of new digital currencies
- **For technologists**, it is the driving force behind the next generation of the Internet
- **For others**, it is a tool for radically reshaping society and economy taking us into a more decentralized world



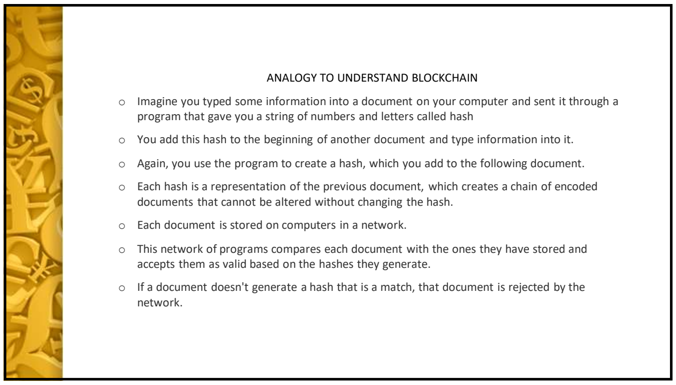
WHAT IS BLOCKCHAIN?

- People anywhere can trust each other and transact with **in large peer-to-peer networks without centralized management**
- A blockchain is a kind of database that stores and secures information in sequential blocks.
- Each "block" contains data, and blocks are linked in a chronological "chain."
- The data can be transactions, votes in an election, product inventories, state identifications, deeds to homes, and much more.
- Most blockchains wouldn't store these items directly; they would likely be sent through a hashing algorithm and represented on the blockchain by a token.
- Unlike traditional databases, a blockchain's contents are not kept on a single server. Instead, a copy of the entire database is recorded and stored in each computer or node.
- This creates redundancy but maintains the fidelity of the data.
- For example, if someone tries to alter a record on one node, the other nodes would prevent it from happening by comparing block hashes.
- This way, no single node can alter information within the chain.
- After a block has been added to the end of the blockchain, previous blocks cannot be altered.



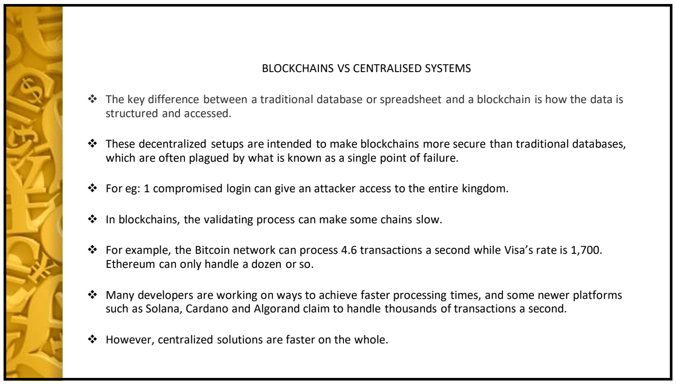
MORE FEATURES OF BLOCKCHAIN

- A blockchain consists of programs called scripts that conduct the tasks you usually would in a database: entering and accessing information, and saving and storing it somewhere.
- Blockchains are fully transparent for anyone to monitor and verify.
- Decentralized blockchains are immutable, which means that the data entered is irreversible.
- This reduces the need for trusted third parties, such as auditors or other humans, who add costs and can make mistakes.
- Blocks of data are chained together by a network of miners or validators.
- *MINERS* are most commonly associated with Bitcoin where participants use powerful computers in a race to solve a complex mathematical problem to earn a bitcoin.
- *VALIDATORS* typically refer to participants on blockchains where operators post digital asset holdings as collateral in exchange for the right to add transactions to the blockchain and earn rewards in kind.
- Mining is the process of verifying and adding transactions to a blockchain.
- Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added.



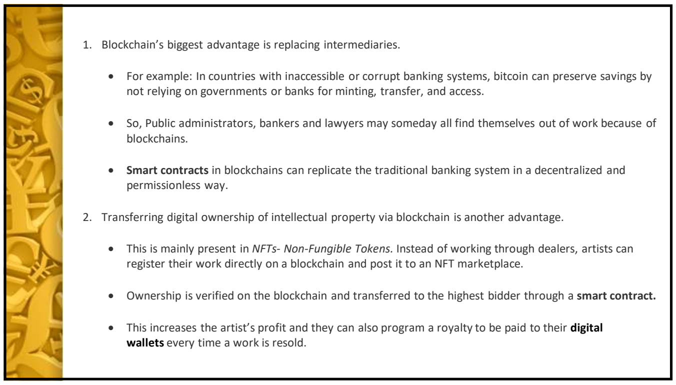
ANALOGY TO UNDERSTAND BLOCKCHAIN

- Imagine you typed some information into a document on your computer and sent it through a program that gave you a string of numbers and letters called hash
- You add this hash to the beginning of another document and type information into it.
- Again, you use the program to create a hash, which you add to the following document.
- Each hash is a representation of the previous document, which creates a chain of encoded documents that cannot be altered without changing the hash.
- Each document is stored on computers in a network.
- This network of programs compares each document with the ones they have stored and accepts them as valid based on the hashes they generate.
- If a document doesn't generate a hash that is a match, that document is rejected by the network.

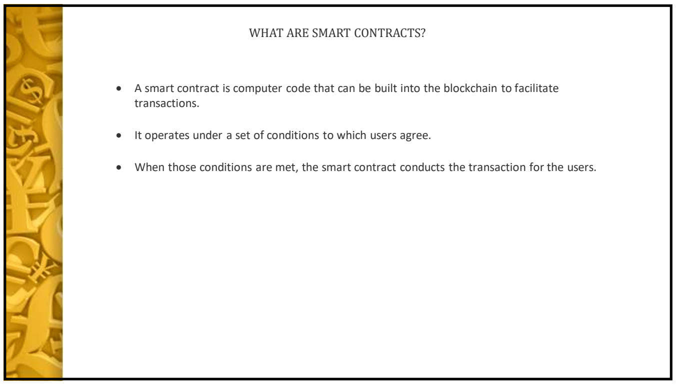


BLOCKCHAINS VS CENTRALISED SYSTEMS

- The key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed.
- These decentralized setups are intended to make blockchains more secure than traditional databases, which are often plagued by what is known as a single point of failure.
- For eg: 1 compromised login can give an attacker access to the entire kingdom.
- In blockchains, the validating process can make some chains slow.
- For example, the Bitcoin network can process 4.6 transactions a second while Visa's rate is 1,700. Ethereum can only handle a dozen or so.
- Many developers are working on ways to achieve faster processing times, and some newer platforms such as Solana, Cardano and Algorand claim to handle thousands of transactions a second.
- However, centralized solutions are faster on the whole.

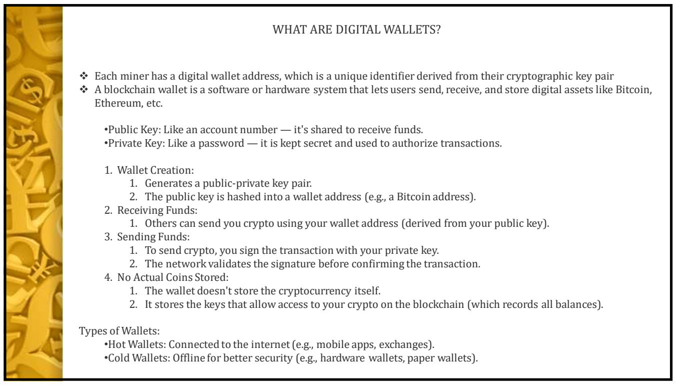


1. Blockchain's biggest advantage is replacing intermediaries.
   - For example: In countries with inaccessible or corrupt banking systems, bitcoin can preserve savings by not relying on governments or banks for minting, transfer, and access.
   - So, Public administrators, bankers and lawyers may someday all find themselves out of work because of blockchains.
   - **Smart contracts** in blockchains can replicate the traditional banking system in a decentralized and permissionless way.
2. Transferring digital ownership of intellectual property via blockchain is another advantage.
   - This is mainly present in *NFTs- Non-Fungible Tokens.* Instead of working through dealers, artists can register their work directly on a blockchain and post it to an NFT marketplace.
   - Ownership is verified on the blockchain and transferred to the highest bidder through a **smart contract.**
   - This increases the artist's profit and they can also program a royalty to be paid to their **digital wallets** every time a work is resold.



WHAT ARE SMART CONTRACTS?

- A smart contract is computer code that can be built into the blockchain to facilitate transactions.
- It operates under a set of conditions to which users agree.
- When those conditions are met, the smart contract conducts the transaction for the users.



WHAT ARE DIGITAL WALLETS?

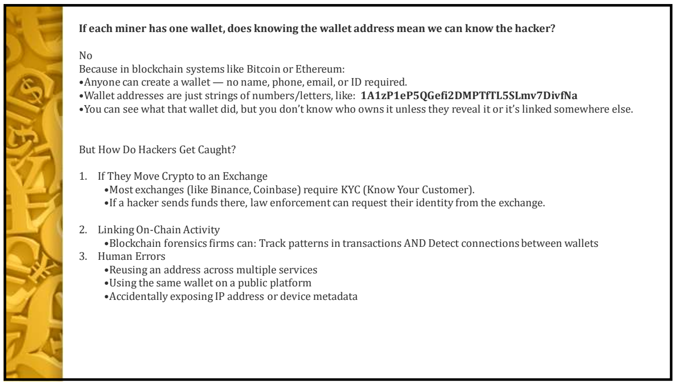
❖ Each miner has a digital wallet address, which is a unique identifier derived from their cryptographic key pair

❖ A blockchain wallet is a software or hardware system that lets users send, receive, and store digital assets like Bitcoin, Ethereum, etc.

•Public Key: Like an account number — it's shared to receive funds.
•Private Key: Like a password — it is kept secret and used to authorize transactions.

1. Wallet Creation:
   1. Generates a public-private key pair.
   2. The public key is hashed into a wallet address (e.g., a Bitcoin address).
2. Receiving Funds:
   1. Others can send you crypto using your wallet address (derived from your public key).
3. Sending Funds:
   1. To send crypto, you sign the transaction with your private key.
   2. The network validates the signature before confirming the transaction.
4. No Actual Coins Stored:
   1. The wallet doesn't store the cryptocurrency itself.
   2. It stores the keys that allow access to your crypto on the blockchain (which records all balances).

Types of Wallets:
•Hot Wallets: Connected to the internet (e.g., mobile apps, exchanges).
•Cold Wallets: Offline for better security (e.g., hardware wallets, paper wallets).

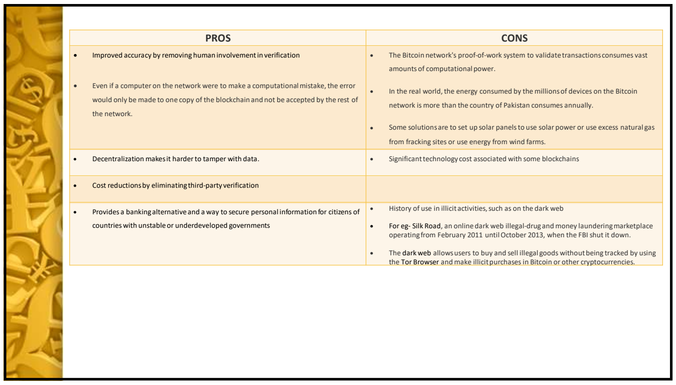


If each miner has one wallet, does knowing the wallet address mean we can know the hacker?

