Blockchain y Criptomonedas I

UCEMA - QUANt

Clase II: 29/10/25

Sobre Mi

Educación:

- 08/2022 - 05/2024 : Maestría en Matemática - *Columbia University*
- 03/2020 - 05/2022 : Maestría en Finanzas - *Universidad Torcuato di Tella*
- 03/2013 - 07/2020 : Ingeniería Electrónica - *Instituto Tecnológico de Buenos Aires*

Experiencia relevante:

- 06/2024 - Actual : Tech Lead - *Terrace.fi*
- 08/2023 - Actual : Execution Lead - *Terrace.fi*
- 08/2022 - 08/2023 : Quantitative Developer - *MRM Analytics*
- 02/2022 - 06/2022 : Quantitative Developer - *Privi Protocol*
- 08/2020 - 01/2022 : Quantitative Developer - *Alma Global Strategies*

Publicación:

- 2021: ¨*Optimal Market Making by Reinforcement Learning*¨

Contacto:

- Email: ms6517@columbia.edu
- LinkedIn: https://www.linkedin.com/in/matias-selser

Agenda

Course Overview

- Module 1: Blockchain Fundamentals & Trading
  - Today's Focus: The critical role of architecture in performance.
- Learning Objectives
  - Gain an understanding of three major blockchain architectures.
  - Compare performance metrics across different chains.
  - Analyze the impact of architecture on trading strategies.

Class Structure (3 hours)

- Part 1 (90 min): Theory + Live Notebooks A & B
- Break (15 min)
- Part 2 (75 min): Applications + Live Notebooks C & D

Trading Scenario: The Problem

Real-World Scenario: Bitcoin Arbitrage

Imagine an arbitrage opportunity:

- Binance: BTC at $45,000
- Kraken: BTC at $45,300 (a potential $300 profit!)

You might consider buying on Binance and selling on Kraken.

Trading Scenario: The Problem

The Challenge:

Bitcoin's architecture presents a hurdle:

- Security Requirement: 6 block confirmations
- Block Time: Approximately 10 minutes per block
- Total Confirmation Time: Roughly 60 minutes

Trading Scenario: The Problem

When Bitcoin transfers to Kraken, the price difference has likely disappeared, leading to a missed opportunity.

Key Questions:

- Why is Bitcoin processing so slow?
- Do all blockchains share this characteristic?
- How does blockchain architecture affect trading profitability?
- Are there any workarounds?

The Architecture Question

Key Insight: Blockchains vary significantly in their architectural approaches.

- Bitcoin: Employs the Unspent Transaction Output (UTXO) model.
- Ethereum: Utilizes an Account/Ethereum Virtual Machine (EVM) model.
- Solana: Features Parallel Processing powered by Sealevel.

The Architecture Question

Architecture is a key determinant of performance, influencing:

- Block time: The frequency at which new blocks are generated.
- Transaction finality: The point at which a transaction becomes irreversible.
- Throughput: Transactions per second (TPS).
- Cost: Associated transaction fees.

The Architecture Question

Optimizing Trading Profitability

Several key performance indicators significantly impact trading profitability:

- Fast Finality: Enables quick execution of trades, crucial for capitalizing on arbitrage opportunities.
- High Transactions Per Second (TPS): Supports high-frequency trading strategies, allowing for rapid execution of numerous trades.
- Low Fees: Increases the profitability of various trading strategies by reducing transaction costs.
- Smart Contracts: Facilitate the development of Decentralized Finance (DeFi) applications and promote composability within the blockchain ecosystem.

Three Architectures Preview

Bitcoin (UTXO Model)

- Security-first design: slow but reliable
- Block time: ~10 minutes
- Finality: 60 minutes
- Best for: Long-term holdings, OTC settlements

Three Architectures Preview

Ethereum:

- Account/EVM Model
- Smart contracts and programmable money
- Block time: ~12 seconds
- Finality: 6.4 minutes
- Ideal for: DeFi trading, DEX strategies

Three Architectures Preview

Solana (Parallel Processing)

- Speed-first, experimental, growing
- Block time: ~0.4 seconds
- Finality: 13 seconds
- Best for: High-frequency trading, market making

Three Architectures Preview

Visual Comparison

- Chart will be generated from live data in Notebook A

Finality

Property of some blockchain consensus mechanisms where a transaction becomes **more likely** to be irreversible as more blocks are added on top of it, but it never reaches **absolute, cryptographic certainty.**

- Offers increasing finality with each new block (confirmations).
- A small chance of chain reorganization exists, potentially removing transactions.
- Longer chains lead to an exponentially lower probability of reversal.
- Relies on probabilistic chain selection, such as the longest-chain rule.
- Transactions become practically irreversible after a sufficient number of confirmations (e.g., 6 in Bitcoin), though never 100% guaranteed.

