Blockchain and Cryptocurrency

What's Blockchain

- A shared, distributed and immutable ledger that facilitates the process of recording transactions and tracking assets in a peer-to-peer network.
- **Key Characteristics**:
  - Shared Distributed Ledger
  - Immutability
  - Decentralization
  - Append-Only
  - Security
  - Transparency
  - Peer-to-peer

The `Block` and The `Chain`

- **The Block**: A block is a list of transactions from a certain timeperiod. It contains all the information processed on the network within the past few minutes.
- **The Chain**: Each block is timestamped, placed in chronological order, and linked to the block before it using cryptographic algorithms.

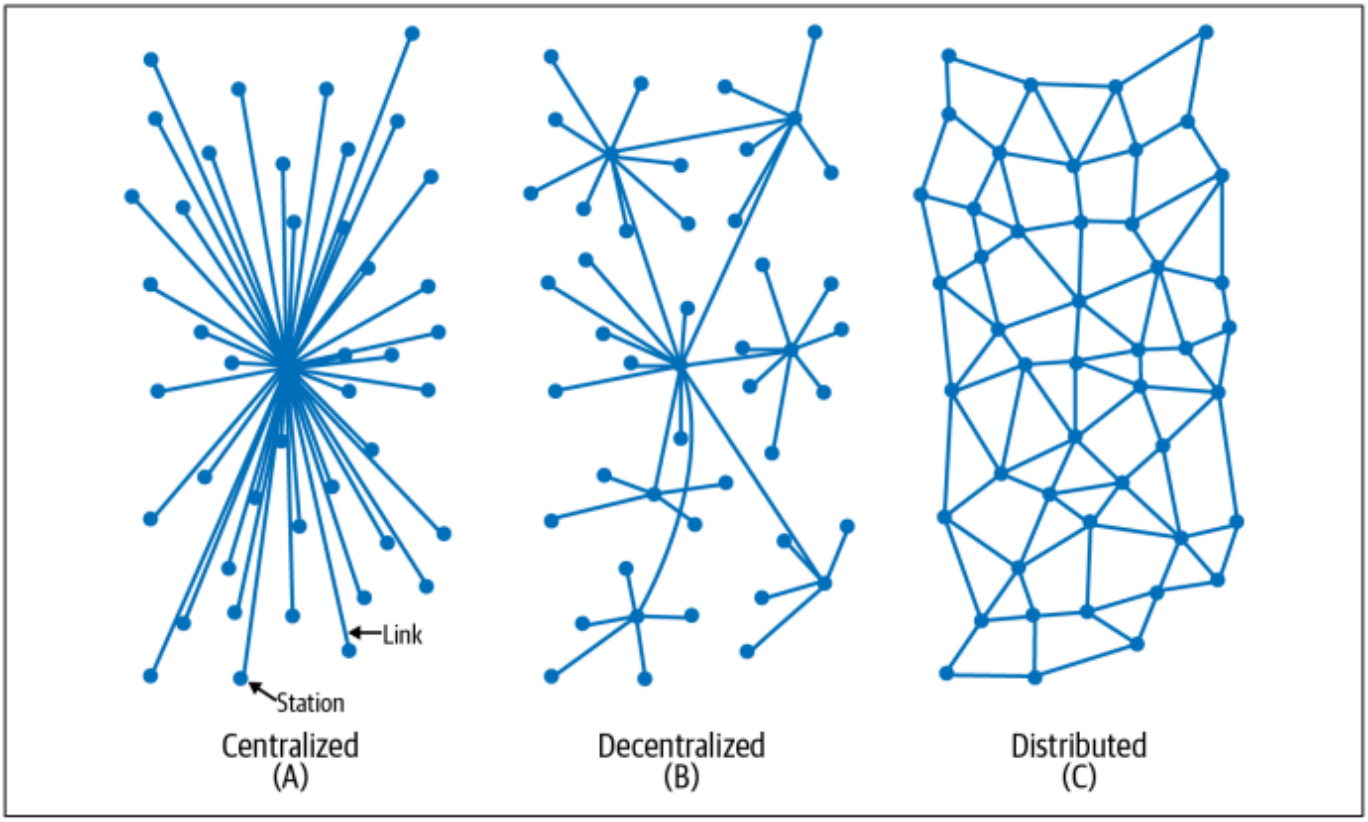
Distributed Ledgers

- It's where information about the accounts on the network is stored.
- An immutable record of all transactions on the network, a record that all network participants can access. With a shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.
- The first blockchain ledger, requires three pieces of information to `input`, `amount`, and `output`.

Distributed vs Centralized vs Decentralized

- **Distributed systems**:
  - Computation is shared across several computing resources.
  - These systems communicate with one another using some form of messaging.
  - The common goal is to use processing power to collectively accomplish a task by distributing responsibility across many computers.
  - Each node can maintain a replicated copy of the same data, each node knows the identity of other nodes, and all nodes are controlled by one entity.

- **Decentralized systems**:
    - Each node may not know the identify of other nodes, and all nodes are controlled by many entities who may be anonymous.
    - In a fully decentralized system, a given node does not necessarily collabo rate with every other node to achieve its objective, and decision making is done through some form of consensus rather than having this responsibility rest in the hands of a single entity.
- **Centralized systems**:
    - All nodes connect to a single, central node that is controlled by one entity.



Bitcoin

- “Bitcoin: A Peer-to-Peer Electronic Cash System,” the paper provided a detailed proposal for creating a value system that existed only on the internet.
- The Bitcoin proposal featured a number of ideas pulled from systems that preceded it. These included:
    - Secure digital transactions, like the smart contracts outlined by Nick Szabo
    - Using cryptography to secure transactions, like in DigiCash
    - The theoretical ability to send small amounts of secured value, as E-gold was able to do
    - The creation of money outside of governmental systems, as B-Money had proposed
    - Using proof-of-work to verify validity of digital funds, as Hashcash was designed to do
- Concepts introduced by the whitepaper:
    - Double spending
    - Proof of work
    - Hashes
    - Nonces

- Since there are no physical Bitcoins, we need to prove that we own n amount of Bitcoin by pointing the transaction where we received those n Bitcoins.

Why Blockchain Ledger?

- **Timestamping**: gives an approximate idea when a document came into existence. If the security property is satisfied, which is the timestamping can't be changed after the fact, it accurately conveys the order of creation of these documents.
- **Pointer**: it signs the document together with a link or a pointer to the previous document. It links to a piece of data instead of a location. That means that if the data in question changes, the pointer automatically become invalid.
- These properties ensure the integrity of the contents of the previous document. Each block essentially fixes the entire history of documents and blocks up until that point.
- In addition to using proof-of-work to secure the Bitcoin network, Satoshi proposed using a timestamp system to verify transactions, like filesystems and databases, uses a hash to store information is also key when preserving large amounts of information, and Opensource.

Three major components of Bitcoin

- **Value**: A unit of account, called bitcoin (often denoted as BTC), is used to record trans actions on the ledger, also known as the Bitcoin blockchain.
- **Distribution**: As the Bitcoin whitepaper outlines, the Bitcoin network uses decentralized nodes in order to maintain a record of transactions.
- **Consensus**: Miners in the Bitcoin network use proof-of-work together to maintain the security and stability of this distributed record of transactions.

Advantages and Disadvantages of Blockchain

- **Advantages**:
    - Decentralization
    - Security
    - Transparency
    - Immutability
    - Efficiency and speed
    - Cost reduction
    - Smart contracts
- **Disadvantages**:
    - Scalability
    - Energy consumption
    - Lack of regulation
    - Complexity

- Limited privacy
- Interoperability

Types of Blockchain

	Public	Private
Accessibility	Open to everyone	Restricted to a specific group of participants
Decentralization	Decentralized	Centralized
Permission	Permissionless	Permissioned
Transparency	Transactions are transparent and visible to all participants	Transactions are private and have restricted visibility
Security	The openness of the network allows for a high level of security through decentralization	The centralization allows for easier coordination and enforcement of security measures
Use-cases	Cryptocurrencies (like BTC and ETH), decentralized finance (DeFi), and open-access projects	Supply chain management, internal record-keeping

Proof of Work (PoW) vs. Proof of Stake (PoS)

- **Proof of Work (PoW)**:
  - In Proof of Work, participants compete to solve complex mathematical puzzles. The first one to solve the puzzle gets the right to add a new block to the blockchain and is rewarded with cryptocurrency.
  - Mining in PoW is computationally intensive and requires substantial computing power.
  - PoW systems, like the one used in Bitcoin, are known for their high energy consumption.
  - Considered highly secure because altering a block's information would require redoing all the work.
- **Proof of Stake (PoS)**:
  - In Proof of Stake, validators are chosen to create a new block and verify transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral.
  - PoS is more resource-efficient compared to PoW since it doesn't require the same level of computational power. Validators are chosen based on their stake in the network.
  - PoS is generally considered more environmentally friendly because it doesn't involve the energy-intensive mining process seen in PoW.
  - PoS relies on the economic incentive of validators not to cheat. Validators have something at stake (their cryptocurrency holdings), making malicious behavior economically irrational.

Other Types of Blockchains

- Permissionless Blockchain
- Permissioned Blockchain
- Federated (Consortium) Blockchain
- Hybrid Blockchain

Brief History of Blockchain

- 1991 -> 2008 -> 2009 -> 2013 -> 2015 -> 2018 -> 2020 -> Present

Layers of Blockchain Architecture

- The underlying structure and design of a blockchain network.
- It refers to the various components and layers that make up a blockchain and how they function together to enable the secure and transparent recording of transactions on a decentralized platform.
- **Layers**:
  - Application Layer (Layer 3) - provides the user interface.
  - Middleware Layer (Layer 2) - enables the integration of the blockchain with other systems.
  - Core Blockchain Layer (Layer 1) - consists of the decentralized ledger and the consensus mechanism.
  - Network Layer (Layer 0) - provides the underlying infrastructure for communication and data exchange.
- Layer 1 and Layer 2 crypto blockchain scaling solutions help increase the overall throughput another name for processing speed of a blockchain network, but may compromise the security of a blockchain.
- Layer 1 scaling includes updates to the block size, consensus mechanism, or database partition.
- Layer 2 scaling includes bundling transactions, processing in parallel, or handling transactions off chain.

Challenges of the Blockchain

- Scalability
- Interoperability
- Regulatory Uncertainity
- Privacy and Security
- Energy Consumption
- User Experience and Adoption
- Governance and Consensus

The Blockchain Trilemma

- The Blockchain Trilemma refers to the difficulty in simultaneously achieving three key properties of blockchain systems: decentralization, security, and scalability. It suggests that blockchain networks must navigate a three-way trade-off problem, where optimizing one or two properties inevitably comes at the expense of the third.

- **Decentralization**: Achieving high levels of decentralization often requires consensus mechanisms that involve all network participants, leading to slower transaction processing times and reduced scalability.
- **Security**: Increasing security may require sacrificing decentralization or scalability, as stronger security measures may centralize control or impose limitations on transaction throughput.
- **Scalability**: Scaling solutions, such as increasing block sizes or implementing off-chain transactions, can improve scalability but may compromise decentralization or security. For example, larger block sizes may increase centralization risks, while off-chain solutions may introduce security vulnerabilities.

