Overview of Blockchain

Chapter – 2

Fall 2025

Middle Tennessee State University

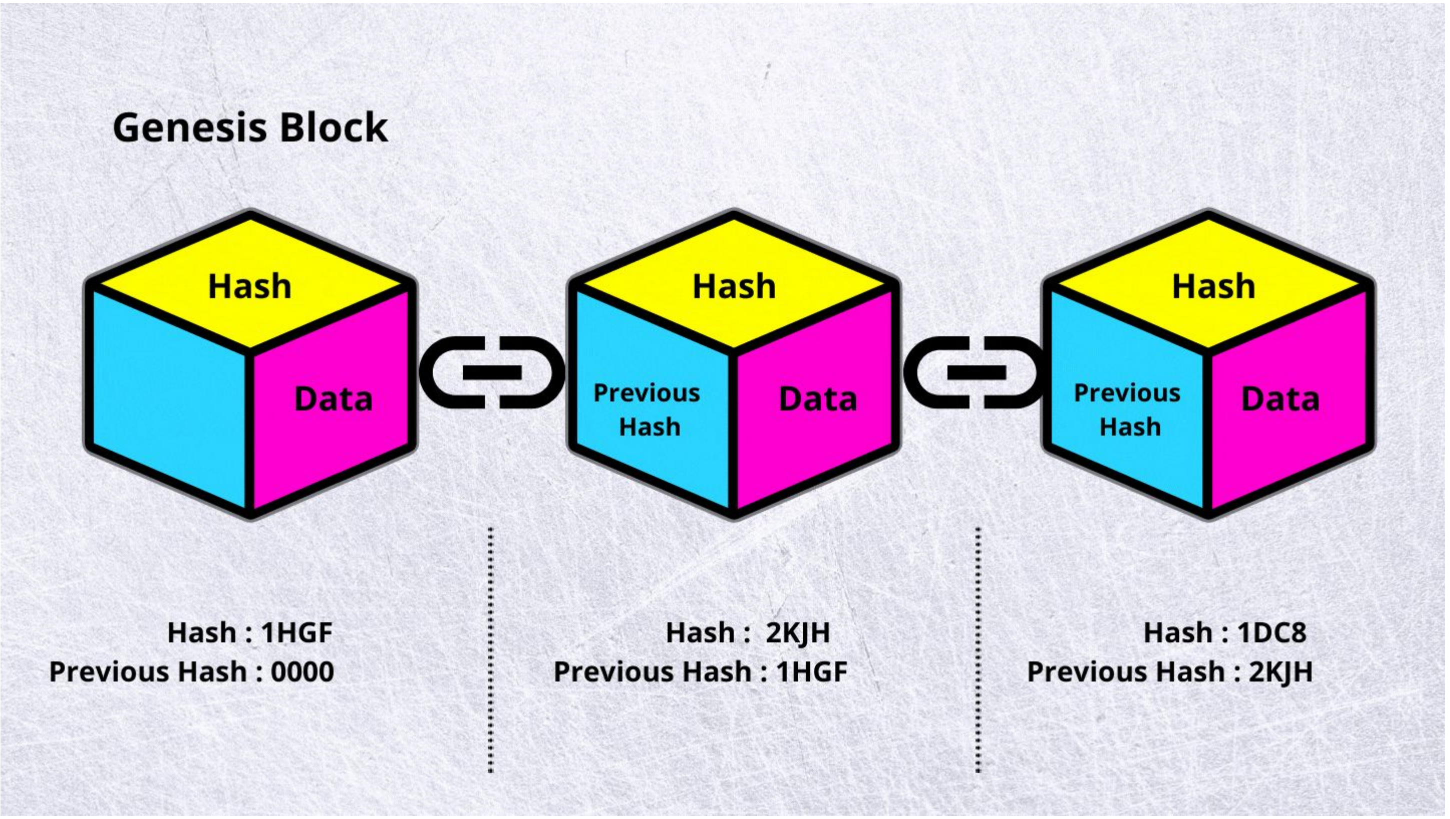
Summary from the last chapter

- Monolithic: simple but not scalable
- Client-Server: scalable but centralized
- P2P: decentralized but no trust
- Distributed: scalable and resilient but complex and still not fully trustless