Class Roadmap

Part 1: Foundations (90 minutes)

- Introduction & Motivation (15 min)
- Bitcoin: UTXO Architecture (20 min)
- Ethereum: EVM Architecture (20 min)
- Solana: Parallel Architecture (20 min)
- LIVE DEMO: Notebook A (15 min)

BREAK (15 minutes)

Part 2: Trading Applications (75 minutes)

- Cross-Chain Tokens (20 min + Notebook B)
- CEX vs. DEX Dynamics (25 min + Notebook C)
- Architecture Performance Scoring (20 min + Notebook D)
- Q&A and Wrap-Up (10 min)

₿ Bitcoin: UTXO Architecture

UTXO Model Explained

Analogy: Cash in Your Wallet

- Physical Bills: You hold physical denominations like $5, $10, or $20.
- Transactions: To pay $15, you might hand over a $20 bill and receive $5 in change.
- Status of Funds: The initial $20 bill is now "spent," while the new $5 bill becomes "unspent."

UTXO Model Explained

- Unspent Transaction Output (UTXO)
- Each "coin" represents an unspent output from a previous transaction.
- Transactions involve consuming existing UTXOs as inputs and generating new UTXOs as outputs.
- Instead of account balances, the system maintains a collection of unspent outputs.

UTXO Model Explained

How Transactions Work

- Alice wants to send 1.5 BTC to Bob. She has a 2 BTC UTXO.
- The transaction consumes the entire 2 BTC input.
- Two outputs are created: 1.5 BTC for Bob and 0.5 BTC returned to Alice as change.

UTXO Model Explained

Key Properties

- Stateless: No global account state
- Parallel Validation: UTXOs (Unspent Transaction Outputs) do not conflict
- Simple but Limited: Lacks native smart contract functionality

Bitcoin Performance Metrics

Bitcoin Block Dynamics & Transaction Security

Block Time:

- Approximately 600 seconds (10 minutes) per block.
- New blocks are mined roughly every 10 minutes.

Difficulty Adjustment:

- Occurs every 2016 blocks (approximately every 2 weeks).
- Maintains a consistent block time regardless of fluctuations in the network's hash rate.

Bitcoin Performance Metrics

Confirmations:

- 6 blocks are generally recommended for high security.
- Each new block progressively increases the probabilistic security of a transaction.
- 6 confirmations provide an approximate 99.9% certainty that a transaction is irreversible.
- Exchanges commonly require 3-6 confirmations before validating a transaction.

Bitcoin Performance Metrics

- Finality: Probabilistic (never 100% final), achieved in approximately 60 minutes (6 blocks at 10 minutes per block). Deep reorgs are theoretically possible but extremely rare.
- Transactions:
  - TPS: Approximately 7 transactions per second.
  - Block Size: 1 MB (effectively 2-4 MB with SegWit).
  - Transaction Size: Approximately 250 bytes on average.
  - Calculation: 1 MB / 250 bytes / 600 seconds ≈ 7 TPS.

Bitcoin Performance Metrics

Why the Delay?

- Proof-of-Work (PoW) Consensus: This energy-intensive mining process contributes to slower transaction times.
- Security Over Speed: Conservative network parameters are prioritized to enhance security, even if it impacts transaction speed.
- Decentralization Challenges: The decentralized nature of blockchain requires time for transactions to propagate globally.

Trading Implications: Bitcoin

Strengths

- Security: Bitcoin boasts the longest track record (since 2009), demonstrating maximum security.
- Liquidity: With the highest market capitalization and global acceptance, Bitcoin offers deep liquidity.
- Store of Value: Often referred to as "digital gold," Bitcoin serves as a robust store of value.
- CEX Dominance: Centralized exchanges handle 98% of Bitcoin's trading volume.

Trading Implications: Bitcoin

Weaknesses:

- Slow settlement: 60-minute finality hinders arbitrage opportunities.
- No native smart contract support: Prevents the development of DeFi protocols.
- High transaction fees: Can surge to $20-50 during network congestion.
- Limited throughput: 7 transactions per second (TPS) is inadequate for high-frequency operations.

Trading Implications: Bitcoin

Best Use Cases

- Long-term holdings and store of value
- Large OTC settlements (security > speed)
- Cross-border payments (though confirmation is slow)

Trading Implications: Bitcoin

Limitations: Not Suitable For

- High-Frequency Trading: Transactions are too slow for rapid execution.
- Arbitrage: Delays in transaction finality hinder effective arbitrage.
- DeFi Protocols: Lacks support for smart contracts.
- Microtransactions: Transaction fees are excessively high.

Real Data: Bitcoin Blocks

Here's a look at live blockchain data (sourced from blockchain.info):

- Block Height: Updates approximately every 10 minutes.
- Transactions per Block: Typically ranges from 2,000 to 3,500 transactions.
- Block Size: Around 1-2 MB (with SegWit enabled).
- Mining Fees: Fluctuates based on network congestion.

Real Data: Bitcoin Blocks

Why Block Times Vary

- Probabilistic Nature of Mining (Proof-of-Work): Block discovery is a random process.
- Fluctuating Discovery Times: While some blocks may be found in as little as 1 minute, others could take up to 30 minutes.
- Long-Term Average: Over an extended period, the average block discovery time settles around 10 minutes.
- Difficulty Adjustment: A mechanism in place to compensate for these variances, with adjustments occurring approximately every two weeks.

