BITCOIN

Peer-to-Peer Network

- A peer-to-peer (P2P) network is based on the concept of decentralisation, which allows the participants to conduct transactions without needing a central server.
- The peers or nodes (usually a computer) communicate with each other on the network freely without an intermediary.

Role of Peer-to-peer (P2P) in Blockchain

- The creator of Bitcoin, Satoshi Nakamoto, referred to it as a “peer-to-peer electronic cash system” which was created with the aim of having a P2P digital form of money.
- Blockchain leverages the P2P network technology to provide a decentralised ledger for one or more digital assets.
- In this decentralised P2P network, all the nodes or computers are connected to one another in some way.
- A complete copy of the ledger is maintained by each node and is compared to other nodes to ensure the accuracy of data.

Bitcoin Protocol

- The Bitcoin protocol, for instance, specifies the rules that govern the Bitcoin network.
- It utilizes a peer-to-peer network that enables individuals to conduct financial transactions without the involvement of a trusted third party.
- Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger, i.e., blockchain.

MINING

- Mining is a **resource-intensive** process by which new blocks are added to the blockchain.
- Blocks contain transactions that are validated via the mining process by mining nodes and are added to the blockchain.
- This process is **resource-intensive** in order to ensure that the required resources have been spent by miners in order for a block to be accepted.
- New coins are minted by the **miners** by spending the required computing resources.
- This also **secures the system against frauds and double spending** attacks

MINING

- Roughly one new block is created (mined) every **10 mins**.
- Miners are rewarded with new **coins** if and when they create new blocks and are paid transaction fees in return of including transactions in their blocks.
- New blocks are created at an approximate fixed rate. Also, the rate of creation of new bitcoin decreases by 50%, every **2,10,000 blocks**, roughly **every 4 years**.
- When bitcoin was initially introduced, the block reward was **50 bitcoin**; then in 2012, this was reduced to **25** bitcoin. In July 2016, this was further reduced to **12.5** coins and the next reduction is estimated to be on july, 2020. This will reduce the coin reward further down to approximately**6 coins**.

MINING

- Approximately **144 blocks**, that is, 1**,728 bitcoin** are generated 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.

TASK OF MINERS

- Once a node connects with the bitcoin network, there are several tasks that a bitcoin miner performs.
- **SYNCHING UP WITH THE NETWORK**
- Once a new node joins the bitcoin network, it **downloads the blockchain** by requesting historical blocks from other nodes.
- This is mentioned here in the context of the

  bitcoin miner; however, this not necessarily a task only for a miner.

TASK OF MINERS

- **Fetch reward: Once a node solves the hash puzzle, it immediately** broadcasts the results, and other nodes verify it and accept the block.

  There is a slight chance that the newly minted block will not be accepted by other miners due to a clash with another block found at roughly the same time, but once accepted, the miner is rewarded with 12.5 bitcoins (as of 2016) and any associated transaction fees.

- **Transaction validation: Transactions broadcasted on the network** are validated by full nodes by verifying and validating signatures and outputs.

TASK OF MINERS

- **Block validation: Miners and full nodes can start validating blocks** received by them by evaluating them against certain rules. This includes the verification of each transaction in the block along with verification of the nonce value.
- **Create a new block: Miners propose a new block by combining** transactions broadcasted on the network after validating them.
- **Perform Proof of Work: This task is the core of the mining process** and this is where **miners find a valid block by solving a computational puzzle**. The block header contains a **32-bit nonce field and miners are required to repeatedly vary the nonce until the resultant hash is less than a predetermined target.**