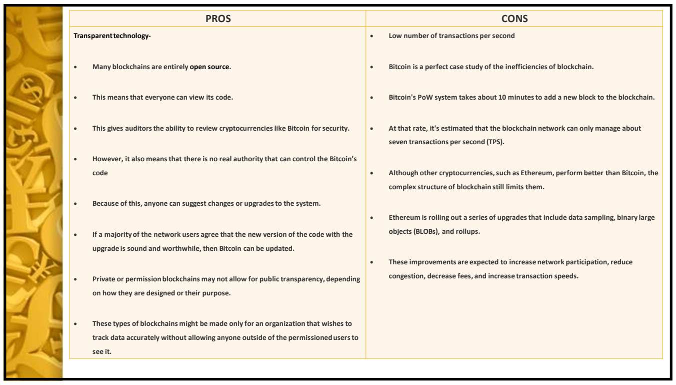
No
Because in blockchain systems like Bitcoin or Ethereum:
•Anyone can create a wallet — no name, phone, email, or ID required.
•Wallet addresses are just strings of numbers/letters, like: **1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa**
•You can see what that wallet did, but you don't know who owns it unless they reveal it or it's linked somewhere else.

But How Do Hackers Get Caught?

1. If They Move Crypto to an Exchange
   •Most exchanges (like Binance, Coinbase) require KYC (Know Your Customer).
   •If a hacker sends funds there, law enforcement can request their identity from the exchange.
2. Linking On-Chain Activity
   •Blockchain forensics firms can: Track patterns in transactions AND Detect connections between wallets
3. Human Errors
   •Reusing an address across multiple services
   •Using the same wallet on a public platform
   •Accidentally exposing IP address or device metadata



PROS	CONS
• Improved accuracy by removing human involvement in verification • Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network.	• The Bitcoin network's proof-of-work system to validate transactions consumes vast amounts of computational power. • In the real world, the energy consumed by the millions of devices on the Bitcoin network is more than the country of Pakistan consumes annually. • Some solutions are to set up solar panels to use solar power or use excess natural gas from fracking sites or use energy from wind farms.
• Decentralization makes it harder to tamper with data.	• Significant technology cost associated with some blockchains
• Cost reductions by eliminating third-party verification	
• Provides a banking alternative and a way to secure personal information for citizens of countries with unstable or underdeveloped governments	• History of use in illicit activities, such as on the dark web • For eg- Silk Road, an online dark web illegal-drug and money laundering marketplace operating from February 2011 until October 2013, when the FBI shut it down. • The dark web allows users to buy and sell illegal goods without being tracked by using the Tor Browser and make illicit purchases in Bitcoin or other cryptocurrencies.



PROS	CONS
Transparent technology- • Many blockchains are entirely **open source**. • This means that everyone can view its code. • This gives auditors the ability to review cryptocurrencies like Bitcoin for security. • However, it also means that there is no real authority that can control the Bitcoin's code • Because of this, anyone can suggest changes or upgrades to the system. • If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated. • Private or permission blockchains may not allow for public transparency, depending on how they are designed or their purpose. • These types of blockchains might be made only for an organization that wishes to track data accurately without allowing anyone outside of the permissioned users to see it.	• Low number of transactions per second • Bitcoin is a perfect case study of the inefficiencies of blockchain. • Bitcoin's PoW system takes about 10 minutes to add a new block to the blockchain. • At that rate, it's estimated that the blockchain network can only manage about seven transactions per second (TPS). • Although other cryptocurrencies, such as Ethereum, perform better than Bitcoin, the complex structure of blockchain still limits them. • Ethereum is rolling out a series of upgrades that include data sampling, binary large objects (BLOBs), and rollups. • These improvements are expected to increase network participation, reduce congestion, decrease fees, and increase transaction speeds.

PROS	CONS
• **Transactions are secure, private, and efficient.**	• Data storage limitations
• Although users can access transaction details, they cannot identify the users making those transactions.	• The **block size debate** has been and continues to be one of the most pressing issues for the scalability of blockchains in the future.
• It is a common misperception that blockchain networks like Bitcoin are fully anonymous.	• Currently, data storage is centralized in large centres.
• They are actually pseudonymous because there is a viewable address that can be accessed.	• But if the world transitions to blockchain for every industry and use, it will force participants to continually upgrade their storage.
	• This could become significantly more expensive in terms of both money and physical space needed.
	• As of September 15th 2024, the Bitcoin blockchain itself was over 600 gigabytes.

DIFFERENCE BETWEEN PUBLIC AND PRIVATE BLOCKCHAINS

- PUBLIC**-** A blockchain that is **open to everyone**. Anyone can join, view, and participate in the network.
- PRIVATE- A blockchain that is **restricted.** Only authorized participants can access it.

PRIVATE BLOCKCHAIN SEEMS SIMILAR TO TRADITIONAL CENTRALISED SYSTEM BUT WHAT IS THE EXACT DIFFERENCE?

- **Traditional bank**: Each bank keeps its own records. And to share money from one bank to another, it requires an intermediary institution.
- **Private blockchain among banks**: All partner banks share one blockchain ledger. When bank a sends money to bank , both see and agree on the transaction instantly, no waiting is required

PRIVATE BLOCKCHAINS

- What if users want the security and transparency of a blockchain but don't need the decentralization or tokens to encourage behaviour?
- Private blockchains are used to upgrade conventional corporate systems.
- Some companies experimenting with private blockchain include Walmart, Pfizer, AIG, Siemens, and Unilever, among others.
- Examples:

1. Shipping and logistics companies like Maersk use blockchain technology to track supply chains and process marine insurance claims.
2. Boeing uses a blockchain-enabled air-traffic-control system to communicate with and track drones.
3. Honeywell maintains transparency with blockchain aircraft records.
4. New York-based signature bank offers a blockchain-based 24/7/365 instantaneous payment system based on a privatized version of Ethereum to help clients move funds around the world in an instant.
5. For example, IBM has created its Food Trust blockchain to trace the journey that food products take to get to their locations.

○ Why do this? The food industry has seen countless outbreaks of E. coli, salmonella, and listeria; in some cases, hazardous materials were accidentally introduced to foods.

○ In the past, it has taken weeks to find the source of these outbreaks or the cause of sickness from what people are eating.

○ Using blockchain allows brands to track a food product's route from its origin, through each stop it makes, to delivery.

○ Not only that, but these companies can also now see everything else it may have come in contact with, allowing the identification of the problem to occur, potentially saving lives.

❖ So, a common trade-off for blockchains is to sacrifice speed and efficiency for security, transparency and decentralization.

❖ Putting your company's transaction information on a blockchain won't be the best option when you can update an Excel file or collaborate with coworkers on a Google Drive.

❖ So what are the APPLICATIONS OF BLOCKCHAIN?

❖ Blockchains are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry

1. Voting systems

❖ The nature of blockchain's immutability means that fraudulent voting would become difficult.

❖ For example, a voting system could work such that each country's citizens would be issued a single cryptocurrency or token.

❖ Each political candidate could then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate they wish to vote for.

❖ The transparent and traceable nature of blockchain would eliminate the need for human vote counting and the ability to tamper with physical ballots.

2. Banks

❖ Financial institutions only operate during business hours, usually five days a week.

❖ That means if you try to deposit a check on Friday at 6 p.m., you will likely have to wait until Monday morning to see the money in your account.

❖ Even if you make your deposit during business hours, the transaction can still take one to three days to verify due to the sheer volume of transactions that banks need to settle.

❖ Blockchain, on the other hand, never sleeps.

❖ By integrating blockchain into banks, consumers might see their transactions processed in minutes or seconds

❖ With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely.

❖ Sometimes banks have to transfer huge sums of money, even the few days the money is in transit can carry significant costs and risks for banks.

❖ The settlement and clearing process for stock traders can take up to three days or more.

❖ This means that the money and shares are frozen for that period.

❖ Blockchain can, in theory, drastically reduce that time.

3. Currency

❖ Blockchain forms the bedrock for cryptocurrencies like Bitcoin.

❖ This design also allows for easier cross-border transactions because it bypasses currency restrictions or any instabilities by using a distributed network that can reach anyone with an internet connection.

4. Healthcare

❖ Healthcare providers can use blockchain to store their patients' medical records securely.

❖ When a medical record is generated and signed, it can be written into the blockchain, which provides patients with proof and confidence that the record cannot be changed.

❖ These personal health records could be encoded and stored on the blockchain with a private key so that they are only accessible to specific individuals, thereby ensuring privacy.

5. Property Records

- ❖ Recording property rights is both burdensome and inefficient.
- ❖ Today, anything related to property must be first delivered to a government employee at the local recording office, where it is manually entered into the county's central database and public index.
- ❖ In the case of a property dispute, claims to the property must be reconciled with the public index.
- ❖ This process is not just costly and time-consuming, but it is also inefficient.
- ❖ Blockchain has the potential to eliminate the need for scanning documents and tracking down physical files in a local recording office.
- ❖ If property ownership is stored and verified on the blockchain, owners can trust that their deed is accurate and permanently recorded.
- ❖ Proving property ownership can be nearly impossible in war-torn countries or areas with little to no government or financial infrastructure and no Recorder's Office.
- ❖ If a group of people living in such an area can use blockchain, then transparent and clear timelines of property ownership could be maintained.

TRANSACTIONS IN BITCOIN

- ○ In Bitcoin's case, the blockchain is decentralized, so no single person or group has control—instead, all users collectively retain control.
- ○ For Bitcoin, transactions are permanently recorded and viewable to anyone.
- ○ Bitcoin's pseudonymous creator is Satoshi Nakamoto
- ○ Bitcoin uses blockchain as a means to transparently record a ledger of payments or other transactions between parties.
- ○ The Bitcoin blockchain collects transaction information and enters it into a file called a block
- ○ Different blockchains have different size blocks. For bitcoin, its 4MB
- ○ Once the block is full, the block data is run through a cryptographic hash function, which creates a hexadecimal number called the block header hash.
- ○ Some common cryptographic hash functions are SHA-256, SHA-3.
- ○ The hash is then entered into the following block header and encrypted with the other information in that block's header, creating a chain of blocks, hence the name "blockchain."
- ○ Transactions follow a specific process, depending on the blockchain.