Real Data: Bitcoin Blocks

Trader's View: Transaction Confirmation Process

- TX Submitted: Enters mempool (unconfirmed).
- 1st Confirmation: Included in block (~10 mins).
- 6th Confirmation: Considered final (~60 mins).
- Fast Confirmations: Possible, but higher risk.

Note: We'll analyze live block data in Notebook A, seeing real block times, variance, and finality calculations.

UTXO vs Account Model

UTXO Model (Bitcoin)

- Stateless: Operates without a global state, relying solely on unspent transaction outputs.
- Parallel Validation: Transactions can be validated concurrently as they utilize distinct UTXOs, preventing conflicts.
- Complex Scripting: Employs Bitcoin Script, which is limited and not Turing-complete.
- Privacy-Friendly: Enhances privacy by generating new addresses for each transaction.
- Analogy: Comparable to a cash-based system.

UTXO vs Account Model

Ethereum's Account Model

- Stateful Design: Each address maintains a balance, contributing to a global state.
- Sequential Transaction Execution: Transactions sequentially alter the shared state, with nonces preventing double-spending.
- Smart Contracts: Turing-complete code combined with persistent state enables advanced functionalities.
- Simplified User Experience: A single address and easily viewable balance enhance user interaction.
- Analogy: Comparable to a traditional bank account system.

UTXO vs Account Model

Trade-offs:

- UTXO (Unspent Transaction Output): Offers enhanced privacy and simpler validation but has limited programmability.
- Account-Based Systems: Enable smart contracts but involve more complex state management.

Which is better? It depends on the specific use case:

- Bitcoin: Prioritizes security and simplicity.
- Ethereum: Focuses on programmability and decentralized finance (DeFi).

♢ Ethereum: EVM Architecture

Account Model / EVM Explained

Think of a bank account; in blockchain, each address (e.g., 0x...) acts like one, maintaining a balance within a global ledger.

How Transactions Function:

Transactions modify these balances. When a transaction happens:

- Funds are subtracted from the sender's address.
- Funds are added to the receiver's address.

Smart Contracts: Code and State:

Some addresses contain "smart contracts," which are code coupled with a stored state, enabling intricate operations beyond simple balance transfers.

Account Model / EVM Explained

Ethereum Virtual Machine (EVM)

The Ethereum Virtual Machine (EVM) serves as a Turing-complete execution environment.

Key Functions:

- Smart Contract Execution: It runs smart contract bytecode, typically compiled from Solidity.
- Consensus Mechanism: Every full node executes every transaction to maintain network consensus.
- Gas System: A gas system is in place to prevent infinite loops and compensate for computational efforts.

Account Model / EVM Explained

State Structure:

- Externally Owned Accounts (EOAs): User wallets controlled by a private key.
- Contract Accounts: Comprise code and storage, not controlled by a private key.
- World State: A comprehensive mapping of all addresses to their corresponding data.

Account Model / EVM Explained

How Transactions Work

- A user initiates a transaction by calling a function on a smart contract.
- The Ethereum Virtual Machine (EVM) executes the smart contract's code, leading to a modification of the blockchain's state.
- Every operation within the transaction consumes "gas," with storage operations being the most costly.
- The transaction concludes with an updated state and the emission of relevant events.

Account Model / EVM Explained

Here's an overview of the Ethereum blockchain's key characteristics:

- Block Time: Approximately 12 seconds (following the September 2022 Merge).
- Consensus Mechanism: Utilizes Proof-of-Stake, which replaced the previous Proof-of-Work system.
- Block Proposal: Validators are responsible for proposing blocks within their assigned 12-second slots. This slot time is fixed, unlike the variable block times seen in Bitcoin.

Account Model / EVM Explained

- Confirmations: An epoch consists of 32 blocks.
- Epoch Duration: Each epoch, comprising 32 slots, takes approximately 6.4 minutes.
- Finality: Deterministic finality is achieved in 2 epochs (64 blocks), which is roughly 12.8 minutes. Practically, finality can be observed in about 6.4 minutes. This differs from Bitcoin's probabilistic finality.

