

# UNIT III

## BITCOIN AND CRYPTO ASSETS

# What are Crypto-assets?

- Crypto assets are **purely digital assets that use public ledgers over the internet to prove ownership.**
- Crypto-assets are the broadest concept of value on a blockchain. They are purely digital and transacted in the form of coins or tokens, but can represent anything from a store of value to a means of payment (or medium of exchange), to a physical asset.
- Crypto-assets have three broad categories that have some differences: **cryptocurrencies, crypto-commodities, and crypto-tokens.**

# CRYPTO ASSETS

- Crypto assets, short for cryptocurrency assets, refer to digital or virtual currencies that use cryptography for security and operate on decentralized networks based on blockchain or similar distributed ledger technology. These assets can serve various purposes, including as a medium of exchange, a store of value, or a unit of account.
- Some common examples of crypto assets include:
  1. **Bitcoin (BTC):** The first and most well-known cryptocurrency, introduced by an anonymous person or group of people using the pseudonym Satoshi Nakamoto in 2009.
  2. **Ethereum (ETH):** A decentralized platform that enables the creation of smart contracts and decentralized applications (DApps) in addition to its native cryptocurrency, Ether.
  3. **Ripple (XRP):** A digital payment protocol and cryptocurrency designed for fast and low-cost international money transfers.

# CRYPTO ASSETS

- 4. Litecoin (LTC):** A peer-to-peer cryptocurrency that is similar to Bitcoin but with faster transaction confirmation times and a different hashing algorithm.
  - 5. Bitcoin Cash (BCH):** A fork of Bitcoin that aims to increase the cryptocurrency's scalability and transaction speed by increasing the block size limit.
  - 6. Cardano (ADA):** A blockchain platform that aims to provide a more secure and scalable infrastructure for the development of smart contracts and DApps.
- These are just a few examples, as there are thousands of different cryptocurrencies and tokens in existence, each with its own unique features, use cases, and underlying technology. Additionally, beyond cryptocurrencies, crypto assets can also include various tokens representing ownership or access rights to digital or physical assets, as well as other forms of digital assets such as non-fungible tokens (NFTs).

# Cryptocurrency

- Any form of currency that only exists digitally,
- Has no central issuing or regulating authority.
- Uses a decentralized system to record transactions and manage the issuance of new units.
- Relies on cryptography to prevent counterfeiting and fraudulent transactions.
- As a currency it functions as a “**digital asset**” that can be used as a medium of exchange that works on a blockchain or a distributed ledger to provide a record of financial transactions.

# Cryptocurrency

- Cryptocurrencies are issued by a set of protocols that control the addition of any new coins.
- **Bitcoin** is an example of the most successful digital coin.
- A digital coin is designed to function like currency in that it represents a store of “value” and can be used as a medium of exchange.
- Cryptocurrencies are digital coins that have their own monetary policies and uses, where value is driven by the market and secured through a blockchain.
- When you pay a transaction fee to use a currency token like bitcoin, you are paying for the service of using the digital ledger on bitcoin’s blockchain.

# Crypto-commodities

- Crypto commodities are a subset of crypto assets that represent digital or virtual versions of traditional commodities, such as precious metals, energy resources, agricultural products, and more.
- These crypto commodities leverage blockchain technology and tokenization to enable ownership, trading, and transfer of commodity assets on decentralized platforms.
- These tokens are also secured with the time, computational power and cost of electricity that cryptocurrencies like bitcoin require.
- **Asset Backing:** Each token is backed by a specific amount or share of the underlying physical commodity stored or reserved by the issuer.
- A subset of crypto-commodities includes “asset-backed tokens,” which are designed to be digital representations of tangible assets – such as precious stones or real estate – as well as intangible assets, such as intellectual property. Ex: Everledger

# Crypto-commodities

## 1. Gold-Backed Tokens:

1. **Examples:** Tether Gold (XAUT), PAX Gold (PAXG), etc.
2. **Purpose:** Each token represents ownership or rights to a specific amount of physical gold stored in secure vaults by the issuer.
3. **Features:** Backed by physical gold, redeemable for physical gold, and often audited for transparency and compliance.

## 2. Silver-Backed Tokens:

1. **Examples:** SilverCoin (SVC), etc.
2. **Purpose:** Similar to gold-backed tokens, silver-backed tokens represent ownership or rights to physical silver assets.
3. **Features:** Backed by physical silver, redeemable for physical silver, and audited for transparency.



# Crypto-commodities

## 3. Oil and Energy Tokens:

1. **Examples:** Oil-backed tokens, renewable energy tokens, etc.
2. **Purpose:** Represent ownership or rights to specific amounts or shares of oil, energy resources, or renewable energy projects.
3. **Features:** Backed by physical or renewable energy assets, transparent ownership and usage tracking.