PROOF OF WORK

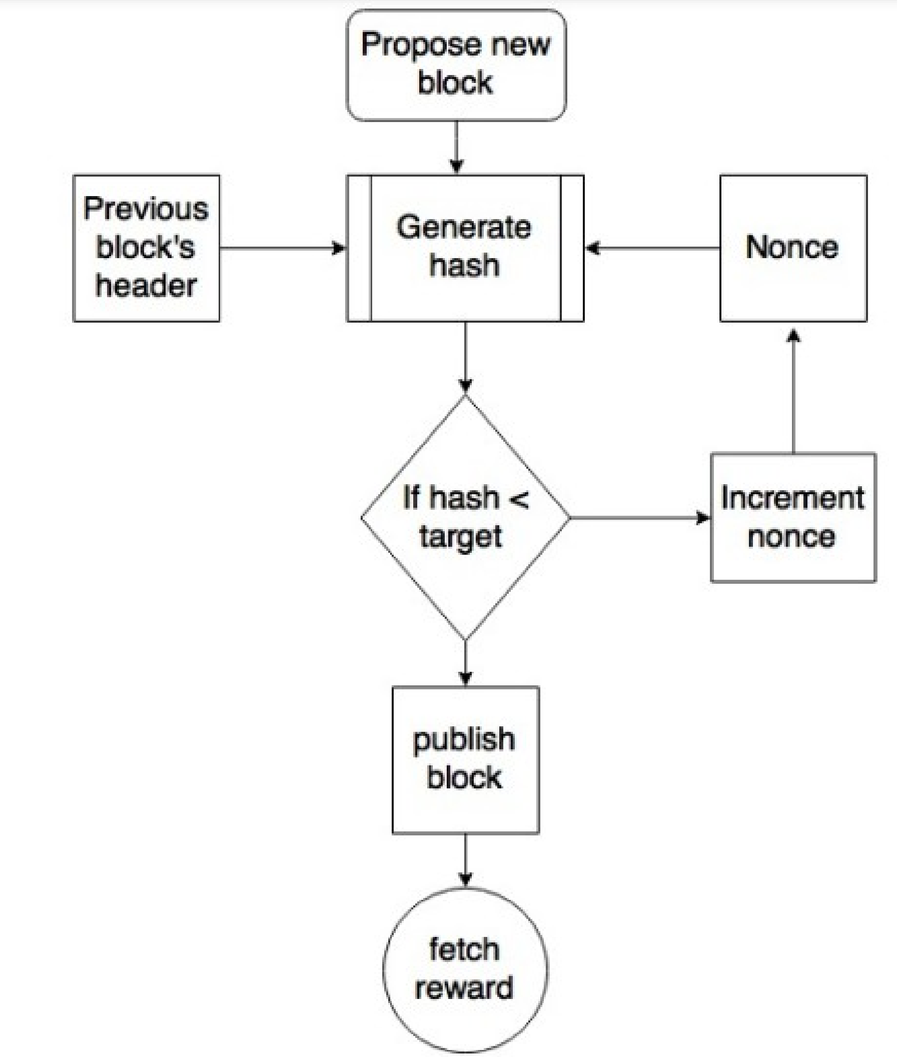
- This is a proof that enough computational resources have been spent in order to build a valid block. **Proof of Work (PoW) is based on the idea that a random node is** selected every time to create a new block. In this model, nodes compete with each other in order to be selected in proportion to their computing capacity.
- The following equation sums up the Proof of Work requirement in bitcoin:
- $H\,(N \,||\, P\_hash \,||\, Tx \,||\, Tx \,||\, .\,.\,.\; Tx) < Target$

PROOF OF WORK

- *H (N || P_hash || Tx || Tx || . . . Tx) < Target*
- Where N -> a nonce, P_hash is a hash of the previous

  block, Tx ->transactions in the block, and **Target** is the target network difficulty 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.

PROOF OF WORK



Mining process

Proof of Stake (PoS)

- Unlike PoW, the PoS protocol does not require miners to solve complex mathematical problems.
- Instead, the protocol assigns the right to add a new block to the blockchain based on the amount of cryptocurrency a miner holds.
- The more cryptocurrency a miner holds, the more likely they are to be selected to add a new block to the blockchain.
- Ethereum is an example of a blockchain that uses the PoS protocol.

THE MINING ALGORITHM

The mining algorithm consists of the following steps.

- The previous hash block is retrieved from the bitcoin network.
- Assemble a set of potential transactions broadcasted on the network into a block.
- Compute the double hash of the block header with a nonce and the previous hash using the SHA256 algorithm.
- If the resultant hash is lower than the current difficulty level (target), then stop the process.
- If the resultant hash is greater than the current difficulty level (target), then repeat the process by incrementing the nonce.

- As the hash rate of the bitcoin network increased, the total amount of 32-bit nonces was exhausted too quickly. In order to address this issue, the *extra nonce solution was implemented, whereby the **coinbase transaction** is* used as a source of extra nonce to provide a larger range of nonces to be searched by the miners.
- 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.

THE HASHING RATE

- The hashing rate basically represents the rate of calculating hashes per second.
- In early days of bitcoin, it used to be quite small as CPUs were used, but with dedicated mining pools and ASICs now, this has gone up exponentially in the last few years.
- This has resulted in increased difficulty.
- The following hash rate graph shows the hash rate increase over time and is currently measured in Exa hashes.
- This means that in 1 second, bitcoin network miners are computing more than 1 000 000 000 000 000 000 hashes per second. Hashing rate as of 06/02/2017.

MINING SYSTEMS

- Over time, bitcoin miners have used **various methods to mine bitcoins**. As the core principle behind mining is
- Based on the **double SHA256 algorithm**, overtime miners have developed sophisticated systems to calculate the hash faster and faster.
- The following is a review of the different types of mining methods used in bitcoin and how they evolved with time.
- **CPU:** mining was the first type of mining available in the original bitcoin client. but no longer profitable

MINING SYSTEMS

- **GPU:** Due to the increased difficulty of the bitcoin network and general tendency **of finding faster methods to mine**, miners started to use **GPUs or graphics cards available in PCs** to perform mining. **GPUs support faster and parallelized** calculations that are usually programmed using the **OpenCL language**.
- **limitations**, such as overheating and the requirement for specialized motherboards and extra hardware to house multiple graphics cards.