Stakeholders or Participants of Blockchain

- Blockchain Users
- Miners/Validators
- Developers
- Node Operators
- Governance Entities
- Regulators and Policy Makers

Terminology

- Consensus Mechanisms
- Smart Contracts
- DAO's
- DApps

Chapter 2: Blockchain and Cryptocurrency

Important attributes of Bitcoin Block

- Block hash:
  - A unique identifier for the block.
  - Generated from input data that provides a `snapshot` of the current state of the blockchain within 256 bits of data. This `snapshot` is like a technical version of a balance sheet for the entire Bitcoin blockchain.
  - A Bitcoin block doesn't contain it's own block hash, but it does contain the hash of the previous block.
  - A block hash can be found by hashing the block header.
- Coinbase transaction:
  - This is the first transaction of each new block mined on the network.
  - It adds new bitcoin to the supply, which is given as a reward to the miner who adds the block to the chain.
- Block height number:
  - This number identifies how many blocks there are between the current block and the first block in the chain (also known as the Genesis block).

- Merkle root:
  - This is a hash that allows proof of the validity of the blockchain.

Why is it hard to cheat in Bitcoin?

- Suppose we are working on a `block b` and we want to alter transaction in `block a`, We had to redo all the computations for blocks a-b before everybody else in the Bitcoin network finished the one block (block b).

Hashes

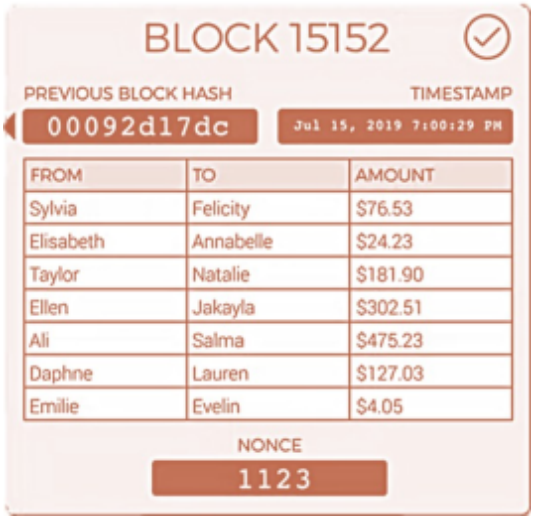
- A function that converts any form of data into a fixed string.
- A one way encryption (easy to encrypt).
- Extremely difficult, if not impossible, to decrypt the hash back to the original input data.
- A hash is `deterministic` (every time the same input data is entered, the resulting hash will always be the same).
- Easy to compare.
- `Collision resistant` (extremely unlikely to find two different input values that yield the same hash value).
- Most common hashes are:
  - `SHA-256` -> commonly used by `Bitcoin`.
  - `Keccak-256` -> commonly used by `Ethereum`.

Block Hashes

- A snapshot of what the entire blockchain looked like at the moment that block was created.
- In accounting terms, it's like a balance sheet for the entire network.
- Every node in the network refers to the block hash to verify that its view of the network is the exact same as everyone else's.
- This is what makes blockchain `tamper-evident`; if the content experiences tampering or corruption, the resulting hash will no longer be the same.

Conceptual view of the Block

- `First Metadata` -> reference to a previous block hash.
- `Second Metadata` -> timestamp and nonce.
- `Third Metadata` -> `merkle tree root`, a data strucutre used to efficiently summarize all the transactions in the block.
- The Block's body will store the transactions and their hashes.
- Block Header:
  - `hashPrevBloc` -> a snapshot of what the Bitcoin network looked like in the previous block.
  - `hashMerkleRoot` -> a snapshot of all the transactions included in the current block.



Field	Description	Size (bytes)
Version	Block version number	4
`hashPrevBlock`	256-bit hash of the previous block header	32
`hashMerkleRoot`	256-bit hash based on all of the transactions in the current block	32
Time	Current block timestamp as seconds since 1970-01-01T00:00 UTC	4
Bits	Current target in compact format	4
Nonce	32-bit number (starts at 0)	4

Transactions

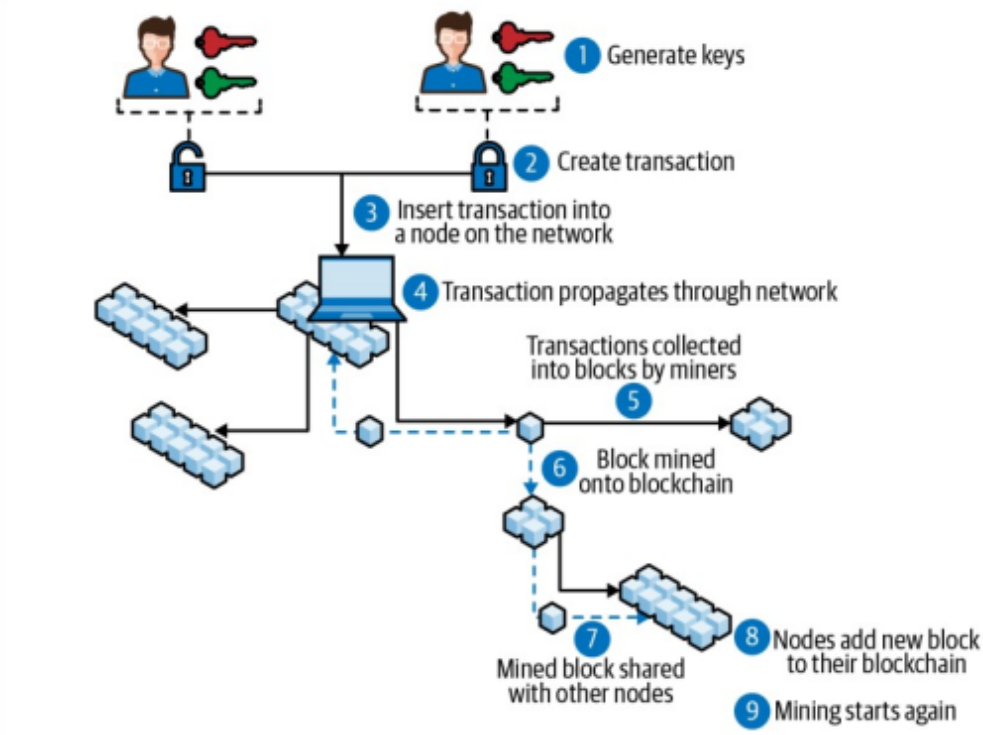
- Bitcoin transactions follow a unique type of accounting called `UTXO`, which stands for `Unspent Transaction Output`.
- UTXO Model:
  - A transaction is basically a list of inputs and a list of outputs.
  - Each input identifies a Bitcoin address that is acting as the source of funds, plus an unspent transaction that address has received in the past.
  - It also contains a digital signature proving that the owner of that address has authorized the transaction.
  - Each output identifies the Bitcoin address receiving the funds and the amount that address will receive.
  - The difference between the input and the output is the `transaction fee`, which will be earned by the `bitcoin miner`.
- Anatomy of Transaction:

Field	Description
Version no.	4 bytes. Identifies which protocol version the node generating the transaction is using (currently 1).
Flag	If the flag is present, showing a value of 0001, then the node is using Segregated Witness (SegWit), which removes signature information from the transaction.
In-counter	The number of inputs.
List of inputs	List of input data.
Out-counter	The number of outputs.
List of outputs	List of output data.
Witnesses	If using SegWit, then this field shows a list of witnesses.
Lock time	4 bytes. If this field is not empty, it identifies the earliest time that the transaction can be added to the blockchain as determined by the network. This field can be represented as either a block height or a Unix-like timestamp.

- Transaction Fees:
  - Bitcoin transaction fees can vary depending on network capacity, how quickly confirmation is needed, and other factors.
  - Because there is a limit on the number of transactions that can be recorded on a block (the current limit is 1 MB of data, or roughly 3,500 transactions per block) a higher fee may be required for greater urgency.

- There is essentially a competition in place for getting miners to confirm a transaction: higher fees mean faster confirmation.

Events involved in executing a bitcoin transaction



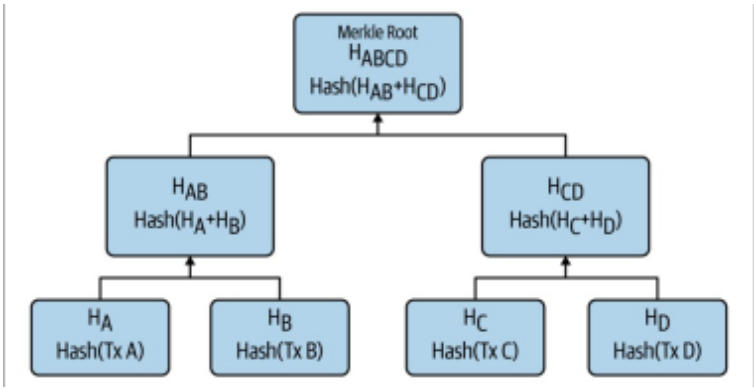
Bitcoin Address

- The Bitcoin address is a translation of the `public key` and is the identity of the wallet where funds can be received and from which they can be sent to other addresses.
- This address can be shared with anybody for receiving and sending.
- The private key is kept secret and is used to unlock stored cryptocurrency.
- Bitcoin private keys are used to digitally sign transactions. That's how the owner of a Bitcoin address proves to the Bitcoin network that they are the rightful owner of that address, and how they authorize a transaction.

Merkle Root

- The Merkle root is used to show a snapshot of the state of all the transactions in the current block, stored in just 256 bits.
- The Merkle root has a special purpose aside from capturing the transaction snapshot. When a node in the network wants to ensure it has the exact same list of transactions as every other node, it does not need to compare each transaction individually.
- Instead, it only needs to compare its Merkle root with every other node's Merkle root. This allows for the building of light software clients that do not require storing the entire blockchain to validate their own transactions.
- To calculate the Merkle root, you first create a Merkle tree, where the leaves are the transactions in the current block. By moving up the Merkle tree and generating hashes of all the leaves, you eventually reach the Merkle root.
- If the number of transactions is odd, then the last transaction is replicated in order to continue this process.

- The Merkle root is an important value that helps to generate the block hash.

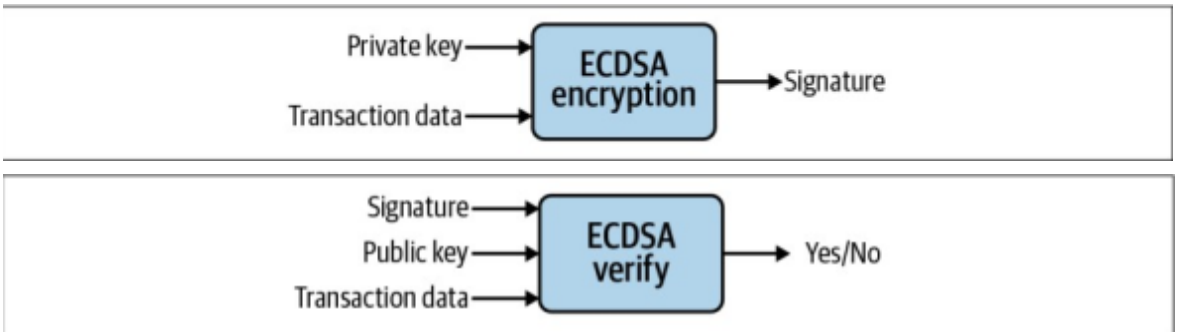


$$HA + HB => SHA256(SHA256(HA + HB))$$

- Merkle root can be used to quickly detect tampering in blockchain nodes. If there has been any tampering or corruption of transactions in the blockchain on any given node, its Merkle root hash will no longer match that of the other nodes.

Signing and Validating Transactions

- Each transaction input contains a signature that provides proof that the owner of the sending address has authorized the transaction. The signature is generated and encrypted using `ECDSA`, a cryptographic algorithm that takes the private key and transaction data as inputs.



The Coinbase Transaction

- The first transaction recorded on every block.
- Made up of:
  - Block reward:
    - This is the `reward` a miner receives from the network for performing the work to `discover a block` and doing their part to provide procesing power to the Bitcoin network.
    - The reward comes in the form of `new bitcoin` being added to the world supply.
  - Transaction fees:
    - The sum of all the transaction fees that are included in each transaction that gets added to the current block.
    - There are often more transactions waiting to be processed than can fit into a block, generating a marketplace for transaction fees.
    - The faster the miner wants a transaction to be processed, the higher the fee.

