Unit 1: Blockchain Fundamentals

Blockchain Basics and Definition

- **Decentralization:** A blockchain is a **decentralized**, **distributed ledger** that coordinates agreement on an **append-only** history of transactions across a peer-to-peer (P2P) network [1] . Unlike a centralized database (e.g. a bank's ledger), no single authority controls the data [2,3]. Every node (computer) on the network holds a copy of the entire ledger, making the system **fault-tolerant** and **trustworthy**.
- **Data Structure:** Data in a blockchain is organized in **blocks**, each containing a set of transactions. Blocks are linked together in chronological order by including the **hash** of the previous block, forming an immutable "chain" [4,5]. This means each block is time-stamped and cryptographically secured, so changing any past transaction would break the chain.
- **Consensus and Trust:** Blockchain uses **consensus protocols** instead of central authorities. All peers run the same rules so that the network **"comes to an agreement"** on the order and validity of transactions [6,7]. Common consensus mechanisms (e.g. Proof-of-Work) ensure a shared "truth" and replace intermediaries (like banks) with a software protocol.
- **Append-Only Ledger:** Once transactions are validated and added to the blockchain, they cannot be altered or deleted [8,4]. The ledger is *immutable*, recording a permanent history of all transactions. This append-only design (like a continuously updated log) preserves provenance and prevents fraud.
- **Distributed Ledger Technology (DLT):** Blockchain is one form of DLT. All DLTs share core features: they operate on a P2P network and use consensus among nodes to agree on the data [9]. In effect, blockchain is a linked-list data structure secured by hashing and consensus [10,5].
- **Real-World Example:** *Bitcoin* was the first practical blockchain, serving as a decentralized digital currency without a bank. It demonstrated how people can exchange value directly over the Internet without trusting a single intermediary, using the blockchain as a public ledger[4] .

Figure: Conceptual illustration of a peer-to-peer blockchain network. All nodes (computers) hold and verify the shared ledger.

Detailed Explanation: The term "blockchain" refers to a system that combines cryptography, network architecture, and consensus to maintain a shared database. As Warburg et al. define, *"a blockchain is a decentralized database that coordinates agreement on an append-only history of transactions across a peer-to-peer network."*[1] In simpler terms, think of it as a community-maintained ledger: no single entity (like a bank) writes the records; instead, every participant maintains their own copy and follows rules to agree on new entries. When a new block of transactions is created, it is broadcast to all nodes, which independently verify and append it to their copy of the chain.

By linking each block to the previous one via a cryptographic hash, the blockchain forms an unbroken chain of data [4]. If anyone tries to alter a past transaction, its block's hash would change and no longer match the stored value in the next block – immediately alerting the network that tampering occurred [5]. This mechanism, combined with consensus rules, makes blockchain **immutable** and **tamper-evident**. Every transaction is timestamped, creating a permanent record that all nodes can verify.

Consensus protocols (like Proof-of-Work) ensure that all honest nodes converge on one “truth” without a central server [7] [10]. For example, in PoW networks, nodes (“miners”) solve a computational puzzle to propose the next block. The first to solve it gets to add the block, and others build on the longest valid chain. This collective process replaces a single authority’s role and enables trustless collaboration.

In summary, a blockchain **eliminates the need for trust in any single party** by dispersing control across many nodes and cryptographically securing the transaction history. It operates as a *distributed, append-only ledger*, offering transparency and resilience far beyond traditional centralized databases.

Quick Facts / Revision Tips:
- *“Append-only”* means transactions can only be added, never deleted or changed [8].
- *Distributed Trust:* Blockchain is sometimes called a “distributed trust network” because it replaces institutions with code [11].
- *CAP Theorem:* In blockchain, Partition tolerance and Availability are given, and *Consistency* (agreement) is achieved over time (eventual consistency).

University-Style Questions (7–10 marks):

1. **Explain what a blockchain is and how it differs from a traditional centralized database.**
Model Answer: A blockchain is a decentralized, distributed ledger where each participant (node) holds a copy of the full database [1]. Transactions are grouped into blocks that are cryptographically linked in a chain [4]. Unlike a centralized database (controlled by one entity), blockchain uses consensus protocols so that all nodes verify and agree on new data [7]. Once added, transactions are immutable (cannot be changed) [8], providing transparency and trust. In contrast, a central database is controlled by a single administrator who can modify records, whereas in a blockchain no one has unilateral control, and all changes must be approved by the network. This makes blockchain more secure and fault-tolerant.