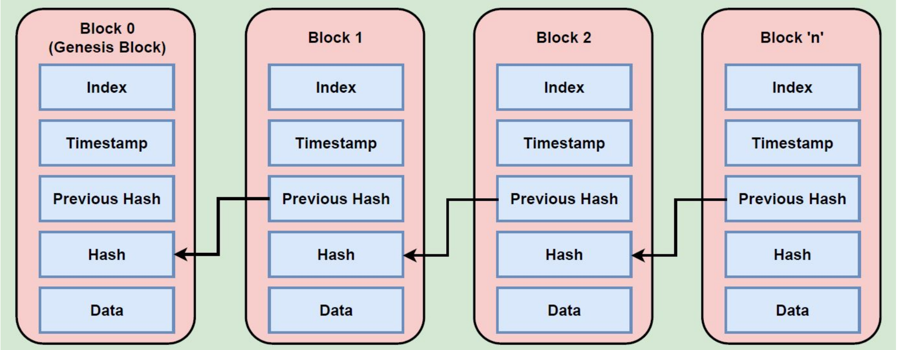
- Can we build an architecture that is scalable, fault-tolerant, decentralized, and trustless, **all at the same time**?

5. Blockchain Architecture

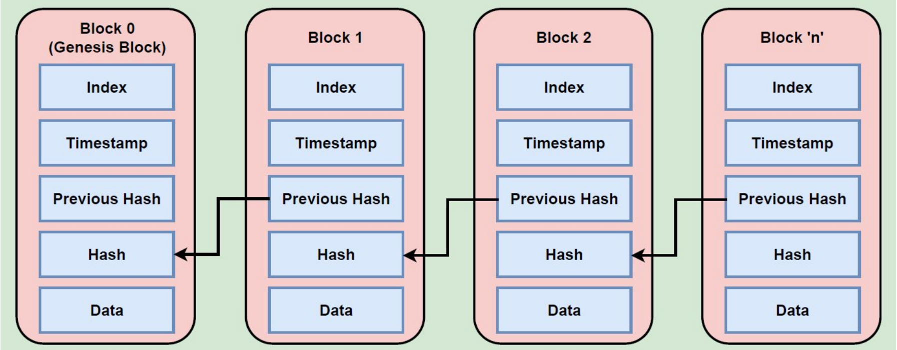
- Is Blockchain better?