Transaction Security

- Bitcoin transactions are `push transactions`, meaning that the sender is the one pushing the funds out of an account (the one to initiate the transaction).
- In contrast, a `pull transaction` is initiated by the receiver and they are significantly less secure because they require the sender to share their account details with the receiver. To compensate for this weakness, pull payment networks (like Visa) provide chargebacks, or the ability to dispute a transaction and ask for a refund.
- When initiating a Bitcoin transaction, a sender never has to reveal any of their account information. The only way a fraudulent transaction can take place is if an unauthorized person gets a copy of someone's private key.

Transaction's Lifecycle

- Broadcast:
  - The first step is generating a valid bitcoin transaction and then broadcasting the transaction details to the Bitcoin network.
- Unconfirmed/Mempool:
  - As every miner in the network receives the transaction, it places that transaction into its `memory pool`, or `mempool`.
  - The mempool is a collection of all the bitcoin transactions that are in an `unconfirmed state` and are still considered `active`.
  - By default, if a transaction has been sitting in the mem- pool for more than two weeks, it is considered inactive and is dropped from the mempool.
- Confirmed by Miner:
  - When a miner discovers a new block, the miner decides which transactions to include in that block, choosing from transactions that are sitting in the mempool.
  - Miners choose transactions in order of transaction fees, starting with the highest ones.
  - A transaction is considered confirmed by a miner when that miner adds a block containing that transaction to its blockchain.
- Confirmed by the Network:
  - As a block is buried under newer blocks, the chances that the Bitcoin network has achieved consensus to include that block increase.
  - A transaction is considered safely confirmed by the network when that transaction has reached at least six confirmations.

Consensus

- Consensus is a way of reaching agreement between various participants who have shared values and goals, and it is an important component of how blockchain networks succeed.
- Unlike centralized payments like PayPal, decentralized network like Bitcoin has no central authority that updates it's ledgar when new transactions are added. Gaining the trust of updating Bitcoin's blockchain with a new block of transactions is called `achieving consensus`.

- `Achieving consensus` is a process that all the miners powering the network to use for the following two purposes:
  - `Block discovery` - To agree on which miner gets the right to add a block of transactions.
  - `Validation of transactions` - To agree that the transactions included in that new block are legitimate.

Hashing Vs Encryption

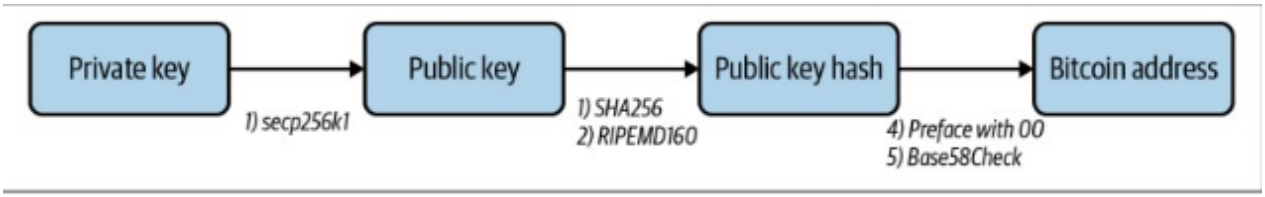
Encryption	Hashing
Process of converting plaintext to cipher text using an algorithm and a key	One-way mathematical function that converts input data into fixed size string of characters
Primary goal is confidentiality	Primary goal are integrity and verification
Reverisible	Irreversible
Involves key management for secure key exchange	Doesn't require keys
Used for securing communication and data storage	Used for data integrity, password storage, and digital signature

Properties of secure Hash Function

- **Collision resistance**:
  - A `collision` occurs when two distinct inputs produce the same output.
  - A hash function H(.) is collision-resistant if it's infeasible to find two values x and y such that $H(x) = H(y)$.
  - Collision-detection algorithm works for every hash function. But, of course, the problem with it is that this takes a very, very long time to do. For a hash function with a 256-bit output, you would have to compute the hash function 2^{256+1} times in the worst case, and about 2^{128} times on average.
- **Hiding**:
  - If we're given the output of the hash function $y = H(x)$, there's no feasible way to figure out what the input, x, was.
  - A hash function H is hiding if: when a secret value r is chosen from a probability distribution that has high `min-entropy` (low predictability), then given $H(r \| x)$ it is infeasible to find x.
- **Puzzle friendliness**:
  - A hash function H is said to be puzzle-friendly if for every possible n-bit output value y, if k is chosen from a distribution with `high min-entropy` , then it is infeasible to find x such that $H(k \| x) = y$ in time significantly less than 2^n.

Cryptography in Bitcoin

- Private keys:
  - 256-bit, hexadecimal, and randomly chosed key.
  - Used to digitally sign bitcoin transactions, which is the way the owner of a Bitcoin address proves to the network that they are the rightful owner of that address.
  - Private keys authorize a transaction.
- Public keys:
  - Used to generate a Bitcoin address.
  - The address is essentially a compressed version of the public key, making it somewhat easier to read.
  - A Bitcoin address is a value that can be shared publicly with anyone, usually when asking someone to send bitcoin.
  - Generated by running the `private key` through an `ECDSA secp256k1` function.
  - A `public key hash` is then generated by running the public key through the cryptographic `SHA256` and `RIPEMD160` functions.
  - The Bitcoin address is generated by first adding `00` to the public key hash and then running that value through a `Base58Check` function.



Digital Signature

- A digital signature scheme consists of the following three algorithms:
  - `(sk, pk) := generateKeys(keysize)`:
    - The `generateKeys` method takes a `key size` and generates a `key pair`.
    - The secret key `sk` is kept privately and used to sign messages. `pk` is the public verification key that you give to everybody. Anyone with this key can verify your signature.
  - `sig := sign(sk, message)`:
    - The sign method takes `a message` and a `secret key`, `sk`, as input and outputs a signature for message under `sk`.
  - `isValid := verify(pk, message, sig)`:
    - The verify method takes a `message`, a `signature`, and a `public key` as input.
    - It return a boolean value true, if `sig` is a valid signature for message under public key `pk`, and false otherwise.
- We require that the following two properties hold:
  - Valid signatures must verify -> `(pk, message, sign(sk, message)) == true`
  - Signatures are existentially unforgetable

Chapter 3: Consensus

What's Consensus?

- A process of agreement between distrusting nodes on the final state of data.
- Consensus is the backbone of a blockchain and, as a result, it provides decentralization of control through an optional process known as `Mining`.
- The choice of the Consensus Algorithm is also governed by the type of blockchain in use; that is, not all consensus mechanisms are suitable for all types of blockchains.

Consensus Mechanism

- A set of steps that are taken by most or all nodes in a blockchain to agree on a proposed state or value.
- **Requirements**:
  - **Agreement**: All honest nodes decide on the same value.
  - **Termination**: All honest nodes terminate execution of the consensus process and eventually reach a decision.
  - **Validity**: The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node.
  - **Fault tolerant**: The consensus algorithm should be able to run in the presence of faulty or malicious nodes (Byzantine nodes).
  - **Integrity**: This is a requirement that no node can make the decision more than once in a single consensus cycle.
- **Types**:
  - **Traditional Byzantine Fault Tolerance (BFT)-based**:
    - With no compute-intensive operations, such as partial hash inversion (as in Bitcoin PoW), this method relies on a simple scheme of nodes that are publisher-signed messages.
    - Eventually, when a certain number of messages are received, then an agreement is reached.
    - Also known as `consortium` or `permissioned` type of consensus mechanism.
  - **Leader election-based**:
    - Also known as `proof-based` `lottery-based`, or `Nakamoto` consensus.
    - This arrangement requires nodes to compete in a leader election lottery, and the node that wins proposes a final value.
    - `Fully decentralized` or `permissionless` type of consensus mechanism.
    - PoW used in Bitcoin fails into this category.

Consensus in Blockchain

- Consensus is a distributed computing concept that has been used in blockchain in order to provide a means of agreeing to a single version of the truth by all peers on the blockchain network.

- `BFT-based` consensus mechanisms perform well when there are a limited number of nodes, but they do not scale well.
- On the other hand, `leader-election lottery based (PoW)` type consensus mechanisms scale very well but perform very slowly.

Consensus Algorithms

- **Proof of Work (PoW)**:
  - This type of consensus mechanism relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network.
  - Used in `Bitcoin` and `Litecoin`.
  - The only algorithm that has proven to be astonishingly successful against any collusion attacks on a blockchain network, such as the Sybil attack.
- **Proof of Stake**:
  - This algorithm works on the idea that a node or user has an adequate stake in the system; that is, the user has invested enough in the system so that any malicious attempt by that user would outweigh the benefits of performing such an attack on the network.
  - Used in `Ethereum`.
  - `Coin age` a criterion derived from the amount of time and number of coins that have not been spent. In this model, the chances of proposing and signing the next block increase with the coin age.
- **Delegated Proof of Stake (DPoS)**:
  - This is an innovation over standard PoS, whereby each node that has a stake in the system can delegate the validation of a transaction to other nodes by voting.
  - Used in `Bitshares` Bitcoin.
- **Proof of Elapsed Time (PoET)**:
  - Introduced by Intel in 2016, PoET uses a `Trusted Execution Environment (TEE)` to provide randomness and safety in the leader election process via a guaranteed wait time.
- **Proof of Deposit (PoD)**:
  - In this case, nodes that wish to participate in the network have to make a security deposit before they can mine and propose blocks.
  - Used in the `Tendermint` blockchain.
- **Proof of Importance (PoI)**:
  - Relies on how large a stake a user has in the system, but it also monitors the usage and movement of tokens by the user in order to establish a level of trust and importance.
- **Federated consensus or federated Byzantine consensus**:
  - Used in the `stellar consensus protocol`.
  - Nodes in this protocol retain a group of publicly-trusted peers and propagate only those transactions that have been validated by the majority of trusted nodes.
- **Reputation-based mechanisms**:
  - A leader is elected by the reputation it has built over time on the network.
  - It is based on the votes of other members.
- **PBFT**: This mechanism achieves state machine replication, which provides tolerance against Byzantine nodes.

- **Proof of Activity (PoA)**:
  - This scheme is a combination of PoS and PoW, which ensures that a stakeholder is selected in a pseudorandom but uniform fashion.
  - This is a comparatively more energy-efficient mechanism as compared to PoW.
  - It utilizes a new concept called `Follow the Satoshi` which combines PoW and PoS together to achieve consensus and good level of security.
- **Proof of Capacity (PoC)**:
  - This scheme uses hard disk space as a resource to mine the blocks which is different from PoW, where CPU resources are used.
  - In in PoC, hard disk space is utilized for mining and as such is also known as `hard drive mining`.
- **Proof of Storage (PoS)**:
  - This scheme allows for the outsourcing of storage capacity.
  - This scheme is based on the concept that a particular piece of data is probably stored by a node which serves as a means to participate in the consensus mechanism.

CAP Theorem

- Also known as `Brewer's` theorem.
- States that any distributed system cannot have `consistency`, `avaliability`, and `partition tolerance` simultaneously.
- `Consistency` : is a property which ensures that all nodes in a distributed system have a single, current, and identical copy of the data.
- `Availability` : means that the nodes in the system are up, accessible for use, and are accepting incoming requests and responding with data without any failures as and when required.
- `Partition tolerance` : ensures that if a group of nodes is unable to communicate with other nodes due to network failures, the distributed system continues to operate correctly. This can occur due to network and node failures.

