#1 Introduction and Motivation

Lecture Notes for CS190N: Blockchain Technologies and Security September 29, 2025

In this lecture, we set out to understand blockchains from their foundations to their role in today's digital economy. First, we explore why decentralization matters and how cryptographic tools such as hash functions, signatures, and Merkle trees make trustless systems possible. Next, we study Bitcoin as a concrete design, examining its transaction model, scripting language, and the Proof-of-Work consensus mechanism that secures the network. Finally, we connect these concepts to practice by looking at current blockchain data, network health, and applications ranging from Bitcoin as digital money to Ethereum, DeFi, and DAOs. By the end, we will not only see how blockchains work technically, but also how they are used in real-world systems.

1 FUNDAMENTAL PRINCIPLES OF DECENTRALIZED SYSTEMS

To understand blockchain, we must first ask why decentralization matters, and how it can function at scale. This chapter begins with the historical motivation for removing trusted intermediaries, then introduces the cryptographic foundations and data structures that make trustless coordination possible.

1.1 The Genesis of Blockchain: A New Paradigm for Collaboration

Any new technology emerges to solve a specific problem. For blockchains, that problem is how to coordinate securely without relying on a single central authority. This section first examines the issue of trusted intermediaries, then reviews the historical evolution from Bitcoin to modern programmable blockchains, and finally considers the tension between privacy and transparency.

1.1.1 Beyond the Trusted Third Party. Blockchains enable participants to transact without banks or governments acting as arbiters of trust. This feature is particularly important in finance, where intermediaries are both expensive and vulnerable to failure. Traditional systems rely on central institutions or expose users to counterparty risks. Early digital cash systems such as DigiCash were innovative but remained centralized, making them susceptible to single points of failure. Satoshi Nakamoto's key contribution was to design a system in which trust is embedded in protocol rules and incentives rather than institutions.

1.1.2 Historical Trajectory. After Bitcoin established the viability of decentralized money, researchers and developers began to explore broader applications. The evolution can be summarized in three stages:

- **Bitcoin (2009):** A secure, peer-to-peer ledger for digital currency.
- **Ethereum (2015):** A general-purpose platform that introduced smart contracts and composability, enabling decentralized applications to interact with one another.
- **Modern Era (2017–2025):** Expansion into DeFi, the rise of high-performance chains such as Solana, and the development of Layer 2 solutions such as Arbitrum, Optimism, and Base for improved scalability.

1.1.3 The Anonymity Spectrum. Another fundamental design question is the balance between privacy and transparency. David Chaum's electronic cash systems demonstrated that anonymity was possible, but they relied on central issuers. Bitcoin instead introduced pseudonymity: participants are identified by public keys rather than real names, but all transactions are publicly recorded. This provides transparency for verification but limits privacy. Achieving stronger anonymity in a decentralized context requires advanced cryptographic tools such as zero-knowledge proofs.

1.2 The Cryptographic Cornerstones

Having considered why decentralization is desirable, we now turn to the cryptographic mechanisms that make it possible. These include hash functions, digital signatures, and data structures designed for verifiable integrity.

1.2.1 Hash Functions: Integrity and Proof-of-Work. Hash functions provide digital fingerprints for data and are fundamental to blockchain security. Their relevance comes from three key properties:

- **Collision Resistance:** It is infeasible to find two distinct inputs that produce the same output.
- **Hiding:** Commitments created with random nonces conceal inputs until they are intentionally revealed.
- **Puzzle-Friendliness:** There is no shortcut to solving hash-based puzzles, which underpins Proof-of-Work.

1.2.2 Digital Signatures: Identity and Authorization. Digital signatures link cryptographic identities to authorization in a decentralized system. They operate through three algorithms: key generation, signing, and verification. Their essential aspects are as follows:

- A private signing key (sk) and a public verification key (pk) form the basis of identity.
- **Unforgeability:** Observing valid signatures does not allow an attacker to forge a new one.
- In blockchain systems, the public key effectively defines an address, and signatures authorize transactions from that address.

1.2.3 Data Structures for Trustless Systems. To maintain integrity at scale, blockchain systems rely on specialized data structures. The three most important are:

- **Hash Pointer:** Stores both the location of data and its hash for verification.
- **Blockchain:** A linked list of blocks connected by hash pointers, producing a tamper-evident history.
- **Merkle Tree:** A binary tree of hashes whose root summarizes all transactions, allowing efficient proofs of inclusion with $\log(n)$ complexity.

2 THE MECHANICS OF BITCOIN AND ITS CONSENSUS ENGINE

With the foundations in place, we now turn to Bitcoin itself. This chapter explains how transactions are represented, how they are grouped into blocks, and how the system achieves consensus without centralized control.

2.1 The Bitcoin Protocol in Operation

Bitcoin's design for value transfer differs fundamentally from account-based ledgers. This section introduces the UTXO model, the scripting system that defines spending rules, and the structure of a block.