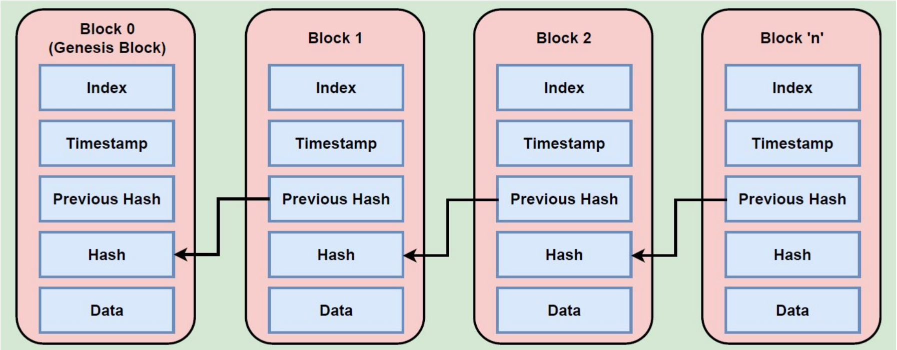
Blockchain Structure



Peer A



Peer B



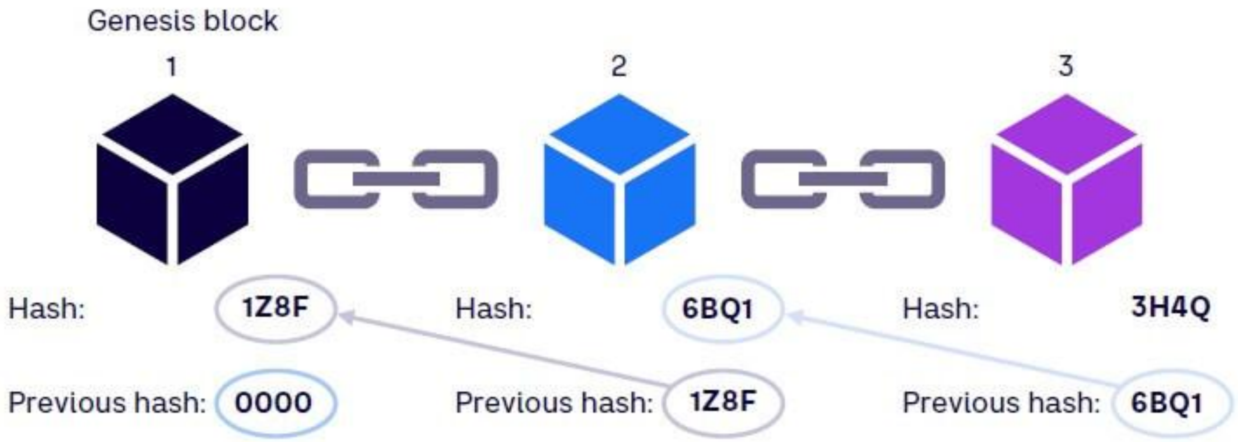
Peer
‘N’

The Evolution of Digital Trust

- **Pre-Blockchain Era:** Centralized systems controlled by banks, governments, and corporations
  - *Example:* Banks controlling financial transactions, Facebook storing private user data
- **The Problem:** Data breaches, lack of transparency, and reliance on intermediaries
  - *Example:* 2017 Equifax data breach (147 million records exposed), SWIFT banking fraud cases
- **The Solution:** A **distributed** and **decentralized**, trustless system powered by cryptography and consensus mechanisms
  - *Example:* Bitcoin enables peer-to-peer transactions without banks, Ethereum allows decentralized applications (DApps)
- **Blockchain is Born:** Introduced in 2008 with Bitcoin by Satoshi Nakamoto
  - *Example:* The first real-world Bitcoin transaction was used to buy two pizzas for 10,000 BTC in 2010

What is Blockchain?

- A distributed, immutable ledger technology
- Decentralized & cryptographically secure
- First introduced by Bitcoin (2008) by Satoshi Nakamoto
- Key stats: Over 83 million blockchain wallet users worldwide (Statista 2023)



Source: Arthur D. Little

Why Blockchain Matters?

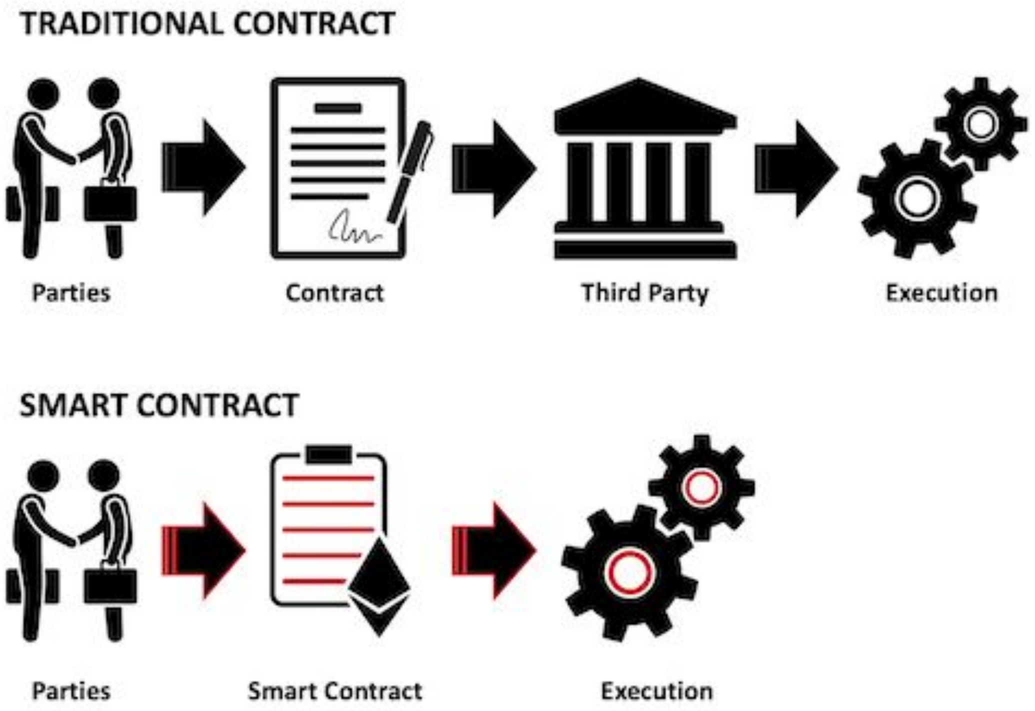
- Trustless System – No dependency and need to trust
- Distributed
- Decentralization
- Peer to Peer (P2P)
- Consensus-based
- Tamper-proof and Immutable
- Privacy
- Faster settlement process