MINING SYSTEMS

- **FPGA :** Even GPU mining did not last long, and soon miners found another way to perform mining using FPGAs. **Field Programmable Gate Array (FPGA) is basically an** integrated circuit that can be programmed to perform specific operations.
- FPGAs are usually programmed in **hardware description languages (HDLs), such as** Verilog and VHDL.
- FPGA offered much better performance as compared to **GPUs**;
- **Issues** such as accessibility, programming difficulty, and the requirement for specialized knowledge to program and configure FPGAs

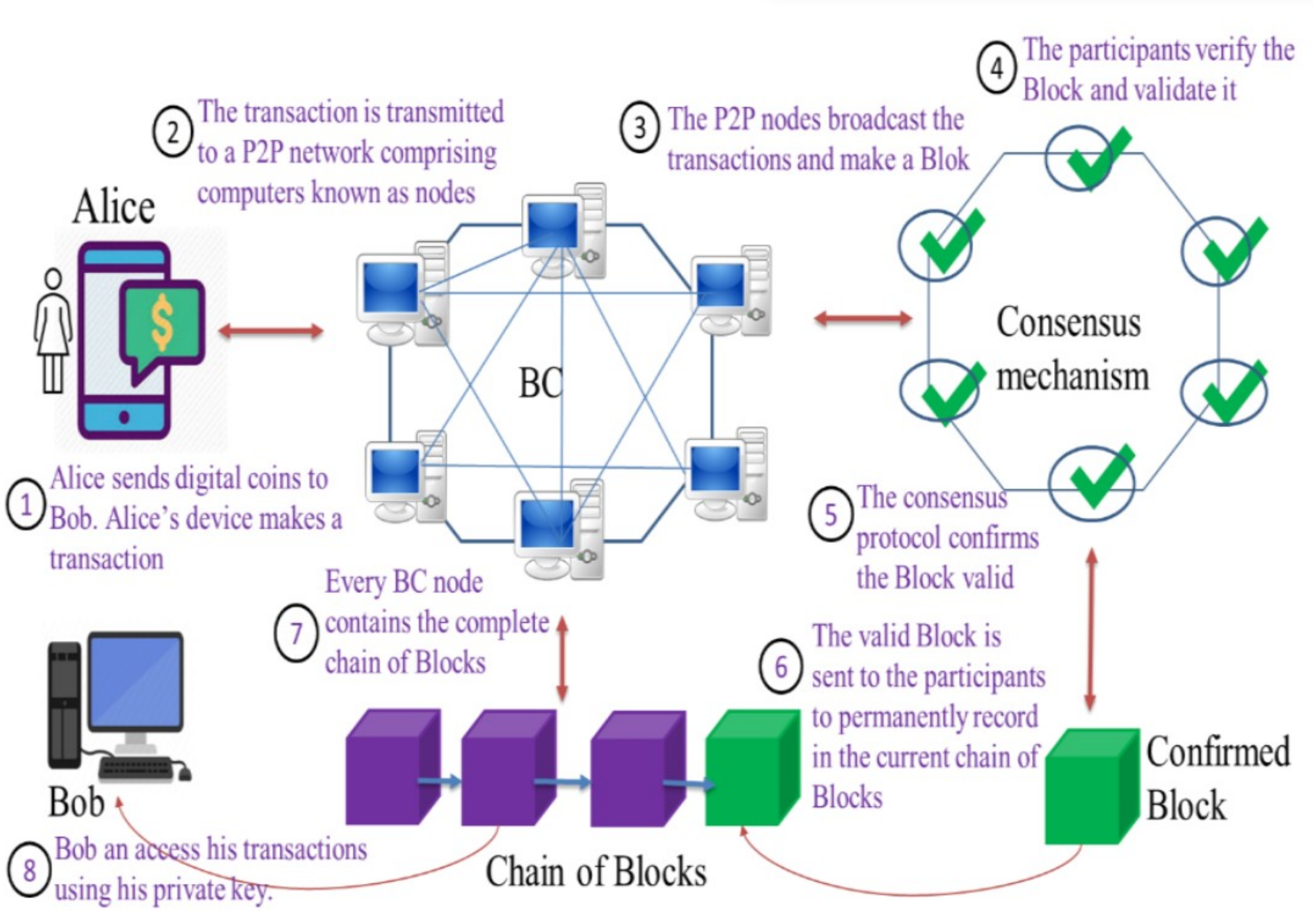
MINING SYSTEMS

- **ASICS: Application Specific Integrated Circuit (ASIC) was** designed to perform the SHA-256 operation. These special chips were sold by various manufacturers and offered a **very high hashing rate.**
- This worked for some time, but due to the quickly increasing mining difficulty level, single-unit ASICs are no longer profitable.
- Currently, mining is out of the reach of individuals and now professional mining centers using **thousands of ASIC units** in parallel are offering mining contracts to users to perform mining on their behalf.

MINING POOLS

- A **mining pool** forms when **group 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.
- This is **profitable** as compared to **solo mining**, where only one sole miner is trying to solve the partial hash inversion function (hash puzzle) because in mining pools, the **reward is paid to each member** of the pool regardless of whether they (more specifically, their individual node) solved the puzzle or not.
- There are various models that a mining pool manager can use to pay to the miners, such as the **pay-per-share model** and the **proportional model**. In the pay per share model, the mining pool manager pays a **flat fee to all miners** who participated in the mining exercise, whereas in the proportional model, the share is calculated based on the amount of computing resources spent to solve the hash puzzle.