- ○ A node is any computer that participates in the Bitcoin network. It can:
  - Store a copy of the Bitcoin blockchain.
  - Help verify transactions and blocks.
  - Communicate with other nodes.
- ○ What is a miner?
  - A miner is a special type of node that does extra work:
  - It collects transactions from the memory pool (mempool).
  - It tries to create new blocks by solving a hard math puzzle using the nonce.
  - If it solves the puzzle first, it adds the new block to the blockchain and gets a reward (new bitcoins + transaction fees).
- ○ All miners are nodes but not all nodes are miners (some just help validate and store data).
- ○ **Bitcoin's mining algorithm is Secure Hash Algorithm 256 (SHA256).**
- ○ This cryptographic hash function takes any data as input and produces a fixed-size output known as a hash, a cryptographic fingerprint for the block's data.
- ○ Each block in the Bitcoin blockchain contains a block header with various data, giving rise to a chain of interconnected blocks.

- ○ In Bitcoin, your transaction is sent to a memory pool, where it is stored and queued until a miner picks it up.
- ○ Once it is entered into a block and the block fills up with transactions, it is closed, and the mining begins.
- ○ Each block has maximum number of transactions it can hold.
- ○ Every node in the network proposes its own blocks and work on their own blocks, trying to find a solution to the difficulty target, using the nonce.
- ○ The nonce value is a field in the block header that is changeable, and its value incrementally increases with every mining attempt.
- ○ If the resulting hash isn't equal to or less than the target hash, a value of one is added to the nonce, a new hash is generated, and so on.
- ○ The nonce rolls over about every 4.5 billion attempts (which takes less than one second) and uses another value called the extra nonce as an additional counter.
- ○ This continues until a miner generates a valid hash, winning the race and receiving the reward.

- ○ Generating these hashes until a specific value is found is the "**PROOF-OF-WORK**" -- it "proves" the miner did the work.
- ○ The sheer amount of work it takes to validate the hash is why the Bitcoin network consumes so much computational power and energy.
- ○ Once a block is closed, a transaction is complete.
- ○ However, the block is not considered as confirmed until five other blocks have been validated.
- ○ Each block takes 10 minutes on average. So, the first block with your transaction and five following blocks multiplied by 10 equals 60 minutes.

TRANSACTIONS IN ETHEREUM

1. Propose Blocks

•At regular intervals, one validator is randomly chosen by the Ethereum network.

•The validator does the following:

- Create a new block
- Include transactions from the mempool
- Collect gas fees and block rewards

2. Attest (Vote) on Blocks

•Other validators check the proposed block and vote on whether it's valid.

•These votes are called attestations and help form consensus.

•Honest participation = more rewards.

3. Add Valid Blocks to Blockchain

•Once enough validators agree (reach consensus), the block becomes part of the chain.

•Finalized blocks are extremely difficult to change — this is what makes blockchain secure.

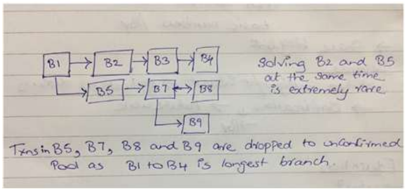
•All transactions can be transparently viewed by downloading and inspecting them or by using blockchain explorers that allow anyone to see transactions occurring live.

ORDER OF TRANSACTIONS

- ❖ Whenever a user initiates a transaction, the transaction goes to an unconfirmed pool.
- ❖ Once they are confirmed and validated they are added to the Blockchain.
- ❖ This would result in two complications —

1. If there is no particular order to transactions, then there could be several branches of the block as plenty of miners would mine transactions and add it to the block in parallel.
2. Double spending –
    - o Double spending means trying to spend the same cryptocurrency twice.
    - o Imagine you have 1 coin. You send that same coin in two (or more) different transactions to different people.
    - o All those transactions go into the unconfirmed pool — a place where transactions wait to be added to the blockchain.
    - o Different miners might pick different versions of those transactions and add them to separate blocks.
    - o This could cause confusion because only one of those transactions should be valid — not both

- To prevent the above two problems, every block carries a mathematical puzzle along with it.
- A block essentially consists of —
    - ❑ Unique identifier to the block (this is the result of the mathematical puzzle),
    - ❑ previous block reference,
    - ❑ the list of transactions
    - ❑ a nonce or random guess.
- SHA256 takes Previous block reference, Transactions, Random guess or Nonce as input and gives a Hash Result.
- The miners keep guessing this 'Random guess or Nonce' so that the output they get is well within a particular target.
- A target value is usually fixed in such a way that the average time for solving is not more than 10 minutes.
- Once the hash result is identified, it is the finger print or the unique identifier to the block.
- Since solving this puzzle is complex, the probability that two or more miners solve blocks at similar times is rare.
- Even if they do it and there are two or three branches to the Blockchain, one simply builds on top of the branch they receive thereby growing the branches.



Solving B2 and B5 at the same time is extremely rare

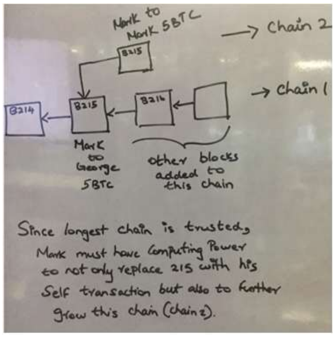
Txns in B5, B7, B8 and B9 are dropped to unconfirmed Pool as B1 to B4 is longest branch.

- Now if there is a tie.
- The first miner to successfully mine the next block (B10) will decide which branch becomes longer.
- Once a block is added to either branch, that branch becomes the longest chain and is considered the main chain.
- This is because the longest network in the Blockchain is usually the trusted link and everybody immediately switches to the longest branch.
- Hence whenever a block is added, it is good to wait for 10 mins or more to confirm that your block is actually added into the longest chain.

•In the above picture, chain 2 goes to unconfirmed list and chain 1 remains the longest chain. This can cause 2 possible issues:

1. It could lead to double spending of chain 2 transactions as these transactions are still not confirmed.
    - To address this problem, look at the second picture
    - There are blocks: B214 → B215 → B216 → ... This is the main chain
    - In block B215, Mark sends 5 BTC to George. This is a real transaction, and everyone accepts it.
    - He makes a new fake version of B215, where instead of sending 5 BTC to George, he sends it back to himself.
    - This is called a double spend — trying to use the same money twice.
    - This new version creates a second chain (Chain 2): But this cannot happen for multiple reasons,
    - Mark cannot randomly replace a block in the middle as the block is already referencing the previous block and introducing a new block would not exactly fit
    - Mark needs to have more than 50% computing power to keep building on the chain to ensure this is the longest network which is impossible.
    - Chain 1 has B214 → B215 → B216 → more blocks.
    - Mark's fake Chain 2 only has B214 → fake B215.
    - To win, Mark must: Create fake B215, Create fake B216, B217... and so on
    - And do all this faster than all other miners in the world
    - Hence, it is not possible for Mark to replace the chain with his self-made chain as that would require immensely large computing power
    - Also, a block cannot be solved before the previous block is solved. As the previous block's reference goes into the cryptographic function too.
    - Mark can't jump ahead and make B216, B217 before B215 — everything must go in order.

2. Users get irritated as their transactions take time to get confirmed. So, users usually pay some incentive to get their transactions confirmed first. This is not a lot and is not always needed.



Since longest chain is trusted, Mark must have Computing Power to not only replace 215 with his Self transaction but also to further grow this chain (chain 2).

ETHEREUM'S MERGE

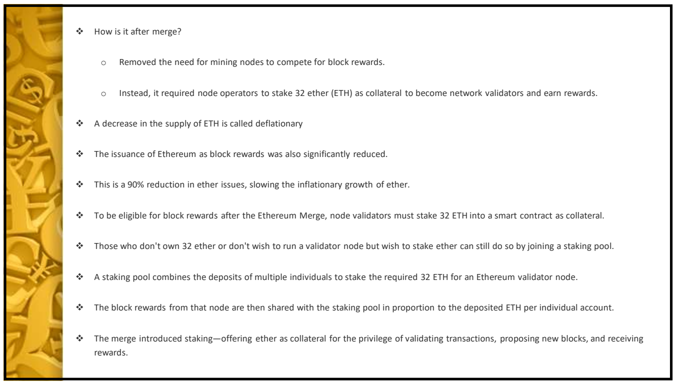
- ❖ Ethereum moved the system over to a Proof-of-Stake mechanism from its proof-of-work (PoW) system.
- ❖ With the move, miners were swapped out for validators.
- ❖ The upside? A 99% reduction in energy use for the entire Ethereum network.
- ❖ The Merge combined the Beacon Chain and the Ethereum mainnet
- ❖ The Merge created a consensus layer from the Beacon Chain and an execution layer from the mainnet.
- ❖ The consensus layer handles blocks, confirmation, and rewards, while the execution layer handles smart contracts and processes transactions.
- ❖ The layers communicate through an application programming interface (API).

What Caused the Merge?

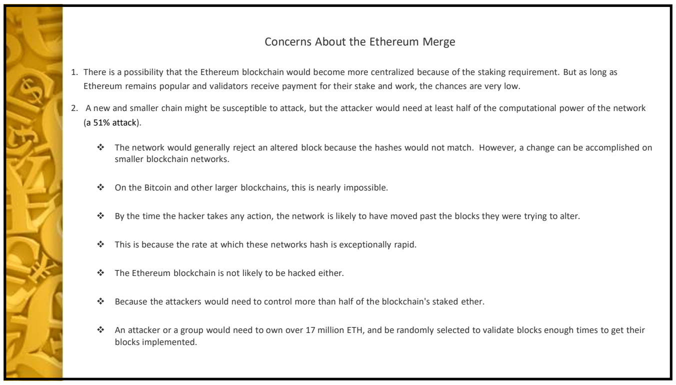
- o Proof-of-stake uses less energy and incentives.

How was it before merge?

- o It required large amounts of processing power to solve a cryptographic puzzle.
- o All miners competed to generate a solution, propose a new block, and receive an ETH reward.

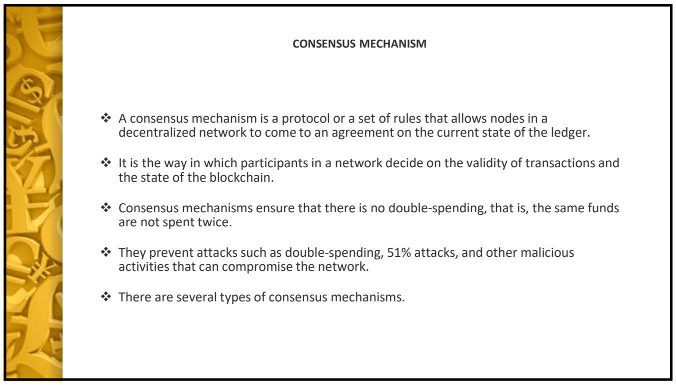


- How is it after merge?
  - Removed the need for mining nodes to compete for block rewards.
  - Instead, it required node operators to stake 32 ether (ETH) as collateral to become network validators and earn rewards.
- A decrease in the supply of ETH is called deflationary
- The issuance of Ethereum as block rewards was also significantly reduced.
- This is a 90% reduction in ether issues, slowing the inflationary growth of ether.
- To be eligible for block rewards after the Ethereum Merge, node validators must stake 32 ETH into a smart contract as collateral.
- Those who don't own 32 ether or don't wish to run a validator node but wish to stake ether can still do so by joining a staking pool.
- A staking pool combines the deposits of multiple individuals to stake the required 32 ETH for an Ethereum validator node.
- The block rewards from that node are then shared with the staking pool in proportion to the deposited ETH per individual account.
- The merge introduced staking—offering ether as collateral for the privilege of validating transactions, proposing new blocks, and receiving rewards.



