Bitcoin and Crypto-Assets: Study Guide

This study guide covers **Unit 3: Bitcoin and Crypto Assets** in depth. We start with simple definitions and progressively delve into advanced concepts. Each section includes examples, case studies, tables or charts where helpful, and ends with a summary and sample exam questions (7–10 marks) with detailed answers. All content is cited from authoritative sources [1] [2].

What Are Crypto-Assets?

- **Definition:** Crypto-assets are purely digital assets that use cryptography and decentralized ledgers (blockchains) to establish and record ownership. They exist only in digital form (no central issuing authority) and can represent value, rights, or ownership of anything from money to physical goods [3] [1].
- **Key Features:** They rely on *public blockchain networks* where transactions are recorded. Crypto-assets can serve as a *medium of exchange*, a *store of value*, or a *unit of account* [3] [1]. Examples include currencies (like Bitcoin), tokens on platforms (like ETH on Ethereum), or digital representations of physical assets.
- **Categories:** All crypto-assets fall into three broad categories [3] [4]:
- **Cryptocurrencies:** Digital currencies (coins) that operate on their own blockchains and function like money (e.g. Bitcoin).
- **Crypto-commodities:** Tokens representing commodities or services (e.g. gold-backed tokens, or Ether used to pay for computation on Ethereum).
- **Crypto-tokens:** Tokens issued on top of existing blockchains to represent utilities, securities, stable values, governance rights, etc.
- **Examples of Crypto-Assets:**
- *Bitcoin (BTC):* The first and most famous cryptocurrency (a digital peer-to-peer cash system) [5].
- *Ethereum (ETH):* A blockchain platform with its own currency (Ether) that enables smart contracts and decentralized apps.
- *Ripple (XRP):* A digital payment protocol/token for fast international money transfers.
- Others include Litecoin, Bitcoin Cash, Cardano, and many hundreds of altcoins and tokens (some acting as digital currencies, others as specialized tokens).
- **Evolution:** Bitcoin launched in 2009 as the first crypto-asset (a "digital peer-to-peer payment system" allowing transfers without banks) [5]. Since then, thousands of crypto-assets have emerged, each with unique uses, rules, and technologies. Many new assets (**altcoins**) try to improve on Bitcoin's model [5] [6].

Table 1: Categories of Crypto-Assets

Category	Description	Examples

Category	Description	Examples
Crypto-Commodities	Tokens representing real-world commodities or resources, secured by proof-of-work or backed by physical goods.	Gold-backed tokens (PAX Gold), Basic Attention Token (digital ad attention)
Crypto-Tokens	Digital tokens built on existing blockchains (e.g. Ethereum) representing utilities, securities, governance rights, stable values, etc.	Utility tokens (BAT), Security tokens (tZero), Stablecoins (USDT)

Summary

Crypto-assets are the broadest value on blockchains: digital coins or tokens secured by blockchain technology [3] [1]. They include decentralized digital currencies (cryptocurrencies), tokens tied to commodities, and other tokens with various uses. Bitcoin pioneered this field as a peer-to-peer currency [5]. Now thousands of crypto-assets exist, each defined by its network and rules.

Sample Exam Question 1 (7 marks): *Define crypto-assets and describe their three main categories with examples.*
Sample Answer: Crypto-assets are purely digital assets that use blockchain technology and cryptography to prove and record ownership [3]. They function as value carriers, similar to digital cash or tokens, on decentralized networks. The three main categories are: (1) **Cryptocurrencies**, which are native digital currencies on their own blockchains, acting as money (e.g., Bitcoin, Litecoin) [6]; (2) **Crypto-commodities**, which represent commodities or resources via tokens (e.g., gold-backed tokens like PAX Gold, or tokens used to pay for computation like Ether) [7]; and (3) **Crypto-tokens**, which are tokens issued on existing blockchains for various utilities or rights (e.g., utility tokens like Basic Attention Token, security tokens like tZero, or stablecoins like USDT) [8] [9]. Each serves different purposes: cryptocurrencies as currency, commodity tokens as digital commodity representation, and other tokens as specialized digital assets or rights.

Cryptocurrencies

- **Definition:** A *cryptocurrency* is any form of currency that exists only in digital form, typically has no central issuing authority, and relies on a decentralized blockchain ledger to record transactions [6]. It uses cryptography to secure transactions and control creation of new units.
- **Characteristics:**
- **Decentralization:** No single bank or government controls it.
- **Digital-only:** No physical coins or notes; balances exist only in blockchain ledgers.
- **Cryptography:** Transactions are secured by digital signatures and hashing to prevent fraud or counterfeiting [6].
- **Currency Function:** Functions as a *digital asset* for buying goods/services or value storage on its blockchain [6].
- **Minting Protocol:** New coins are issued according to protocol rules (e.g., Bitcoin's supply is capped at 21 million, issued via mining rewards) [6].
- **Examples:**
- **Bitcoin (BTC):** The first cryptocurrency, created in 2009. It was designed as a peer-to-peer payment system allowing transfers without banks [5].

- **Altcoins:** Any cryptocurrency launched after Bitcoin on its own blockchain (e.g., Litecoin, Ripple, Ethereum's Ether). These often try to improve on Bitcoin's features (e.g., faster transactions) [6] [10].
- **Ether (ETH):** While primarily a platform token for Ethereum, Ether itself functions like a cryptocurrency used to pay transaction fees on Ethereum.
- **Economic Role:** Cryptocurrencies have their own built-in monetary policies (like controlled supply schedules), and market dynamics set their value [6]. They are often called "currency tokens" and can be traded on exchanges.