A Bitcoin blockchain Example



Alice
1 Alice sends digital coins to Bob. Alice's device makes a transaction
2 The transaction is transmitted to a P2P network comprising computers known as nodes
BC
3 The P2P nodes broadcast the transactions and make a Blok
4 The participants verify the Block and validate it
Consensus mechanism
5 The consensus protocol confirms the Block valid
6 The valid Block is sent to the participants to permanently record in the current chain of Blocks
Confirmed Block
7 Every BC node contains the complete chain of Blocks
Chain of Blocks
Bob
8 Bob an access his transactions using his private key.

Wallets

- A cryptocurrency wallet is a device or program that stores your cryptocurrency keys and allows you to access your coins.
- Wallets contain an address and the private keys needed to sign cryptocurrency transactions. Anyone who knows the private key can control the coins associated with that address.
- There are several different types of wallets, each with its own features and levels of security.
- Many cryptocurrency wallets can be used to store keys for different cryptocurrencies.

Wallets

- The wallet software is used to store **private or public keys** and Bitcoin address.
- It performs various functions, such as **receiving and sending bitcoins**. Nowadays, software usually offers both **functionalities: Bitcoin client and wallet.**
- On the disk, the Bitcoin core client wallets are stored as the **Berkeley DB Private keys are generated by randomly choosing a 256-bit number by wallet software.**
- The rules of generation are predefined. Public Key Cryptography. **Private keys are used by wallets to sign the outgoing transactions.**
- Wallets **do not store any coins,** and there is no concept of wallets storing balance or coins for a user.
- In fact, in the **Bitcoin network, coins do not exist; instead, only transaction information is stored on the blockchain** (more precisely, UTXO, unspent outputs), which are then used to calculate the number of bitcoins.
- As a software program, they also provide some functions to the users to manage and carry out transactions on the Bitcoin network.

Wallets

- **Non-deterministic wallets:** contain randomly generated private keys and are also called just a bunch of key wallets.
- The Bitcoin core client generates some keys when first started and generates keys as and when required.
- Managing a large number of keys is very difficult and an error-prone process can lead to theft and loss of coins.
- Moreover, there is a need to create regular backups of the keys and protect them appropriately, for example, by **encrypting them in order** to prevent theft or loss.

Wallets

- **Deterministic wallets:** keys are derived out of a seed value via hash functions.
- This seed number is generated randomly and is commonly represented by human-readable mnemonic code words.
- Mnemonic code words are defined in BIP 39, a Bitcoin improvement proposal for mnemonic code for generating deterministic keys.
- This phrase can be used to recover all keys and makes private key management comparatively easier.

Wallets

- Defined in BIP32 and BIP44, **Hierarchical Deterministic (HD)** wallets store keys in a tree structure derived from a seed.
- The seed generates the parent key (master key), which is used to generate child keys and, subsequently, grandchild keys.
- Key generation in HD wallets does not generate keys directly; instead, it produces some information (private key generation information) that can be used to generate a sequence of private keys.
- The complete hierarchy of private keys in an HD wallet is easily recoverable if the master private key is known.
- It is because of this property that HD wallets are very easy to maintain and are highly portable. There are many free and commercially available HD wallets available.
- For example, Trezor (https://trezor.io), Jaxx (https://jaxx.io/) and Electrum (https://electrum.org/).

Wallets

- **Brain wallets:** The master private key can also be derived from the hash of passwords that are memorized.
- The key idea is that this passphrase is used to derive the private key and if used in HD wallets, this can result in a full HD wallet that is derived from a single memorized password.
- This is known as a brain wallet. This method is prone to password guessing and brute force attacks but techniques such as key stretching can be used to slow down the progress made by the attacker.
- **Paper wallets:** As the name implies, this is a paper-based wallet with the required key material printed on it. It requires physical security to be stored.

Wallets

- **Brain wallets:** The master private key can also be derived from the hash of passwords that are memorized.
- The key idea is that this passphrase is used to derive the private key and if used in HD wallets, this can result in a full HD wallet that is derived from a single memorized password.
- This is known as a brain wallet. This method is prone to password guessing and brute force attacks but techniques such as key stretching can be used to slow down the progress made by the attacker.
- **Paper wallets:** As the name implies, this is a paper-based wallet with the required key material printed on it. It requires physical security to be stored.

Wallets

- **Hardware wallets:** Another method is to use a tamper-resistant device to store keys.
- This tamper-resistant device can be custombuilt or with the advent of NFC-enabled phones, this can also be a Secure Element (SE) in NFC phones.
- Trezor and Ledger wallets (various types) are the most commonly used Bitcoin hardware wallets. The following is the photo of a Trezor wallet

Trezor wallet

Wallets

- **Online wallets** Online wallets, as the name implies, are stored entirely online and are provided as a service usually via the cloud.
- They provide a web interface to the users to manage their wallets and perform various functions such as making and receiving payments.
- They are easy to use but imply that the user trusts the online wallet service provider. An example of online wallet is GreenAddress,
- **Mobile wallets:** as the name suggests, are installed on mobile devices.
- They can provide various methods to make payments, most notably the ability to use smartphone cameras to scan QR codes quickly and make payments.
- Mobile wallets are available for the Android platform and iOS,

  for example, Blockchain, breadwallet, Copay, and Jaxx.