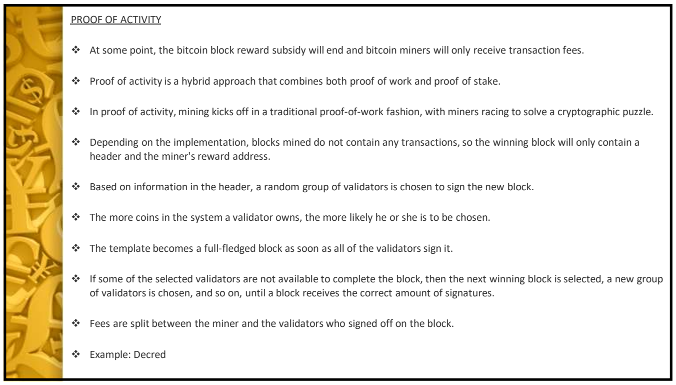
Concerns About the Ethereum Merge

1. There is a possibility that the Ethereum blockchain would become more centralized because of the staking requirement. But as long as Ethereum remains popular and validators receive payment for their stake and work, the chances are very low.
2. A new and smaller chain might be susceptible to attack, but the attacker would need at least half of the computational power of the network (a 51% attack).
   - The network would generally reject an altered block because the hashes would not match. However, a change can be accomplished on smaller blockchain networks.
   - On the Bitcoin and other larger blockchains, this is nearly impossible.
   - By the time the hacker takes any action, the network is likely to have moved past the blocks they were trying to alter.
   - This is because the rate at which these networks hash is exceptionally rapid.
   - The Ethereum blockchain is not likely to be hacked either.
   - Because the attackers would need to control more than half of the blockchain's staked ether.
   - An attacker or a group would need to own over 17 million ETH, and be randomly selected to validate blocks enough times to get their blocks implemented.



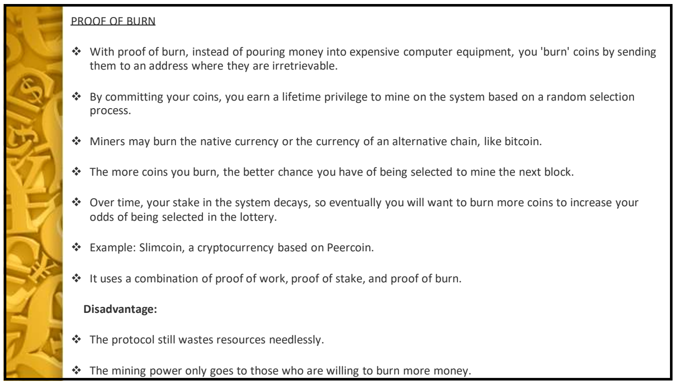
CONSENSUS MECHANISM

- A consensus mechanism is a protocol or a set of rules that allows nodes in a decentralized network to come to an agreement on the current state of the ledger.
- It is the way in which participants in a network decide on the validity of transactions and the state of the blockchain.
- Consensus mechanisms ensure that there is no double-spending, that is, the same funds are not spent twice.
- They prevent attacks such as double-spending, 51% attacks, and other malicious activities that can compromise the network.
- There are several types of consensus mechanisms.



PROOF OF ACTIVITY

- At some point, the bitcoin block reward subsidy will end and bitcoin miners will only receive transaction fees.
- Proof of activity is a hybrid approach that combines both proof of work and proof of stake.
- In proof of activity, mining kicks off in a traditional proof-of-work fashion, with miners racing to solve a cryptographic puzzle.
- Depending on the implementation, blocks mined do not contain any transactions, so the winning block will only contain a header and the miner's reward address.
- Based on information in the header, a random group of validators is chosen to sign the new block.
- The more coins in the system a validator owns, the more likely he or she is to be chosen.
- The template becomes a full-fledged block as soon as all of the validators sign it.
- If some of the selected validators are not available to complete the block, then the next winning block is selected, a new group of validators is chosen, and so on, until a block receives the correct amount of signatures.
- Fees are split between the miner and the validators who signed off on the block.
- Example: Decred

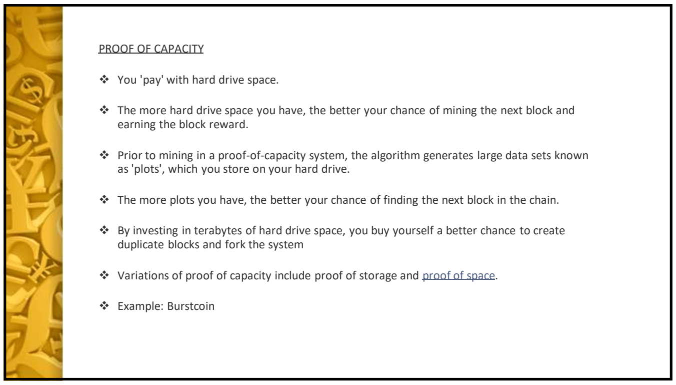


PROOF OF BURN

- With proof of burn, instead of pouring money into expensive computer equipment, you 'burn' coins by sending them to an address where they are irretrievable.
- By committing your coins, you earn a lifetime privilege to mine on the system based on a random selection process.
- Miners may burn the native currency or the currency of an alternative chain, like bitcoin.
- The more coins you burn, the better chance you have of being selected to mine the next block.
- Over time, your stake in the system decays, so eventually you will want to burn more coins to increase your odds of being selected in the lottery.
- Example: Slimcoin, a cryptocurrency based on Peercoin.
- It uses a combination of proof of work, proof of stake, and proof of burn.

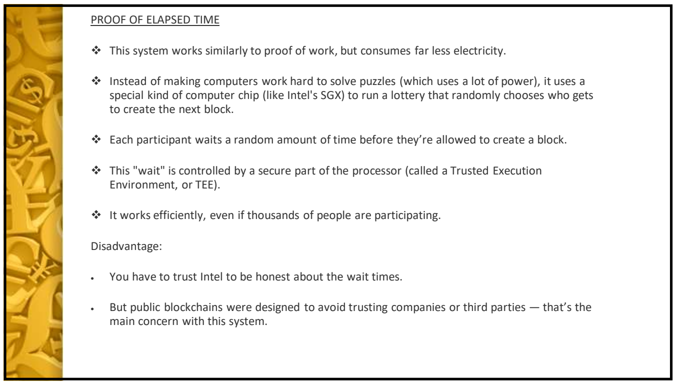
Disadvantage:

- The protocol still wastes resources needlessly.
- The mining power only goes to those who are willing to burn more money.



PROOF OF CAPACITY

- You 'pay' with hard drive space.
- The more hard drive space you have, the better your chance of mining the next block and earning the block reward.
- Prior to mining in a proof-of-capacity system, the algorithm generates large data sets known as 'plots', which you store on your hard drive.
- The more plots you have, the better your chance of finding the next block in the chain.
- By investing in terabytes of hard drive space, you buy yourself a better chance to create duplicate blocks and fork the system
- Variations of proof of capacity include proof of storage and proof of space.
- Example: Burstcoin

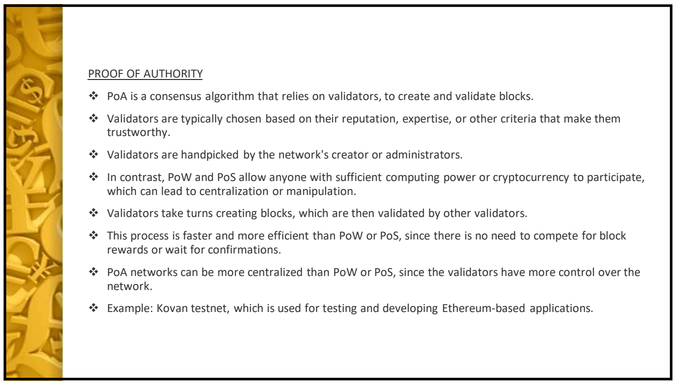


PROOF OF ELAPSED TIME

- This system works similarly to proof of work, but consumes far less electricity.
- Instead of making computers work hard to solve puzzles (which uses a lot of power), it uses a special kind of computer chip (like Intel's SGX) to run a lottery that randomly chooses who gets to create the next block.
- Each participant waits a random amount of time before they're allowed to create a block.
- This "wait" is controlled by a secure part of the processor (called a Trusted Execution Environment, or TEE).
- It works efficiently, even if thousands of people are participating.

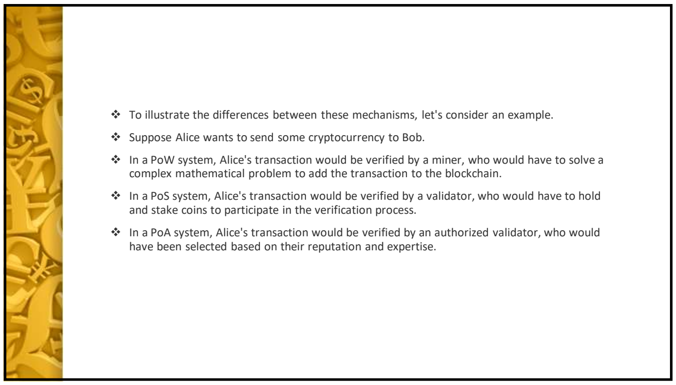
Disadvantage:

- You have to trust Intel to be honest about the wait times.
- But public blockchains were designed to avoid trusting companies or third parties — that's the main concern with this system.

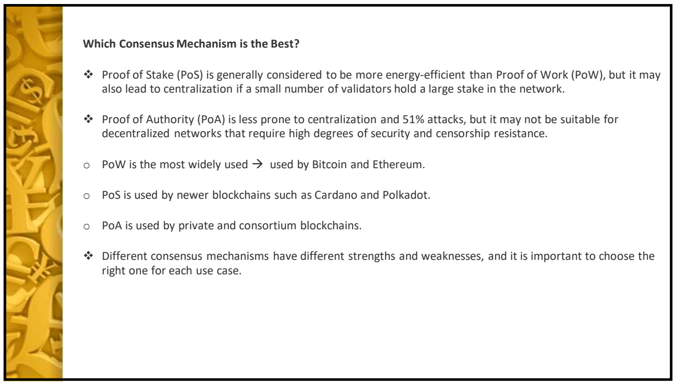


PROOF OF AUTHORITY

- PoA is a consensus algorithm that relies on validators, to create and validate blocks.
- Validators are typically chosen based on their reputation, expertise, or other criteria that make them trustworthy.
- Validators are handpicked by the network's creator or administrators.
- In contrast, PoW and PoS allow anyone with sufficient computing power or cryptocurrency to participate, which can lead to centralization or manipulation.
- Validators take turns creating blocks, which are then validated by other validators.
- This process is faster and more efficient than PoW or PoS, since there is no need to compete for block rewards or wait for confirmations.
- PoA networks can be more centralized than PoW or PoS, since the validators have more control over the network.
- Example: Kovan testnet, which is used for testing and developing Ethereum-based applications.