1. **Describe the role of consensus in a blockchain network and why it is important.**
   Model Answer: Consensus is the process by which all participating nodes in the network agree on the next valid block of transactions [6] [7]. It replaces the need for a central authority to validate transactions. For example, in Proof-of-Work, miners compete to solve a cryptographic puzzle; the winner’s block is accepted by the majority [12]. Consensus ensures there is a *single version of truth* shared across the network [7]. It prevents double-spending and conflicting histories because once a block is agreed upon, all honest nodes adopt the longest valid chain [13]. Without consensus, nodes could have divergent ledgers, defeating the purpose of a shared database.

2. **What does it mean that a blockchain ledger is “append-only”, and why is this property useful?**
   Model Answer: “Append-only” means new transactions can be added to the blockchain, but existing records cannot be altered or removed [8]. Each block is finalized once created; any change would require recalculating hashes of that block and all following blocks, which is computationally infeasible [5]. This immutability is useful because it creates a permanent audit trail: the entire transaction history is recorded in chronological order. It prevents tampering and fraud, since participants know past records cannot be secretly modified. For example, real estate titles on blockchain would have an unchangeable chain of custody, reducing the need for title insurance.

Elements of a Blockchain

- **Nodes:** Any computer on the network is a *node*. A **full node** keeps a complete copy of the blockchain and validates all transactions and blocks [14] [15]. Running a full node requires significant storage (hundreds of GB) and bandwidth. A *partial node* (or light/SPV node) relies on full nodes for data. The more full nodes there are, the more decentralized and secure the network [16]. (E.g. Bitcoin has thousands of full nodes worldwide.)
- **Blocks:** A *block* is a data structure that batches together multiple transactions. Each block contains a header (with metadata) and a list of transactions [4] [17]. The block header typically includes: the hash of the previous block, a timestamp, a nonce (for PoW), and the Merkle root of transactions. By referencing the previous block's hash, blocks form a **chain** [4] [5]. For example, Bitcoin's blocks are ~1 MB each and are created roughly every 10 minutes [18]. This chaining of hashes links the history securely.
- **Transactions:** A *transaction* is the basic data unit, representing a transfer of value (or change of state). In cryptocurrencies, it typically moves tokens/coins from one address to another. Transactions are verified by nodes and included in blocks. Every valid block in the chain has a collection of transactions recorded in order.
- **Public and Private Keys:** Blockchain uses *asymmetric cryptography*. Each user has a **private key** (secret) and a corresponding **public key** (shared). The public key (or its derived address) is used as an identity on the blockchain[19]. To spend or transfer assets, the user signs the transaction with their private key. Other nodes can then verify the signature using the user's public key[19]. This ensures authenticity without revealing the private key. A helpful analogy is a safety deposit box: the private key is like your unique key to open the box; the public key/address is like the box's number that everyone can see [20].
- **Mining (Proof-of-Work):** *Mining* is the process by which new blocks are created in many public blockchains. Miners are full nodes that perform heavy computation (hashing) to solve a difficult puzzle [21]. The first miner to find a valid solution earns the right to add the next block to the chain and receives a reward (newly minted tokens)[22]. This competitive process secures the network: it's costly to produce blocks (in electricity/computation), so attackers cannot easily rewrite history. Mining thus both validates transactions and issues new currency.
- **Tokens/Coins:** A *token* or *coin* is a digital asset native to the blockchain (e.g. Bitcoin). Tokens serve two main roles: they can represent value for transactions, and they provide **incentives**. For instance, Bitcoin miners earn new BTC tokens for their work [22]. This reward motivates participants to dedicate resources to running nodes and securing the network [23]. Tokens can also represent other assets (e.g. loyalty points, digital tickets) on blockchain platforms.
- **Consensus (Proof-of-Work):** Beyond mining, *consensus* is the method by which nodes agree on the blockchain's state. In Proof-of-Work (PoW), all miners race to solve a cryptographic puzzle; the first to succeed broadcasts the new block, and others verify and accept it if valid[24]. The protocol then requires that participants always build on the "longest" (most proof-of-work) chain. This means even though PoW by itself only defends against Sybil attacks, it indirectly leads to agreement through economic incentives[25] [26]. In PoW, consensus arises from a *grand competition*: whoever wins packages the transactions, and the rest of the network acknowledges that block as the next official block [13].