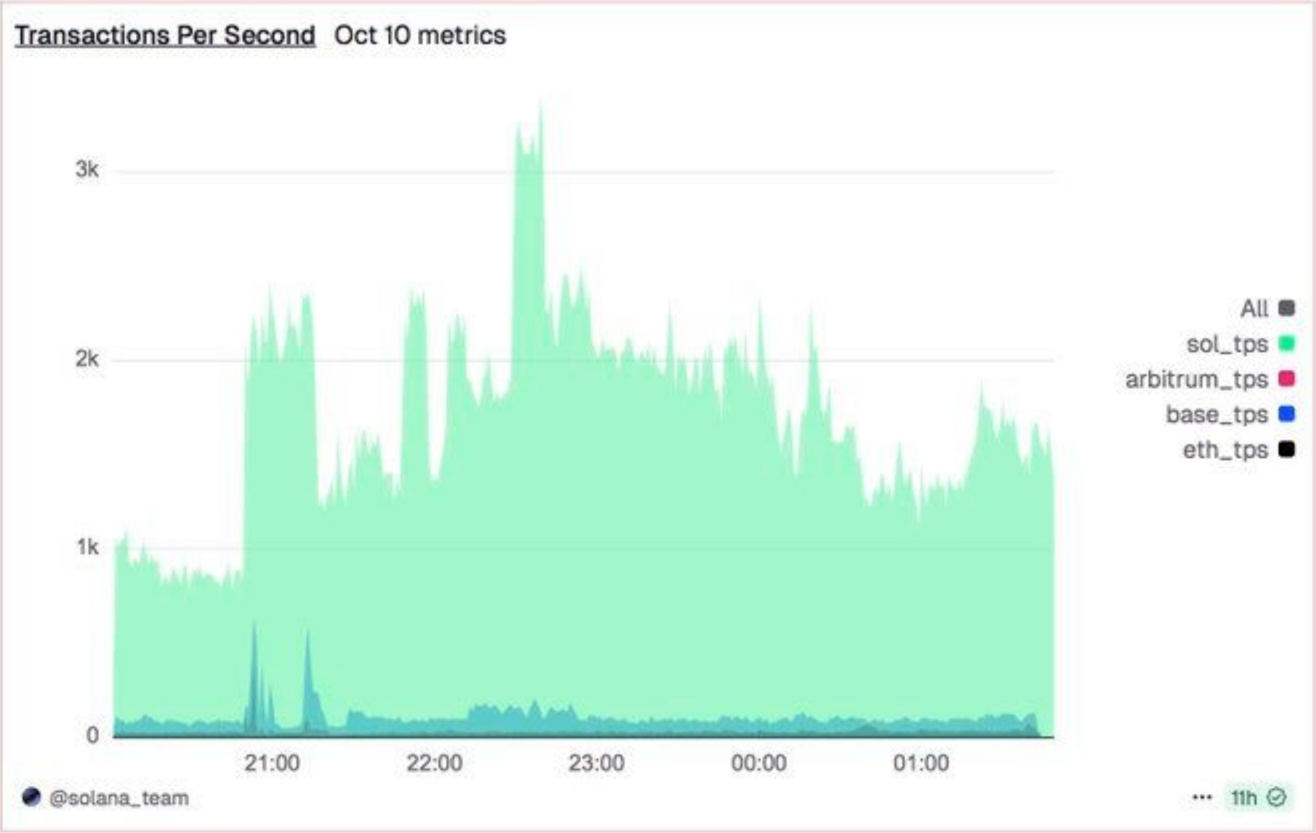
Account Model / EVM Explained

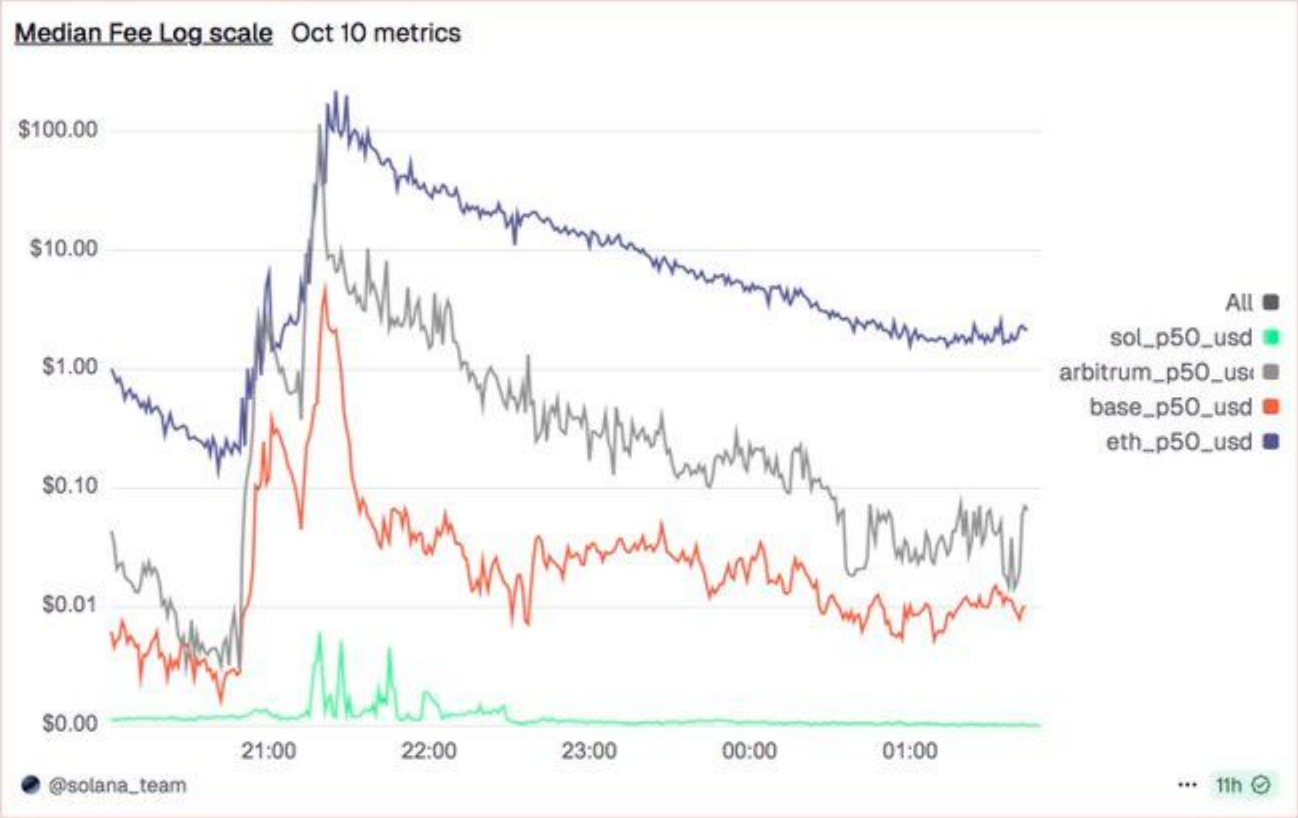
- Finality: Approximately 6.4 minutes.
  - Blocks are justified and then finalized after two epochs, providing an economic guarantee that makes them irreversible.
  - This finalization process is ten times faster than Bitcoin.
- Transactions Per Second (TPS): Approximately 15 on the base layer.
  - Block Gas Limit: 30M gas (variable).
  - Simple Transfer Cost: Approximately 21,000 gas.
  - Calculation: (30M gas / 21,000 gas per transfer) / 12 seconds ≈ 15 TPS.
  - Note: Complex smart contract calls will reduce the effective TPS.