Summary

A cryptocurrency is a digital currency secured by cryptography and recorded on a decentralized blockchain [6]. Bitcoin is the archetype, enabling trustless peer-to-peer payments without banks [5]. Altcoins are cryptocurrencies derived from or inspired by Bitcoin, each with unique protocols. They are digital stores of value and media of exchange, governed by their code and market forces.

Sample Exam Question 2 (7 marks): *Explain what a cryptocurrency is and how it functions, using Bitcoin as an example.*
Sample Answer: A cryptocurrency is a form of digital currency that exists only in electronic form, without a central issuing authority, and secured by a blockchain [6]. It uses a decentralized ledger to record all transactions and relies on cryptography to prevent fraud. Cryptocurrencies are issued and transferred according to algorithmic rules; for example, Bitcoin's protocol controls the creation of new coins and the ledger of transactions. Bitcoin, the first cryptocurrency, allows users to send and receive digital coins peer-to-peer without banks [5]. Its blockchain verifies transactions via mining (proof-of-work) and ensures no double-spending. Bitcoin serves as a store of value and medium of exchange, with its value determined by supply limits and market demand [6].

Crypto-Commodities

- **Definition:** Crypto-commodities are tokens that represent ownership or rights to real-world commodities or economic resources. They are essentially *digital versions of traditional commodities*, secured by blockchain protocols. Like commodities, their value comes from the underlying asset or service.
- **Characteristics:**
- **Asset-Backed:** Many are *backed by physical assets* (e.g., each token may correspond to a gram of gold in vault) [11].
- **Blockchain Security:** They leverage the security of major cryptocurrencies (often Bitcoin's proof-of-work) to secure transactions [7].
- **Value Pegging:** Their value tends to track the real-world commodity (e.g., a gold token's price follows gold's price).
- **Fractional Ownership:** They can fractionalize ownership of high-value items (e.g., gold bars, real estate) and make them tradable globally.
- **Examples:**
- **Gold-Backed Tokens:** Tether Gold (XAUT), PAX Gold (PAXG) are tokens where each unit represents a fixed amount of physical gold in a secure vault [12] [13]. Holders can redeem tokens for actual gold or sell them like cryptocurrency.
- **Silver-Backed Tokens:** Similar to gold tokens (e.g., SilverCoin), each token equals some silver in storage [14].

- **Oil/Energy Tokens:** Tokens pegged to barrels of oil or renewable energy projects (e.g., oil-backed tokens track crude oil price) [15].
- **Agricultural Commodity Tokens:** Tokens representing rights to grain, coffee, etc., with blockchain-verified supply chains [16].
- **Digital Attention (BAT):** The *Basic Attention Token* is a crypto-commodity that represents user attention in digital advertising. It's earned by viewing ads on the Brave browser and spent to reward content creators [17].
- **Asset-Backed Tokens:** Platforms like Everledger tokenize unique assets (diamonds, art) to prove authenticity. For example, Everledger issues digital tokens for each diamond on the blockchain [11].
- **Significance:** Crypto-commodities make illiquid or hard-to-transfer assets easily tradable. They enable new markets (e.g., investing in gold via blockchain) and improve transparency (via tokenized supply-chain tracking) [7] [11].

Summary

Crypto-commodities are digital tokens representing commodities or physical assets [7]. Examples include gold- or oil-backed tokens, and tokens for carbon credits or renewable energy. They are secured like cryptocurrencies but derive value from real-world assets. This tokenization allows fractional ownership and global trading of commodities (e.g., gold tokens like PAX Gold) [11].

Sample Exam Question 3 (7 marks): *What are crypto-commodities? Give examples of two crypto-commodity tokens and explain how they work*.

Sample Answer: Crypto-commodities are blockchain tokens that digitally represent ownership of traditional commodities or resources [7]. They are backed by, or pegged to, physical assets. For example, *Tether Gold (XAUT)* is a token where each unit equals one troy ounce of gold stored in vaults. The token's value tracks the real gold price, and holders can redeem tokens for actual gold. *PAX Gold (PAXG)* works similarly. Another example is the Basic Attention Token (*BAT*), which represents user attention in the digital advertising ecosystem: users earn BAT by viewing ads, and advertisers spend BAT to purchase attention [17]. In all cases, the token's blockchain ledger ensures transparency (ownership and provenance are recorded) and security, while the underlying commodity provides intrinsic value.

Crypto-Tokens and Token Taxonomy

- **Cryptotokens:** Crypto-tokens are digital assets issued on top of existing blockchains (usually Ethereum). They do not have their own blockchain but leverage another's infrastructure. Tokens can represent utilities, assets, or rights within a platform. In finance terms, they mirror asset classes like stocks or bonds (e.g., governance rights, dividends) but in digital form [18].
- **Coins vs. Tokens:**
- *Coins* (cryptocurrencies) are native to a blockchain (e.g., BTC on Bitcoin, ETH on Ethereum) [19] [20].
- *Tokens* are created and operate on existing blockchains. For example, the ERC-20 tokens run on Ethereum, ERC-721 (NFTs) also on Ethereum.
- **Key differences:** Coins serve as the primary currency of a blockchain, securing it and paying fees [21] [20]. Tokens can represent anything (utility, security, etc.) and derive value from their use-case in an application [22].

- **Token Classification:** Blockchain tokens are often classified by their function or value type [18]. The major categories include:

- **Network Tokens:** Tokens created by the network itself, used to operate the blockchain's core functions (node staking, governance, or transaction fees) [8]. For example, *Ether (ETH)* is a network token: it's traded on exchanges like a coin but primarily used to pay for computation (gas) on Ethereum [8] [23]. Another example: Steem (STEEM) is used for posting and rewarding on the Steem social platform.