## 4. Agricultural and Commodity Tokens:

1. **Examples:** Grain-backed tokens, coffee-backed tokens, etc.
2. **Purpose:** Represent ownership or rights to specific agricultural products or commodities.
3. **Features:** Backed by physical agricultural products or commodities, transparent supply chain tracking and verification.

# Crypto-commodities

The “**Basic Attention Token**,” which allows for a blockchain-based model for digital advertising using the Ethereum blockchain and Brave platform to offer services that can be obtained with the token.

**Generally, crypto-commodities enable us to make the value of an asset digitally-divisible and unique, enabling new value exchange and liquidity.**

# Crypto-Tokens

- A digital asset that runs on other cryptocurrency's blockchain.
- In the traditional world of finance as a reference point, there are usually four classes of assets: **cash, commodities, fixed income, and stocks.**
- Besides cryptocurrencies, today we have terms like network tokens, security tokens, utility tokens, stable coins/tokens, and reputation/reward tokens.

# COIN

VS

# TOKEN

A COIN WORKS SIMILAR  
TO A PHYSICAL  
CURRENCY

IT IS USED AS A SOURCE  
OF PAYMENT

IT MOSTLY OPERATES ON  
ITS OWN BLOCKCHAIN  
AND HAS ITS OWN  
PROTOCOL

EXAMPLES INCLUDE  
BITCOIN, ETHEREUM AND  
RIPPLE



A TOKEN IS A DIGITAL  
ASSET ISSUED ON A  
PARTICULAR PROJECT

THEY ARE USED FOR  
PAYMENTS AND  
SIGNING DIGITAL  
AGREEMENTS

TOKENS DO NOT  
OPERATE ON THEIR OWN  
BLOCKCHAIN

EXAMPLES INCLUDE  
LITECOIN, ENJIN AND  
REN



## • Key Differences between Cryptocoins and Cryptotokens:

### 1. Purpose and Functionality:

1. **Cryptocoins:** Serve as native currencies or assets on specific blockchain networks, platforms, or ecosystems, facilitating transactions, payments, and value transfer.
2. **Cryptotokens:** Represent a variety of assets, rights, utilities, or functionalities within blockchain ecosystems, enabling new forms of digital assets, investments, applications, and decentralized finance (DeFi) innovations.

### 2. Blockchain Networks:

1. **Cryptocoins:** Operate as primary or native tokens on specific blockchain networks, platforms, or ecosystems, providing the foundation for transactions and operations within the network.
2. **Cryptotokens:** Can be issued, managed, and exchanged on various blockchain platforms, networks, or ecosystems, leveraging blockchain technology to create, manage, and transact tokenized assets or functionalities.

### 3. Utility and Value:

1. **Cryptocoins:** Derive value from their use as digital currencies or assets within blockchain ecosystems, influenced by supply and demand, investor sentiment, and market dynamics.
2. **Cryptotokens:** Derive value from their utility, demand, scarcity, adoption, and market dynamics within the blockchain ecosystem, serving specific use cases, functionalities, or purposes.

### 4. Examples:

1. **Cryptocoins:** Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), Ripple (XRP), and other cryptocurrencies.
2. **Cryptotokens:** Utility tokens (BAT, MANA, ENJ), security tokens (tZero, Polymath), payment tokens (USDT, USDC, DAI), stablecoins (USDC, USDT, DAI), and governance tokens (COMP, MKR, UNI) among others.

# Taxonomy of Token Classification

Category	Crypto-currency	Crypto-commodity	Network Token	Utility Token	Security Token	Stable Coin
Description	Volatile store of value with an (approximately) fixed supply	Digital way to represent commodities or physical assets on a blockchain	Needed to participate in an open network	Needed to participate in an open service	Token as call on assets held / custodied by a company	Token with value stabilized by algorithms and collateral
Creation	Created by network protocol	Created by Dapp software	Created by network protocol	Created by Dapp software	Created by Dapp software	Created by Dapp software
Example	Bitcoin	Everledger	Dfinity	Numeral	Digix	Maker DAI
Sample Purpose	Frictionless secured payment / transactions	Representing an asset, but not necessarily collateralized by a company / entity	Usage or participation fees of a network	Dapp usage / participation	Linking real-world and digital asset value	Decreased volatility for transactions using digital token

*Figure 3-1: Simple taxonomy of token classification and usage*

# Network Tokens

- Network tokens are a broad category that encapsulates tokens created by their network, rather than by a Dapp.
- Usually you need these tokens to install software, run software, store data, pay for computation, or participate in governance on a given blockchain network. An example is the **Dfinity network**.
- Another example might be if a social network issued its own token. As long as you are on their platform, you could use their token to execute transactions. In effect, this is what the platform Steemit has done: it's a social media platform that integrates STEEM as a token for posting, searching, or commenting on their platform.