Figure: A block in the blockchain contains a header (including the hash of the previous block) and a list of transactions. Chaining each block by hash links them into an immutable ledger.

Detailed Explanation: Each element plays a specific role in the blockchain ecosystem. **Nodes** form the P2P network: some act as **miners/validators**, others as lightweight clients. Full nodes carry the entire blockchain and independently check every transaction and block for correctness [14]. They ensure no invalid transactions slip into the chain. For example, anyone can run a Bitcoin full node by downloading the official software and blockchain data (~200+ GB and growing) [14].

A **block** groups verified transactions into an ordered container. Blocks are "chained" by including the previous block's hash in each header[4]. This linking means that altering one block would break all subsequent hashes, so historical data is effectively sealed. Blocks also include a timestamp, nonce, and a Merkle root summarizing all transactions[17] [5] .

Blockchain relies on **public/private keys** for security. When Alice sends coins to Bob, she creates a transaction and signs it with her *private* key. This signature proves Alice's identity (ownership of the funds) without revealing her private key. Everyone can verify the signature with Alice's *public* key (which functions as her address on the blockchain) [19]. Thus, funds are only transferable if the private key holder approves.

In **mining (PoW)** blockchains like Bitcoin, miners expend computational effort (hashing) to earn the right to publish a block. Each miner continuously tries different nonces in the block header until the block's hash meets a difficulty target. The first miner to succeed broadcasts the block and collects the mining reward[22] . This process does two things: it throttles block creation (so blocks appear roughly at a steady interval) and makes rewriting history prohibitively expensive (an attacker would need to redo the proof-of-work for all blocks).

Finally, **tokens/coins** align economic incentives. In addition to paying transaction fees, miners receive new tokens (e.g. BTC) for successful mining[22] . This reward motivates participants to keep the network healthy. Tokens themselves enable value exchange: they are units of account recorded and transferred on the blockchain. The ingenious design uses game-theory: participants are rewarded for honest work and penalized (economically) for deviations, ensuring network security [23].

Quick Facts / Tips:

- A blockchain is *verifiable* without revealing secrets: public keys and signatures let anyone confirm a transaction's validity without seeing private data [19] .
- **Merkle root:** Each block's transactions are hashed into a single root hash, which is included in the block header. This allows efficient proof of any transaction's inclusion.
- **Mining reward halving:** In Bitcoin, the miner's reward halves roughly every 4 years, controlling token supply.

University-Style Questions (7–10 marks):

1. **What is a "full node" in a blockchain network and what functions does it perform?**

Model Answer: A full node is a computer that has downloaded the entire blockchain and participates fully in the network [14]. It stores all historical blocks and transactions locally. The full node checks and validates every new transaction and block against consensus rules (e.g., checking digital signatures and ensuring no double-spends)[27]. When it validates a new block, it adds it to its copy of the ledger. If a transaction or block is invalid, the node rejects it. Full nodes also help relay data: they forward valid transactions and blocks to peers, contributing to the peer-to-peer network. By running many independent full nodes, the blockchain achieves decentralization, because no single node can maliciously change the ledger; all honest full nodes must agree on state.

1. **Describe the structure of a blockchain block and explain how blocks are linked together.**
   Model Answer: A blockchain block consists of a *header* and a list of transactions[4]. The header contains metadata fields: (1) the hash of the previous block's header (4 bytes in Bitcoin)[28], (2) the Merkle root hash of all transactions in the block[29], (3) a timestamp[30], (4) a difficulty target, and (5) a nonce[30]. By including the previous block's hash in its header, each block is cryptographically **chained** to the one before it[4]. An example from Bitcoin: Block N's header has the SHA-256 hash of Block N-1's header. This linkage makes the chain tamper-evident: if any data in Block N-1 changed, its hash would change, so Block N would no longer properly reference it[5]. This ensures the integrity of the entire chain from the genesis block onward.

2. **Explain the role of public and private keys in blockchain transactions.**
   Model Answer: Public/private keys enable secure and verifiable transactions on blockchain. Each user has a private key (kept secret) and a corresponding public key (or address)[19]. To create a transaction (e.g. sending coins), the user signs the transaction data with her private key. This signature mathematically binds the transaction to the signer. Other nodes then use the signer's public key to verify the signature's validity. If the signature is valid, the network accepts that the owner of the corresponding private key authorized the transaction[19]. This process ensures *authenticity* (only the key owner can spend funds) and *non-repudiation* (the signer cannot later deny the transaction). The combination of public/private key cryptography and digital signatures is fundamental to blockchain security.