Why Blockchain Matters? (Contd…)

- Removes intermediaries (banks, governments)
- Transparency & Security with cryptographic hashing
- Use cases: Finance, Healthcare, Supply Chain, Gaming, AI
- Cool Fact: El Salvador made Bitcoin legal tender in 2021!
- Countries like the United States, Canada, the United Kingdom, and Japan allow Bitcoin usage under specific regulatory frameworks

Smart Contracts

- Self-executing contracts on the blockchain
- **No third-party needed** (lawyers, banks)
- **Ethereum pioneered smart contracts –** then 21 years old **Vitalik Buterin (2015)**
- **Use Cases of Smart Contracts:**
    - **Finance (DeFi):** Automated lending, borrowing, staking
    - **Supply Chain:** Transparent tracking of goods (e.g., IBM Food Trust for food safety)
    - **Healthcare:** Secure patient records and insurance claims (e.g., MediBloc for medical data sharing)
    - **Real Estate:** Tokenized property ownership and automatic sales
    - **Gaming & NFTs:** Play-to-earn games and digital ownership (e.g., Axie Infinity)
    - **Insurance:** Automated claims processing
- **Fun Fact:** The DeFi market hit $100B in total locked value (DeFiLlama, 2023)



Career & Earnings in Blockchain

- **Blockchain Developers:** $120K–$250K/year (Glassdoor, 2023)
- **Smart Contract Auditors:** $100K–$180K/year
- **Top skills:** Solidity, Rust, Hyperledger, Cryptography
- **Big names hiring:** Google, Microsoft, Binance, JPMorgan
- **Fact:** The demand for blockchain developers grew by **400%** in 2022!

Blockchain, AI, IoT & Cybersecurity

- **AI & Blockchain:** Secure, verifiable AI models (e.g., decentralized AI)
- **IoT & Blockchain:** Securing smart devices from cyber threats
- **Cybersecurity:** Zero-trust security & decentralized identity
- **Interesting Research:** Post-quantum cryptography in blockchain!

Blockchain Research & Future Trends

- **Privacy-preserving blockchains (ZK-SNARKs, MPC)**
- **Consensus Mechanisms:** Proof of Stake (PoS), DAG, BFT, Sharding
- **Quantum-Resistant Blockchain** for post-quantum era
- **Interoperability:** Cross-chain communication (Polkadot, Cosmos)
- **Metaverse & NFTs:** Digital ownership & tokenized assets

Where to Start? (Resources & Learning)

- **Programming:** Solidity, Rust, Python
- **Platforms:** Ethereum, Hyperledger, Binance Smart Chain
- **Certifications:** Certified Blockchain Developer (CBDE), Solidity Developer
- **Communities:** Ethereum forums, GitHub, Twitter spaces
- **Fun & Self-Learning Exercise:** Try deploying your first smart contract in the Ethereum Blockchain!

Blockchain demo

- Blockchain is revolutionizing multiple industries
- Smart contracts automate and decentralize processes
- High-paying career opportunities in blockchain tech
- The future is decentralized – Web3

- A Short Demo: https://andersbrownworth.com/blockchain/

Blockchain Use-Cases

- **Finance and Banking**
  - Cross-border payments: Used by global banks (e.g., Santander, JPMorgan) to reduce transaction costs and settlement time from days to minutes
  - Trade finance platforms: Used by HSBC and Standard Chartered to digitize letters of credit and reduce fraud
- **Healthcare**
  - Patient record sharing: Hospitals in Estonia use blockchain to give patients and doctors controlled, auditable access to medical records
  - Pharmaceutical supply chain: Companies like Pfizer use blockchain pilots to track drugs and prevent counterfeits