# Network Tokens

- Ether, the token that powers the Ethereum network can be classified as both a cryptocurrency token and a network token: you can trade its value on an exchange or you can use it to manage transactions on the Ethereum platform itself.
- You might be using ether to pay for transactions or to pay for the computer power needed to execute a smart contract.



# Utility Tokens

- Utility tokens are sometimes called “**app coins**” because they are usually linked to a specific company or project’s blockchain application.
- These tokens are often created at the beginning of a new Decentralized Application (Dapp) and are given to investors as part of their Initial Coin Offering (ICO).
- Example: Numerai, which is an application built on the Ethereum network that aims to crowdsource trading algorithms for hedge funds, and requires Numeraire (NMR) tokens to participate.

# Security Tokens

- Security tokens represent an investment in an asset.
- Like a security, they are backed by the tradable resources of the issuing entity. For example, Digix and Goldmint
- A number of platforms such as The Elephant have been set up to assist companies in launching their own tokenized securities.
- **One way to conceptualize the difference between a utility token and a security token is to think of utility tokens more like “coupons” for services by a specific company, rather than partial ownership of assets.**
- Utility tokens are more like going to an arcade and winning tickets which can only be redeemed at the arcade prize counter. Outside of the arcade, the tickets lose their value, but inside the arcade, they continue to be useful.

# Stablecoins

- Stablecoins are cryptocurrencies whose value is pegged, or tied, to that of another currency, commodity, or financial instrument.
- Stablecoins are more useful than more-volatile cryptocurrencies as a medium of exchange.
- Stablecoins may be pegged to a currency like the U.S. dollar or to the price of a commodity such as gold.





















# What Are ICOs? (Initial Coin Offerings)

- This is when a project opens up for investment by individuals and institutions. Similar to IPO (Initial Public Offering).
- In return for sending cryptocurrencies like bitcoin or ether to a project, investors receive some amount of tokens related to the project that either exist already or will be dispersed upon technical development of the project.
- Because of the ease in launching these fundraising efforts – crowdfunding campaigns on steroids – a large percentage of recent ICOs have used the ERC-20 Ethereum standard.

# Disadvantages of ICOs

- The Wall Street Journal did an intensive study of 1,450 ICOs and found that 271 of them appeared to be fraudulent.
- Many of these ICOs used stock photographs of people to create fictitious boards and celebrity endorsements.
- Still, the 271 fraudulent ICOs generated about \$1 billion in investment money between them

# Top Ten Cryptocurrencies by Market Capitalization

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)	
1	 Bitcoin	\$131,515,310,275	\$7,702.97	\$4,872,780,000	17,073,325 BTC	0.78%		...
2	 Ethereum	\$61,859,704,528	\$619.50	\$1,847,780,000	99,854,728 ETH	4.35%		...
3	 Ripple	\$27,301,781,469	\$0.695737	\$440,276,000	39,241,525,848 XRP *	8.11%		...
4	 Bitcoin Cash	\$20,497,651,843	\$1,194.20	\$919,821,000	17,164,338 BCH	10.26%		...
5	 EOS	\$12,994,526,096	\$14.50	\$1,453,480,000	896,149,492 EOS *	-0.04%		...
6	 Litecoin	\$7,111,385,191	\$125.15	\$324,083,000	56,823,348 LTC	1.89%		...
7	 Cardano	\$5,877,070,568	\$0.226677	\$116,274,000	25,927,070,538 ADA *	-1.07%		...
8	 Stellar	\$5,655,679,506	\$0.304403	\$65,895,400	18,579,578,737 XLM *	1.50%		...
9	 IOTA	\$4,977,916,374	\$1.79	\$164,873,000	2,779,530,283 MIOTA *	-5.24%		...
10	 TRON	\$4,048,393,951	\$0.061574	\$247,907,000	65,748,111,645 TRX *	0.86%		...

# Bitcoin

- Bitcoin was the first successful cryptocurrency.
- Bitcoin is important because it has proven that a digital asset running on a decentralized network is feasible.
- All the other cryptocurrencies created after this are called “**altcoins**” since they represent alternatives to Bitcoin that attempt to make improvements to the Bitcoin network model in some capacity.
- Combined with the use of consensus and cryptography, it was the first successful decentralized application running on blockchain technology.