Account Model / EVM Explained

Why Gas Fees Surge:

- Auction-based fee markets: Increased demand directly translates to higher prices.
- Scarce blockspace during peak usage: Volatility, NFT mints, and hype events create congestion.
- Historical context:
  - 2021 DeFi summer saw fees frequently ranging from $50 to over $200 per swap.
  - Currently, fees are typically $1–10, but still spike during congestion.
- On-chain demand bursts: High leverage and liquidations can trigger sudden increases in demand.
- User behavior: Users are willing to pay more to ensure their transactions are included quickly in the next block.


Transactions Per Second
Oct 10 metrics
3k
2k
1k
0
21:00
22:00
23:00
00:00
01:00
All
sol_tps
arbitrum_tps
base_tps
eth_tps
@solana_team
11h



Median Fee Log scale Oct 10 metrics
$100.00
$10.00
$1.00
$0.10
$0.01
$0.00
21:00
22:00
23:00
00:00
01:00
All
sol_p50_usd
arbitrum_p50_us
base_p50_usd
eth_p50_usd
@solana_team
11h

Account Model / EVM Explained

Key Observations from Network Charts

- Sudden TPS Spikes: Around 21:00, a sharp increase in Transactions Per Second (TPS) is observed across all networks.
- Ethereum Ecosystem Fee Surges: Fees on Ethereum, Arbitrum, and Base experience significant increases as blockspace becomes fully utilized.
- Solana's Performance: Solana demonstrates the capacity to handle the highest TPS, maintaining fees at approximately $0.01 or less.
- Divergent Scaling Strategies: This highlights the distinct scaling approaches employed by different networks when faced with real-world demand.
- Throughput and Fee Relationship:
  - Networks with limited throughput are prone to fee volatility.
  - High-throughput designs, conversely, tend to exhibit fee stability, even during peak stress periods.

Ethereum Performance Metrics

Key Innovations:

Programmable Money

- Assets are code-driven, moving beyond simple balances.
- Automates lending, trading, and settlement processes.
- Forms the basis for DeFi, NFTs, DAOs, and novel financial instruments.

Composability

- Smart contracts interact seamlessly, like "money Legos."
- Developers can build upon existing protocols.
- Drives rapid innovation: staking → collateral → yield → derivatives.

Smart Contracts & DeFi

EVM: The Foundation for Programmable Money

- Trustless Execution: Code runs precisely as written, ensuring reliability.
- Direct Control: Write code to manage and control assets.
- Eliminates Intermediaries: No third parties are required for transactions.

Smart Contracts & DeFi

DeFi Explosion (2020–2024)

- Key Platforms:
  - Uniswap: Decentralized Automated Market Maker (AMM) exchange.
  - Aave: Lending and borrowing platform requiring collateral.
  - Curve: Facilitates low-slippage stablecoin swaps.
- Total Value Locked (TVL) Peak: Over $50 billion.

Smart Contracts & DeFi

Composability: "Money Legos"

- Smart contracts can interact to enable complex, atomic transactions.
- For example, a single transaction could include a flash loan, a swap, arbitrage, and loan repayment.

MEV + Trader Implications

- MEV involves reordering or inserting transactions for profit, leading to front-running and sandwich attacks.
- Flashbots formalized MEV extraction.
- This has led to new trading strategies compared to centralized exchanges (CEXs).
- Key risks include front-running, smart-contract bugs, and gas wars.

Trading Implications: Ethereum

Strengths

- Massive DeFi ecosystem: Uniswap, Aave, Curve, etc.
- Composability: Combine protocols for advanced strategies.
- ~6.4 minute finality: Sufficient for many trading workflows.
- Smart contracts: Build custom on-chain trading bots.