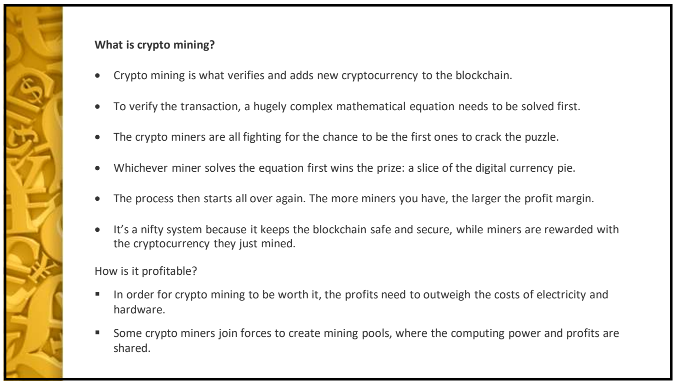


- To illustrate the differences between these mechanisms, let's consider an example.
- Suppose Alice wants to send some cryptocurrency to Bob.
- In a PoW system, Alice's transaction would be verified by a miner, who would have to solve a complex mathematical problem to add the transaction to the blockchain.
- In a PoS system, Alice's transaction would be verified by a validator, who would have to hold and stake coins to participate in the verification process.
- In a PoA system, Alice's transaction would be verified by an authorized validator, who would have been selected based on their reputation and expertise.



Which Consensus Mechanism is the Best?

- Proof of Stake (PoS) is generally considered to be more energy-efficient than Proof of Work (PoW), but it may also lead to centralization if a small number of validators hold a large stake in the network.
- Proof of Authority (PoA) is less prone to centralization and 51% attacks, but it may not be suitable for decentralized networks that require high degrees of security and censorship resistance.
  - PoW is the most widely used → used by Bitcoin and Ethereum.
  - PoS is used by newer blockchains such as Cardano and Polkadot.
  - PoA is used by private and consortium blockchains.
- Different consensus mechanisms have different strengths and weaknesses, and it is important to choose the right one for each use case.

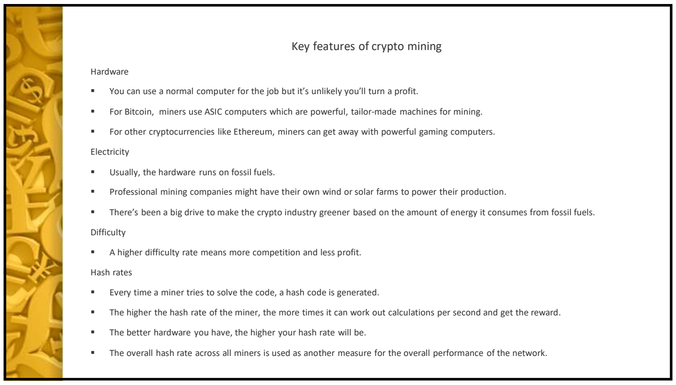


What is crypto mining?

- Crypto mining is what verifies and adds new cryptocurrency to the blockchain.
- To verify the transaction, a hugely complex mathematical equation needs to be solved first.
- The crypto miners are all fighting for the chance to be the first ones to crack the puzzle.
- Whichever miner solves the equation first wins the prize: a slice of the digital currency pie.
- The process then starts all over again. The more miners you have, the larger the profit margin.
- It's a nifty system because it keeps the blockchain safe and secure, while miners are rewarded with the cryptocurrency they just mined.

How is it profitable?

- In order for crypto mining to be worth it, the profits need to outweigh the costs of electricity and hardware.
- Some crypto miners join forces to create mining pools, where the computing power and profits are shared.



Key features of crypto mining

Hardware

- You can use a normal computer for the job but it's unlikely you'll turn a profit.
- For Bitcoin, miners use ASIC computers which are powerful, tailor-made machines for mining.
- For other cryptocurrencies like Ethereum, miners can get away with powerful gaming computers.

Electricity

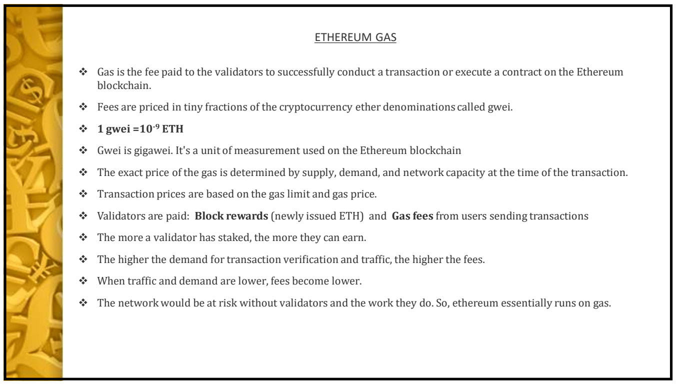
- Usually, the hardware runs on fossil fuels.
- Professional mining companies might have their own wind or solar farms to power their production.
- There's been a big drive to make the crypto industry greener based on the amount of energy it consumes from fossil fuels.

Difficulty

- A higher difficulty rate means more competition and less profit.

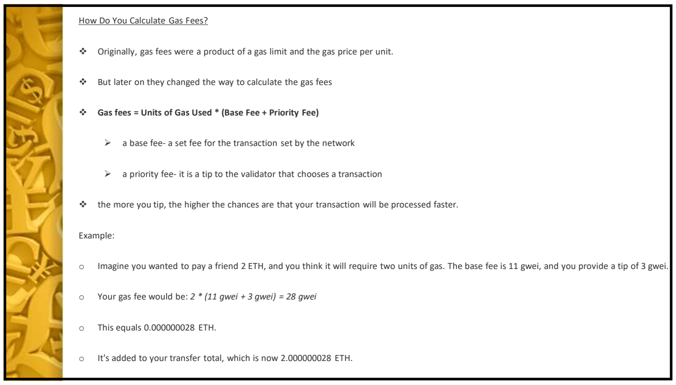
Hash rates

- Every time a miner tries to solve the code, a hash code is generated.
- The higher the hash rate of the miner, the more times it can work out calculations per second and get the reward.
- The better hardware you have, the higher your hash rate will be.
- The overall hash rate across all miners is used as another measure for the overall performance of the network.



ETHEREUM GAS

- ❖ Gas is the fee paid to the validators to successfully conduct a transaction or execute a contract on the Ethereum blockchain.
- ❖ Fees are priced in tiny fractions of the cryptocurrency ether denominations called gwei.
- ❖ **1 gwei =10^{-9} ETH**
- ❖ Gwei is gigawei. It's a unit of measurement used on the Ethereum blockchain
- ❖ The exact price of the gas is determined by supply, demand, and network capacity at the time of the transaction.
- ❖ Transaction prices are based on the gas limit and gas price.
- ❖ Validators are paid: **Block rewards** (newly issued ETH) and **Gas fees** from users sending transactions
- ❖ The more a validator has staked, the more they can earn.
- ❖ The higher the demand for transaction verification and traffic, the higher the fees.
- ❖ When traffic and demand are lower, fees become lower.
- ❖ The network would be at risk without validators and the work they do. So, ethereum essentially runs on gas.

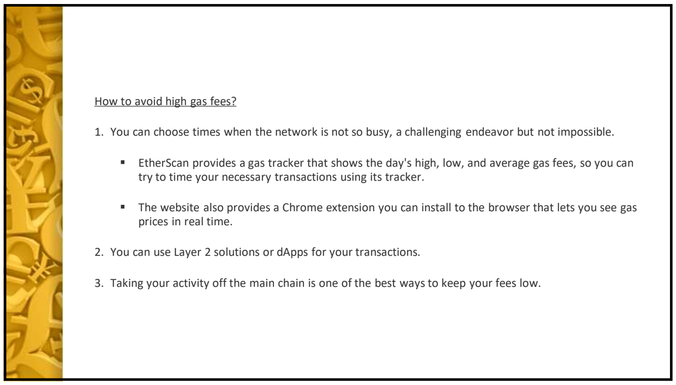


How Do You Calculate Gas Fees?

- ❖ Originally, gas fees were a product of a gas limit and the gas price per unit.
- ❖ But later on they changed the way to calculate the gas fees
- ❖ **Gas fees = Units of Gas Used * (Base Fee + Priority Fee)**
  - ➢ a base fee- a set fee for the transaction set by the network
  - ➢ a priority fee- it is a tip to the validator that chooses a transaction
- ❖ the more you tip, the higher the chances are that your transaction will be processed faster.

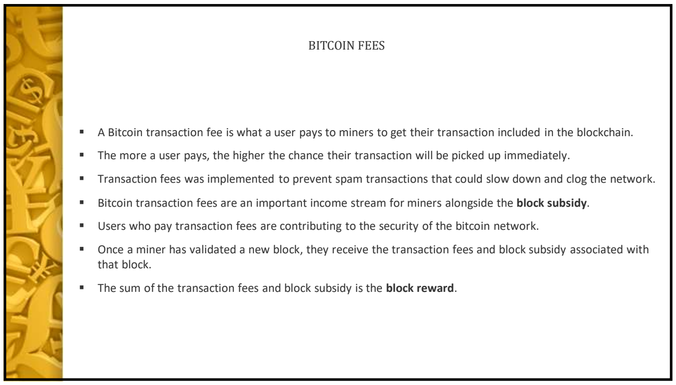
Example:

- ○ Imagine you wanted to pay a friend 2 ETH, and you think it will require two units of gas. The base fee is 11 gwei, and you provide a tip of 3 gwei.
- ○ Your gas fee would be: *2 * (11 gwei + 3 gwei) = 28 gwei*
- ○ This equals 0.000000028 ETH.
- ○ It's added to your transfer total, which is now 2.000000028 ETH.



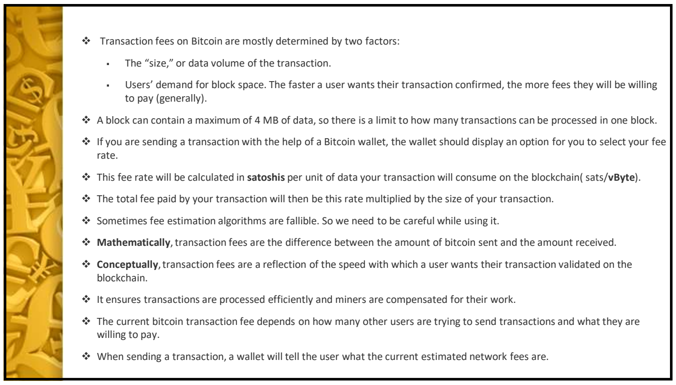
How to avoid high gas fees?