# Bitcoin

- **Why Was Bitcoin Created?**

- While Bitcoin's creator remains anonymous, the reasons behind its creation remain a speculation. However, it may have been driven by several factors, as mentioned from the white paper:
- **First**, Bitcoin aimed to address the flaws of traditional financial (TradFi) systems based on trust, such as centralized control, high transaction fees, and limited accessibility.
- **Second**, Bitcoin's underlying principles include decentralization, trustlessness, security, and privacy — all achieved through blockchain technology. By eliminating intermediaries, Bitcoin enables fast and low-cost transactions, financial inclusivity, and greater transparency.
- These factors also mirror public criticism of the global financial system at the time of Bitcoin's launch — soon after the 2007–08 global financial crisis.



# Bitcoin

- Bitcoin is not governed by one centralized institution; rather, a group of stakeholders maintain the ledger (the blockchain) together to reach agreement on which transactions are right or wrong.
- This is called a consensus mechanism. Bitcoin relies on the Proof of Work (PoW) consensus mechanism, the first blockchain consensus ever created.

# Bitcoin

- **Architecture of the existing monetary system**

- Existing monetary systems are known as *fiat money*. Fiat is a Latin term that means '*by decree*' and it is used to describe how currencies such as the US Dollar, Euro, and Yen are created and managed.
- Anyone using fiat money must trust a central authority to establish the rules of the monetary system and how they are enforced. This can broadly be broken down into:

1. **A monetary framework & settlement system** - Rules & policy; infrastructure to issue new money & achieve consensus on transaction settlement.

2. **System hierarchy** - Assigning different levels of privilege to different participants to implement the framework and settlement function - internally and externally.

- At the top of the system hierarchy is some kind of governing body that sets the rules of the overall framework (rules and policy) and oversees/delegates the settlement system.

# Bitcoin

- In specific relation to a monetary system, the problem is what is known as a 'Double Spend' - the chance that a balance can be spent more than once.
- The Double Spend problem undermines trust in a financial system and therefore justifies the need for a central authority to have the final word - to be the general - but at the same time, that central authority creates a point of weakness because of the power they wield.
- In the case of fiat money, that weakness has resulted in the abuse of the power that governments have over the money supply, creating more and more of it. This results in the real world problem of inflation; eroding purchasing power of your savings and wages.

# Bitcoin

## Bitcoin's monetary framework

- Satoshi Nakamoto - Bitcoin's creator - solved the Double Spend issue by creating a monetary system with fixed rules defined in computer code, not a government policy document.
- Those rules run as a piece of software across a distributed network of computers without hierarchy, permission, or trust.
- No central authority enforces the rules; participants in the Bitcoin network follow them because of economic incentives provided for issuing Bitcoin at a predictable and unchangeable rate toward a maximum fixed supply.
- This removes the risk of monetary abuse and generates ongoing consensus on balances, solving the double spend problem.

# Bitcoin

## Bitcoin's monetary framework

- The key rules of Bitcoin's monetary system can be summarised as:
- There is a fixed supply schedule of bitcoin towards a maximum of 21 million.
- New bitcoins are created roughly every ten minutes (currently set at 6.25); the system is self-regulating to ensure this
- There is no other way that Bitcoin can be created.

# Bitcoin

- The Main Functions Of Bitcoin's Monetary System
- In order to function as a monetary system, without a central mediator, Bitcoin needs different participants in its network to achieve the following:
  1. Maintaining an accurate historic ledger of transactions & unspent balances
  2. Validate new transactions that confirm with the rules (consensus mechanism)
  3. Add those transactions to the historic ledger, in the correct data format
  4. Issue new bitcoin at the defined rate, halving after roughly 4-5 years. This is currently 6.25 BTC per new block until approximately May 2024, where it will halve to 3.125 BTC
  5. Allow wallets to spend & receive transactions & sync to the ledger
  6. Act as a service for external users/services to reference transactional data
  7. Route information across participants in its peer-to-peer network

# Bitcoin

- In order to provide a functioning monetary system, without a central mediator, Bitcoin needs to settle transactions with ‘finality’. There can be no rolling back, or replaying transactions.
- Full Nodes will ensure transactions are valid; they present the correct digital signatures proving the unspent funds (UTXO) associated with an address, can be spent.
- But those transactions need to be confirmed in the blockchain - ensuring no double spends have taken place - which is the role played by Miners.

# Bitcoin

## Miners & transaction confirmation

- As the Bitcoin blockchain has a fixed block size of 1MB, it can only accommodate an average of seven transactions per second, so unconfirmed transactions sit in something called a Mempool, waiting for Miners to take over.
- Miners' function is to watch the Mempool, waiting for these unconfirmed transactions, then package them into a candidate block; every ten minutes, one of the candidate blocks is chosen to be added to the existing blockchain confirming (settling) all the transactions within it.
- Miners are paid for this settlement function for every confirmed block. The first block - aka Genesis block - was mined on January, 3rd 2009, with a reward of 50BTC.