Qualities of Blockchain

- **Security (Integrity):** Blockchain uses strong cryptography. Each block is **hash-secured**, and transactions are verified by all nodes. As Warburg notes, a new block is "cryptographically secured through hash functions," and to tamper with it would require controlling a majority of the network ("51% attack")[31]. In large public blockchains (like Bitcoin), this is practically impossible due to the enormous computational power required. The result is that the chance of fraudulent modification is extremely low.
- **Resiliency (Fault Tolerance):** Because every node has a copy of the blockchain, the system tolerates failures. If one or many nodes go offline, others continue operating. Warburg explains that the design is *very resilient*: even if a node drops out or suffers a power issue, other nodes keep the network running[32]. Geographically distributed nodes mean blockchains are unlikely to all fail due to a localized problem (e.g. natural disaster). This decentralization provides **redundancy** and "fault tolerance" – there is no single point of failure.
- **Immutability:** Once data is recorded in the blockchain, it cannot be changed. As one source states, blockchain is "designed to be append-only, or 'immutable.'"[8] This means records can only be added, never altered or deleted. The append-only nature preserves a transparent history of asset ownership or transactions. For instance, once a property sale is recorded on-chain, it remains forever as proof of transfer. This immutability builds trust: participants know that the recorded history is permanent and agreed upon by the community.
- **Transparency:** Blockchain's ledger is visible to all participants (in a public blockchain). Warburg notes that *"all of the transactions stored in a blockchain are visible to all of its participants.[33]"* Every transaction is time-stamped and publicly viewable (though users may be pseudonymous). This

transparency means transactions can be audited by anyone on the network. For example, one can look up any Bitcoin transaction and verify amounts and timestamps. Time-stamping of blocks ensures chronological order. This openness helps catch errors or suspicious activity quickly. (In permissioned blockchains, transparency can be scoped to members, but verifiability is maintained.)

- **Verifiability:** Because every node can independently verify transactions using the public keys and consensus rules, blockchain data is **self-auditing**. Peers can check any transaction or block against the rules without trusting a third party. This means that once a transaction is on the chain, everyone *can* verify it is legitimate according to the code. For example, you can verify that funds weren't double-spent simply by checking prior blocks. This property follows from transparency and cryptographic validation [33] .
- **Permissibility (Access Control):** Blockchain systems vary in who can participate. A *permissionless* blockchain (like Bitcoin) allows anyone to read, write, and verify without permission. In contrast, a *permissioned* blockchain restricts participation to approved identities. Warburg describes that some networks permit scoping who participates, achieving privacy while retaining verifiability [34] . Permissioned blockchains (often used by businesses) can hide sensitive data from the public yet still leverage a shared ledger. Both approaches maintain the above qualities, but trade off openness for control as needed.

Detailed Explanation: Blockchain's design inherently secures data. Hashing links make retroactive tampering virtually infeasible – altering any past record would require re-mining all subsequent blocks, which would be noticed by honest nodes [5]. This makes blockchain records effectively immutable. Even at the software level, blockchains are updated by consensus only when the community agrees on their validity [8] .

Blockchain is also highly **robust**. A blockchain network does not rely on any single server; if one node fails, others carry on seamlessly [32]. The decentralized P2P architecture means data is replicated everywhere. This replication is why Warburg calls blockchain "fault tolerant": it can survive hardware failures, power outages, or even targeted attacks on parts of the network.

However, this open transparency has nuances. While transactions are visible, personal identities usually are not (only public keys are exposed). The system achieves a balance between transparency and privacy: you can see *what* happened and *when*, but not necessarily *who* (unless on-chain identity is revealed). Some newer blockchain designs allow *privacy-preserving transactions*, but they still allow verification of the blockchain's correctness by outsiders.

Finally, "51% attacks" are often mentioned. In practice, mounting such an attack (controlling a majority of mining/validation power) is prohibitively expensive on large networks [31]. For example, Bitcoin's network has never been successfully taken over, demonstrating its security in the wild. Minor incidents (like a 2010 software bug that let someone create trillions of BTC) were resolved by community hard forks, further reinforcing that attacks tend to target applications or exchange platforms, not the core protocol itself [35] .