- **Utility Tokens:** Also called *app tokens* or *app coins*, these give holders access to a service or product. They are issued by a project at launch (often via ICO) and used within that ecosystem [24]. For instance, *Basic Attention Token (BAT)* lets users earn and spend tokens for attention in the Brave browser. *Numeraire (NMR)* is used to participate in the Numerai data trading platform [24].
- **Security Tokens:** These represent investment contracts or shares in a company, backed by real assets or profit streams [25]. They are analogous to stocks or bonds and often regulated as securities. For example, tokens issued by platforms like Polymath or tZERO represent equity in a business or assets. *Digix Gold Tokens (DGX)*, while commodity-backed, act similarly by representing gold ownership and are subject to regulation [26].
- **Stablecoins:** Cryptocurrencies pegged to stable assets (like fiat currency or commodities) to reduce volatility [27]. For example, *Tether (USDT)* and *USD Coin (USDC)* are pegged 1:1 to the US dollar [9]. They're used as a stable medium of exchange or for trading pairs to avoid crypto price swings.
- **Governance Tokens:** Grant holders voting rights in a protocol (e.g., Maker's MKR, Compound's COMP) allowing them to influence system parameters.

- **Others:** Reputation or reward tokens in specific platforms (e.g., Steem reward tokens).

- **Examples of Tokens:**

- Network: *Ether (ETH)* (Ethereum), *DfN* (Dfinity token).
- Utility: *Basic Attention Token (BAT)*, *Enjin Coin (ENJ)*, *Filecoin (FIL)* (storage utility).
- Security: *tZero (TZROP)*, *Swarm (SWM)*.
- Stable: *Tether (USDT)*, *Dai (DAI)*, *PAX Gold (PAXG)*.
- **Token Uses:** The token classification often overlaps (e.g., ETH is both currency and network token) [23]. The classification helps understand a token's role: whether it provides utility access, investment exposure, or stable value.

Table 2: Token Types and Characteristics

Token Type	Function	Example
Network Token	Powers a blockchain network (pay fees, governance)	Ether (ETH) on Ethereum [8]
Utility Token	Access/use a product/service in a decentralized app	Basic Attention Token (BAT), Numeraire (NMR) [24]
Security Token	Investment contracts backed by real-world assets/earnings	tZERO (TZROP), Digix Gold (DGX) [25]
Stablecoin	Pegged to a fiat or commodity for price stability	Tether USD (USDT), USD Coin (USDC) [9]

Token Type	Function	Example
Governance Token	Voting/control rights in a protocol	Maker (MKR), Uniswap (UNI)

Summary

Crypto-tokens are digital units built on other blockchains (mostly Ethereum) to represent utilities, assets, or currencies. They differ from coins in that coins (like BTC, ETH) are native to a blockchain, while tokens run on top of one [19] [20]. Major token categories include network tokens (for blockchain operation), utility tokens (access services), security tokens (investment shares) and stablecoins (fiat-pegged tokens). Each has unique roles and examples (e.g. ETH, BAT, USDT) [8] [25].

Sample Exam Question 4 (10 marks): *Compare and contrast cryptocurrencies (coins) with crypto-tokens. Then classify and define network tokens, utility tokens, and security tokens with examples.*
Sample Answer: Cryptocurrencies (coins) are digital currencies native to their own blockchains (e.g., Bitcoin's BTC or Ethereum's ETH). They serve as the blockchain's primary asset and medium of exchange. Crypto-tokens, however, are assets created on top of existing blockchains (usually Ethereum) using smart contracts. Tokens may represent anything (services, assets, rights) and rely on another blockchain for security [19] [20].

Network tokens are created by the blockchain protocol itself to power its core functions. For example, *Ether (ETH)* is the network token of Ethereum: it's used to pay for transaction fees and computation on the network while also being tradable as a cryptocurrency [8]. Similarly, *DfN* tokens are needed to use the Dfinity blockchain.

Utility tokens (or "app tokens") give holders access to a specific platform or service. They are often sold in ICOs to fund projects. For instance, *BAT* tokens are used within the Brave browser's advertising system: users earn BAT by viewing ads, and creators are paid in BAT [24]. These tokens function like "coupons" for a service.

Security tokens are digital tokens that represent investment assets, similar to stocks or bonds [25]. They are backed by real-world assets or company equity. For example, *tZERO's* token represents equity in the tZERO firm, and regulators treat it like a security. *Digix Gold (DGX)* is another example: each DGX token represents ownership of physical gold and is subject to securities laws [28].

In summary, coins operate as blockchain-native currencies, while tokens run on established blockchains and serve varied purposes. Network tokens enable blockchain utility (ETH), utility tokens provide platform services (BAT), and security tokens grant investment rights (tZERO) [8] [25].

Initial Coin Offerings (ICOs)

- **What is an ICO?** An *Initial Coin Offering* (ICO) is a fundraising mechanism where a blockchain project sells new cryptocurrency tokens to investors in exchange for established cryptocurrencies (often Bitcoin or Ether) [29]. It's analogous to an IPO (Initial Public Offering) but for crypto projects.

Investors receive project tokens which may entitle them to use the service, dividends, or simply speculative value.