Wallets

- The choice of Bitcoin wallet depends on several factors such as **security,** ease of use, and available features.
    - security should be of paramount importance. Hardware wallets tend to be more secure as compared to web.
    - Web wallets by nature are hosted on websites, which may not be as secure as a tamper resistant hardware device.
- Generally, mobile wallets for smartphone devices are quite

  popular due to a balanced combination of features and security.
- There are many companies offering these wallets on the iOS App Store and Android Play.
- It is however quite difficult to suggest that which type
- should be used, it also depends on personal preferences and features available in a wallet.
- It is advisable that security should be kept in mind while making decision on which wallet to choose.

Orphan blocks

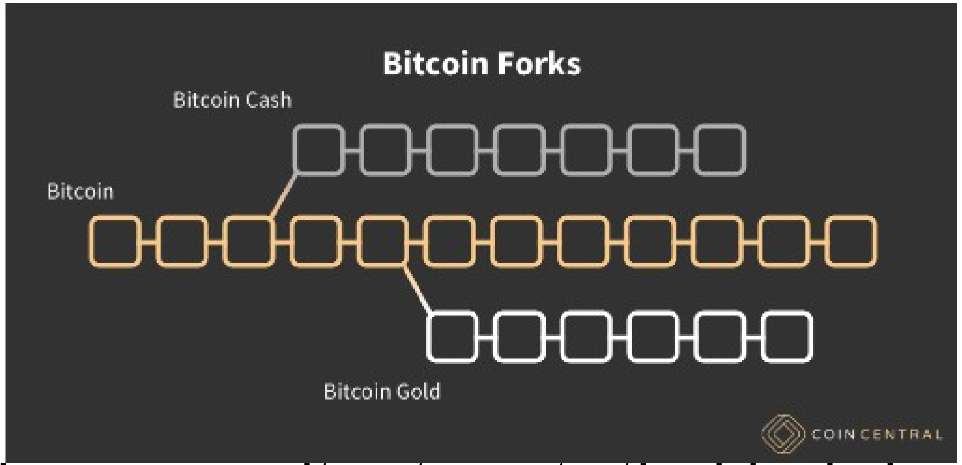
- **Orphan blocks** are also called detached blocks and were accepted at one point in time by the network as valid blocks but were rejected when a proven longer chain was created that did not include this initially accepted block.
- They are not part of the main chain and can occur at times when two miners manage to produce the blocks at the same time.

Forks

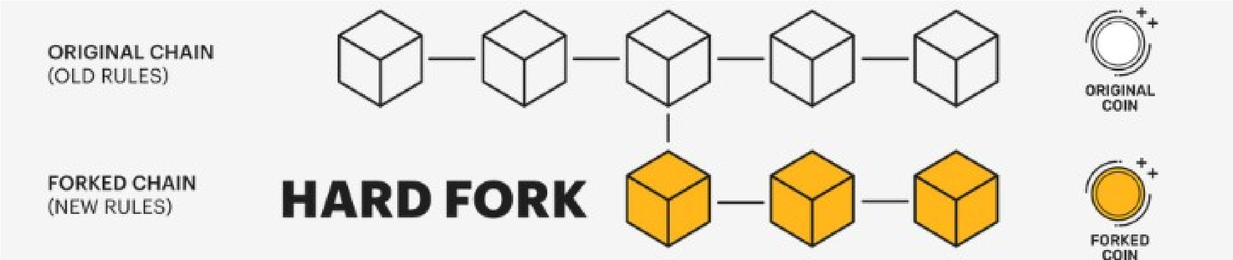
- Any changes to the protocol is a fork.
- **Reasons for forks**
- Blockchain developers often claim that forks are needed to improve blockchain technology and optimize the network.
- The most common changes are:
  - block size increase to increase throughput rate(transactions/sec);
  - lowering transaction fees.
- **Types of forks**
- Forks are divided into two depending on the scale of the modification of the blockchain protocol.
  - **Hard fork**
  - **Soft fork**

Forks

- **A hard fork** is a significant alteration of a **blockchain's algorithms and code**, which results in either a **completely new version of the blockchain** or **blockchain splitting into two separate networks.** Hard forks are often used to launch new crypto-projects (crypto currencies).

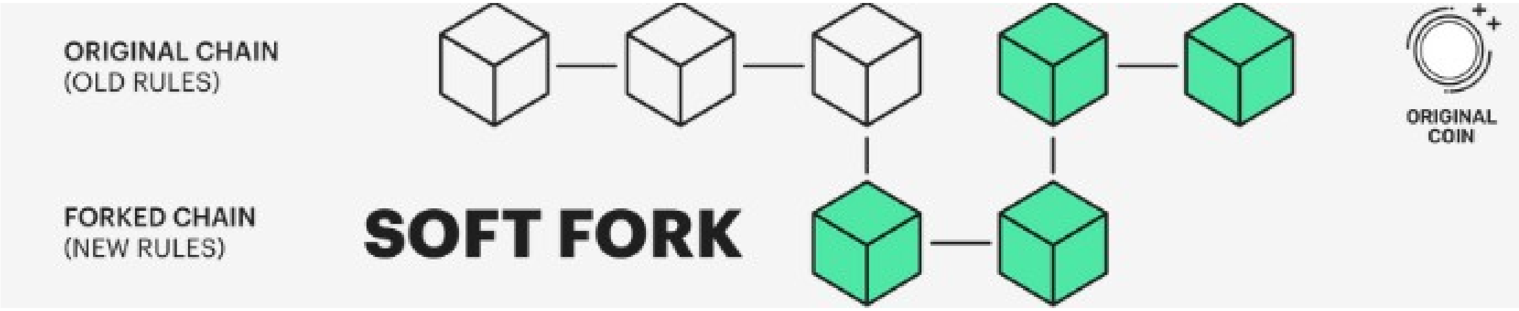


- A hard fork used to make serious alterations to the blockchain operations, causing blockchain split into two separate networks.