Trading Implications: Ethereum

Weaknesses

- High gas fees: $10–100+ during congestion
- Moderate throughput: ~15 TPS (not HFT-friendly)
- MEV exposure: front-running + sandwich attacks
- Complexity: contract bugs can cause losses

Trading Implications: Ethereum

Key Applications

- Decentralized Exchange (DEX) Trading: Platforms like Uniswap, SushiSwap, and Curve facilitate direct peer-to-peer cryptocurrency trades.
- Decentralized Finance (DeFi) Strategies: Engage in activities such as yield farming and providing liquidity (LP provision) to earn returns.
- Maximal Extractable Value (MEV) Extraction: Advanced participants can capitalize on MEV opportunities.
- Arbitrage: Exploit price differences between DEXs when transaction costs (gas fees) are less than the potential profit.

Trading Implications: Ethereum

Challenges / Notes

- Gas optimization is crucial, as every operation incurs a cost.
- The public mempool reveals trade intent, leading to front-running risks.
- Smart contracts are susceptible to bugs, exploits, and rug pulls.
- While L2s (Arbitrum, Optimism) enhance speed and reduce costs, the primary focus here is on L1.

Layer 2 Solutions (Brief)

Problem: Ethereum L1's Scalability Issues

- Low Transaction Speed: Approximately 15 transactions per second (TPS) is insufficient for widespread global adoption.
- High Costs: Elevated gas fees make the platform inaccessible for many retail users.
- Network Congestion: The network experiences significant slowdowns during periods of high demand.

Layer 2 Solutions (Brief)

Layer 2 Solutions

- Optimistic Rollups:
  - Arbitrum (~4,000 TPS)
  - Optimism (~2,000 TPS)
- ZK-Rollups:
  - zkSync (off-chain proofs)
- Sidechains:
  - Polygon (formerly Matic)

Layer 2 Solutions (Brief)

How L2s Work + Trade-offs

L2s execute transactions off-chain, then post compressed data to L1, inheriting Ethereum's security at a lower cost.

Benefits:

- Faster: 100–4,000 TPS
- Cheaper: ~$0.10–1 per transaction

Trade-offs:

- Slightly reduced security
- Fragmented liquidity

Layer 2 Solutions (Brief)

For This Class: Focusing on the Ethereum Base Layer

We will concentrate on Ethereum's Base Layer (L1) due to its fundamental importance. While L2 solutions are significant, they introduce additional architectural complexity. The core principles discussed will remain consistent across all layers.

◎ Solana: Parallel Architecture

Parallel Processing Explained

Analogy: Multi-Lane vs. Single-Lane

- Traditional Blockchains: Single-threaded execution, processing one transaction at a time, leading to bottlenecks.
- Solana: Multi-threaded execution, enabling simultaneous processing of many transactions.

Parallel Processing Explained

Sealevel: Parallel Execution

- Transactions specify accounts for reading and writing.
- Transactions without overlapping account access execute in parallel.
- Example: 100 independent swaps can all run concurrently.
- Increased core count leads to higher throughput (horizontal scaling).

Parallel Processing Explained

Sealevel: Parallel Execution

- Transactions specify accounts for reading and writing.
- Transactions without overlapping account access execute in parallel.
- Example: 100 independent swaps can all run concurrently.
- Increased core count leads to higher throughput (horizontal scaling).

Parallel Processing Explained

No Global State Lock

- Ethereum: Global state, sequential execution
- Solana: Local state access, parallelizable
- Designed for scalability with hardware improvements

Parallel Processing Explained

Proof of History (PoH)

- PoH acts as a cryptographic clock, establishing a clear order for transactions.
- This innovation significantly reduces latency by minimizing the need for validator coordination.
- Its hardware-optimized architecture enables a very high transaction per second (TPS) rate.
- However, this comes with a trade-off: higher hardware costs, which raise concerns about centralization.

Parallel Processing Explained

Key Innovations:

- Massive Scalability:
  - High throughput design from the start.
  - Sealevel parallel execution engine for significant scaling.
  - Proof of History reduces consensus overhead.
- Performance:
  - Ultra-fast block times.
  - Low transaction fees for real-time applications.
- Hardware Optimization:
  - Utilizes modern hardware like multi-core processors and GPUs.

Are there any downsides to these innovations?

Solana Performance Metrics

Block Time & Speed

- Effective block time: 0.4–0.5 seconds
  - This is based on approximately 0.4-second slots, though not all slots produce blocks.
- Significantly faster than other cryptocurrencies:
  - 120 times faster than Bitcoin
  - 24 times faster than Ethereum

Solana Performance Metrics

Finality

- Economic Finality: ~13 seconds (32 slots), the recommended duration for absolute transaction finality.
- Practical Finality: 1–2 seconds (1 slot), representing the near-instantaneous confirmation of transactions.
- This makes it 277 times faster than Bitcoin and 30 times faster than Ethereum.

Solana Performance Metrics

Throughput & Fees

- Sustained Throughput: 2,000–4,000 TPS, capable of over 3,000 TPS consistently.
- Peak Throughput: Exceeds 7,000 TPS (e.g., during NFT mints).
- Theoretical Maximum: 65,000 TPS.
- Median Transaction Fee: Approximately $0.00025.
- Congestion Fees: Remains below $0.01, even during peak network activity.
- Cost Efficiency: 1,000 to 100,000 times more affordable than Ethereum.