Quick Facts / Tips:

- **51% Attack:** Occurs if one miner/business controls >50% of hashing power [31] . In big networks, this is extremely unlikely.
- **Fault-Tolerance:** Blockchain networks can sustain failures – they are even called *"self-healing"*.
- **Transparency vs. Privacy:** Public blockchains let everyone see transactions, but users are pseudonymous. Permissioned blockchains can hide data off-chain while proving ledger integrity.

University-Style Questions (7–10 marks):

1. **List and explain three security or integrity features of blockchain technology.**

Model Answer: (a) **Cryptographic Hashing:** Each block includes a hash of its data and the previous block's hash [4]. This binds blocks together; any change in a block breaks the chain. (b) **Decentralization:** The ledger is replicated on many nodes [32]. An attacker would have to compromise a majority of nodes to rewrite history (the 51% problem) [31]. (c) **Consensus Protocol:** All transactions are validated according to strict rules by many independent nodes [7]. This means no invalid transaction can enter the chain without being detected. Together, these features ensure data integrity.

1. **What does it mean that the blockchain is "immutable," and how is this property achieved?**
   Model Answer: Immutability means that once a transaction is recorded in the blockchain, it cannot be altered or deleted [8]. This is achieved through cryptographic chaining and consensus. Each block's header includes the hash of the previous block [4]. If someone tries to change a past transaction, the block's hash changes, so the next block's stored hash no longer matches [5]. Additionally, nodes only accept new blocks that build on the valid "longest" chain. Because it would require redoing all subsequent blocks' proof-of-work, altering history is practically impossible. Thus the ledger is append-only and tamper-evident [8].

2. **Explain how blockchain networks can continue operating even if some nodes fail or go offline.**
   Model Answer: Blockchain is inherently fault-tolerant because of its distributed nature. Every block is stored on many nodes across the network [32]. If one node (or several) crashes, others still have the complete ledger and can continue to validate transactions. There is no single point of failure: the network does not rely on any central server. Warburg describes this resiliency: even if a node quits or a group is inaccessible, remaining nodes carry on all functions [32]. Data is replicated globally, so local outages (power, regional issues) do not bring down the chain. This high availability is a key quality of blockchain systems.

Blockchain and Economics

- **Lowering Uncertainty in Trade:** Blockchain is often called a *distributed trust network*. By using many nodes rather than a single trusted intermediary (like a bank), blockchains can remove or reduce middlemen in transactions [11]. Economically, this lowers counterparty risk and transaction costs. For example, instead of relying on escrow services, two parties can transact directly on the Bitcoin blockchain with trust guaranteed by cryptography. Warburg explains that blockchain technology can **replace some trusted third parties** and enable one-to-one value exchange [11]. It effectively brings trust back to a more peer-to-peer economic model.
- **Smart Contracts:** These are programs stored on the blockchain that execute automatically when certain conditions are met. Smart contracts encode business rules or contract terms in code. For instance, an insurance payout contract could automatically trigger a payment if data (like weather reports) indicate a flood. By running on the blockchain, smart contracts are transparent and immutable; once deployed, anyone can see the code and its execution results. This changes the role of firms by automating verification and execution of agreements. (Ethereum was built around smart contracts.) Smart contracts can streamline supply chains, enforce licensing, and reduce delays and disputes.
- **Decentralized Autonomous Organizations (DAOs):** A DAO is an organization governed by smart contracts rather than a traditional hierarchy. Members hold tokens that give them voting rights on proposals. Warburg describes examples: *DASH* (a cryptocurrency started in 2014) operates as a self-

governing DAO by allocating 10% of mining rewards to a treasury, funding community projects [36]. *The DAO* (launched in 2016 on Ethereum) was a crowdfunded venture fund where token-holders voted on which projects to finance [36]. These DAOs can perform many functions of companies (funding, governance) automatically. While *The DAO* famously experienced a hack (leading to an Ethereum hard fork), it demonstrated that blockchains can power transparent, collaborative organizations. The promise is to automate and decentralize decision-making in economics.