Blockchain Use-Cases (Contd…)

- **Voting and Governance**
  - Online voting: West Virginia tested blockchain-based voting for overseas military personnel
  - Transparent land governance: Georgia's government uses blockchain for land title registration to prevent corruption

- **Real Estate**
  - Property transactions: Dubai Land Department uses blockchain for property sale and transfer records
  - Digital deeds: Sweden piloted blockchain for real estate transactions to cut paperwork and fraud

Blockchain Use-Cases (Contd…)

- **Ownership and Deeds**
  - Land registry modernization: Rwanda and Georgia are digitizing land ownership records on blockchain for transparency
  - Intellectual property: Media companies use blockchain to timestamp and track digital rights
- **Cars and Inventory Tracking**
  - Vehicle history records: Automakers and service providers test blockchain to track car ownership, repairs, and recalls
  - Parts traceability: BMW’s PartChain ensures authenticity and quality tracking of car components

Blockchain Use-Cases (Contd…)

- **Supply Chain**
  - Food traceability: Walmart tracks mangoes and lettuce through IBM Food Trust to ensure food safety
  - Shipping logistics: Maersk’s TradeLens records shipping data to reduce paperwork delays in ports
- **Insurance**
  - Parametric insurance: AXA’s blockchain project (Fizzy) automatically compensated travelers for delayed flights
  - Crop insurance: Farmers in developing countries use blockchain-based weather data to trigger automated payouts

What is a Blockchain?

- A blockchain is:
  - Distributed and decentralized digital ledger
  - Records transactions (tx/txn) across multiple computers
  - In a way that is secure, transparent, and immutable

- Analogy:
  - Imagine a shared digital notebook
  - Multiple people can write on this shared notebook
  - Once something is written, it can’t be altered or erased
  - This notebook is accessible to everyone and is constantly updated

Historical Background

- Originally created in 2008
- By an anonymous individual or a group using the pseudonym Satoshi Nakamoto as the underlying technology for Bitcoin
- Brief timeline highlighting key developments
    - 2008: Bitcoin whitepaper published
    - 2009: Bitcoin network launched
    - 2015: Ethereum, a blockchain platform for smart contracts, was introduced

Key Characteristics of Blockchain

- **Decentralization**:
  - No central authority or intermediary (middleman) controlling the network
  - No single point of failure
  - Data and decision-making are distributed across a network of nodes (computers operated by individuals) that work together
  - Decentralization enhances security by eliminating the need of trust in a central entity

- **Transparency**:
  - Visibility of all transactions to all network participants
  - Anyone can view the entire transaction history, making it highly transparent
  - Useful for auditability and accountability, in public blockchains: https://etherscan.io/
  - Useful for cases such as Supply Chain Management and Financial Auditing

Key Characteristics of Blockchain (Contd…)

- **Immutability:**
  - Once the transaction is added to the blockchain, it cannot be altered or deleted
  - Transactions become permanent part of the ledger
  - Maintain the historical record and auditability of transactions
  - Useful for financial and legal contexts

- **Consensus Mechanisms:**
  - Protocols used to achieve agreement among network participants (nodes) on the validity of the transaction
  - No agreement, no adding of new transactions in the block
  - Examples: Proof-of-Work(PoW) and Proof-of-Stake (PoS)
  - *More discussion on this in detail later*

Key Characteristics of Blockchain (Contd…)

- **Anonymity and Pseudonymity:**
  - Blockchain offers different degrees of anonymity
  - Identities of participants are addressed by cryptographic addresses
  - Privacy to users
  - Also, can raise concerns about illicit activities such as crypto scams

- **Public and Private Keys (Cryptography):**
  - Cryptographic key pairs in asymmetric cryptography (a.k.a. public-key cryptography)
  - Public keys -> visible
  - Private keys -> must remain secret
  - Essential for identity and transaction security
  - In blockchain, public keys serve as account addresses whereas private keys provide access and control over assets
  - For example, in Ethereum, when you send ETH (Ethereum native cryptocurrency) to someone, you use their public key as their destination address. Your private key is used to create a digital signature to authorize the transaction

Key Characteristics of Blockchain (Contd…)