Solana Performance Metrics

Hardware Requirements

Validators require powerful servers (e.g., 128GB+ RAM), leading to:

- Higher operating costs compared to most other chains.
- Fewer validators, which raises concerns about centralization.

Speed at What Cost?

Advantages

- Near-instant finality: Approximately 13 seconds, compared to Bitcoin's 60 minutes.
- Ultra-low fees: Around $0.00025, significantly less than Ethereum's $10+ during congestion.
- High throughput: Over 3,000 transactions per second (TPS), outperforming others' 7–15 TPS.
- Growing DeFi ecosystem: Includes platforms like Jupiter, Raydium, and Orca.

Speed at What Cost?

Disadvantages

- Centralization concerns: approximately 2,000 validators compared to over 1 million on Ethereum.
- High hardware requirements lead to expensive validation.
- A history of network outages occurred between 2021 and 2022.
- The ecosystem is smaller and newer than Ethereum's.

Speed at What Cost?

Network Stability History

- 2021: Frequent halts due to bot spam.
- 2022: Enhanced stability with fewer disruptions.
- 2023–2024: Marked improvements in network stability.

Speed at What Cost?

The Trade-off

- Solana: Focuses on speed and low cost, sacrificing some decentralization.
- Bitcoin/Ethereum: Prioritize security and decentralization, which can limit scalability.
- The "best" choice depends on user priorities and specific use cases.

Trading Implications: Solana

Strengths

- High-Frequency Trading (HFT) Friendly:
  - Achieves ~13-second finality, ideal for rapid trading strategies.
  - Low fees support profitable tight-spread market making.
- On-Chain Order Books:
  - Central Limit Order Book (CLOB) functionality, similar to Centralized Exchanges (CEXs).
- Arbitrage Maximization:
  - Fast finality ensures maximum capture of arbitrage opportunities.

Trading Implications: Solana

Optimal Applications

- High-frequency trading
- Market making with reduced fee impact
- Cross-DEX or CEX-DEX arbitrage
- NFT trading: rapid minting and cost-effective transactions

Trading Implications: Solana

Ecosystem Notes

- Rapid evolution and adoption growth (2024 surge)
- Key DEXs include Jupiter, Raydium, Orca, and Phoenix/OpenBook
- Monitor network stability before deploying large capital

Trading Implications: Solana

Weaknesses

- Reliability: History of outages, though improving.
- Ecosystem & Liquidity: Smaller ecosystem compared to Ethereum, leading to lower liquidity.
- Centralization: Risk due to fewer validators.
- Maturity: Newer and more experimental environment.

LIVE DEMO: Notebook A

Live Notebook Demo: Blockchain Finality

Notebook A: Blockchain Finality Comparison

What We'll Do (15 minutes)

- Execute cells to fetch live blockchain data
- Calculate real-time finality metrics
- Generate 9+ visualizations comparing architectures

Live Notebook Demo: Blockchain Finality

Key Analyses

- Block time variance across 10 recent blocks
- Finality calculations from real data
- TPS capacity comparisons
- Trading speed scores

Learning Points

- How to query blockchain RPCs
- Dynamic calculations vs. static assumptions
- Interpreting real-world variance

Let's switch to Jupyter and run Notebook A!

☕ BREAK - 15 Minutes

Break Time!

15-Minute Break

Take a moment to stretch, hydrate, and rest your eyes. If you need to review the Part 1 materials, feel free to do so. I will be available to answer any questions you may have in the chat.

When We Return:

We'll dive into Part 2: Trading Applications, covering:

- Cross-chain tokens and wrapped assets
- CEX vs DEX volume analysis
- Architecture performance scoring
- Three more live notebook demos!

Part 2: Trading Applications

Cross-Chain Tokens

The Token Mapping Problem

- BTC is tied to the Bitcoin blockchain.
- Over $10 billion of Wrapped Bitcoin (WBTC) also circulates on Ethereum.
- This allows access to Ethereum's decentralized finance (DeFi) ecosystem.
- DeFi offers opportunities for lending, trading, and yield generation.

The Token Mapping Problem

Liquidity Fragmentation of BTC

BTC liquidity is fragmented across multiple chains, with various wrapped versions existing on different platforms:

- Ethereum: WBTC, renBTC, sBTC
- Solana: Wrapped BTC via Wormhole/Portal

Each of these versions maintains separate liquidity pools.

The Token Mapping Problem

Trading Implications

- Price Discrepancies: Variations exist between native and wrapped token prices.
- Cross-Chain Arbitrage: Opportunities arise from differing prices across various blockchains and token representations.
- Liquidity Differences: Liquidity depth varies significantly between chains and specific trading pools.
- Bridge Impact: Transaction fees and potential delays associated with blockchain bridges can negatively affect the quality of trade execution.

The Token Mapping Problem

Crucial Questions for Traders

- Liquidity: Where can the deepest liquidity be found at present?
- Execution: Which asset offers the most favorable execution?
- Bridge Risks: What bridge-related risks are involved (e.g., smart contracts, delays)?