# Bitcoin

## Miners & Proof of Work

- To ensure against double spend, the mining process has to be difficult and incentivize honest behaviour. This is achieved through something called Proof of Work (Pow).
- PoW requires Miners to compete against each other to earn the right to broadcast their candidate block to the network by solving a mathematical puzzle.
- Every 2,016 blocks, which is approximately every two weeks, the network automatically adjusts the difficulty of the mathematical puzzle that miners must solve to mine a new block. This adjustment ensures that, on average, a new block is mined every 10 minutes, regardless of changes in the total computational power (hash rate) of the network.
- While the puzzle itself is meaningless, the work required to arrive there is not: it proves that the miner hasn't cheated, and ensures that no single entity can discover all of the blocks - keeping all the bitcoin rewards to themselves - or removing transactions, which would bring the whole system to a halt.
- PoW is therefore integral to the process of maintaining digital scarcity, and improving on the current failings of the fiat system, with its infinite supply.

# Bitcoin

## Bitcoin's mining puzzle

- The computational puzzle is in the form of a hashing algorithm called SHA256.
- A hash is a unique one-way identifier for a digital record that enables privacy and security.
- The hashed block details are: version number, a timestamp, the hash from the previous block, the hash of something called the Merkle Root, a random number called a nonce etc.
- In the early days, Bitcoin could be mined using the GPU - Graphics Processing Unit - in an ordinary home computer, originally designed to speed up the rendering of graphics, especially in PC gaming.
- Today, Miners use specialist hardware, known as mining rigs, that use application-specific integrated circuits, or ASICs. These are computer processors that have been optimised to solve the math problem that is at the heart of bitcoin mining.

# Potential benefits of Bitcoin

- Maintaining a permanent and transparent record of transactions on the blockchain
- Faster payment processing
- Cutting down on transaction fees from third parties
- Supporting international payment processing
- Simplifying processing of high-value payments
- Reducing the paperwork associated with banking accounts by using wallets
- Domestic and international transactions confirmed within an hour regardless of size
- First truly global (and non-national) currency

# Issues with Bitcoin

- The fact that there is no centralized control means that there is no arbitrator if issues arise.
- For instance, if a wallet owner loses his/her private key, that user cannot participate in the network.
- Also, even though the blockchain itself may be very challenging to hack, attackers have become very creative with respect to how they can steal from wallets.
- The growth in cryptocurrencies has also spawned many fraudulent tokens which continue to attract investors.

# Issues with Bitcoin

- How to get the overall Bitcoin community to upgrade its software and protocols with respect to changing the size of the blocks that are mined.
- **The Scaling Problem:** One of the biggest controversies is with respect to changing the size of the blocks that are mined.
- Currently, the standard protocol is that they are about 1 MB in size and it takes roughly ten minutes to mine a new block. However, the more transactions that use bitcoin, the longer it may take for those transactions with low or no transaction fees to get verified and included in a new block.
- This is because transaction fees are incentives for miners.

# Issues with Bitcoin

- This means that only three or four transactions are processed per second as compared to a credit card company like Visa which can process over 20,000 transactions a second.
- Those unprocessed transactions will sit longer in a queue. This issue is what is termed a “scaling” problem.
- One solution that has been hotly debated among Bitcoin Core developers is the idea of increasing the block size to 2 MB instead of 1 MB.
- This would double the number of transactions that could be bundled into a block. This change has not been incorporated into the BTC protocols since some were concerned that it would put smaller miners at a disadvantage.
- For now, increasing transaction fees is being employed as a more natural way to manage the growth of BTC.

# Forks

- A **fork** is a mechanism for adding new features to the blockchain or for dealing with the effects of hacking or some kind of disastrous bug in the system.
- In order for a change to the protocol to occur, there must be a consensus of the users of the network.
- A **hard fork** is when a majority of the nodes agree to change the protocol in a way that is incompatible with the old rules. For example, a hard fork would be required if a consensus of BTC miners decided to increase the size of blocks to 2 MB.

# Forks (Contd.)

- A **soft fork** is a change to the protocol that is backward-compatible, meaning it does not require all nodes on the network to upgrade to the new rules.