Forks

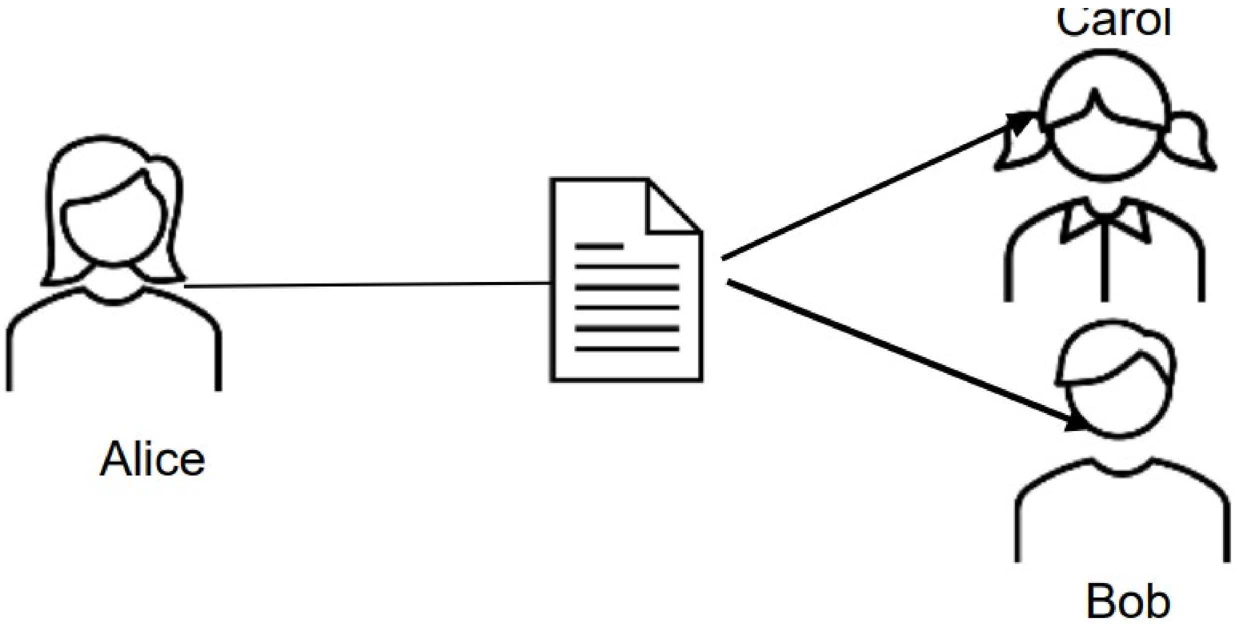
- **A soft fork** is a minor change of a blockchain protocol that results in **two parallel versions of the protocol,** meaning that all blockchain nodes operate on the same network, but some of them under the old rules and some under the new ones.
- a soft fork is an improvement of the blockchain's performance, with the old and new protocols functioning harmoniously in the same network.



Double-Spending

- Assume Alice wishes to pay Bob $1. If Alice and Bob pay with actual currency, Alice will lose the $1 when the transaction is completed.
- The dilemma becomes more difficult if Alice and Bob use digital money.
- Digital money is in the form of a digital file that can be easily copied. If Alice sends Bob a $1 digital file over email, for example, Bob has no way of knowing if Alice has deleted her copy of the file.
- If Alice still has the $1 digital file, she has the option of sending it to Carol.
- Double spending is the term for this issue.

Double-Spending



If Alice sends money in digital format to Bob. Bob cannot know for sure if Alice has deleted her copy of the file and she can choose to send the same file to Carol.

Bitcoin Blockchain

- New blocks are added to the blockchain approximately

  every 10 minutes.

- Network difficulty is adjusted dynamically every 2016 blocks in order to maintain a steady addition of new blocks to the network.

- **Network difficulty is calculated** using the following equation:

  *Target = Previous target * Time/2016 * 10 minutes*

- Previous target -> old target value,

  time -> the time spent to generate previous 2016 blocks.

- **Network difficulty basically means how hard it is for miners to find a new block**, that is, how difficult the hashing puzzle is now.