1. You can choose times when the network is not so busy, a challenging endeavor but not impossible.
   - ▪ EtherScan provides a gas tracker that shows the day's high, low, and average gas fees, so you can try to time your necessary transactions using its tracker.
   - ▪ The website also provides a Chrome extension you can install to the browser that lets you see gas prices in real time.
2. You can use Layer 2 solutions or dApps for your transactions.
3. Taking your activity off the main chain is one of the best ways to keep your fees low.

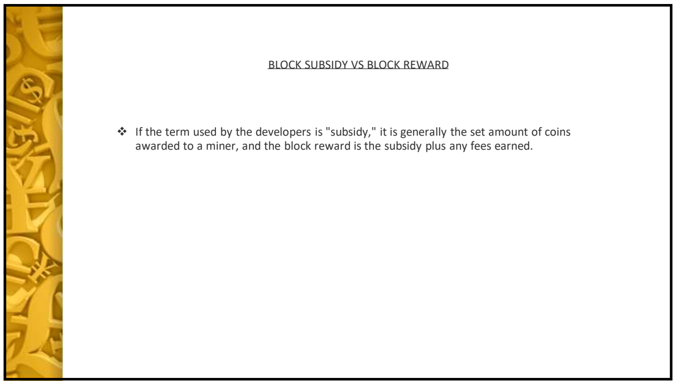


BITCOIN FEES

- ▪ A Bitcoin transaction fee is what a user pays to miners to get their transaction included in the blockchain.
- ▪ The more a user pays, the higher the chance their transaction will be picked up immediately.
- ▪ Transaction fees was implemented to prevent spam transactions that could slow down and clog the network.
- ▪ Bitcoin transaction fees are an important income stream for miners alongside the **block subsidy**.
- ▪ Users who pay transaction fees are contributing to the security of the bitcoin network.
- ▪ Once a miner has validated a new block, they receive the transaction fees and block subsidy associated with that block.
- ▪ The sum of the transaction fees and block subsidy is the **block reward**.

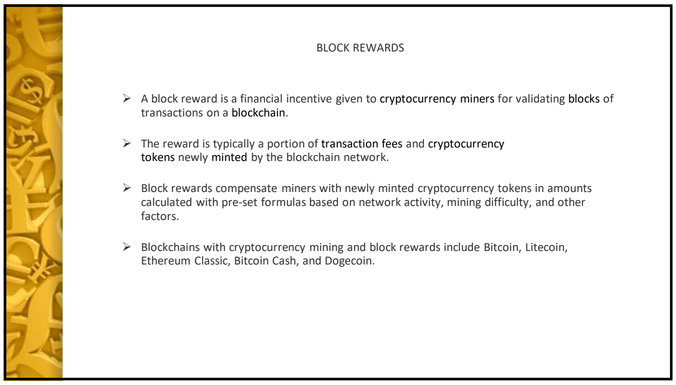


- ❖ Transaction fees on Bitcoin are mostly determined by two factors:
  - • The "size," or data volume of the transaction.
  - • Users' demand for block space. The faster a user wants their transaction confirmed, the more fees they will be willing to pay (generally).
- ❖ A block can contain a maximum of 4 MB of data, so there is a limit to how many transactions can be processed in one block.
- ❖ If you are sending a transaction with the help of a Bitcoin wallet, the wallet should display an option for you to select your fee rate.
- ❖ This fee rate will be calculated in **satoshis** per unit of data your transaction will consume on the blockchain(sats/**vByte**).
- ❖ The total fee paid by your transaction will then be this rate multiplied by the size of your transaction.
- ❖ Sometimes fee estimation algorithms are fallible. So we need to be careful while using it.
- ❖ **Mathematically**, transaction fees are the difference between the amount of bitcoin sent and the amount received.
- ❖ **Conceptually**, transaction fees are a reflection of the speed with which a user wants their transaction validated on the blockchain.
- ❖ It ensures transactions are processed efficiently and miners are compensated for their work.
- ❖ The current bitcoin transaction fee depends on how many other users are trying to send transactions and what they are willing to pay.
- ❖ When sending a transaction, a wallet will tell the user what the current estimated network fees are.



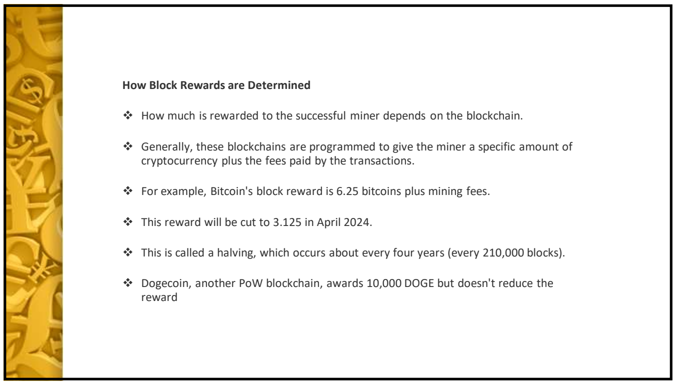
BLOCK SUBSIDY VS BLOCK REWARD

- ❖ If the term used by the developers is "subsidy," it is generally the set amount of coins awarded to a miner, and the block reward is the subsidy plus any fees earned.



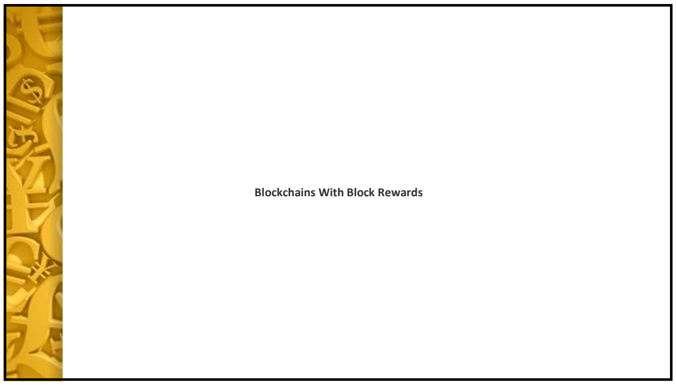
BLOCK REWARDS

- A block reward is a financial incentive given to cryptocurrency miners for validating blocks of transactions on a blockchain.
- The reward is typically a portion of transaction fees and cryptocurrency tokens newly minted by the blockchain network.
- Block rewards compensate miners with newly minted cryptocurrency tokens in amounts calculated with pre-set formulas based on network activity, mining difficulty, and other factors.
- Blockchains with cryptocurrency mining and block rewards include Bitcoin, Litecoin, Ethereum Classic, Bitcoin Cash, and Dogecoin.

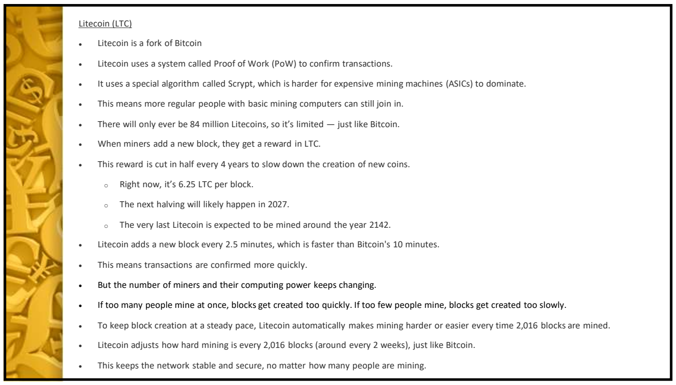


How Block Rewards are Determined

- How much is rewarded to the successful miner depends on the blockchain.
- Generally, these blockchains are programmed to give the miner a specific amount of cryptocurrency plus the fees paid by the transactions.
- For example, Bitcoin's block reward is 6.25 bitcoins plus mining fees.
- This reward will be cut to 3.125 in April 2024.
- This is called a halving, which occurs about every four years (every 210,000 blocks).
- Dogecoin, another PoW blockchain, awards 10,000 DOGE but doesn't reduce the reward

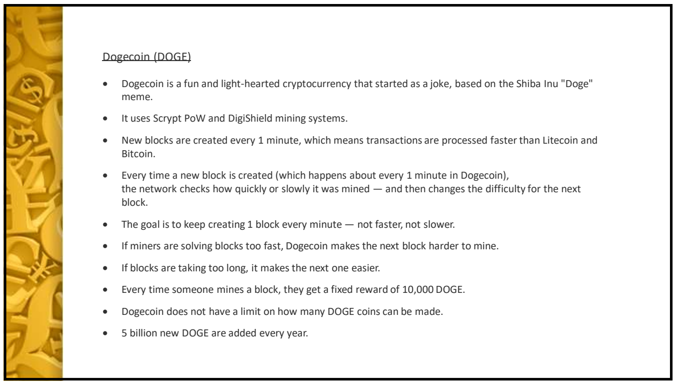


Blockchains With Block Rewards



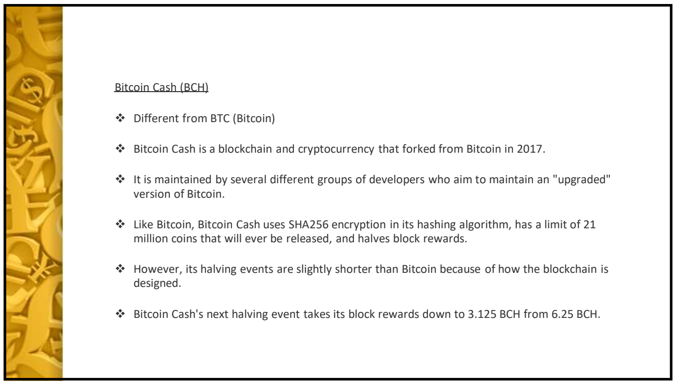
Litecoin (LTC)

- Litecoin is a fork of Bitcoin
- Litecoin uses a system called Proof of Work (PoW) to confirm transactions.
- It uses a special algorithm called Scrypt, which is harder for expensive mining machines (ASICs) to dominate.
- This means more regular people with basic mining computers can still join in.
- There will only ever be 84 million Litecoins, so it's limited — just like Bitcoin.
- When miners add a new block, they get a reward in LTC.
- This reward is cut in half every 4 years to slow down the creation of new coins.
  - Right now, it's 6.25 LTC per block.
  - The next halving will likely happen in 2027.
  - The very last Litecoin is expected to be mined around the year 2142.
- Litecoin adds a new block every 2.5 minutes, which is faster than Bitcoin's 10 minutes.
- This means transactions are confirmed more quickly.
- But the number of miners and their computing power keeps changing.
- If too many people mine at once, blocks get created too quickly. If too few people mine, blocks get created too slowly.
- To keep block creation at a steady pace, Litecoin automatically makes mining harder or easier every time 2,016 blocks are mined.
- Litecoin adjusts how hard mining is every 2,016 blocks (around every 2 weeks), just like Bitcoin.
- This keeps the network stable and secure, no matter how many people are mining.