How Blockchain manages to achieve all of CAP properties

- To achieve fault tolerance, replication is used. This is a standard and widely-used method to achieve fault tolerance.
- Consistency is achieved using consensus algorithms in order to ensure that all nodes have the same copy of the data. This is also called state machine replication.
- Strangely, it seems that the CAP theorem is violated in the blockchain, especially in its most successful implementation, `Bitcoin`.
- However, this is not the case. In blockchains, consistency is sacrificed in favour of availability and partition tolerance.

State Machine Replication

- In general, there are two types of faults that a node can experience:
  - `Fail-stop fault` :
    - This type of fault occurs when a node merely has crashed.

        - Easier ones to deal with of the two fault types.
    - `Byzantine faults`:
        - The faulty node exhibits malicious or inconsistent behaviour arbitrarily.
        - Difficult to handle since it can create confusion due to misleading information.
        - This can be a result of an attack by adversaries, a software bug, or data corruption.
- In this scenario, Consistency © on the blockchain is not achieved simultaneously with Partition tolerance § and Availability (A), but it is achieved over time. This is called `Eventual Consistency`, where consistency is achieved as a result of validation from multiple nodes over time. The concept of mining was introduced in Bitcoin for this purpose.

Mining

- A process that facilitates the achievement of consensus by using the PoW consensus algorithm.
- A process that is used to add more blocks to the blockchain.
- New coins are minted by the miners by solving the PoW problem, also known as `partial hash inversion problem`. This process consumes a high amount of resources including computing power and electricity.
- This process also secures the system against frauds and double spending attacks while adding more virtual currency to the Bitcoin ecosystem.

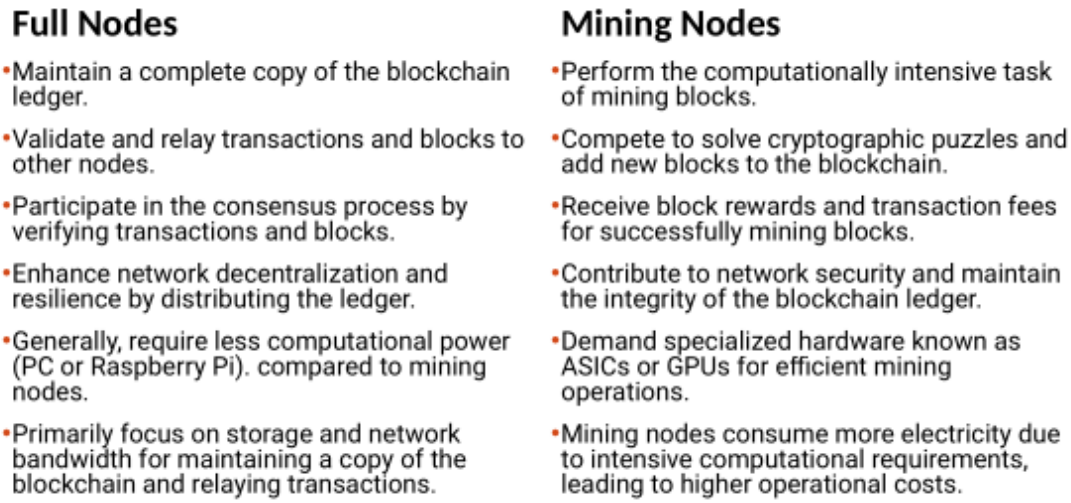
Mining the Block

- When a candidate block has been constructed by a node, it is time for the hardware mining rig to “mine” the block, to find a solution to the Proof-of-Work algorithm that makes the block valid.
- The hash function `SHA256` is the function used in bitcoin’s mining process.
- You can take Mining as the process of hashing the block header repeatedly, changing one parameter, until the resulting hash matches a specific target.
- The hash function’s result cannot be determined in advance, nor can a pattern be created that will produce a specific hash value.
- This feature of hash functions means that the only way to produce a hash result matching a specific target is to try again and again, randomly modifying the input until the desired hash result appears by chance.

Tasks of the Miners

- Synching up with the network.
- Transaction validation.
- Block validation.
- Create a new block.
- Perform Proof of Work.
- Fetch reward.

Full Nodes vs Mining Nodes



Bitcoin Mining

- Roughly one new block is created (mined) every 10 minutes to control the frequency of generation of bitcoins. This frequency needs to be maintained by the Bitcoin network and is encoded in the bitcoin core clients in order to control the money supply.
- Miners are rewarded with new coins if and when they discover new blocks by solving PoW. Miners are paid transaction fees in return for including transactions in their proposed blocks.
- The rate of creation of new bitcoins decreases by 50% (Halving), every 210,000 blocks, roughly every 4 years. When bitcoin was initially introduced in 2009, the block reward was 50 bitcoins.
- Approximately 144 block per day, that is, 450 bitcoins are generated per day with the current 3.125 block reward per day. The number of actual coins can vary per day; however, the number of blocks remains at 144 per day.
- Bitcoin supply is also limited and in 2140, almost 21 million bitcoins will be finally created and no new bitcoins can be created after that. Bitcoin miners, however, will still be able to profit from the ecosystem by charging transaction fees.

Proof of Work

- A proof that enough computational resources have been spent in order to build a valid block.
- It is based on the idea that a random node is selected every time to create a new block. In this model, nodes compete with each other in order to be selected in proportion to their computing capacity.

$$H(N||P_{hash}||Tx||Tx||...Tx) < Target$$

- Where `N` is a nonce, `P_hash` is a hash of the previous block, `Tx` represents transactions in the block, and `Target` is the target network difficulty value.

- This means that the hash of the previously mentioned concatenated fields should be less than the target hash value.
- The only way to find this nonce is the brute force method. Once a certain pattern of a certain number of zeroes is met by a miner, the block is immediately broadcasted and accepted by other miners.

Steps in the mining algorithm

- The previous block's header is retrieved from the bitcoin network.
- Assemble a set of transactions broadcasted on the network into a block to be proposed.
- Compute the double hash of the previous block's header combined with a nonce and the newly proposed block using the SHA-256 algorithm.
- Check if the resultant hash is lower than the current difficulty level (target) then PoW is solved. As a result of successful PoW the discovered block is broadcasted to the network and miners fetch the reward.
- If the resultant hash is not less than the current difficulty level (target), then repeat the process after incrementing the nonce.
- Mining difficulty increased over time and bitcoins that could be mined by single CPU laptop computers now require dedicated mining centers to solve the hash puzzle.
- Difficulty indicates how difficult it is to find a hash which is lower than the network difficulty target. All successfully mined blocks must contain a hash that is less than this target number. This number is updated every 2 weeks or 2016 blocks to ensure that on average 10-minute block generation time is maintained.

Target, Difficulty & Hash rate

- All a miner has to do is discover a new block and generate a Bitcoin block hash that is considered valid by the network, using the following criteria:
  - It is a hash of a valid block header.
  - The resulting block hash is a number that is lower than the current network target.
- `Target` is a constantly changing number that must always be higher than a valid block hash.
- `Difficulty` is the average number of attempts required to discover a valid block hash.
- `Network hash rate` refers to how many times per second the miners in the network collectively attempt to generate a valid block hash.
- The Proof-of-Work must produce a hash that is less than the Target. A higher target means it is less difficult to find a hash that is below the target. A lower target means it is more difficult to find a hash below the target. The target and difficulty are inversely related.
- The Hashing Rate basically represents the rate of calculating hashes per second. In other words, this is the speed at which miners in the Bitcoin network are calculating hashes to find a block.

Difficulty Adjustment

- The idea behind difficulty regulation in bitcoin is that a generation of 2016 blocks should take roughly around two weeks (inter-block time should be around 10 minutes).
- If it takes longer than two weeks to mine 2016 blocks, then the difficulty is decreased, and if it takes less than two weeks to mine 2016 blocks, then the difficulty is increased.
- When ASICs were introduced due to a high block generation rate, the difficulty increased exponentially, and that is one drawback of PoW algorithms that are not ASIC resistant. This leads to mining power centralization.
- This also poses another problem; if a new coin starts now with the same PoW based on SHA-256 as bitcoin uses, then it would be easy for a malicious user to just simply use an ASIC miner and control the entire network.
- Also, multipools pose a more significant threat where a group of miners can automatically switch to the currency that is becoming profitable. This phenomenon is known as `pool hopping`.
- Pool hopping impacts the network adversely because pool hoppers join the network only when the difficulty is low and they can gain quick rewards; the moment difficulty goes up (or is readjusted) they hop off and then come back again when the difficulty is adjusted back.

Mining Systems

- As the core principle behind mining is based on the double SHA-256 algorithm, overtime experts have developed sophisticated systems to calculate the hash faster and faster.
- `CPU`, `GPU`, `FPGA – Field Programmable Gate Array (FPGA)` and `ASIC Mining - Application Specific Integrated Circuit (ASIC)`.

Mining Pools

- A mining pool forms when group of miners work together to mine a block. The pool manager receives the coinbase transaction if the block is successfully mined, which is then responsible for distributing the reward to the group of miners who invested resources to mine the block.
- **Models**:
  - Pay Per Share (PPS) model:
    - the mining pool manager pays a flat fee to all miners who participated in the mining exercise.
  - Proportional model:
    - the share is calculated based on the amount of computing resources spent to solve the hash puzzle.
- Mining centralization can occur if a pool manages to control more than 51% of the network by generating more than 51% hash rate of the Bitcoin network.
- Successful blocks pay the reward to a pool bitcoin address, rather than individual miners. The pool server will periodically make payments to the miners' bitcoin addresses, once their share of the rewards has reached a certain threshold. Typically, the pool server charges a percentage fee of the rewards for providing the pool-mining service.

- Miners participating in a pool split the work of searching for a solution to a candidate block, earning “shares” for their mining contribution.
- The mining pool sets a higher target (lower difficulty) for earning a share, typically more than 1,000 times easier than the bitcoin network’s target. When someone in the pool successfully mines a block, the reward is earned by the pool and then shared with all miners in proportion to the number of shares they contributed to the effort.
- Most mining pools are “managed,” meaning that there is a company or individual running a pool server. The owner of the pool server is called the `pool operator`.

Peer-to-peer mining pool (P2Pool)

- In 2011, to resolve these issues of pool centralization, a new pool mining method was proposed and implemented: P2Pool, a peer-to-peer mining pool without a central operator.
- `P2Pool` works by decentralizing the functions of the pool server, implementing a parallel blockchain-like system called a `share chain`.
- A share chain is a blockchain running at a lower difficulty than the bitcoin blockchain. The share chain allows pool miners to collaborate in a decentralized pool by mining shares on the share chain at a rate of one share block every 30 seconds.
- Each of the blocks on the share chain records a proportionate share reward for the pool miners who contribute work, carrying the shares forward from the previous share block.
- When one of the share blocks also achieves the bitcoin network target, it is propagated and included on the bitcoin blockchain, rewarding all the pool miners who contributed to all the shares that preceded the winning share block.
- Essentially, instead of a pool server keeping track of pool miner shares and rewards, the share chain allows all pool miners to keep track of all shares using a decentralized consensus mechanism like bitcoin’s blockchain consensus mechanism.

Consensus Attacks

- If a miner or group of miners can achieve a significant share of the mining power, they can attack the consensus mechanism so as to disrupt the security and availability of the bitcoin network.
- It is important to note that consensus attacks can only affect future consensus, or at best, the most recent past (tens of blocks). Bitcoin’s ledger becomes more and more immutable as time passes.
- Consensus attacks also do not affect the security of the private keys and signing algorithm (ECDSA) and cannot steal bitcoin, spend bitcoin without signatures, redirect bitcoin, or otherwise change past transactions or ownership records. It only affect the most recent blocks and cause denial-of-service disruptions on the creation of future blocks.