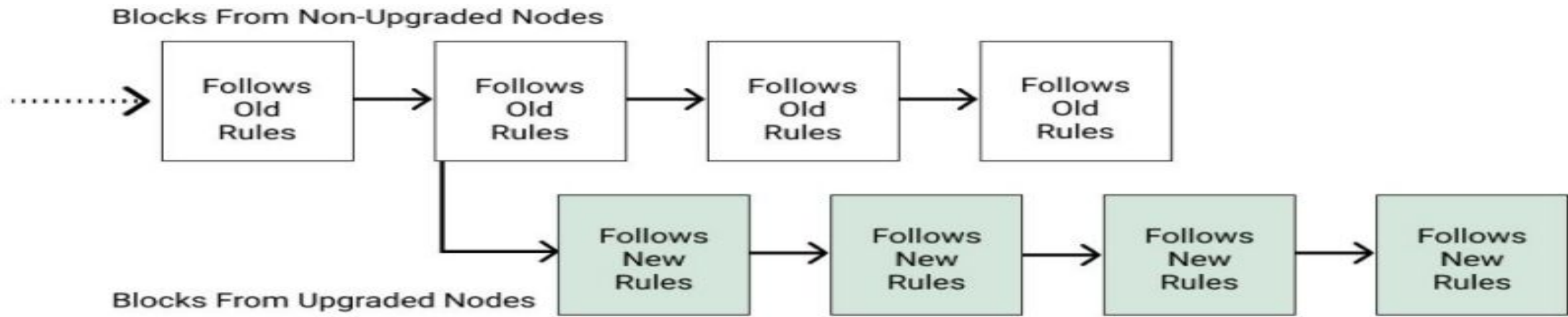


# Forks (Contd.)

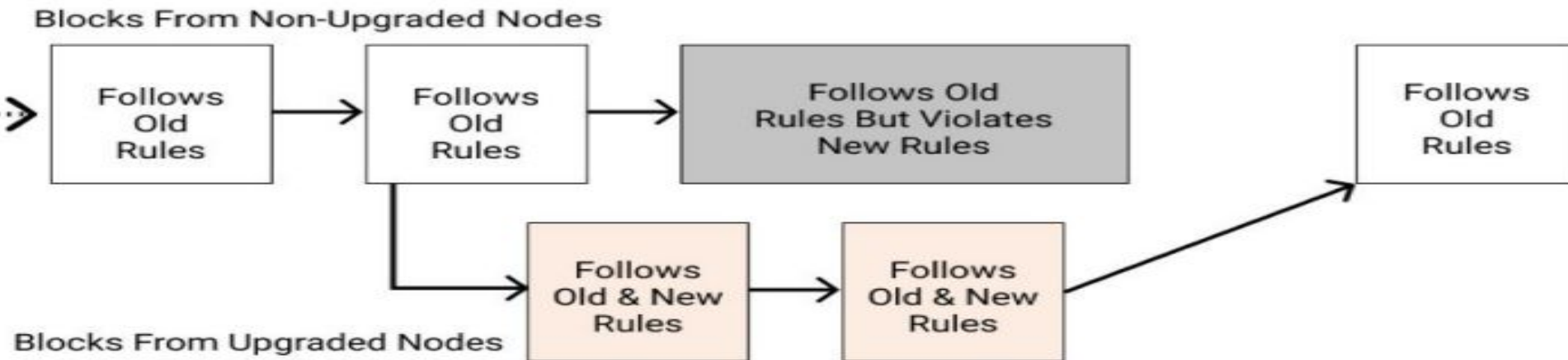
- **Soft fork:** It refers to a change or update to the protocol that is backward-compatible, meaning it does not result in a permanent divergence of the blockchain. Instead, it introduces new rules that are more restrictive than the existing ones, allowing nodes that have not upgraded to continue participating in the network without disruption.
- **1. Backward Compatibility:** In a soft fork, the changes made to the protocol are designed to be compatible with the existing rules. This means that nodes running the old version of the software will still recognize blocks produced by nodes running the updated software as valid.
- **2. New Rules:** Despite being backward-compatible, a soft fork introduces new rules or restrictions to the protocol. These rules typically involve tightening the consensus mechanism or adding additional validation criteria for blocks to be considered valid.
- **3. Continued Consensus:** Despite the introduction of new rules, nodes that have not upgraded to the latest software version can still participate in the network. They will accept blocks that comply with both the old and new rules, ensuring that consensus is maintained across the network.

# Forks (Contd.)

- **4. Temporary Fork:** During a soft fork, there may be a temporary split in the blockchain, where some nodes follow the old rules and others follow the new rules. However, because the new rules are backward-compatible, the split is temporary, and the network eventually converges back to a single chain once a supermajority of nodes have upgraded to the new software.
- **5. No Chain Split:** Unlike a hard fork, which results in a permanent divergence of the blockchain, a soft fork does not lead to a chain split. Both upgraded and non-upgraded nodes continue to operate on the same blockchain, with the new rules being gradually adopted by the majority of the network.