Coinbase transactions

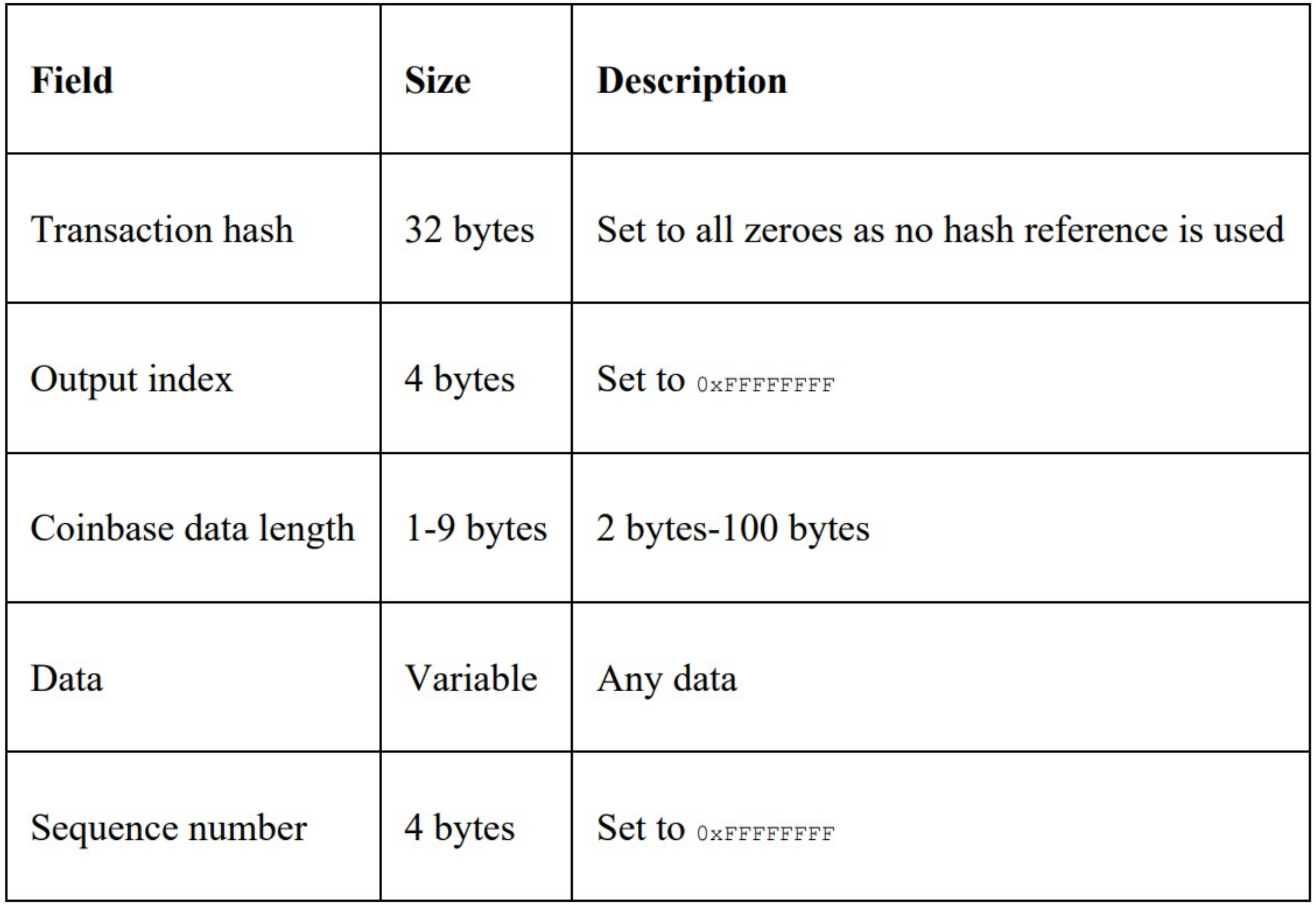
- A coinbase transaction or generation transaction is **always created by a miner** and is the first transaction in a block.
- It is used to create new coins. It includes a special field, also called **coinbase,** which acts as an **input to the coinbase transaction**.
- This transaction also allows up **to 100 bytes** of arbitrary data that can be used to store arbitrary data.
- In the genesis block, this transaction included the most famous comment taken from The Times newspaper:

  "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

- This message is a proof that the genesis block was not mined earlier than January 3, 2009. because first Bitcoin block (genesis block) was created on January 3, 2009 and this news excerpt was taken from that day's newspaper.

Coinbase transactions

- A coinbase transaction input has the same number of fields as usual transaction input, but the structure contains coinbase data size and coinbase data fields instead of unlocking script size and unlocking script fields**. it does not have a reference pointer to the previous transaction**. This structure is shown in the following table:



Field	**Size**	**Description**
Transaction hash	32 bytes	Set to all zeroes as no hash reference is used
Output index	4 bytes	Set to `0xFFFFFFFF`
Coinbase data length	1-9 bytes	2 bytes-100 bytes
Data	Variable	Any data
Sequence number	4 bytes	Set to `0xFFFFFFFF`

Coinbase transactions

Purpose

1. **Reward miners/validators** for securing the network (block reward).
2. **Collect transaction fees** from all transactions in that block.