- **Incentive Mechanisms:** Blockchain protocols embed economic incentives to ensure the network behaves correctly. For example, Bitcoin miners invest in hardware and electricity; in return, they earn Bitcoin rewards. This game-theoretic design (crypto-economics) is crucial: participants are motivated to follow rules for profit, and deviate at a cost. Warburg mentions that blockchain's incentives (like token rewards) must be carefully balanced to prevent gaming of the system [37]. These incentives are why one can *trust* a permissionless network without knowing the participants personally.
- **Tokenization and New Business Models:** Though beyond the strict Unit1 scope, it's worth noting that blockchains enable new economic models (like ICO fundraising, micropayments, and digital scarcity). By representing assets as tokens, blockchain can fractionalize ownership and open up liquidity. For example, in supply chains, tokenizing invoices or inventory can speed up financing and traceability.

Real-World Use Case (Blockchain in Supply Chain): Major companies are already deploying blockchains to improve economic processes. For instance, Walmart and IBM built a food traceability system on Hyperledger Fabric (a permissioned blockchain) to track pork and mango shipments[38]. Blockchain's immutability and real-time data allow Walmart to trace products from farm to shelf, dramatically speeding up response to contamination. McDermott of IBM remarked that *"blockchain solves business problems where trust is part of the solution"* by providing data immutability, speed, and security[39]. This illustrates blockchain's economic impact: by ensuring data integrity across multiple businesses, it reduces uncertainty and friction in trade.

Quick Facts / Memory Pegs:
- *Distributed Trust:* Blockchains "disintermediate" traditional brokers by encoding trust in code[11]. Think of it as moving from bank-mediated transfers back to 1-to-1 barter, but with digital tokens.
- *"Code is law":* Smart contracts enforce agreements automatically. Remember the DAO hack story: code bugs can have huge economic consequences (The DAO hack in 2016 led to an Ethereum fork[40]).
- *Token Rewards:* Incentive alignment is key in blockchain economics – miners/stakers are paid with tokens for securing the network [22].

University-Style Questions (7–10 marks):
1. **How can blockchain technology reduce the need for intermediaries in financial transactions? Give an example.**
Model Answer: Blockchain provides a trustless platform, so parties can transact directly without a central intermediary. For example, using Bitcoin, Alice can pay Bob directly, and the network of miners will verify and record the transaction on the blockchain. This replaces the need for a bank to clear the payment. Warburg describes this as a *"distributed trust network"*[11]. In supply chains, companies like Walmart use blockchain to eliminate delays from manual reconciliation between partners[39]. By having a shared, immutable ledger, all parties see the same data, reducing disputes and removing the middleman.

1. **Explain what a smart contract is and describe one potential benefit and one risk associated with them.**
Model Answer: A smart contract is a computer program stored on the blockchain that automatically

executes specified actions when certain conditions are met. **Benefit:** It automates trust: for example, an escrow contract could release funds to a seller automatically when delivery is confirmed, without a lawyer or broker [41]. This saves time and cost. **Risk:** The code may have bugs or unintended logic. As in the case of *The DAO*, a flawed smart contract led to a large theft of funds[40]. Because blockchain is immutable, bugs can be irreversible. Also, "code is law": parties must trust the code's correctness, so any error can cause financial loss.

2. **What is a Decentralized Autonomous Organization (DAO)? Give an example and explain how it differs from a traditional corporation.**
   Model Answer: A DAO is an organization governed by code (smart contracts) on a blockchain, rather than by a centralized management structure. Decision-making and funding are carried out via rules encoded in the blockchain, and stakeholders vote with tokens. For example, *The DAO* (2016) was a blockchain-based investment fund where contributors received DAO tokens that allowed them to vote on project proposals[36]. It differed from a traditional corporation in that there was no board of directors or legal entity; the code defined how votes translated into fund releases. Another example is *Dash*, a cryptocurrency that allocates 10% of mining rewards to a treasury that is governed by masternode votes, effectively a DAO-funded development budget[36]. Unlike a corporation, a DAO is fully transparent (all transactions and rules are public on-chain) and operates 24/7 without human intermediaries.