The 51% Attack

- In this scenario a group of miners, controlling a majority (51%) of the total network’s hashing power, collude to attack bitcoin. If, somehow, an attacker were able to amass 51% of the mining

power on a blockchain, the attacker could feasibly create phony transactions.
- On major blockchains today, a 51% attack is highly unlikely. Established, valuable currencies already have tens of thousands of miners with incredible amounts of computing power. In order to gain 51% of the computing power on the mining network, you'd need to invest millions of dollars in hardware.
- A 51% attack can result in successful double-spending attacks, and it can impact consensus and in fact impose another version of transaction history on the Bitcoin network.
- Theoretical solutions, such as two-phase PoW have been proposed in academia to disincentivize large mining pools. This scheme introduces a second cryptographic puzzle that results in mining pools to either reveal their private keys or provide a considerable portion of the hash rate of their mining pool, thus reducing the overall hash rate of the pool.

Proof of Stake (PoS)

- Also known as `virtual mining`.
- In this scheme, the idea is that users are required to demonstrate possession of a certain amount of currency (coins) thus proving that they have a stake in the coin.
- The simplest form of the stake is where mining is made comparatively easier for those users who demonstrably own larger amounts of digital currency.
- **Benefits**:
  - Acquiring large amounts of digital currency is relatively difficult as compared to buying high-end ASIC devices.
  - Results in saving computational resources.
- **Types**:
  - Proof of Coinage:
    - The age of a coin is the time since the coins were last used or held. This is a different approach from the usual form of PoS where mining is made easier for users who have the highest stake in the altcoin. The miner is rewarded for holding and not spending coins for a period of time.
  - Proof of Deposit (PoD):
    - The core idea behind this scheme is that newly minted blocks by miners are made unspendable for a certain period. More precisely the coins get locked for a set number of blocks during the mining operation. The scheme works by allowing miners to perform mining at the cost of freezing a certain number of coins for some time.
  - Proof of Burn (PoB):
    - PoB, in fact, destroys a certain number of coins to get equivalent altcoins. This is commonly used when starting up a new coin projects as a means to provide a fair initial distribution. This can be considered an alternative mining scheme where the value of the new coins comes from the fact that previously a certain number of coins have been destroyed.

Chapter 4: Blockchain Applications

Banking and Insurance

- `Central Bank Digital Currencies (CBDCs)`:
  - Digital forms of a country's fiat currency.
  - Instead of requiring intermediaries or third parties like banks, CBDCs could enable real-time payments directly between parties.
  - While CBDCs may use existing databases for implementation, there is consideration of deploying blockchain or distributed ledger technologies.
- `Cross-Border Payments`:
  - This can be a long-complicated process and it can take many days for the money to arrive at its destination.
  - Blockchain has helped in simplifying these cross-border payments by providing end-to-end remittance services without any intermediaries.
- `Asset Management`:
  - Asset management involves the handling and exchange of different assets that an individual may own such as fixed income, real estate, equity, mutual funds, commodities, and other alternative investments.
  - Normal trading processes in asset management can be very expensive, especially if the trading involves multiple countries and cross-border payments.
  - In such situations, Blockchain can be a big help as it removes the need for intermediaries such as brokers, custodians, brokers, settlement managers.
- `Insurance`:
  - Blockchain technology can help to stop fradulent claims, increase the speed of claim processing, and enable transparency.

Government

- Government or electronic government is a paradigm where information and communication technology are used to deliver public services to citizens.
- Many governments are researching the possibility of using blockchain technology for managing and delivering public services including but not limited to `identity cards`, `driving licenses`, `secure data sharing` among various government departments and contract management.
- `Blockchain-based` voting systems can resolve traditional election issues by introducing end-to-end security and transparency in the process.

Digital Identity

- A blockchain-based online digital identity allows control over personal information sharing.
- Users can see who used their data and for what purpose and can control access to it.

- The key benefit is that a single identity issued by the government can be used easily and in a transparent manner for multiple services via a single government blockchain.

Healthcare

- With the adaptability of blockchain in the health sector, several benefits can be realized, ranging from `cost saving`, `increased trust`, `faster processing of claims`, `high availability`, `no operational errors` due to complexity in the operational procedures, and preventing the distribution of counterfeit medicines.
- Blockchains can also be used to provide processing power to solve scientific problems that can help to find cures for certain diseases.

IoT

- The usual IoT model is based on a centralized paradigm where IoT devices usually connect to a cloud infrastructure or central servers to report and process the relevant data back. This centralization poses certain possibilities of exploitation including hacking and data theft.
- Blockchain for IoT can help to build trust, reduce costs, and accelerate transactions.

Media

- Blockchain can provide a network where digital music is cryptographically guaranteed to be owned only by the consumers who pay for it.
- This payment mechanism is controlled by a smart contract instead of a centralized media agency or authority.
- The payments will be automatically made based on the logic embedded within the smart contract and number of downloads.

Supply Chain Management

- Blockchain technology coupled with the ability to program business logic with the use of smart contracts enables the following:
  - Transparency into the provenance of consumer goods from the source point to end consumption.
  - Accurate asset tracking.
  - Enhanced licensing of services, products, and software.
- Supply chains contain complex networks of suppliers, manufacturers, distributors, retailers, auditors, and consumers.
- A blockchain's shared IT infrastructure would streamline workflows for all parties, no matter the size of the business network. Additionally, a shared infrastructure would provide auditors with greater visibility into participants' activities along the value chain.
- Enterprise blockchain technology can transform the supply chain with these three use cases:
  - `Traceability` - improves operational efficiency by mapping and visualizing enterprise supply chains.
  - `Transparency` - builds trust by capturing key data points, such as certifications and claims, and then provides open access to this data publicly.

    - `Tradeability` - is a unique blockchain offering that redefines the conventional marketplace concept.

Real estate and Property Records

- In real estate, `tokenization` refers to the digitization of securities, alternative assets, and financial instruments.
- With blockchain technology, digital assets can be programmed to include `ownership rights`, `transaction history`, and `rules to ensure asset issuance`, distribution and transfers are regulation compliant.

Other applications

- `Legal`：
    - Blockchain, as an immutable technical innovation, can help to verify information during legal proceedings. In addition, technology to automate a number of legal processes is advancing; using concepts from smart contract development could be helpful.
- `Gaming`：
    - Blockchain assists the in game purchase prcess and combat cheating on gameplay.
- `Blockchain as a Service`：
    - The concept of BaaS, where vendors provide easy-to-implement solutions that can be customized, is likely to grow as use cases for the technology increase.
    - Similar to SaaS these blockchain products provide elements such as centeralized management of users and distribution of nodes.

Cryptocurrency Narratives

- Serve as guiding forces, delineating the landscape of innovation and possibility.
- Crypto narratives emerge from a combination of factors, including the technological capabilities of crypto and the blockchain, social and economic events, and the beliefs and motivations of the individuals involved in the cryptocurrency industry.
- **Decentralized Finance (DeFi)**:
    - Refers to a decentralized financial ecosystem built on blockchain technology, allowing users to access financial services such as `lending`, `borrowing`, `trading`, and `earning interest` without the need for traditional financial intermediaries like banks.
    - DeFi platforms leverage smart contracts and decentralized protocols to automate and enforce financial transactions, providing greater transparency, accessibility, and efficiency in the financial system.
    - Decentralized finance leverages key principles of the blockchain to increase financial security and transparency, unlock liquidity and growth opportunities, and support an integrated and standardized economic system:
        - Programmability
        - Immutability
        - Interoperability
        - Transparency
        - Permissionless

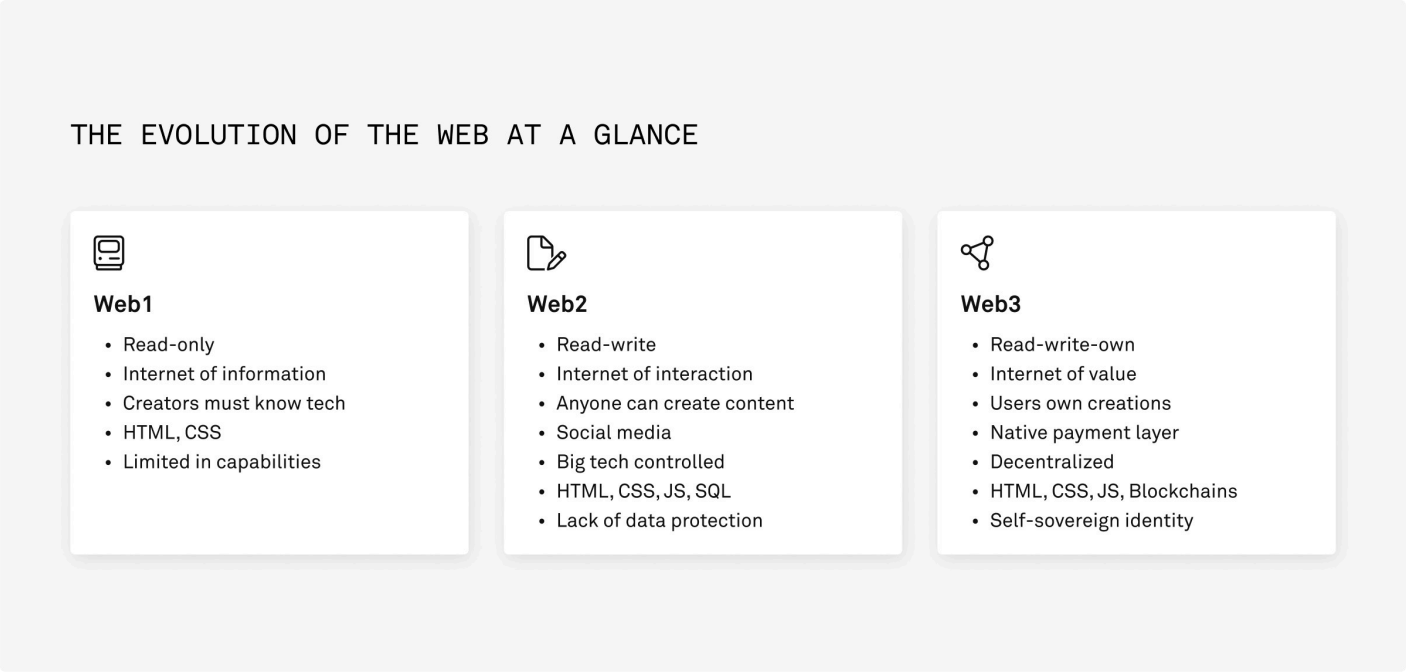
        - Self-Custody
- **Non-Fungible Tokens (NFTs)**:
    - Assets that have been tokenized via a blockchain.
    - Tokens are unique identification codes created from metadata via an encryption function. These tokens are then stored on a blockchain, while the assets themselves are stored in other places.
    - NFTs can represent digital or real-world items like artwork and real estate.
    - NFTs are created through a process called minting, in which the asset's information is encrypted and recorded on a blockchain. At a high level, the minting process entails a new block being created, NFT information being validated by a validator, and the block being closed. This minting process often entails incorporating smart contracts that assign ownership and manage NFT transfers.
- **Game Finance (GameFi)**:
    - Refers to decentralized finance protocols with gamified elements.
- **Artificial Intelligence (AI)**:
    - Blockchain capabilities can be leveraged for AI model development, deployment, and operation.
    - They enable the following fundamental properties, that are all highly relevant for AI use-cases:
        - Data security
        - Data provenance, traceability, auditability
        - Decentralized decision making
- **Real World Assets (RWAs)**:
    - Blockchain based digital tokens that represent physical and traditional financial assets such as `cash`, `commodities`, `equities`, `bonds`, `credit`, `artwork`, and intellectual property.
    - The tokenization of RWAs marks a significant shift in how these assets can be `accessed`, `exchanged`, and `managed`, unlocking an array of new opportunities for both blockchain-powered financial services and a wide variety of non-financial use cases underpinned by cryptography and decentralized consensus.
    - Benefits:
        - `Liquidity`: By enabling globally accessible liquidity conditions on a unified substrate—the blockchain ecosystem with cross-chain activity.
        - `Transparency`: Since the tokenized assets are represented onchain, transparency and auditable asset management are ensured, which decreases overall systemic risks, as the amount of leverage and risk in the entire system can be more accurately determined.
        - `Accessibility`: Tokenized RWAs can broaden the potential user base of certain asset types by enabling easier access through blockchain-based applications and allowing a broader set of users to utilize assets that would otherwise be unavailable to them through fractional ownership.
- **Decentralized Science (DeSci)**:
    - An approach to scientific research that uses decentralized technologies to revolutionize traditional science.