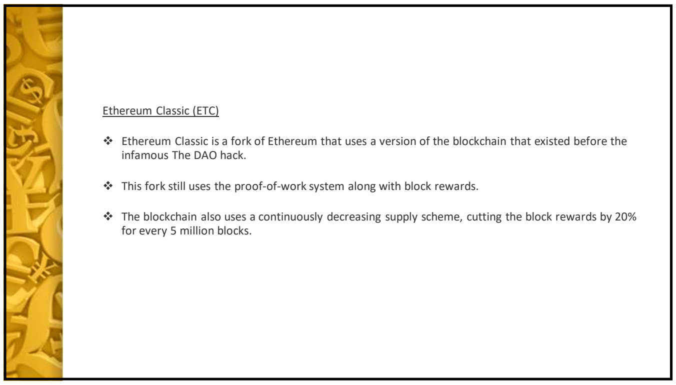
Dogecoin (DOGE)

- Dogecoin is a fun and light-hearted cryptocurrency that started as a joke, based on the Shiba Inu "Doge" meme.
- It uses Scrypt PoW and DigiShield mining systems.
- New blocks are created every 1 minute, which means transactions are processed faster than Litecoin and Bitcoin.
- Every time a new block is created (which happens about every 1 minute in Dogecoin), the network checks how quickly or slowly it was mined — and then changes the difficulty for the next block.
- The goal is to keep creating 1 block every minute — not faster, not slower.
- If miners are solving blocks too fast, Dogecoin makes the next block harder to mine.
- If blocks are taking too long, it makes the next one easier.
- Every time someone mines a block, they get a fixed reward of 10,000 DOGE.
- Dogecoin does not have a limit on how many DOGE coins can be made.
- 5 billion new DOGE are added every year.



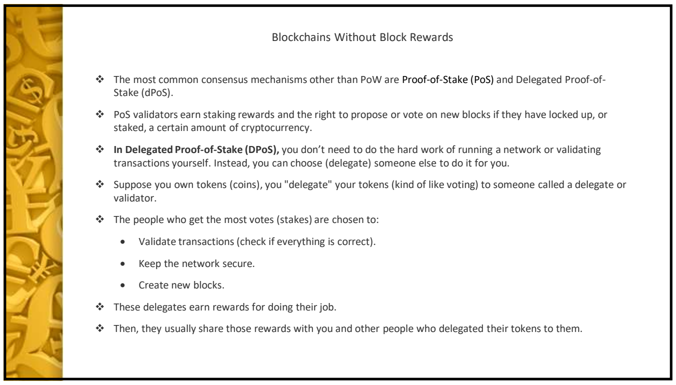
Bitcoin Cash (BCH)

- Different from BTC (Bitcoin)
- Bitcoin Cash is a blockchain and cryptocurrency that forked from Bitcoin in 2017.
- It is maintained by several different groups of developers who aim to maintain an "upgraded" version of Bitcoin.
- Like Bitcoin, Bitcoin Cash uses SHA256 encryption in its hashing algorithm, has a limit of 21 million coins that will ever be released, and halves block rewards.
- However, its halving events are slightly shorter than Bitcoin because of how the blockchain is designed.
- Bitcoin Cash's next halving event takes its block rewards down to 3.125 BCH from 6.25 BCH.



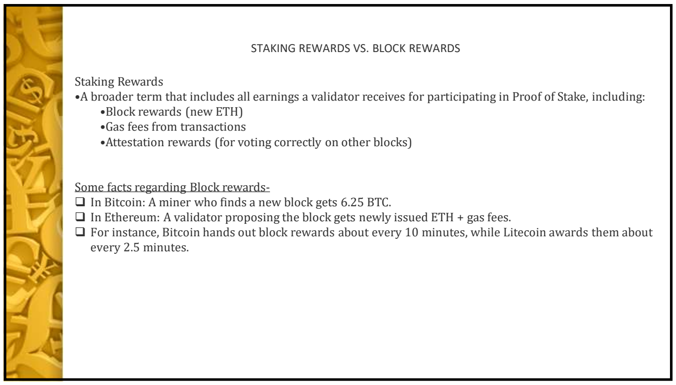
Ethereum Classic (ETC)

- ❖ Ethereum Classic is a fork of Ethereum that uses a version of the blockchain that existed before the infamous The DAO hack.
- ❖ This fork still uses the proof-of-work system along with block rewards.
- ❖ The blockchain also uses a continuously decreasing supply scheme, cutting the block rewards by 20% for every 5 million blocks.



Blockchains Without Block Rewards

- ❖ The most common consensus mechanisms other than PoW are Proof-of-Stake (PoS) and Delegated Proof-of-Stake (dPoS).
- ❖ PoS validators earn staking rewards and the right to propose or vote on new blocks if they have locked up, or staked, a certain amount of cryptocurrency.
- ❖ **In Delegated Proof-of-Stake (DPoS),** you don't need to do the hard work of running a network or validating transactions yourself. Instead, you can choose (delegate) someone else to do it for you.
- ❖ Suppose you own tokens (coins), you "delegate" your tokens (kind of like voting) to someone called a delegate or validator.
- ❖ The people who get the most votes (stakes) are chosen to:
  - Validate transactions (check if everything is correct).
  - Keep the network secure.
  - Create new blocks.
- ❖ These delegates earn rewards for doing their job.
- ❖ Then, they usually share those rewards with you and other people who delegated their tokens to them.

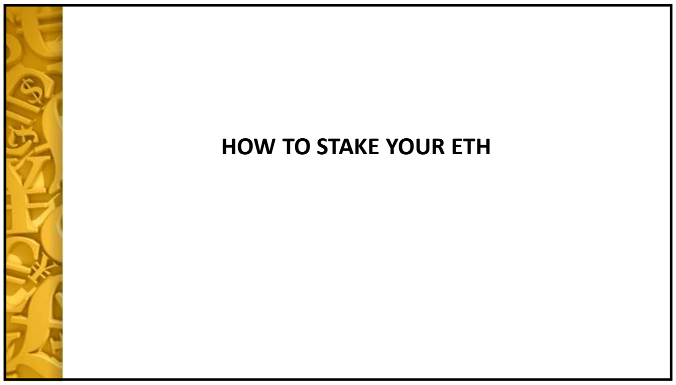


STAKING REWARDS VS. BLOCK REWARDS

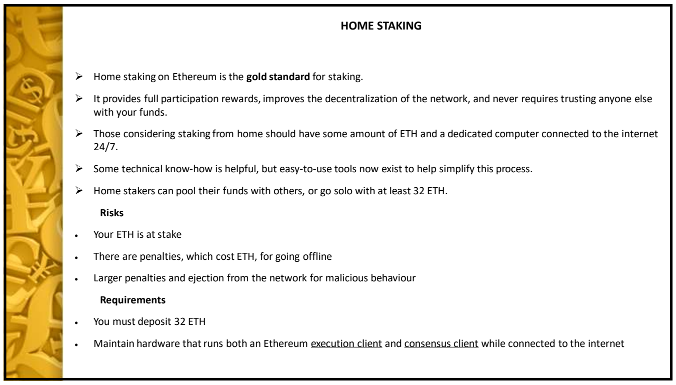
Staking Rewards
•A broader term that includes all earnings a validator receives for participating in Proof of Stake, including:
•Block rewards (new ETH)
•Gas fees from transactions
•Attestation rewards (for voting correctly on other blocks)

Some facts regarding Block rewards-

- ❑ In Bitcoin: A miner who finds a new block gets 6.25 BTC.
- ❑ In Ethereum: A validator proposing the block gets newly issued ETH + gas fees.
- ❑ For instance, Bitcoin hands out block rewards about every 10 minutes, while Litecoin awards them about every 2.5 minutes.



HOW TO STAKE YOUR ETH



HOME STAKING

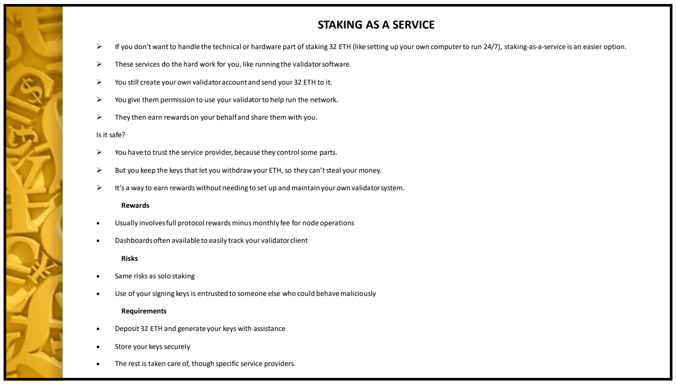
- ➢ Home staking on Ethereum is the **gold standard** for staking.
- ➢ It provides full participation rewards, improves the decentralization of the network, and never requires trusting anyone else with your funds.
- ➢ Those considering staking from home should have some amount of ETH and a dedicated computer connected to the internet 24/7.
- ➢ Some technical know-how is helpful, but easy-to-use tools now exist to help simplify this process.
- ➢ Home stakers can pool their funds with others, or go solo with at least 32 ETH.

Risks

- Your ETH is at stake
- There are penalties, which cost ETH, for going offline
- Larger penalties and ejection from the network for malicious behaviour

Requirements

- You must deposit 32 ETH
- Maintain hardware that runs both an Ethereum execution client and consensus client while connected to the internet



STAKING AS A SERVICE

- ➢ If you don't want to handle the technical or hardware part of staking 32 ETH (like setting up your own computer to run 24/7), staking-as-a-service is an easier option.
- ➢ These services do the hard work for you, like running the validator software.
- ➢ You still create your own validator account and send your 32 ETH to it.
- ➢ You give them permission to use your validator to help run the network.
- ➢ They then earn rewards on your behalf and share them with you.

Is it safe?

- ➢ You have to trust the service provider, because they control some parts.
- ➢ But you keep the keys that let you withdraw your ETH, so they can't steal your money.
- ➢ It's a way to earn rewards without needing to set up and maintain your own validator system.

Rewards

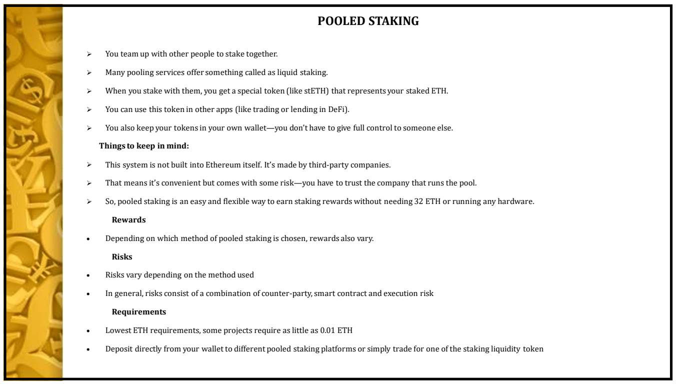
- Usually involves full protocol rewards minus monthly fee for node operations
- Dashboards often available to easily track your validator client

Risks

- Same risks as solo staking
- Use of your signing keys is entrusted to someone else who could behave maliciously

Requirements

- Deposit 32 ETH and generate your keys with assistance
- Store your keys securely
- The rest is taken care of, though specific service providers.