- **How It Works:** A project creates a new token (often on Ethereum using ERC-20 standard) and launches a smart contract to distribute tokens to investors. Investors send funds (e.g., BTC/ETH) to the contract and receive a proportional amount of the new token once the ICO concludes [29] . Many ICOs follow Ethereum's ERC-20 standard because it simplifies token creation (reportedly taking only ~30 minutes of coding) [30] .
- **Advantages:** ICOs allow startups to quickly raise capital from a global investor base without traditional intermediaries. They can bootstrap decentralized projects by distributing tokens to early backers.
- **Disadvantages/Risks:**
- **Fraudulent ICOs:** Many ICOs have been scams. Studies show a large fraction of ICOs were fraudulent [31] . Red flags include guarantees of huge returns, plagiarized whitepapers, fake team profiles, and celebrity endorsements. For example, WSJ found 271 out of 1,450 ICOs were likely fraudulent, raising ~$1 billion [31] .
- **Regulatory Uncertainty:** Tokens might be classified as securities by regulators (e.g., SEC in the US), imposing legal constraints. Some projects use frameworks like **SAFT** to pre-empt regulation by treating tokens as future deliverables [31] .
- **Volatility and No Guarantee:** There is no guarantee token prices will rise; many fail after launch. Investors can lose their entire investment if the project falters.
- **Real-World Note:** The ease of launching ICOs (via open-source Ethereum tools) means virtually anyone can create a token and raise funds. This democratizes fundraising but also means that due diligence is crucial. [29] [31] .

Summary

An ICO is a blockchain fundraising event where investors buy project tokens with established cryptocurrencies [29]. It's like a crowd-funded IPO. While ICOs have raised billions, they carry high risk: many projects are scams or fail, as highlighted by fraud studies [31]. The ERC-20 Ethereum standard has made token launches easy, fueling the ICO boom (and scams) [30].

Sample Exam Question 5 (10 marks): *Describe the process of an Initial Coin Offering (ICO). What are the potential advantages and disadvantages of ICOs for fundraising?*

Sample Answer: An ICO (Initial Coin Offering) is a method for a blockchain project to raise funds by issuing new cryptocurrency tokens to investors [29] .The process typically involves: (1) **Token Creation:** The project creates a digital token (often using Ethereum's ERC-20 standard) with defined functionalities or rights. (2) **Fundraising Phase:** Investors contribute established cryptocurrencies (like Ether or Bitcoin) to a specified smart contract address. (3) **Token Distribution:** The smart contract automatically issues new tokens to investors' wallets in proportion to their contribution once the ICO closes [29]. Many ICOs provide a white paper explaining the project, token economics, and roadmap.

Advantages: ICOs allow startups to quickly raise large amounts of capital from global investors without traditional intermediaries (like banks or venture capital). They democratize funding: anyone can invest, and contributors receive tokens that may grant use of a service or governance rights. The use of standard token protocols (e.g., ERC-20) makes launching an ICO relatively easy and fast [30] .

Disadvantages/Risks: The ICO space has seen **many fraudulent and poorly planned projects**. As noted by a Wall Street Journal study, a significant percentage of ICOs were scams [31]. Risks include: *fraudulent white papers or teams*, *impossible profit promises* (some ICOs guaranteed 40%+ monthly returns), and *pump-and-dump schemes*. Investors often lack legal protection. Tokens may be unregulated securities, leading to regulatory crackdowns. In fact, because some tokens may be deemed securities, projects might face SEC enforcement. Overall, while ICOs can yield high rewards, they carry high risk and require caution [31].

Bitcoin: The First Cryptocurrency

- **Origin (2009):** Bitcoin was introduced in Satoshi Nakamoto's 2008 white paper and launched with a genesis block in January 2009 [5]. It was designed as a **peer-to-peer digital cash system** that requires **no central authority** [5].
- **Purpose:** To enable direct online payments between users, eliminating intermediaries like banks or credit card companies [5]. It addresses the double-spending problem (preventing the same coin from being spent twice) through its blockchain mechanism.
- **Blockchain and Transactions:**
- Bitcoin's blockchain is a public ledger where all transactions are recorded in blocks, each linked to the previous. Each transaction references unspent outputs (UTXOs) from prior transactions.
- **Nodes and Wallets:** Anyone can run a Bitcoin **node** (full ledger copy). Users store Bitcoin in digital *wallets* (key pairs). When spending, a transaction is created (consuming UTXOs) and broadcast to the network.
- **Transaction Finality:** A valid transaction cannot be altered once included in a block on the blockchain. Confirmations accumulate as more blocks are added, making reversals practically impossible.
- **Mining and Consensus (Proof-of-Work):**
- Bitcoin uses the PoW consensus algorithm. **Miners** collect pending transactions from the network (the *mempool*) and package them into a candidate block. They then perform computational work to find a hash below a target difficulty. The first miner to solve this puzzle broadcasts the block, which is added to the chain [2].
- **Double-Spend Prevention:** Because adding blocks requires solving hard puzzles (PoW), altering a past transaction would require re-mining all following blocks, which is computationally infeasible [2]. Thus, PoW ensures trust: it's prohibitively costly for any malicious actor to overwrite history, effectively solving double spending [2].
- **Difficulty Adjustment:** Every 2,016 blocks (~2 weeks), Bitcoin's protocol adjusts the mining difficulty so that blocks remain ~10 minutes apart, regardless of total network hashrate.
- **Mining Rewards:** Miners are rewarded with new bitcoins and transaction fees. Initially 50 BTC per block, the reward halves approximately every four years (to 25 BTC, 12.5 BTC, etc.) until all 21 million BTC are minted.
- **Monetary Policy:**
- **Fixed Supply:** Bitcoin's total supply is capped at 21 million. This scarcity is built into the protocol to mimic deflationary assets (akin to gold) and resist inflation [32].
- **Halving:** The scheduled halving of block rewards is meant to approximate a controlled supply increase, eventually tapering to zero new issuance.
- **Store of Value:** Many view Bitcoin as "digital gold" due to its scarcity and security. It allows for censorship-resistant value storage because no government can arbitrarily create more or seize it (except by confiscating private keys).
- **Key Functions:**