A Hard Fork: Chain Diverges And Non-Upgraded Nodes Continue With Old Rules



A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

# Ethereum

- Ethereum is the leading candidate for Blockchain 2.0.
- Vitalik Buterin, after studying Bitcoin, first proposed the idea of Ethereum in a 2013 whitepaper.
- The core idea was that a distributed ledger could be used not just to store and validate transaction records but also contracts or instructions and the scripts required to execute the instructions.
- Ethereum is a permissionless and public blockchain where miners obtain “ether” as the digital token for validating transactions and creating new blocks.

# Ethereum Attack

- Ether does function as a cryptocurrency and can be traded on altcoin exchanges, but it should also be thought of as a token that allows for the management of a finite resource, namely computing power.
- “The DAO” attack.
- Hackers attacked DAO because it was vulnerable. It allowed the hackers to drain almost one-third of ether. There was a token sale for 28 days. Many investors invested money and DAO raised \$150 million worth of ethers, But before the end of the token sale, one of the onlookers was concerned about vulnerability. There was a bug in smart contract wallets. While the programmers were fixing the bug issue, the attacker exploited other loopholes in the code and started to steal funds. He attacked by making a small contribution and requested withdrawal using a recursive function. In this way, the attacker was able to draw almost 3.6 million ether. At that time 3.6 million ether was equivalent to **70 million dollars and the price of ether dropped from \$20 to \$13.**

# Response to DAO attack

- The DAO Hack resulted in financial losses. It also posed a threat to upcoming Ethereum and Blockchain technologies. The hack also put a question mark on the security of Ethereum.
- The Ethereum community was tensed and held many discussions.
- The failure of DAO had a negative impact on cryptocurrency as investors were afraid to invest money.
- Ethereum founder Vitalik Buterin proposed a soft fork proposal that allowed them to blacklist the hacker so that no further funds were siphoned.
- In response to this proposal, attackers claimed that they had done it in a legal way in accordance with the smart contract. The attackers were ready to take legal action

# DAO Hack Remedy Forks Ethereum

- The majority of the investors agreed to the Hard Fork Proposal and it was implemented. Those who didn't agree with the proposal led to the division of the blockchain. The pre-forked version is known as Ethereum Classic(ETC). Some of the consequences are:
- The history of Blockchain was altered due to the hard fork proposal.
- The attacker did not lose all the money despite the restoration of funds to their respective owners. It is estimated that \$8.5 million were in their possession.
- The DAO Hack and the hard fork proposal shook the entire community.
- The DAO realized the importance of Blockchain security.

# Soft fork proposal

- Vitalik Buterin introduced a soft fork proposal.
- It allowed them to insert a code snippet that would blacklist the attackers from performing any further transactions.
- On the other hand, this proposal reduced the amount of ether.
- In response to the soft fork proposal, the hackers tried to prevent the soft fork proposal by bribing the miners. This also put a question on the moral ethics of the miners.



# Hard fork proposal

- The hard fork proposal is the proposal that allowed the community to make a permanent divergence from the original Blockchain. It makes it compulsory that all nodes in the Blockchain should be updated to the latest version. All miners should adhere to the new rules. The consequences of the proposal are as follows:
- It leads to the separation of the Blockchain so that the two versions are not compatible with one another.
- Doing the divergence, it allowed the investors to withdraw their original money.

# Response to Hard Fork Proposal

- This proposal had the capacity to withdraw all the cryptos and transfer them to a new smart contract. The function of this smart contract was to withdraw. The consequences are as follows:
- The reaction was mixed as Blockchain was supposed to be immutable and rolling back to a different Blockchain was against the law.
- Lots of discussions among Miners, community members, etc were held. Voting was done.
- The majority of the miners about 89% agreed to the hard fork proposal. Finally, this proposal was accepted.
- This proposal was implemented in the 19,20,000th block that is on 20 July 2016.

# Response to Hard Fork Proposal

- The blockchain split into two:
- 1. **Ethereum (ETH)**: Implemented the hard fork, effectively reversing the attack.
- 2. **Ethereum Classic (ETC)**: Continued on the original chain without any alterations, maintaining the principle of immutability.

# Digital Token Exchanges

- In the early days of cryptocurrencies and digital tokens it was difficult to buy and sell coins.
- There was special software to install and difficult financial transfers to set up depending on the geographical location.
- This led to many potential investors to turn away from investing in cryptocurrencies.