2.1.1 The Unspent Transaction Output (UTXO) Model. Bitcoin represents value as discrete units called unspent transaction outputs (UTXOs), rather than as account balances. Each transaction consumes existing UTXOs and creates new ones. The total value of outputs must not exceed the total value of inputs.

- UTXOs are indivisible. For example, spending a 2 BTC UTXO to pay 0.5 BTC requires creating two outputs: 0.5 BTC to the recipient and 1.5 BTC as change.
- The complete set of all unspent outputs defines the available supply and is maintained by every full node.

2.1.2 Bitcoin Script: Spending Conditions. The next component is the system that enforces transaction rules. Bitcoin uses a simple, stack-based scripting language.

- **P2PKH:** Locks a UTXO to a public key hash. Spending requires the corresponding public key and a valid signature.
- **P2SH and Multisig:** Locks a UTXO to the hash of a script. This is used in multisignature wallets where multiple parties must approve spending.

Bitcoin Script is intentionally limited and non-Turing-complete, which ensures predictability and security.

2.1.3 Anatomy of a Block. Transactions are recorded in blocks. A block consists of two parts:

- **Header (80 bytes):** Contains metadata including the hash of the previous block, the Merkle root of current transactions, a timestamp, the difficulty target, and a nonce.
- **Coinbase Transaction:** The first transaction in a block, which rewards the miner with new bitcoin and transaction fees.

2.2 Achieving Decentralized Consensus

The final step is to understand how Bitcoin nodes agree on a single ledger despite unreliable networks and potentially malicious participants. This is the problem of consensus.

2.2.1 The Consensus Problem. Distributed systems must contend with latency, network partitions, crashes, and adversarial behavior. Bitcoin addresses this by assigning voting power not to identities, which could be forged, but to computational work.

2.2.2 Proof-of-Work (PoW). In Bitcoin, miners must demonstrate computational effort before proposing a block. This mechanism has several important consequences:

- It is computationally expensive to solve but trivial for others to verify.
- It functions as a lottery, where the probability of winning is proportional to hash power.
- The rule of consensus is to follow the longest valid chain. Altering history would require the majority of network hash power.

2.2.3 The Economics of Mining. For consensus to be sustainable, miners must be incentivized. This is achieved through two mechanisms:

- **Block Rewards:** Newly minted bitcoin distributed via the coinbase transaction. This amount halves every 210,000 blocks (approximately every four years). The current reward since April 2024 is 3.125 BTC [2].
- **Transaction Fees:** The difference between input and output values, which become increasingly important as block rewards diminish.

Together, rewards and fees form the "security budget." If this budget falls too low relative to the cost of attacks, long-term network security may weaken.

2.2.4 Difficulty Adjustment. To ensure stability, the system periodically adjusts the difficulty of the Proof-of-Work puzzle. Every 2016 blocks, the network recalibrates so that blocks continue to arrive at an average of roughly ten minutes. This adjustment maintains predictable issuance regardless of changes in total mining power.

3 THE REAL-WORLD BLOCKCHAIN ECOSYSTEM: DATA & ANALYSIS

The previous chapters focused on the design of blockchains. To complete the picture, we now examine how these systems perform in practice. This chapter uses data from 2025 to evaluate network activity, scalability, and applications.

3.1 On-Chain Activity & Network Health (Q3/Q4 2025)

Network activity can be measured through transaction costs, throughput, storage requirements, and mining resources. These metrics illustrate both adoption and technical limitations.

3.1.1 Transaction Throughput and Fees. Transaction costs and throughput directly affect usability. Current data show that blockchains can be cheaper than traditional payment systems but remain constrained in scale.

- **Cost Comparison:** A wire transfer of $200 costs around $30-45 depending on domestic or international [1, 12], PayPal international transfers cost $4.99 [13], while sending USDC on Base costs less than $0.01 [3]. Bitcoin transactions average around $0.84 in late 2025 [17].
- **Fee Volatility:** Bitcoin fees fluctuate with demand, peaking at $2.40 in May 2025 [14].
- **Throughput:** With an average of 2,724 transactions per block and variable block times, Bitcoin processes only a few transactions per second [4].

3.1.2 UTXO Set and Storage. The size of the UTXO set reflects adoption but also creates storage costs. As of September 2025, nodes track about 169 million UTXOs [5], and the blockchain continues to grow steadily in size.

3.1.3 Mining Ecosystem: Hash Rate and Difficulty. Network health also depends on the resources securing it.

- **Hash Rate:** Between 900 and 1100 EH/s in September 2025, representing significant hardware and energy investment [2, 4].
- **Difficulty:** Approximately 129.7 T [2].
- **Mining Centralization:** The top three pools control around 56.14% of total hash rate [11].

3.2 The Broader Application Landscape

Beyond performance metrics, the blockchain ecosystem is defined by how it is used in practice. The main applications today are digital currency, decentralized finance, and programmable governance.