- **Ledger Maintenance:** Bitcoin's network maintains an accurate ledger of all unspent transactions [33].
- **Transaction Validation:** Nodes verify digital signatures and UTXO availability.
- **Finality:** Once a transaction is 6+ confirmations deep, it is considered final.
- **Incentives:** Miners are economically incentivized to behave honestly (earning rewards) [2].
- **Benefits:**
- **Decentralization and Security:** No central point of failure or control.
- **Immutable Records:** Transactions cannot be modified once confirmed.
- **Global Transfer:** Enables censorship-resistant, cross-border transfers without intermediaries.
- **Fixed Monetary Policy:** Predictable inflation schedule (e.g., programmed halvings).
- **Trustlessness:** Users do not need to trust any intermediary; trust is placed in cryptography and consensus.
- **Challenges:**
- **Scalability:** Bitcoin's 1MB block size limits throughput (~7 transactions/sec). This causes delays and higher fees during congestion (see *Scalability* below).
- **Energy Use:** PoW mining consumes large electricity, raising sustainability concerns.
- **Irreversibility:** No way to reverse transactions; user mistakes or theft of keys result in permanent loss.
- **Custody:** Users are responsible for securing private keys; if lost, bitcoins are irretrievable.
- **Volatility:** As an emerging asset, Bitcoin's price can be highly volatile, making it challenging as a stable medium of exchange.
- **Scalability Issue and Forks:** As usage grew, debate emerged on how to scale Bitcoin. Two main proposals:
- **Increasing Block Size (Hard Fork):** Some (Bitcoin Cash) increased block size to allow more transactions. This is a *hard fork* – incompatible protocol change.
- **Layer-2 Solutions:** Others advocate second-layer protocols (e.g., Lightning Network) to handle transactions off-chain, settling on-chain later.
- **Forks:**
- **Hard Fork:** A permanent split in the blockchain. Old nodes not upgraded cannot validate the new chain. Example: Bitcoin Cash (BCH) hard-forked from Bitcoin in 2017 to increase block size.
- **Soft Fork:** A backward-compatible change. Old nodes still recognize new blocks as valid. For example, SegWit was a soft fork introduced to fix transaction malleability and optimize block usage.
- Forks affect holders: after a fork, holders of the original coin at the fork point typically receive equal amounts on the new chain. For instance, Bitcoin holders received an equivalent balance in Bitcoin Cash after the split.

Summary

Bitcoin is the first and largest cryptocurrency, designed as a decentralized digital currency and ledger [5]. It uses Proof-of-Work mining to secure its blockchain and prevent double spending [2]. Bitcoin has a fixed supply schedule and no central authority. While it offers secure, censorship-resistant transfers, it faces challenges like limited transaction capacity and high mining energy use. Forks (hard or soft) have led to variants (e.g., Bitcoin Cash) as the community debates upgrades and scaling.

Sample Exam Question 6 (10 marks): *Describe how Bitcoin's consensus mechanism works to secure transactions and prevent double-spending. Include in your answer the role of mining and proof-of-work.*
Sample Answer: Bitcoin uses a **Proof-of-Work (PoW)** consensus mechanism to secure its network[2]. In this system, special participants called **miners** collect pending transactions and bundle them into blocks. To

add their block to the blockchain, miners must solve a computationally difficult cryptographic puzzle: they repeatedly change a value called a *nonce* in the block header and compute its hash. The goal is to find a hash value below a target threshold. This process requires significant computational power and energy.

When a miner finds a valid hash, their block is broadcast to the network. Other nodes verify the block's transactions and PoW. If valid, the block is **added to the blockchain** and the miner receives newly minted bitcoins and transaction fees as a reward. This mechanism secures the network because altering any past transaction would require redoing the PoW for that block and all subsequent blocks, which is computationally infeasible [2]. Thus, the PoW puzzle creates a barrier against double-spending and fraud.

Double-Spending Prevention: The PoW scheme means only the longest valid chain is accepted by nodes. If an attacker tries to reverse a transaction (double-spend), they would have to outpace the honest miners and create a longer chain. Given the immense computing power of the honest network, this is virtually impossible. As a result, once a transaction is 6+ blocks deep, it is considered final and irreversible.

In summary, mining and PoW ensure transaction finality: miners validate and commit transactions by doing real work [2]. This creates a secure, tamper-resistant ledger where double-spending is virtually eliminated.

Sample Exam Question 7 (10 marks): *Discuss the scalability challenges of Bitcoin and compare solutions involving hard forks versus layer-2 protocols.*
Sample Answer: Bitcoin's scalability challenge arises from its **block size limit (1 MB)** and target block time (~10 minutes), which cap the network at about 7 transactions per second. As usage grew, transaction backlogs increased, causing higher fees and delays.

To address this, two broad approaches emerged:

- **Hard Fork (On-Chain Scaling):** Some stakeholders propose increasing the block size or changing core rules. A hard fork is an incompatible protocol change; older nodes must upgrade or be left on an old chain. For example, *Bitcoin Cash* (BCH) hard-forked in 2017 to raise block size, allowing more transactions per block. The advantage of a hard fork is immediate increase in capacity. However, it can divide the community and risk security (larger blocks can centralize mining).

- **Soft Fork and Layer-2 (Off-Chain Scaling):** Other solutions keep the base layer unchanged or only use backward-compatible soft forks. A major soft fork was *Segregated Witness (SegWit)*, which restructured transactions to make blocks effectively carry more transactions and fix malleability. Layer-2 solutions like the **Lightning Network** take transactions off-chain: users open a payment channel and conduct many micro-transactions between them. Only the opening and closing of the channel are recorded on-chain. This greatly increases throughput and reduces fees without altering Bitcoin's core protocol.

In summary, hard forks (increasing block size) provide on-chain scaling at the cost of splitting consensus [29]. Layer-2 and soft-fork solutions aim to scale by moving activity off the main chain or optimizing data, preserving decentralization but requiring additional trust in protocols. Each approach has trade-offs in compatibility, security, and community agreement.