    - DeSci aims to broaden access to scientific data, promote more transparent peer review processes, and incentivize international collaboration among researchers.
    - By leveraging blockchain technology, DeSci can ensure the integrity and immutability of scientific records while eliminating barriers to entry:
        - `Academic publishing` - Some DeSci platforms can provide decentralized repositories for academic publications.
        - `Research funding` - Decentralized funding mechanisms, facilitated by smart contracts, may promote the transparent allocation of research funds.
        - `Data sharing and collaboration` - DeSci platforms may facilitate the secure and transparent sharing of research data and resources among scientists.
        - `Peer review` - Blockchain-based reputation systems may enhance the credibility and trustworthiness of scientific publications.
- **Decentralized Physical Infrastructure Networks (DePIN)**:
    - Refers to physical infrastructure networks, which use blockchains and token rewards to develop infrastructure in the physical world across different fields.
    - The goal of DePIN is to create resource-efficient physical infrastructure through incentivizing providers to commit their physical resources to a decentralized network.
    - The DePIN then makes these resources available to users who are looking for cheaper service charges (relative to centralized facilities), and the network generates revenue through fees paid by the users.

Web 3.0

- The third generation of the WWW, which involves direct immersion into the digital world.
- Encompasses individual control of personal data and use of cryptocurrencies and blockchain.
- Built upon the core concepts of decentralization, openness, and greater user utility.
- Berners Lee's key concepts on Web3:
    - `Decentralization` : "No permission is needed from a central authority to post anything on the web, there is no central controlling node, and so no single point of failure…and no 'kill switch'! This also implies freedom from indiscriminate censorship and surveillance."
    - `Bottom-up design` : "Instead of code being written and controlled by a small group of experts, it was developed in full view of everyone, encouraging maximum participation and experimentation."

Evolution of the Web



Features of Web3.0

- **Decentralization**:
  - Web 3.0 emphasizes decentralization, allowing data to be stored in multiple locations simultaneously.
  - Breaks down centralized databases held by internet giants like Meta and Google, handing greater control to users.
  - Users sell data through decentralized data networks, ensuring ownership control.
- **Trustless and Permissionless**:
  - Based on open-source software, enabling direct interaction without intermediaries (trustless) and participation without authorization (permissionless).
  - Web 3.0 applications run on blockchains or decentralized peer-to-peer networks, known as dApps.
- **Artificial Intelligence (AI) and Machine Learning**:
  - Web 3.0 integrates AI and machine learning technologies, allowing computers to understand information like humans.
  - Utilizes Semantic Web concepts and natural language processing, enabling faster and more relevant results in various fields.
- **Connectivity and Ubiquity**:
  - Promotes increased connectivity and ubiquity of information and content.
  - Accessible across multiple applications and everyday devices, including those in the Internet of Things (IoT).

Chapter 5: Security Fundementals

Common security issues in Blockchain

- `Transaction malleability` :
  - Opens up the possibility of double withdrawal or deposit by allowing a hacker to change a transaction's unique ID before the Bitcoin network can confirm it, resulting in a scenario where it would seem that transactions did not occur.
  - BIP 62 is one of the proposals along with SegWit that have suggested solutions to solve this issue.
- `Information eclipse attacks` :
  - Can result double spending.
  - Bitcoin node is tricked into connecting only with the attacker node IPs.
  - This opens up the possibility of a 51 % attack by the attacker.
- `Smart contract security` :
  - Particularly formal verification, has gained traction.
  - Formal verification ensures a computer program meets specific formal statements.
  - The process involves converting the source program into understandable statements for automated provers.

Blockchain Attack Vectors

- **Peer to peer attacks**:
  - Sybil attack:
    - A hacker takes control of multiple network nodes.
    - Then the victim is surrounded by fake nodes that close all their transactions.
    - Finally, the victim becomes open to double-spending attacks.
  - Eclipse attack:
    - Requires a hacker to control many IP addresses or to have a distributed botnet.
    - Then the attacker overwrites the addresses in the tried table of the victim node and waits until the victim node is restarted.
    - After restarting, all outgoing connections of the victim node will be redirected to IP addresses controlled by the attacker.
    - This makes the victim unable to obtain transactions they're interested in.
  - Timejacking:
    - Exploits a theoretical vulnerability in blockchain's timestamp handling.
    - A hacker alters the network time counter of the node and forces the node to accept an alternative blockchain.
    - This can be achieved when a malicious user adds multiple fake peers to the network with inaccurate timestamps.
- Some protective solutions:
  - Using an HTTPS connection,

    - Verify SSL certificates,
    - Validating resource authenticity,
    - Increasing user trustworthiness.
- **RPC (Remote Procedure Call) Node Protocol Attacks**:
    - DDoS:
        - Hackers bring down network nodes by consuming all their processing resources with repeated requests.
        - Attackers aim to disconnect a network's mining pool, e-wallets, data exchanges, and other elements.
    - Eavesdropping:
        - Doesn't stop node operations, but it allows a malicious actor to listen to a node's communication.
        - A hacker can inject malicious code or exploit a backdoor to gain unauthorized access to node data, network routing, and sensitive information transmitted through the node.
        - Based on this information, the hacker can find vulnerabilities in the blockchain and plan their next attack.
    - Phising:
        - Widespread type of social engineering attack where a hacker steals user's sensitive information by making them click malicious links or submit their data to a fake website.
        - Hacker can gain information about the user's communication with blockchain nodes, mimic it, and gain access to the user's wallet.
- Some protective solutions:
    - Running valdiators
    - Enforcing user authentication
    - Access control

Bitcoin Improvement Proposals (BIPs)

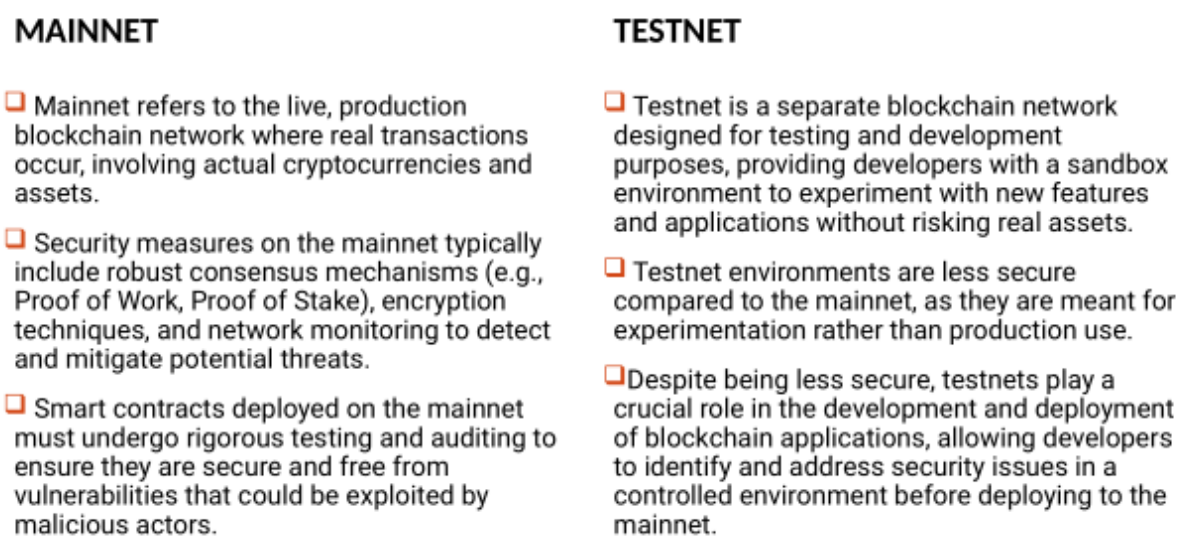
- Documents used to propose or inform the Bitcoin community about the improvements suggested, the design issues, security issues or information about some aspects of bitcoin ecosystem.

- **Types**:

    - Standard BIP:
        - Used to describe the major changes that have a major impact on the Bitcoin system. - `Example` : block size changes, network protocol changes, or transaction verification changes.
    - Process BIP:
        - A major difference between standard and process BIPs is that standard BIPs cover protocol changes, whereas process BIPs usually deal with proposing a change in a process that is outside the core Bitcoin protocol.
        - These are implemented only after a consensus among bitcoin users.

    - Informational BIP:
        - These are usually used to just advise or record some information about the Bitcoin ecosystem, such as design issues.
- Similarly, Ethereum blockchain has EIPs (Ethereum Improvement Proposals). EIPs are standards that aim to specify potential upgrades or functionalities to the Ethereum protocol. They allow developers and community members to propose new solutions, protocol specifications, modifications, and features to the network.

Mainnet vs Testnet



Forks and Altchains

- `Forking` involves taking the Bitcoin Core software, changing some parameters, and launching it on mailing lists and message boards.
- The result is alternative coins, also known as `altcoins`.
- Some of these altcoins are so different from Bitcoin that it is better to refer to them as `altchains`.
- Because of the distributed nature of bitcoin, network forks can occur naturally. In cases where two nodes simultaneously announce a valid block can result in a situation where there are two blockchains with different transactions. This is an undesirable situation but can be addressed by the Bitcoin network only by accepting the longest chain. In this case, the smaller chain will be considered orphaned.

Types of Forks

- `Software Fork` : developer takes a piece of open-source software and changes some parameters to meet their needs.
- `Soft Fork` : an upgrade to mining software that makes a change to the network but does not require that all miners participate. Makes it compatible with older software and usually done to upgrade transaction functions.
- `Hard Fork` : an upgrade to mining software that makes a change to the network that requires that participation of all miners. Implement key security or functionality changes, and it's incompatible with older software.

Contentious Hard Fork

- Backward-incompatible upgrade to mining software that makes a change to the network that is not accepted by all miners.
- Because some miners disagree with the fork and therefore don't upgrade to the new software version incorporating the proposed changes, the blockchain effectively splits in two.

Replay Attacks

- Occurs when an attacker takes data from a legitimate transaction on one blockchain and "replays" or mirrors that transaction on the second blockchain.
- Two blockchains are vulnerable to replay attacks if they both have the exact same process for generating a transaction signature.

Bitcoin Cash and Bitcoin Gold

- `Bitcoin Cash (BCH)`:
  - Increases the block limit to 8MB.
  - Uses PoW as consensus algorithm and mining hardware is still ASIC based.
  - Block interval is changed from 10 minutes to 10 seconds and up to 2 hrs.
  - Provides replay protection and wipe-out protection.
- `Bitcoin Gold (BTG)`:
  - New blockchain created from hard fork of Bitcoin blockchain.
  - The core idea is to address the issue of mining centralizationwhich has hurt the original Bitcoin idea of decentralized digital cash whereby more hash power has resulted in a power shift towards miners with more hashing power.
  - BTG uses the Equi-hash algorithm as its mining algorithm instead of PoW; hence it is inherently ASIC resistant and uses GPUs for mining.