Types of Blockchains

- **Public (Permissionless) Blockchain:** Open to anyone for reading, writing, and validating. Anyone can join the network, run a node, and participate in consensus. Examples include Bitcoin and Ethereum. These blockchains rely on trustless consensus (PoW, PoS) because validators may be anonymous. As Warburg notes, a public blockchain is like **Wikipedia** – anyone can contribute content and the community verifies it [42]. Public blockchains maximize decentralization and censorship-resistance but may sacrifice throughput and privacy.
- **Private (Permissioned) Blockchain:** Access is restricted to a known group (e.g. within a company or consortium). Only authorized participants can read or write data, and often only select nodes validate transactions. For example, IBM and Walmart's supply-chain blockchain is permissioned (only approved suppliers and auditors can use it) [39]. Private blockchains can be faster (no expensive mining) and keep data confidential, but they reintroduce some centralization and trust assumptions among the parties. They are useful for enterprise settings where full openness is not needed.
- **Permissionless:** Essentially synonymous with *public* – anyone can join and participate without permission. Permissionless blockchains use economic incentives (e.g. mining rewards) and consensus to secure the network. Bitcoin is the archetype: no gatekeepers. Nodes follow the protocol rules, and new participants don't need approval to join.
- **Permissioned:** Generally synonymous with *private*, but can also mean that anyone can read the chain but only authorized entities can write/validate (a hybrid model). In pure permissioned blockchains, every validator is vetted (e.g. banks in a financial network). Permissioned systems trade off some decentralization for efficiency and privacy.
- **Public-Permissioned (Consortium):** A hybrid approach: the ledger might be visible to all (public access), but only a set of known validators (permissioned committee) can create blocks. This could look like a public blockchain with restricted mining. One envisioned use-case is a government-sponsored blockchain: citizens can view records, but only approved agencies can write entries. Another example might be a consortium where member organizations run the consensus nodes,

but allow public audit of transactions. (Note: this category is less common in practice, but merges the transparency of public chains with the governance of permissioned ones.)

Comparison Table:

Type	**Who Can Read?**	**Who Can Write/ Validate?**	**Consensus Model**	**Example / Use-Case**
Public (Permissionless)	Anyone (public)	Anyone (node, miner)	Open (PoW/PoS, decentralized)	Bitcoin, Ethereum (public cryptocurrency)
Private (Permissioned)	Restricted group	Restricted group (peers known)	Consortium (e.g. Raft, PBFT)	Hyperledger Fabric (enterprise supply chain)
Permissionless	Anyone (public)	Anyone (anyone can join)	PoW/PoS	Bitcoin, Ethereum (same as public)
Permissioned	Often restricted	Only approved entities	Restricted committee	Corda (finance), private consortium blockchains
Public-Permissioned	Anyone (or many)	Pre-approved validators	Semi-open consortium	(Emerging) e.g. open audit chains with controlled writing (e.g. SDGs tracking)

Detailed Explanation:

- *Public vs. Private:* Public blockchains maximize openness: anyone worldwide can join, run a node, and transact (with no prior permission). They use broad consensus (often PoW/PoS) to secure the network because participants are not trusted. Private blockchains limit participation to a defined group. For example, a company might have a blockchain only among its branches. The consensus mechanism in private chains can be lighter (like voting) because nodes are known and semi-trusted. The trade-off is between decentralization and control.
- *Permissionless vs. Permissioned:* The key difference is whether joining the validation process requires approval. Permissionless systems allow open participation; permissioned ones require permission (identity verification) to join consensus. Permissionless blockchains like Bitcoin use economic incentives and anonymous consensus, whereas permissioned ones (like Hyperledger-based systems) often use simpler protocols because nodes are identified.
- *Use-Case Insights:* Public blockchains are well-suited for open-value networks (cryptocurrencies, public data ledgers). Private/permissioned blockchains are popular in industries where participants already trust each other to some extent but want shared records – e.g. banks using R3 Corda (permissioned) or supply chain partners using Hyperledger Fabric (permissioned). Warburg likens public blockchains to Wikipedia (open editing) vs. permissioned to a controlled encyclopedia.
- *Example - Supply Chain:* The IBM-Walmart food blockchain is permissioned: only qualified suppliers and auditors can write to it [39]. Everyone in the network agrees on what's added, but outsiders cannot inject false data. This gives data immutability (security) while meeting privacy and regulatory needs.

Quick Fact:
- **"Like Wikipedia" Analogy:** Warburg points out that a public blockchain operates like Wikipedia – any user can make an entry (transaction) and the community of verifiers keeps the record accurate [42].

University-Style Questions (7–10 marks):

1. **Compare public and private blockchains. What are the advantages and disadvantages of each?**

Model Answer: Public blockchains (e.g. Bitcoin) are open to all, achieving high decentralization and censorship-resistance [42]. Advantages: no gatekeepers; anyone can verify or use the network; data is fully transparent to participants. Disadvantages: relatively slow and resource-intensive (PoW), limited privacy, and hard to enforce legal compliance. Private blockchains restrict access (e.g. a company consortium). Advantages: higher transaction throughput, more privacy (data only shared among members), and governance is easier. Disadvantages: less decentralized (could have central points of failure), trust must exist among the permissioned parties, and users outside cannot benefit from the ledger.