3.2.1 Digital Currency. The original application of blockchain remains central. Bitcoin is widely used as a store of value and medium of exchange. As of September 2025, the total cryptocurrency market capitalization exceeds $3.8 trillion [7, 9], with Bitcoin alone trading about $35-47 billion daily [6, 8].

3.2.2 DeFi and DAOs. Programmable blockchains such as Ethereum have enabled decentralized financial instruments and governance organizations.

- **DeFi:** Protocols such as Aave manage over $50 billion [15], while LIDO manages approximately $40 billion through liquid staking [16].
- **DAOs:** Communities use decentralized governance to manage pooled assets and collective decision-making.

3.2.3 The Developer Ecosystem. Finally, developer activity highlights where innovation is concentrated. According to the 2024 Electric Capital Developer Report [10], Ethereum leads with 6,244 monthly active developers, while Base has emerged as the leading Layer 2 with 4,287 developers. Bitcoin's focus as a monetary asset rather than a programmable platform is reflected in its smaller developer community. This divergence underscores the bifurcation of the ecosystem: Bitcoin as digital gold, and programmable chains as Web3 computing platforms.

REFERENCES

[1] Bank of America. 2025. Personal Schedule of Fees. https://www.bankofamerica.com/salesservices/deposits/resources/personal-schedule-fees/ Accessed: 2025-09-27.

[2] Bitcoin Block Half. 2025. Bitcoin Block Reward Halving Countdown. https://bitcoinblockhalf.com/ Accessed: 2025-09-27.

[3] Bitget. 2025. Gas Fees for Transferring USDC on the Base Network. *Bitget Wiki* (2025). https://www.bitget.com/wiki/gas-fees-for-transferring-usdc-on-the-base-network Accessed: 2025-09-27.

[4] BitInfoCharts. 2025. Bitcoin (BTC) Statistics - Price, Blocks Count, Difficulty, Hashrate, Value. https://bitinfocharts.com/bitcoin/ Accessed: 2025-09-27.

[5] Blockchain News. 2025. Bitcoin UTXO Set Jumps to 169M in Ordinals Era. *Blockchain News* (September 2025). https://blockchain.news/flashnews/bitcoin-utxo-set-jumps-to-169m-in-ordinals-era-brc-20-flagged-as-key-scaling-issue-for-btc Accessed: 2025-09-27.

[6] CoinGecko. 2025. Bitcoin Price: BTC Live Price Chart, Market Cap & News Today. https://www.coingecko.com/en/coins/bitcoin Accessed: 2025-09-27.

[7] CoinGecko. 2025. Global Cryptocurrency Market Cap Charts. https://www.coingecko.com/en/charts Accessed: 2025-09-27.

[8] CoinMarketCap. 2025. Bitcoin price today, BTC to USD live price, marketcap and chart. https://coinmarketcap.com/currencies/bitcoin/ Accessed: 2025-09-27.

[9] CoinMarketCap. 2025. Cryptocurrency Prices, Charts And Market Capitalizations. https://coinmarketcap.com Accessed: 2025-09-27.

[10] Electric Capital. 2024. *Electric Capital Developer Report 2024.* Technical Report. Electric Capital. https://www.developerreport.com/reports/devs/2024 Accessed: 2025-09-27.

[11] Hashrate Index. 2025. Bitcoin Mining Pool Data. https://hashrateindex.com/hashrate/pools Accessed: 2025-09-27.

[12] NerdWallet. 2025. Wire Transfer Fees: What Banks Charge. *NerdWallet* (2025). https://www.nerdwallet.com/article/banking/wire-transfers-what-banks-charge Accessed: 2025-09-27.

[13] PayPal. 2025. PayPal Consumer Fees. https://www.paypal.com/us/digital-wallet/paypal-consumer-fees Accessed: 2025-09-27.

[14] The Block. 2025. Bitcoin transaction fees hit 2025 highs as BTC price challenges recent $106,000 top. *The Block* (May 2025). https://www.theblock.co/post/354735/bitcoin-transaction-fees-hit-2025-highs-as-btc-price-challenges-recent-106000-top Accessed: 2025-09-27.

[15] The Block. 2025. Decentralized lender Aave surpasses $50 billion in net deposits. *The Block* (September 2025). https://www.theblock.co/post/362412/aave-deposits-tvl Accessed: 2025-09-27.

[16] The Defiant. 2025. Liquid Staking TVL Hits Record $86B amid ETH Rally and Growing Institutional Adoption. *The Defiant* (September 2025). https://thedefiant.io/news/defi/liquid-staking-tvl-hits-record-usd86b-amid-eth-rally-and-growing-institutional-adoption Accessed: 2025-09-27.

[17] YCharts. 2025. Bitcoin Average Transaction Fee. https://ycharts.com/indicators/bitcoin_average_transaction_fee Accessed: 2025-09-27.