POOLED STAKING

- ➢ You team up with other people to stake together.
- ➢ Many pooling services offer something called as liquid staking.
- ➢ When you stake with them, you get a special token (like stETH) that represents your staked ETH.
- ➢ You can use this token in other apps (like trading or lending in DeFi).
- ➢ You also keep your tokens in your own wallet—you don't have to give full control to someone else.

Things to keep in mind:

- ➢ This system is not built into Ethereum itself. It's made by third-party companies.
- ➢ That means it's convenient but comes with some risk—you have to trust the company that runs the pool.
- ➢ So, pooled staking is an easy and flexible way to earn staking rewards without needing 32 ETH or running any hardware.

Rewards

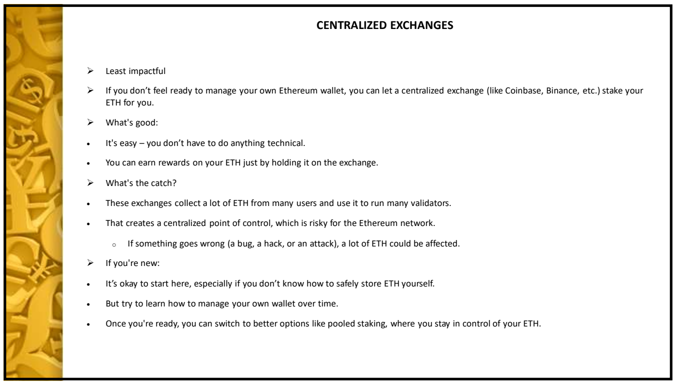
- Depending on which method of pooled staking is chosen, rewards also vary.

Risks

- Risks vary depending on the method used
- In general, risks consist of a combination of counter-party, smart contract and execution risk

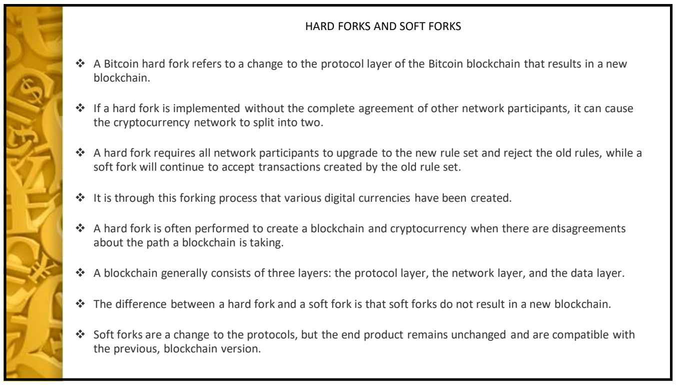
Requirements

- Lowest ETH requirements, some projects require as little as 0.01 ETH
- Deposit directly from your wallet to different pooled staking platforms or simply trade for one of the staking liquidity token



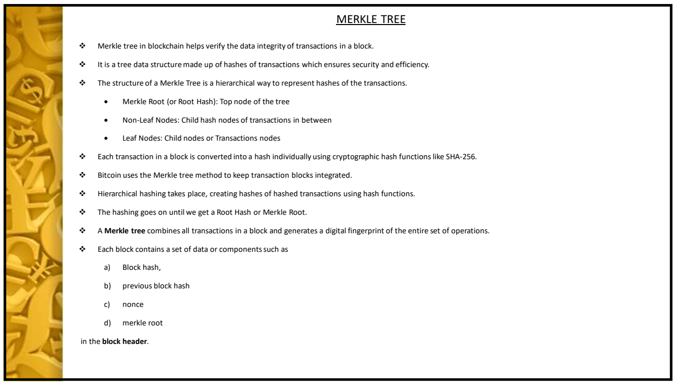
CENTRALIZED EXCHANGES

- ➢ Least impactful
- ➢ If you don't feel ready to manage your own Ethereum wallet, you can let a centralized exchange (like Coinbase, Binance, etc.) stake your ETH for you.
- ➢ What's good:
- It's easy – you don't have to do anything technical.
- You can earn rewards on your ETH just by holding it on the exchange.
- ➢ What's the catch?
- These exchanges collect a lot of ETH from many users and use it to run many validators.
- That creates a centralized point of control, which is risky for the Ethereum network.
  - o If something goes wrong (a bug, a hack, or an attack), a lot of ETH could be affected.
- ➢ If you're new:
- It's okay to start here, especially if you don't know how to safely store ETH yourself.
- But try to learn how to manage your own wallet over time.
- Once you're ready, you can switch to better options like pooled staking, where you stay in control of your ETH.



HARD FORKS AND SOFT FORKS

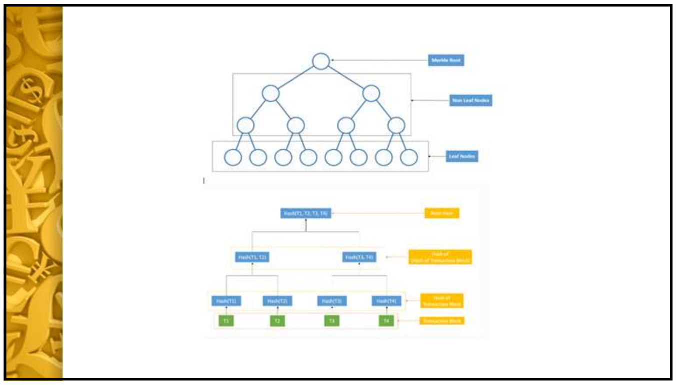
- ❖ A Bitcoin hard fork refers to a change to the protocol layer of the Bitcoin blockchain that results in a new blockchain.
- ❖ If a hard fork is implemented without the complete agreement of other network participants, it can cause the cryptocurrency network to split into two.
- ❖ A hard fork requires all network participants to upgrade to the new rule set and reject the old rules, while a soft fork will continue to accept transactions created by the old rule set.
- ❖ It is through this forking process that various digital currencies have been created.
- ❖ A hard fork is often performed to create a blockchain and cryptocurrency when there are disagreements about the path a blockchain is taking.
- ❖ A blockchain generally consists of three layers: the protocol layer, the network layer, and the data layer.
- ❖ The difference between a hard fork and a soft fork is that soft forks do not result in a new blockchain.
- ❖ Soft forks are a change to the protocols, but the end product remains unchanged and are compatible with the previous, blockchain version.

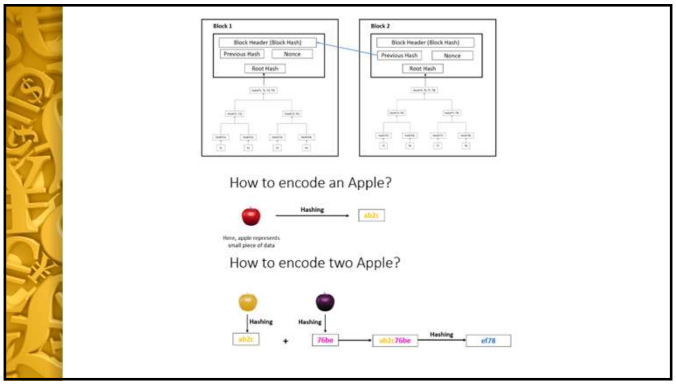


MERKLE TREE

- ❖ Merkle tree in blockchain helps verify the data integrity of transactions in a block.
- ❖ It is a tree data structure made up of hashes of transactions which ensures security and efficiency.
- ❖ The structure of a Merkle Tree is a hierarchical way to represent hashes of the transactions.
  - Merkle Root (or Root Hash): Top node of the tree
  - Non-Leaf Nodes: Child hash nodes of transactions in between
  - Leaf Nodes: Child nodes or Transactions nodes
- ❖ Each transaction in a block is converted into a hash individually using cryptographic hash functions like SHA-256.
- ❖ Bitcoin uses the Merkle tree method to keep transaction blocks integrated.
- ❖ Hierarchical hashing takes place, creating hashes of hashed transactions using hash functions.
- ❖ The hashing goes on until we get a Root Hash or Merkle Root.
- ❖ A **Merkle tree** combines all transactions in a block and generates a digital fingerprint of the entire set of operations.
- ❖ Each block contains a set of data or components such as
  - a) Block hash,
  - b) previous block hash
  - c) nonce
  - d) merkle root

in the **block header**.

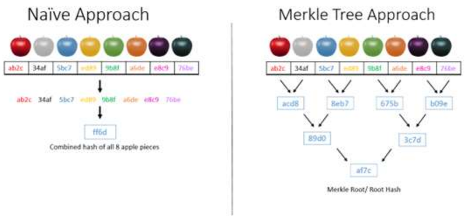




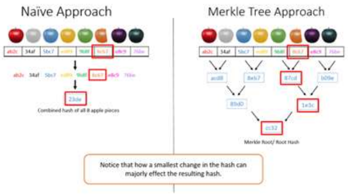
How to encode an Apple?

How to encode two Apple?

MERKLE TREE ENCRYPTION THE INFORMATION VS NORMAL ENCRYPTION OF INFORMATION

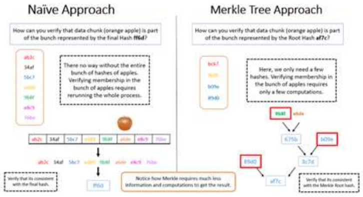


What if 1 apple got bitten by someone. How will it affect the hashes?



- Even if the smallest alteration happened to the data, it heavily reflects on the final hash.
- Mapping cryptography using a tree data structure helps in easy identification and verification.

How can you verify that the data chunk got corrupted?


Naïve Approach
How can you verify that data chunk (orange apple) is part of the bunch represented by the final Hash ff6d?
There no way without the entire bunch of hashes of apples. Verifying membership in the bunch of apples requires rerunning the whole process.
ab2c
34af
5bc7
9b8f
e8c9
76be
Verify that its consistent with the final hash.
ff6d
Notice how Merkle requires much less information and computations to get the result.
Merkle Tree Approach
How can you verify that data chunk (orange apple) is part of the bunch represented by the Root Hash af7c?
Here, we only need a few hashes. Verifying membership in the bunch of apples requires only a few computations.
b09e
89d0
9b8f
a6de
675b
b09e
89d0
3c7d
af7c
Verify that its consistent with the Merkle Root hash.

- In the above picture we can understand the difference –
- Suppose you have a basket of apples and you want to prove that a specific apple (orange apple) is really part of that basket.
- In the naïve approach , you need to show all the apples and combine all of them together to get the final hash (ff6d).
- But in the merkle tree approach, the apples are arranged in pairs and their hashes are combined step by step into a tree.
- You just need a few specific apples and hashes from the tree to check if the orange apple is really in the basket.
- You don't need to look at the whole basket anymore.