Ethereum and Blockchain 2.0

- **Ethereum Overview:** Ethereum is a blockchain platform introduced in 2015 that extends Bitcoin's concepts by supporting a Turing-complete scripting language for *smart contracts* [34]. Its native cryptocurrency is **Ether (ETH)**, used both as a currency and to pay for computation on the network.
- **Smart Contracts:** Unlike Bitcoin's limited scripts, Ethereum allows developers to write complex programs ("smart contracts") that run on the blockchain. These contracts automatically execute when conditions are met. This enables decentralized applications (DApps) in finance, gaming, supply chain, etc.
- **Ether (ETH):** Serves as *fuel* for the network. Every operation (transaction, contract execution) requires a small fee paid in ETH ("gas"), preventing abuse of resources. Ether is also traded on exchanges as a cryptocurrency.
- **Use-Cases:** Ethereum's flexibility led to many innovations like DAOs (decentralized organizations), DeFi platforms, and token standards (ERC-20, ERC-721 NFTs).
- **The DAO Attack (Case Study):** In 2016, a project called **The DAO** (Decentralized Autonomous Organization) raised ~$150M via a smart contract acting as a venture fund. In June 2016, a flaw in The DAO's contract was exploited: an attacker siphoned ~3.6M Ether (~$50M) into a "child DAO" [35]. To mitigate the loss, Ethereum's developers proposed a **hard fork**: they would rewrite history to move the stolen Ether to a rescue address.
- **Controversy and Result:** This decision was controversial because it violated the principle that "code is law." However, ~89% of miners agreed, and the fork was executed [36].
- **Split Blockchains:** The fork created two separate blockchains:
  - **Ethereum (ETH):** The new chain where the hack was reversed.
  - **Ethereum Classic (ETC):** The original chain that refused the fork to uphold immutability [36] [37].
- Today, Ethereum Classic continues as a separate cryptocurrency, while Ethereum moved on with the forked chain.
- **Ethereum 2.0 (Future Upgrades):** Ethereum is transitioning to Proof-of-Stake (Casper) to improve scalability and energy use, and implementing sharding to increase throughput (but details beyond this unit).

Summary

Ethereum generalizes Bitcoin's blockchain by supporting smart contracts and decentralized apps. Its cryptocurrency, Ether, powers the network. A key event was the DAO hack, which led to a contentious hard fork, creating Ethereum (ETH) and Ethereum Classic (ETC) [35] [36]. This highlighted both the power and risks of blockchain governance. Ethereum remains the leading platform for DApps and token issuance.

Sample Exam Question 8 (7 marks): *What is Ethereum and how does it differ from Bitcoin? Describe the DAO incident and its impact on Ethereum's blockchain.*

Sample Answer: Ethereum is a blockchain platform launched in 2015 that enables *smart contracts*—programmable code that executes on the blockchain. Unlike Bitcoin, which is primarily a digital currency, Ethereum's blockchain is Turing-complete, allowing developers to build decentralized applications (DApps) [34]. Its native currency, Ether (ETH), is used to pay for transactions and computation on the network.

The **DAO incident** occurred in June 2016. The DAO was a crowdfunded smart contract project (a decentralized venture fund). A hacker exploited a flaw in The DAO's code and drained about 50 million USD

worth of Ether [35]. To remedy this, Ethereum's developers executed a *hard fork*: they changed the protocol so that the stolen funds were returned to the investors. This decision broke the rule of immutable blockchain history, causing a split. The majority followed the new fork (now called Ethereum/ETH), while a minority stayed on the original chain, which became Ethereum Classic (ETC) [37] [36]. The DAO event showed Ethereum's flexibility but also raised debates on decentralization and code governance.

Other Crypto-Assets (Bitcoin Cash, Litecoin, Ripple)

- **Bitcoin Cash (BCH):** A hard-fork of Bitcoin launched in August 2017, increasing the block size limit (from 1MB to 8MB initially, then more). Its goal was to improve Bitcoin's transaction throughput [38]. BCH proponents believe larger blocks keep fees lower. It functions similarly to Bitcoin but with more capacity.
- **Litecoin (LTC):** Created in 2011 by Charlie Lee, it's a Bitcoin "light" (Lite-coin) with a few changes: faster average block time (2.5 min vs 10), different hashing algorithm (Scrypt vs SHA-256) [39]. It intended to be the silver to Bitcoin's gold, with faster confirmations and easier mining algorithm (though now also ASIC-mined).
- **Ripple (XRP):** Not a blockchain in the traditional sense. Ripple is a company/network with a consensus protocol and native token XRP. It's designed for fast, low-cost international settlements. Unlike Bitcoin, Ripple consensus does not rely on mining; instead, it uses a set of trusted validators to confirm transactions. XRP is used as a bridge currency between fiat in Ripple's network. Ripple Labs promotes it to banks and remittance services.
- **Others:** The crypto-asset space has many more (Cardano, Stellar, EOS, etc.), but Bitcoin, Ethereum, and top ones like XRP and Litecoin are most prominent in terms of market cap and recognition [40].

Summary

Besides Bitcoin and Ethereum, other notable crypto-assets include Bitcoin Cash (a Bitcoin fork with larger blocks) and Litecoin (a faster Bitcoin-like coin) [41]. Ripple (XRP) is a payment-focused crypto with a different consensus model (no mining). Each has unique design choices and use-cases, illustrating the diversity of crypto-assets.

Sample Exam Question 9 (7 marks): *Briefly describe Bitcoin Cash, Litecoin, and Ripple (XRP). How do they relate to Bitcoin or blockchain technology?*
Sample Answer: Bitcoin Cash is a cryptocurrency that forked from Bitcoin in 2017. Its main change is a larger block size limit, allowing more transactions per block to improve scalability. It shares Bitcoin's codebase and philosophy but raises throughput [38].