# Digital Token Exchanges

- But the emergence of **digital token** or **cryptocurrency exchanges** has made this much more straightforward.
- Cryptocurrency exchanges are similar to the exchanges we understand in our financial markets today, such as the New York Stock Exchange, where stocks are traded.
- An **exchange** or “**digital currency exchange**” (**DCE**) might be considered as an entry and exit ramp into the world of cryptocurrencies. **DCEs are set up as online platforms to allow users to trade their digital currencies and tokens for other digital currencies or for traditional fiat money like dollars and euros.**

# Digital Token Exchanges

- Recently governmental regulation has focused on controlling exchanges and the cryptocurrencies that they are allowed to handle.
- This makes sense because regulatory bodies often pay most attention to places where an asset is exchanged for fiat value (traditional money), since that is where fraud, money laundering, and investment regulations can come into play.

# Digital Token Exchanges

- Exchanges make money by charging fees for each transaction, but these can vary widely from a flat fee to a certain percentage.
- Also, cryptocurrency exchanges may be quite different in terms of what payment options they accept.
- Some accept credit cards like Visa or PayPal but charge a relatively higher fee.
- Many banks and exchanges have disallowed this practice, since banks do not want to have to protect against fraud in cryptocurrency transactions.
- Some are limited to customers in the country where they are located and others like Kraken, can handle customers worldwide.

# Digital Token Exchanges

- Exchanges can serve as:
- **1. Trading Platforms** – basic websites that connect buyers to sellers and take a transaction fee. May provide access to **sophisticated trading tools** and require an account to be set up.
- **2. Brokers** – similar to currency trading dealers, they allow anyone to buy and sell but at the prices which they determine.
- **3. Direct Trading Platforms** – function to connect individual traders to each other to buy and sell at the prices which the individual sellers determine. Popular in global trading settings.



# Digital Coin Exchange

- A few of the most stable exchanges today are

- Coinbase
- Bitstamp
- Kraken

# Decentralized Exchanges

- The exchanges listed above are essentially third parties or intermediaries helping you exchange your tokens.
- By using an exchange, you are re-intermediating the direct transactions that blockchains enable.
- **Several groups are working on creating decentralized exchanges – or simply, protocols that allow you to exchange across tokens with others without using a company in the middle.**
- **The centralized exchanges we know today are more readily targeted by attackers since they hold many accounts worth of tokens at any given time.**

# Decentralized Exchanges

- Currently there exist several projects to try to decentralize the way that tokens can be exchanged.
- These include but are not limited to OmiseGo, Ox Protocol, and Airswap.
- The functionality of decentralized exchanges is being built, but does not yet rival the centralized versions.
- They are harder to use and lack the liquidity of the larger, centralized exchanges. In the long run however, they should grow since they are designed to have less down-time, more privacy, and less censorship potential.

# OTC exchanges

- OTC (“over the counter”) exchanges for cryptocurrencies have grown immensely in recent years.
- The idea of OTC token trading is that they can handle large blocks of tokens by negotiating more directly with brokers.
- Trades are not on a typical exchange and so are considered to be “off the books” and just involve transfers to and from individual wallets.
- Messaging between buyers and sellers is handled by texting or by tools like Skype.
- Genesis Trading is an example of this type of firm. Based in New York City, they began connecting institutional investors to 192 buy/sell large blocks of bitcoin in 2015. They have since expanded to include ether, Litecoin, and Ripple in their stable of cryptocurrencies. Their minimum transaction size is \$25,000, so they are generally not focused on the consumer market.

# Financial modelling for cryptocurrencies

- The goal of financial modeling is to try and predict a firm's financial performance.
- Mathematical models are built to make use of historical data, often coming from three key financial statements: **the income statement, balance sheet, and cash flow statement.**
- This **Three-Statement Model** is part of the basic education of all business students.
- More advanced financial models are used to analyze mergers and acquisitions, discounted cash-flows (using NPV-Net Present Value), IPO valuation models for pricing initial public offerings, forecasting, and also options pricing models.

# Financial modelling for cryptocurrencies

- There are some **relative valuation models** that attempt to value cryptocurrencies relative to others.
- One such model is called the **Equation of Exchange Monetary Model** which attempts to put a value on the network, supply, and velocity of a cryptocurrency.
- On-chain transactions are used here as a measure of the value of the network itself.
- Other metrics that are used to value cryptocurrencies include:
  - **1. Network Value to Transactions Ratio (NVT)** – this measures the currencies market cap relative to daily transaction volume Transactions Per Second – this is an especially important ratio for those digital tokens aspiring to reach the consumer market.
  - **2. User Characteristics** – namely, how is the ownership of a token distributed throughout the wallets
  - **3. Mining Profitability** – measuring the number of big and small miners and their profitability.
  - **4. Exchange Trading** – Looking at how many exchanges are supporting a token, and how trading is dispersed among them.