Key Characteristics

- No input from a previous transaction (it “creates” coins).
- Has a special "coinbase" field instead of referencing prior outputs.
- Amount = **Block reward + Total transaction fees** in the block.
- **Example (Bitcoin)**

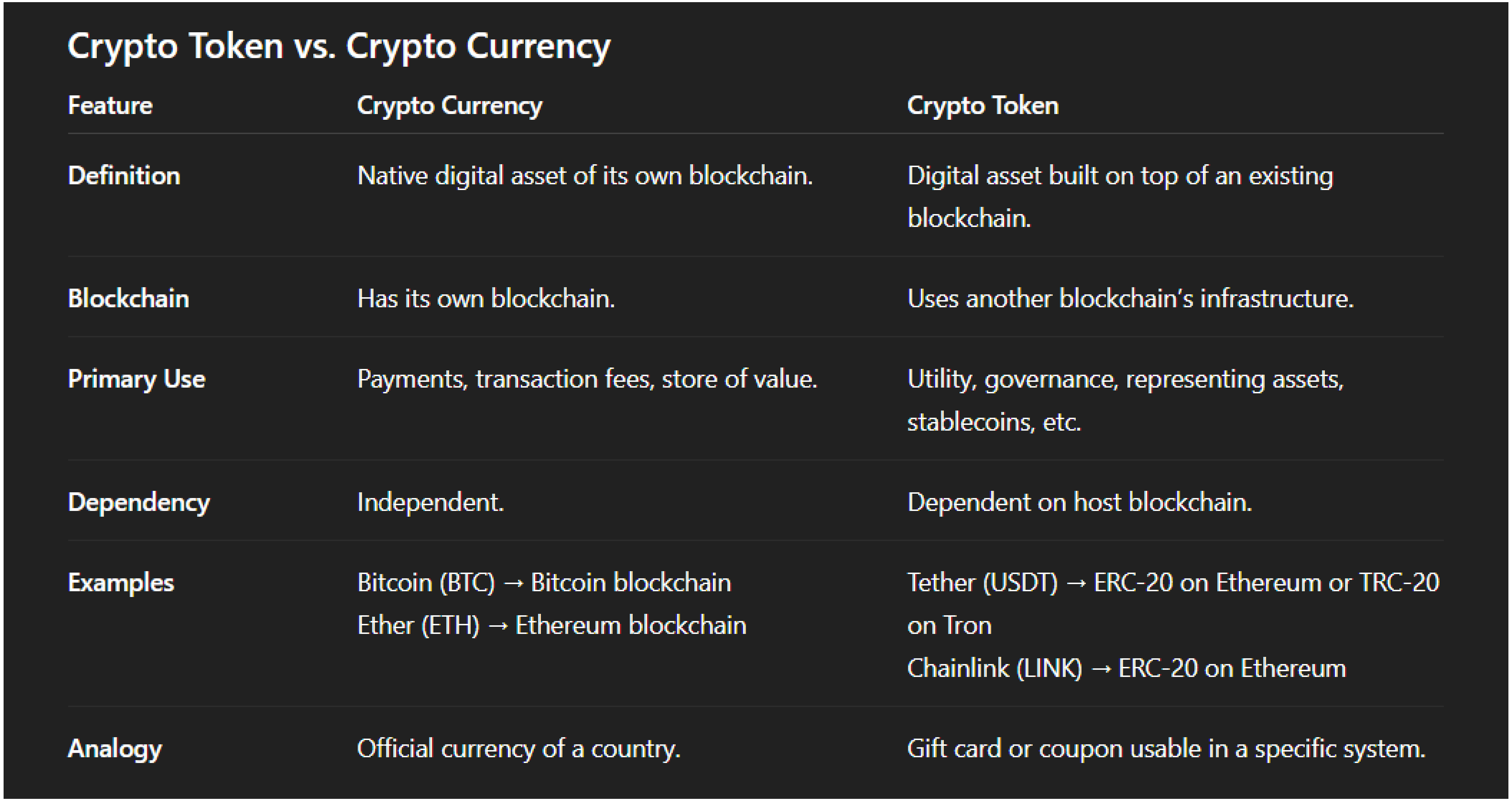
If a miner mines block #800,000:

- Block reward (as of 2025) = **3.125 BTC**
- Transaction fees in block = **0.25 BTC**
- Coinbase transaction output = **3.375 BTC** to the miner’s address.

Token

- Crypto tokens are a digital representation of an asset or interest in something and are built on a blockchain.
- Crypto tokens can also be used as investments, to store value, or to make purchases.
- Cryptocurrencies are digital representations of value designed to facilitate transactions (making and receiving payments) using blockchain technology.
- Often purchased through an initial coin offering, crypto tokens are generally used to raise funds to develop projects.

Crypto Token vs Currency



Crypto Token vs. Crypto Currency

Feature	Crypto Currency	Crypto Token
Definition	Native digital asset of its own blockchain.	Digital asset built on top of an existing blockchain.
Blockchain	Has its own blockchain.	Uses another blockchain's infrastructure.
Primary Use	Payments, transaction fees, store of value.	Utility, governance, representing assets, stablecoins, etc.
Dependency	Independent.	Dependent on host blockchain.
Examples	Bitcoin (BTC) → Bitcoin blockchain Ether (ETH) → Ethereum blockchain	Tether (USDT) → ERC-20 on Ethereum or TRC-20 on Tron Chainlink (LINK) → ERC-20 on Ethereum
Analogy	Official currency of a country.	Gift card or coupon usable in a specific system.

THANK YOU