Litecoin is an early altcoin (2011) derived from Bitcoin's code. It uses a different hashing algorithm (Scrypt) and has a faster block time (2.5 minutes vs Bitcoin's 10 minutes) [39]. It was created to allow quicker confirmations and for more people to mine with CPUs/GPUs (though now also ASIC). Essentially, Litecoin's design makes it like "silver" to Bitcoin's gold.

Ripple (XRP) is different: it's both a company and a digital payment protocol. XRP is its native token used for cross-border payments. Unlike Bitcoin, Ripple does **not** use proof-of-work mining. Instead, a set of trusted validator nodes reach consensus to confirm transactions quickly (every few seconds). XRP is mainly used by banks and fintech for fast, low-cost international settlements. It is centralised relative to Bitcoin, as Ripple Labs controls much of its ecosystem.

All three are crypto-assets, but Bitcoin Cash and Litecoin are blockchains similar to Bitcoin (coins), while Ripple/XRP uses a different consensus and is geared toward banking use.

Digital Token Exchanges

- **Centralized Exchanges (CEX):** These are online platforms (like Coinbase, Bitstamp, Kraken) that act as intermediaries, matching buy and sell orders. Users deposit funds (crypto or fiat) into the exchange and trade with others on the platform. Key points [42] [43]:
- **Entry/Exit Ramps:** CEXs serve as gateways between fiat and crypto. They handle fiat deposits/withdrawals so users can buy crypto with dollars, euros, etc.
- **Trading Platforms:** Many exchanges offer a matching engine (order book) where users place limit or market orders [44]. They may also offer broker services (instant buy/sell at set prices) and peer-to-peer services.
- **Fees:** Exchanges charge transaction fees (e.g., 0.1–0.5% per trade) or flat fees for buying crypto. Fees vary by payment method (credit cards incur higher fees) [45].
- **Regulation:** Exchanges are often regulated as financial entities because they deal with fiat. They must comply with KYC/AML rules, which means users need to provide ID. Regulation focuses on exchanges to prevent fraud and money laundering [46].
- **Liquidity:** Large centralized exchanges have high liquidity and many trading pairs. However, they are often targets for hacking (e.g., Mt. Gox) and may restrict services by country.
- **Decentralized Exchanges (DEX):** Peer-to-peer platforms that allow users to trade directly from their wallets without a central party. They use smart contracts or protocols (e.g., Uniswap, 0x) [47]:
- **On-Chain Trading:** Trades happen on-chain or via atomic swaps. Users retain custody of funds, reducing counterparty risk.
- **Features:** DEXs often have lower liquidity and can be more complex, but offer privacy (no accounts/KYC), lower risk of central hacks, and censorship resistance [48].
- **Example:** Platforms like Uniswap use liquidity pools: users trade against a pool of tokens (and prices adjust algorithmically). Others like 0x protocol facilitate peer matching.
- **Over-The-Counter (OTC) Trading:** Large-scale trades negotiated directly between parties, usually via a broker or trading desk [49]:
- **Usage:** For institutions or high net-worth individuals needing to buy/sell large volumes (e.g., $100k+ in crypto) without slippage on exchanges.
- **How It Works:** Deals are often done “off-book.” The buyer and seller settle by transferring tokens from wallet to wallet, often communicated via private channels (chat, calls) [50].
- **Advantages:** Privacy and avoiding market impact. Firms like Genesis Trading facilitate large block trades in BTC, ETH, LTC, XRP, etc.[50].
- **Exchange Types Summary:**

Exchange Type	Characteristics	Examples
Centralized (CEX)	Fiat and crypto deposits, order books, KYC/AML, high liquidity, fees.	Coinbase, Kraken, Bitstamp [46] [44]
Decentralized (DEX)	On-chain peer-to-peer trades, no custody of funds, privacy, often lower liquidity.	Uniswap, 0x, Airswap [48]
OTC Trading	Direct large-volume trades off-exchange, negotiated pricing, minimal slippage.	Genesis Trading [50]

Summary

Cryptocurrency exchanges facilitate buying/selling tokens. **Centralized exchanges** (Coinbase, Kraken) act like traditional brokerages: users deposit funds, trade on order books, and face KYC checks[46]. **Decentralized exchanges** (e.g., Uniswap) let users trade directly via smart contracts, preserving privacy and custody[48]. **OTC services** handle large trades privately to avoid moving market prices[49]. Exchanges charge fees for trades and are increasingly regulated to prevent fraud.

Sample Exam Question 10 (7 marks): *Compare centralized, decentralized, and OTC cryptocurrency exchanges. What are their roles, and what are the trade-offs between them?*
Sample Answer: A **centralized exchange (CEX)** is a company-run platform (like Coinbase or Kraken) where users deposit crypto or fiat and trade via an order book. CEXs offer high liquidity and user-friendly interfaces, and handle fiat conversions (entry/exit to the crypto economy)[46][44]. However, they require user accounts, personal verification (KYC/AML), and control custody of funds (introducing counterparty risk). They can be targets for hacks (e.g., Mt. Gox) and may impose country restrictions.

A **decentralized exchange (DEX)** operates on blockchain protocols and smart contracts (e.g., Uniswap, 0x). Trades are peer-to-peer and on-chain, meaning users keep custody in their own wallets. DEXs enhance privacy (no account needed) and are harder to shut down or censor[48]. The downsides include generally lower liquidity and more complex user experience. Gas fees and slower settlement can also be issues.