Segregated Witness (SegWit)

- Soft fork update to Bitcoin protocol which addresses some weaknesses such as throughput and security in the Bitcoin protocol.
- Activated on Bitcoin main network on August 24, 2017.
- The key idea behind SegWit is the separation of signature data from transaction data, which results in reduced size of the transaction.
- Two types of transaction can be constructed using SegWit wallets, `Pay to Witness Public Key Hash (P2WPKH)` and `Pay to Witness Script Hash (P2WSH)`.
- Offers a number of improvements:
  - Fix for transaction malleability due to the separation of signature and transactional data.
  - Reduction in transaction size results in cheaper transaction fees.
  - Reduction in transaction signing and verification times, which results in faster transactions.
  - Script versioning, which allows version number to be prefixed to locking scripts.
  - Reduction in input verification time.

Wallets

- Software that's used to store private or public keys and wallet address.
- It performs various functions, such as receiving and sending tokens.
- Generates a 256 bit number to sign outgoing transactions.
- Wallets don't store any coins, and there is no concept of wallets storing user's coin or balance.

Non deterministic vs Deterministic (Seeded) wallets

Non deterministic	Deterministic (seeded)
Generates random private keys	Private keys are derived out of a seed value via hash functions
Core client generates some keys when first started and required	Seeds are randomly generated and represented by human readable mnemonic code words
Managing large number of keys is error prone and very difficult	Phrases can be used to recover all keys and makes private key management easy
There is a need to create regular backups of the keys and protect them appropriately	HD wallets store keys in a tree structure derived from a seed

Types of Wallets

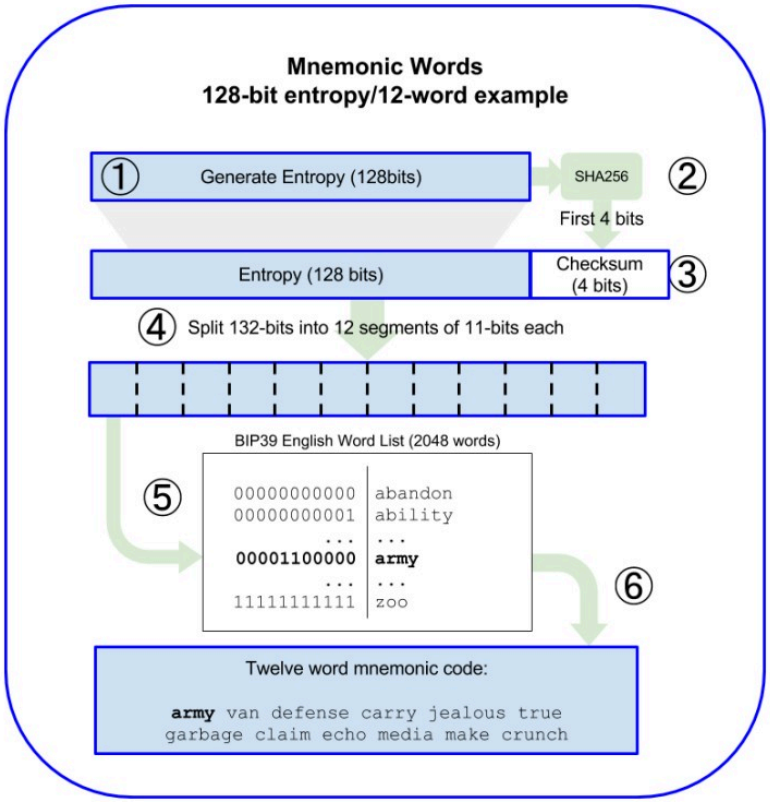
- `Brain Wallets` :
  - Master private key can be derived from the hash passwords that are memorized.
  - Prone to password guessing and brute force attacks.
- `Paper Wallets` :
  - Paper based wallet with the required key material printed on it.
  - It requires physical security to be stored.
- `Online Wallets` :
  - Provide a web interface to the users to manage their wallets and perform various functions such as making and receiving payments.
  - Easy to use but imply that the user trusts the online wallet service provider.
- `Mobile Wallets` :
  - Installed on mobile devices.
  - Provide various methods to make payments, most notably the ability to use smartphone cameras to scan QR codes quickly and make payments.
  - Available for the Android platform and iOS.
- `Hardware Wallets` :
  - Uses a tamper-resistant device to store keys.
  - Can be custom built or with the advent of NFC enabled phones (or Secure Elements).
  - Trezor and Ledger wallets are the most popular hardware wallets.

Recovery Seed

- Series of words that can be used to retrieve a private key stored in a non custodial wallet.
- Commonly used as a memory aid because it is very difficult to remember a private key.
- Store enough info to allow the user to recover their wallet.
- `Mnemonic code` words are word sequences that represent (encode) a random number used as seed to derive a deterministic wallet.
- Wallet application shows the user a sequence of 12 to 24 words when first creating a wallet.

Generating Mnemonic Words

- Mnemonic words are generated automatically by the wallet using the standardized process defined in BIP-39.
- The wallet starts from a source of entropy, adds a checksum, and then maps the entropy to a word list:
  - Create a random sequence (entropy) of 128 to 256 bits.
  - Create a checksum of the random sequence by taking the first (entropylength/32) bits of its SHA256 hash.
  - Add the checksum to the end of the random sequence.
  - Divide the sequence into sections of 11 bits.
  - Map each 11-bit value to a word from the predefined dictionary of 2048 words.
  - The mnemonic code is the sequence of words.



Custodial and Non-custodial Wallets

Custodial Wallet	Non-custodial Wallet
Controlled by trusted entity with the user typically having to access it via web interface	Users have a complete control of keys
These sites store private keys for users	User is responsible for the security of their private keys
Binance	Metamask

Wallet Attack Vectors

- `Fake Wallet` - As soon as the user installs the wallet and enters his seed words, the fake wallet sends all ada to an address stored by the attacker.
- `Clipboard Hijack`：
  - Malicious programs that change the clipboard, so called `clipboard hijackers`.
  - They constantly monitor the clipboard and as soon as you copy an address which is silently and secretly replaced with the attacker's address.
  - If you don't check the address again after pasting, you're out of luck.
- `DNS-Hijacks`：
  - In order to display the information of a website, the computer must first receive the IP addresses from the readable address entered, such as coinbase.com.
  - The computer must look in a phone book (DNS server) which number belongs to the name.
  - If someone with access to the PC or a malicious program manipulates this file, he could enter a different number for any website.
- `Phishing Mails / Messages` - You can also be redirected to a fake website by phishing emails or messages with links to a "airdrop", "important update" or other tempting things.

Security Risk

- `Balancing Risk` - users must be careful not to go too far and end up losing bitcoin in the effort to secure their bitcoin wallets/
- `Diversifying Risk` - users should spread the risk among multiple and diverse bitcoin wallets.
- `Multisig` - Companies or individual should consider using multi signature bitcoin address and should store signing keys on different locations and under the control of different people.
- `Survivability` - Users using complex passwords and keeping their keys secure makes it impossible for the user's family to recover any funds if the user isn't avaliable to unlock them.

Sidechains

- More precisely known as pegged sidechains.
- The concept whereby coins can be moved from one blockchain to another and moved back again.

- Typical uses include the creation of new altcoins (alternative cryptocurrencies) whereby coins are burnt as a proof of an adequate stake.
- This mechanism is also called Proof of Burn (PoB) and is used as an alternative method for distributed consensus to PoW and Proof of Stake (PoS).
- PoB only applies to a one way pegged sidechain. The second type is called a two-way pegged sidechain, which allows the movement of coins from the main chain to the sidechain and back to the main chain when required.

Tokenized and Tokenless Blockchains

Tokenized	Tokenless
Generate cryptocurrency as a result of a consensus pricess via mining or initial distribution	Don’t have the basic unit for the transfer of value

Oracles

- Service that provides external data to smart contracts that enables them not only to fetch data from other blockchains but also from the outside or off-chain world.
- Since smart contracts (are inherently isolated and deterministic) cannot access or retrieve data from external environments without an intermediary, The oracle serves as this intermediary, bridging the gap between off-chain and on-chain data sources.
- Are capable of digitally signing the data proving that the source of the data is authentic.
- Shouldn’t be able to manipulate the data they provide and must be able to provide authentic data.

Zero-Knowledge Proofs (ZKPs)

- A method that allows one party to prove to another that they know something without revealing the exact information itself.
- Used to verify transactions and interactions without revealing personal details and by providing confidentiality while upholding the integrity of the distributed ledger.
- Sophisticated combination of cryptographic privacy techniques and blockchain technology, providing a platform where transactions and interactions can be verified and recorded without compromising the confidentiality of the data involved.
- **Key Elements**:
  - Completeness: If the statement is true, the honest verifier will be convinced by the honest prover’s proof.
  - Soundness: If the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
  - Zero-Knowledge Property: If the statement is true, the verifier learns nothing other than the fact that the statement is true. The proof does not reveal any additional information about the secret itself.

- **Usecases**:
  - Private Transactions - to allow users to create privacy-preserving transactions that keep the monetary amount, sender, and receiver addresses private (ex. Zcash).
  - Verifiable Computations - oracle networks, which provide smart contracts with access to off-chain data and computation, can also leverage ZKPs to prove some fact about an off-chain data point, without revealing the underlying data on-chain.
  - Highly Scalable and Secure Layer 2s - zk-Rollups, Validiums, and Volitions enable highly secure and scalable layer 2s.
  - Decentralized Identity and Authentication - ZKPs can underpin identity management systems that enable users to validate their identity, while protecting their personal information.

Chapter 6: Bitcoin

What's Bitcoin?

- A protocol, a digital currency, and a platform.
- It is a combination of peer-to-peer network, protocols, software that facilitate the creation and usage of the digital currency named `bitcoin`.
- Nodes in this peer-to-peer network talk to each other using the `Bitcoin` protocol.
- Bitcoin uses scripting language called `Script` that isn't Turing complete (lacks several logical functions like loops) because to ensures that no Bitcoin script can consume inordinate computing power and harm nodes on the network.
- Script is used in Bitcoin transaction to determine to whom the bitcoin was sent.
- Pay-to-Public-Key-Hash (P2PKH) is the most popular type of Script.

Why does Bitcoin have value?

- Scarcity
- Divisibility
- Acceptability
- Portability
- Durability
- Unifomity

Ethereum

- The critical idea proposed by Vitalik Buterin in Nov 2013 was the development of a Turing-complete language that allows the development of arbitrary programs (smart contracts) for blockchain and decentralized applications.
- Can be visualized as a transaction based state machine.
- The core idea is that in Ethereum blockchain, a genesis state is transformed into a final state by executing transactions incrementally. The final transformation is then accepted as the absolute undisputed version of the state.

- Ethereum is now a low-carbon blockchain while boosting its security and scalability.

Ethereum Virtual Machine

- Simple stack-based execution machine that runs bytecode instructions to transform the system state from one state to another. The word size of the virtual machine is set to 256-bit.
- It is a Turing-complete machine but is limited by the amount of gas that is required to run any instruction. This means that infinite loops that can result in denial of service attacks are not possible due to gas requirements.
- It also supports exception handling.
- It is an entirely isolated and sandboxed runtime environment. The code that runs on the EVM does not have access to any external resources, such as a network or filesystem.
- Generally, EVM is a runtime environment for executing smart contracts in a secure and decentralized manner across the largest smart contract platform, Ethereum.