- **Tokenization:**
  - Represents real-world assets (e.g., real estate, art) as digital tokens on a blockchain
  - Each token represents a share or ownership of the asset
  - Allows fractional ownership
  - Fungible Tokens, Non-Fungible Tokens (NFTs), Multi Tokens, Soulbound Tokens (SBTs)

- **Smart Contract:**
  - Self-executing contracts
  - Terms of agreement written into code
  - Resides in the blockchain
  - Executes when the terms of agreement trigger
  - Also has the ability to act as an account itself and hence has its own account address
  - Example, Decentralized Insurance
    - **Policy Creation** -> Insurance policy created as a smart contract
      - For example, “If a flight is delayed by more than 3 hours, pay out insurance”
    - **Premium Payments** -> Customers pay their insurance premiums in cryptocurrency
    - **Claims Process** -> If covered event occurs, then smart contract triggers the claims process.
      - Inputs to the contract to validate the claim??? IoT devices, police reports, or other trusted data sources can automatically provide input to the contract to validate the claim.
    - **Claim Settlement** ->If the condition for a valid claim are met, automatic payout to policyholder’s account in cryptocurrency
      - No need for middlemen, central authority, or lengthy paperwork

Announcement/Reminder

- No lecture on Wednesday, Sept 17
- Deadline for Assignment 1: Tuesday, Sept 16 (Tomorrow)
- Assignment 2 has been posted on D2L
  - **Will be available on Wednesday, Sept 17**
  - **Deadline: Tuesday, Sept 23**

Key steps in Blockchain

1. **Transaction Creation:**
   - Imagine a digital ledger, like an online spreadsheet, where we record transactions
   - Transactions can represent various things, like sending money, transferring digital assets, or even recording data
   - Each transaction is like an entry in this ledger, showing who sent something to whom and when

   - E.g., Alice wants to send 5 digital coins to Bob. She creates a transaction specifying the amount and Bob's address as the recipient

Key steps in Blockchain (Contd…)

2. Verification by a Group of Nodes:

- Instead of just one person managing the ledger, many people (or computers/nodes) all over the world check it
- The nodes work together to make sure the transactions are real and legitimate. This prevents fraud and errors
- Think of it as a team effort to verify and validate each entry in the ledger

- E.g., Alice’s transaction is broadcasted to the blockchain network, where many participants (nodes) verify its validity
- These nodes check if Alice has 5 or more coins in her account and if her digital signature is valid

Key steps in Blockchain (Contd…)

3. **Grouping into Blocks:**
    - To keep things organized, verified transactions are grouped together into a “block”
    - Blocks are like pages in a ledger, and each block can hold a certain number of transactions
    - This grouping makes it easier to manage and store all the information

    - E.g., Let’s say a block can hold 10 transactions. So, the first block might include transactions from Alice to Bob, Charlie to David, and so on, up to 10 transactions

Key steps in Blockchain (Contd…)

4. **Adding Securely (Consensus Mechanism):**
    - Before a new block is added to the chain, everyone in the network must agree that the transactions in it are **valid**
    - This agreement process depends on the blockchain's consensus mechanism
    - E.g., in Bitcoin, miners solve complex math puzzles (*Proof of Work*) to validate the block. In Ethereum, *Proof of Stake* is used to validate the block
    - Once everyone agrees, the new block is added to the chain, and the information becomes part of the permanent ledger
    - All participants can see the transactions in the new block and verify that it's part of the chain
    - It cannot be altered or deleted, hence **immutable**

Key steps in Blockchain (Contd…)

5. **Chaining Blocks:**
   - Each block has a unique hash that connects it to the previous block
     - This connection is called a "**chain**"
   - Changing anything in a block is extremely difficult because it would break the chain
   - E.g., Like trying to remove a page from a book without tearing the whole book apart. This makes the blockchain very secure

Why Consensus Matters?

- Ensures agreement among participants
- In a blockchain network, participants must agree on the state of the ledger to prevent disputes and maintain trust
- Prevents double-spending and fraud
- Consensus mechanisms verify that a user hasn't spent the same cryptocurrency twice
- Enables trust in decentralized networks
- By agreeing on transactions collectively, participants trust that the blockchain's history is accurate and secure

Summary of Key Steps in Blockchain

- 1. Transaction
- 2. Verification
- 3. Block Formation
- 4. Consensus
- 5. Chaining

End of Chapter-2