OTC trading involves direct negotiation between large traders/brokers to exchange significant volumes. It bypasses public order books, preventing large trades from slippage or signaling. Firms like Genesis Trading arrange these deals[49]. OTC is suitable for institutional needs ($25K+ trades) and offers confidentiality. Its trade-off is that it is not accessible to average users and lacks the transparent pricing of public markets.

Financial Modeling for Cryptocurrencies

- **Valuation Challenges:** Cryptocurrencies lack traditional cash flows or earnings, making them hard to value with conventional methods. Their extreme volatility and novel nature require new metrics.
- **Relative Valuation Models:** Analysts use relative and on-chain metrics to gauge crypto value:
- **Equation of Exchange (Monetary Model):** Treats a cryptocurrency like a monetary system. It relates the *network's transaction volume (velocity)* to supply. One form:
  $$M \times V = P \times Q$$
  Where *M* is money supply (market cap), *V* is velocity (tx/sec), *P* is price, *Q* is quantity of transactions. A high transaction value (Q) and velocity (V) can justify a high market cap (M)[51].
- **Network Value to Transactions (NVT) Ratio:** Analogous to Price/Earnings ratio. It is market cap divided by daily transaction volume. A low NVT suggests the coin's price is justified by usage; a high NVT may indicate overvaluation or low utility[51].
- **Transactions Per Second (TPS):** For token to serve broad use (like a consumer currency), it needs high TPS capacity. Measuring actual TPS vs design TPS can indicate scalability.
- **User Adoption Metrics:** How many active wallets/users hold or transact the token. A wide distribution of token ownership can suggest greater decentralization and adoption[51].
- **Mining Profitability:** For mineable coins (like Bitcoin), metrics on miner activity and costs can impact price (e.g., if mining becomes unprofitable, fewer miners may threaten security).
- **Exchange Support:** Number and size of exchanges listing a cryptocurrency. More exchange availability and trading volume generally signal stronger adoption and liquidity[51].

- **Market Factors:** Speculation, regulatory news, macro trends (e.g., institutional investment, inflation hedging) heavily influence crypto prices, making modeling partly art.

Summary

Valuing cryptocurrencies often uses unconventional metrics. The *Equation of Exchange* model compares a coin's market cap to its network usage [51]. Ratios like NVT (market cap/transaction volume) help assess value relative to usage. Other factors include user adoption and miner economics. There is no universally accepted model, so analysts use a combination of technical indicators and market sentiment.

Sample Exam Question 11 (7 marks): *What financial metrics or models can be used to estimate the value of a cryptocurrency? Provide at least two examples and explain their rationale.*
Sample Answer: Traditional valuation (e.g., discounted cash flow) doesn't apply to cryptocurrencies, so analysts use usage-based and relative metrics [51].

One model is the *Equation of Exchange* (monetary model) which relates a token's market capitalization (supply * price) to its transaction volume and velocity [51]. If a network has high transaction throughput and fast token velocity, its market cap should reflect that usage. For instance, Bitcoin's market cap could be partly justified by its high transaction volume and number of daily transfers.

Another metric is the *Network Value to Transactions (NVT) Ratio*. It is calculated as:

$$\text{NVT} = \frac{\text{Market Capitalization}}{\text{Daily Transaction Volume}}$$

This is like a P/E ratio for crypto: a lower NVT (large transaction volume relative to market cap) suggests active usage, possibly undervaluation [51]. A high NVT may indicate speculation. For example, if a cryptocurrency has a $1B market cap and $100M of on-chain daily transactions, its NVT is 10. Analysts compare NVT across assets to gauge relative valuation.

Other factors include the number of users (wallets), exchange listing breadth, and mining costs. All these inform but don't definitively determine value due to crypto's volatile nature.

Final Revision Summary

- **Crypto-Assets:** Digital value units on blockchains; includes cryptocurrencies, commodity tokens, and various utility/security tokens [3] [18].
- **Cryptocurrencies:** Native blockchain coins (e.g., Bitcoin) used as money; decentralized, cryptographically secured [6].
- **Crypto-Commodities:** Tokens representing tangible or intangible assets (e.g., gold-backed coins) [7] [17].
- **Crypto-Tokens:** Assets on existing blockchains; include network, utility, security, stable tokens [8] [25].
- **ICOs:** Token crowdfunding events like IPOs; easy funding but high fraud risk [29] [31].
- **Bitcoin:** First cryptocurrency; PoW consensus secures ledger, fixed 21M supply [5] [2].
- **Ethereum:** Smart-contract blockchain; Ether powers it; DAO hack led to Ethereum Classic fork [35] [36].

- **Exchanges:** Platforms for trading crypto. Centralized (Coinbase) vs decentralized (Uniswap) vs OTC (Genesis) [42] [49].
- **Valuation:** Use network/usage models (Equation of Exchange, NVT, etc.) to estimate token value [51].

This guide should arm you with detailed knowledge across all aspects of Unit 3. It combines definitions, real examples (e.g., BAT, DAO), conceptual summaries, and exam-style Q&As for thorough understanding.

---

[1] [3] [4] [5] [6] [7] [8] [9] [10] [11] [17] [18] [20] [23] [24] [25] [26] [28] [29] [30] [31] [42] [43] [44] [45] [46] [49] [50] [51]
Bettina Warburg_ Tom Serres_ Bill Wagner - Basics of Blockchain.pdf
file://file-4sh3eW8894NLxBQPgsDsnb

[2] [32] [34] [35] [37] Mastering Blockchain_full book.pdf
file://file-VMuff6FT4vapX8PMgkEVpD

[12] [13] [14] [15] [16] [19] [21] [22] [27] [33] [36] [38] [39] [40] [41] [47] [48] unit 3.pdf
file://file-27VDXhio179DpnX76LVbfN