1. **What is a permissioned blockchain and when might it be used? Give an example.**
   Model Answer: A permissioned blockchain restricts who can participate in the network (usually requiring an invitation or identity check). It is often used by enterprises or consortia where participants are known organizations. For example, banks might set up a permissioned blockchain for interbank settlements. In Walmart's food traceability project, the blockchain is permissioned: only approved suppliers and regulators can add or view data [39]. This model is used when privacy or compliance is important, but parties still want a shared, tamper-proof record.

2. **Explain the term "public-permissioned" blockchain. Is it the same as a public blockchain?**
   Model Answer: A *public-permissioned* blockchain is a hybrid: the ledger may be public (everyone can read it), but only a permissioned set of validators can write new blocks. This differs from a fully public (permissionless) chain, where anyone can write. Public-permissioned chains combine transparency (public visibility) with controlled consensus (e.g. known validators). An example might be a government-issued land registry: citizens can view records, but only authorized clerks can record new transactions.

3. **Provide a real-world example of a use case for each blockchain type (public, private, permissioned).**
   Model Answer:

4. *Public:* Bitcoin is the prime example – a cryptocurrency network open to any user, enabling P2P digital cash. Also Ethereum for smart contracts.
5. *Private/Permissioned:* Hyperledger Fabric used by IBM and Walmart for a food supply chain blockchain [39], where only authorized companies can participate. R3 Corda is used by banks for interbank transactions (permissioned).
6. *Public-Permissioned:* This is emerging; one example is the Celo network, which is permissioned for some core validators but whose transactions are visible to anyone. (Or imagine a future public land registry blockchain with permissioned consensus.)

Revision Summary (Key Points)

- **Blockchain = Decentralized Ledger:** No single authority; consensus by many nodes.
- **Block Structure:** Blocks link via hashes (each has prev-hash) forming an immutable chain [4].
- **Nodes:** Full nodes store whole chain and validate; partial (light) nodes rely on full nodes [14]. More nodes = more decentralization.
- **Transactions & Keys:** Transfers of tokens; signed with private key, verified by public key [19]. Public key = address, private key = signature.
- **Mining (PoW):** Nodes solve puzzles to add blocks and earn token rewards[22]. This secures blockchain against tampering.
- **Tokens:** Represent value and reward participation. Incentives align network security (crypto-economics).
- **Security Features:** Cryptographic hashes, 51% attack hard, all nodes verify. Immutable & append-only (no edit) [8].
- **Resilience:** Copies on all nodes – network survives node failures [32].
- **Transparency:** All verified transactions are visible and time-stamped[33]. Blockchain = open audit trail.
- **Permission Models:**
- *Public/Permissionless:* Anyone can join and validate (e.g. Bitcoin). Like Wikipedia [42].
- *Private/Permissioned:* Restricted access (e.g. Hyperledger for businesses [39]). Faster but more centralized.
- *Public-Permissioned:* Hybrid (public read, permissioned write). Used when public auditability plus control is needed.
- **Economic Role:** Enables trustless trade – replaces middlemen (banks, brokers) [11]. Smart contracts automate agreements.
- **DAOs:** Organizations run by code. E.g. DASH (funded by 10% mining fee), The DAO (Ethereum venture fund) [36].
- **Quick Mnemonics:** "Append-only = append → never edit." "51% = controlling chain is costly." "Public = Wiki; Private = private ledger." "Digital signature: lock=public, key=private."

---

[1] [2] [3] [6] [8] [9] [11] [12] [13] [14] [15] [16] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [31] [32] [33] [34] [35] [36] [37] [40] [41] [42] Bettina Warburg_ Tom Serres_ Bill Wagner - Basics of Blockchain.pdf
file://file-S8aQWoy9iNPafGNqo5WQpK

[4] [5] [7] [10] [17] [28] [29] [30] Mastering Blockchain_full book.pdf
file://file-9PLYBvx1AqHAvgBMAptAim

[38] [39] iscap.us
https://iscap.us/proceedings/conisar/2020/pdf/5340.pdf