Smart Contracts and dApps

- **Smart Contracts**:
  - Self-executing contracts with the terms of the agreement directly written into lines of code, which are deployed on a blockchain.
  - They automatically enforce and execute the conditions of a contract when predetermined rules are met, without the need for intermediaries.
  - Smart contracts are the building blocks or backend of these dapps, enabling them to function autonomously and reliably in a decentralized ecosystem.
- **Decentralized Applications (dApps)**:
  - Applications that run on a blockchain network leveraging the capabilities of smart contracts to offer services that are decentraalized and tamper-resistant.

Smart Contract Languages

- Solidity, Low Level Lisp like language (LLL), Serpent, and Vyper.

Solidity

- Domain-specific language of choice for programming contracts in Ethereum.
- Object-oriented, high-level language for implementing smart contracts.
- Statically typed and supports inheritance, libraries and complex user defined types.
- Has two categories of data types: `value types` and `reference types`.
- Solidity cam be used to create contracts for uses such as voting, crowdfunding, blind auctions, and multi-signature wallets.

EVM vs Non-EVM Blockchains

EVM	Non-EVM
Can run smart contracts and dApps designed for EVM	Don’t adhere to the standards and specifications set by EVM for smart contracts and EVM
Can execute the same code written for Ethereum	They often use different programming language, consensus mechanism and architectural designs
Can leverage Ethereum’s ecosystem	Can carve out unique niches, address specific market needs, and foster innovation outside the Ethereum framework
Avalanche, Polygon, Arbitrum	Bitcoin, Solana, Cardano

How to buy/sell cryptocurrency?

- The easiest and most accessible way is to create an account on an exchange where you’ll need to submit your personal details for KYC (Know Your Customer) verification.
- `CEX` refers to centralized exchanges, such as Binance, Coinbase, Mexc, Kraken, Kucoin, Bitfinex, and others.
- Some of these exchanges require KYC (Know Your Customer) verification for buying/selling crypto and withdrawing funds to crypto wallets like MetaMask.
- `Exchange Rate`：On a centralized exchange, the exchange rate in a market trade is set to a price that both a buyer and seller agree to. That logic is programmed into the backend server of the exchange. On a DEX, the exchange rate is programmed into the smart contract that executes the trade and can be audited.

Centeralized vs Decentralized Exchanges

- `Centeralized Exchanges`：
  - All of the infrastructure is controlled by a single entity, usually a company, and is delivered to the user through a website.
- `Decentralized Exchanges`：
  - Allows traders to hold their own private keys and swap cryptocurrencies (usually in the form of wrapped tokens).
  - The goal is to provide users with 100% functionality without depending on one centeralized authority to power any part of the exchange.
  - This can lead to a more transparent, secure, and trustworthy service that allows users to maintain custody of their funds at all times.
  - The downside of a DEX is that its speed and scalability are limited by the blockchain it runs on.

Terminologies

- `Marketcap` - It represents the total value of a specific cryptocurrency and can be calculated by multiplying the current price per token by the total number of coins in circulation.

- `FDV` - Fully diluted valuation (FDV) is the total value of a cryptocurrency project considering all of its tokens that are in circulation.
- `Liquidity` - refers to the ease with which an asset can be bought or sold without significantly affecting its price.
- `Contract address` - a unique address allocated when a smart contract is deployed.

Stablecoins

- A blockchain-based assets that peg to the US dollar and other fiat currencies which underpin services that don't require banking intermediaries.
- `USDC`：
  - An ERC-20 stablecoin.
  - Supported by `Coinbase` and `Circle`.
  - Part of a larger consortium called `Centre`, whose members collaborate on the stablecoin's governance and use cases.
- `USDT`：
  - Reaches across several blockchains, including Ethereum, TRON, EOS, Liquid, and Algorand.
  - Nominally pegged to the US dollar and is by far the largest stablecoin in the cryptocurrency ecosystem.
  - It is the most popular trading pair for moving into and out of more volatile cryptocurrencies (for example, ETH/USDT or BTC/USDT).
- `DAI`：
  - Launched in 2018, was originally a "single-collateral token" backed by Ethereum.
  - Now DAI is a multi-collateral token backed by several cryptocurrencies, including ETH and BAT (Basic Attention Token, the Ethereum token that powers the Brave browser) and others.

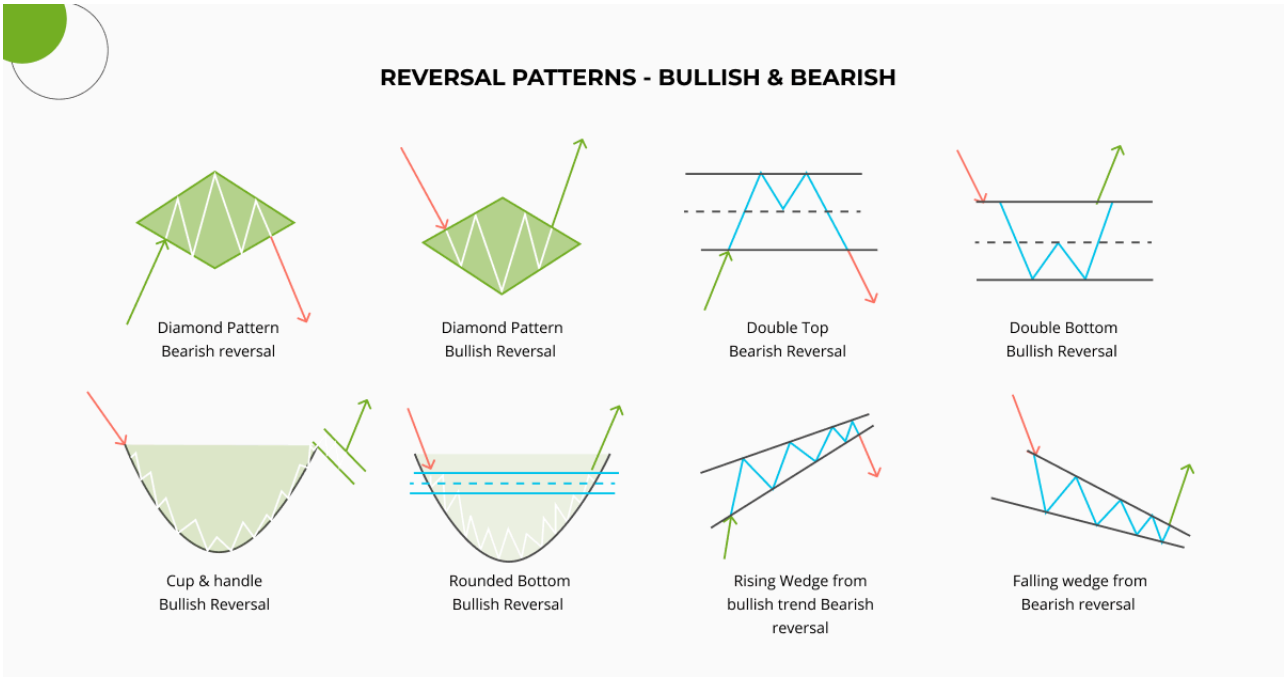
Cryptocurrency Trading

- It's a 24 hour market unlike stock exchange.
- **Types**:
  - Spot trading:
    - Directly buying and selling like in the real world.
    - Properties:
      - `Immediate Exchange`：You get the actual assets right away.
      - `Ownership`：You possess the asset, and it can be stored in your wallet.
      - `No Leverage`：You utilize your own assets to trade without employing leverage.
  - Spot Margin trading:
    - Adds a variation to Spot trading by allowing you to borrow funds from the platform to make bigger trades.
    - Properties:
      - `Leverage`：You can buy or sell more assets by borrowing funds from the platform.
      - `Collateral`：You will need to have other margin assets as collateral to secure your borrowing.

        - `Ownership` : While you retain ownership of the asset, there's a liquidation risk if things take a downturn, such as when your loan-to-value ratio becomes too high.
    - Future trading:
        - When you buy or sell a Futures contract, you do not own the underlying crypto assets. Instead, you are entering into agreements to buy or sell assets at a predetermined price on a specific future date.
        - In the Futures market, you don't necessarily need to buy or sell the underlying assets upon the delivery date. Instead, your profit or loss is based on the difference between the value of the assets when you entered the market and its value on the delivery date or the day you sell the contract.
        - Properties:
            - `Leverage` : You can hold a larger position size with a smaller margin required. However, it increases the risk of liquidation.
            - `Expiration Date` : For a Futures contract, there is an expiration date and you must settle it by closing the position when the contract expires unlike Perpetual contracts.
            - `Speculation and Hedging` : Used for both speculation (profit-seeking) and hedging (risk mitigation) purposes.

Trading Strategies

- **Day Trading**:
    - One of the most popular methods.
    - Professional traders get the majority of their gains, it is also the riskiest.
    - To place precise transactions, day traders examine the momentum of assets through charting patterns. Either they buy initially and sell afterward, or they first sell and then buy.
    - However, it is advised against trading on margin if you are a beginner trader. If the trade turns out badly for you, margin trading could multiply your losses.



- **Swing Trading**:
    - The normal trading period for swing traders is a few days or a week.

    - They rarely utilize a lot of leverage, unlike day traders, and almost always position overnight.
    - To maximize their profit from a price movement, most swing traders employ technical analysis tools to forecast trend reversals or the swing in price from low to high or high to low.
- **Position Trader**:
    - Due to their extended time horizons, position traders are frequently mistaken for investors.
    - Position traders typically trade over the course of weeks or even months.
    - Position traders, as opposed to swing traders, prefer to spot a trend and enter a trade along with it rather than trying to catch the proverbial falling knife by forecasting a reversal.
- **Diversified Investor**:
    - Long-term asset holding is a common practice among investors.
    - Unlike swing or position traders, their objective is often portfolio diversification rather than a simple bet on price appreciation.
- **Dollar Cost Averaging (DCA)**:
    - An investment strategy where rather than investing all the available capital at once, incremental investments are gradually made over time.

Bridges, Swapping, and Wrapping

- **Bridges**:
    - Establish a connection between two different blockchain networks, allowing the transfer of assets and data between them. They do this by maintaining unified liquidity pools and unique resource balancing algorithms.
    - These liquidity pools have native assets linked to all chains at the same time, allowing for efficient swaps.
    - Crypto bridges provide a gateway to explore different blockchain ecosystems. This is especially useful when chains like Ethereum become congested due to high user activity.
- **Swapping**:
    - Refers to the process of directly exchanging a cryptocurrency with another without the involvement of any crypto-to-fiat exchange.
    - You simply can exchange any token for another token. Buy eth using stablecoin.
- **Token Wrapping**:
    - Tokenization of another cryptocurrency.
    - They are tokens that are pegged to a particular cryptocurrency but can operate on another blockchain network.
    - It is supposed to match the asset value it is representing, and it can normally be redeemed at it anytime.

DAOs

- An emerging form of legal structure that has no central governing body and whose members share a common goal to act in the best interest of the entity.
- DAOs are used to make decisions in a bottom-up management approach.
- Power is distributed across token holders who collectively cast votes.

- DAOs operate using smart contracts, which are essentially chunks of code that automatically execute whenever a set of criteria are met. These smart contracts establish the DAO's rules.
- All votes and activity through the DAO are posted on a blockchain, making all actions of users publicly viewable.
- One of the first DAOs named The DAO was an organization created by developers to automate decisions and facilitate cryptocurrency transactions.
- A DAO must ensure security is prioritized, as exploits can leave a DAO drained of millions of dollars of its treasury savings.

Other Blockchains

- Binance Smart Chain (BSC)
- Polkadot (DOT)
- Cardano (ADA)
- Solana (SOL)
- Avalanche (AVAX)
- Algorand (ALGO)
- Cosmos (ATOM)
- NEAR Protocol (NEAR)
- Tezos (XTZ)
- XRP (Ripple)
- Polygon (MATIC)
- Arbitrum (ARB)
- TON (The Open Network)
- Hyperledger