Native vs Wrapped Tokens

Native Tokens

- BTC (Bitcoin blockchain)
- ETH (Ethereum blockchain)
- SOL (Solana blockchain)
- Offer true ownership with no counterparty risk.

Wrapped Tokens

- WBTC: Bitcoin on Ethereum (ERC-20)
- wETH: Wrapped Ether (ERC-20 version of ETH)
- wSOL: Wrapped SOL (SPL token)
- Backed 1:1 by a custodian or smart contract.

Native vs Wrapped Tokens

Bridged Tokens & Cross-Chain Communication

- Key Platforms:
  - Portal (Wormhole): Facilitates cross-chain bridging.
  - Multichain: A bridge protocol that ceased operations in 2023.
  - CCTP: Bridges USDC across chains.
  - Stargate: Bridges (and swaps) tokens across chains as well.
  - LayerZero: Enables omnichain messaging.
- Security Concerns: Over $2 billion was stolen from bridge exploits in 2022 alone.

Native vs Wrapped Tokens

Token Flow Across Chains (Diagrammatic Representation):

1. Lock native BTC: The original Bitcoin is locked on its native blockchain.
2. Mint WBTC on Ethereum: An equivalent amount of Wrapped Bitcoin (WBTC) is minted on the Ethereum blockchain.
3. Bridge WBTC to Solana: The WBTC is then bridged to the Solana blockchain.
4. Receive wrapped-WBTC: On Solana, the user receives a wrapped version of WBTC.

Associated Risks: Each cross-chain hop introduces counterparty risk and incurs fees.

Wrapped Token Mechanics: WBTC Example

How WBTC Functions

- 1:1 Backing: Each WBTC is fully backed by one Bitcoin.
- Centralized Custody: BitGo acts as the custodian for the underlying BTC.
- Minting Process: To mint WBTC, Bitcoin is locked, and an equivalent amount of WBTC is created on the Ethereum blockchain.
- Burning Process: To burn WBTC, the WBTC is destroyed, and the corresponding Bitcoin is released from custody.

Wrapped Token Mechanics: WBTC Example

Minting Process

- User sends BTC to BitGo custody.
- BitGo verifies the deposit (requires 6 confirmations).
- Merchant mints WBTC (an ERC-20 token).
- User receives WBTC on Ethereum.

Wrapped Token Mechanics: WBTC Example

Burning Process

- User initiates WBTC burn by sending it to a burn address.
- Merchant informs BitGo of the burn.
- BitGo releases an equivalent amount of BTC to the user's BTC address.
- The total WBTC supply is reduced accordingly.

Wrapped Token Mechanics: WBTC Example

Risks & Transparency

Risks:

- Custodian Trust: Centralization risk as BitGo holds keys.
- Smart Contract Vulnerabilities: Potential exploits in smart contract code.
- Bridge/Cross-Chain Exploit Risk: Vulnerabilities in cross-chain interactions.
- Regulatory Shutdown Risk: Potential for government intervention or bans.

Transparency:

- Public proof of reserves.
- On-chain supply is auditable.

Trading Implications: Cross-Chain

Price Discrepancies: WBTC vs. BTC

- WBTC can experience a $10–100 premium or discount compared to BTC.
- These spreads widen significantly during periods of high volatility.
- This creates arbitrage opportunities to buy low and sell high.

Trading Implications: Cross-Chain

Arbitrage Strategies

- Cross-chain Arbitrage:
    - BTC on CEX ↔ WBTC on Ethereum (e.g., Uniswap)
    - Wrapped token across different chains (e.g., ETH → Solana)
- Intra-chain Arbitrage:
    - Native token ↔ Wrapped token on the same chain

Trading Implications: Cross-Chain

Liquidity Considerations

- WBTC on Ethereum: Deep liquidity (over $500M in Curve pools).
- Wrapped BTC on Solana: Thinner liquidity (around $50M).
- Slippage: Larger trades will experience higher slippage in smaller pools.

Trading Implications: Cross-Chain

Bridge Fees, Delays & Risk Management

- Bridge ETH → Solana: ~$5–20 + 15–30 minutes delay (now can be done in <1m for USDC with CCTP v2!).
- Bridge fees and delays must be factored into profit calculations.
- Risk Management:
  - Diversify across multiple bridges.
  - Monitor bridge Total Value Locked (TVL).
  - Review audit reports.
  - Be aware that bridges are frequent hack targets.

LIVE DEMO: Notebook B

Live Notebook Demo: Token Mapping

What We'll Do (5-10 minutes)

- Fetch metadata for BTC, ETH, SOL
- Analyze wrapped versions (WBTC, wETH, wSOL)
- Compare price history and volatility
- Visualize market cap and trading volume

Key Analyses

- Price correlation: Native vs Wrapped
- Liquidity depth across chains
- Trading volume distribution
- Volatility comparisons

Live Notebook Demo: Token Mapping

Learning Points:

- Querying CoinGecko API for token data
- Identifying arbitrage opportunities
- Understanding liquidity fragmentation

Let's switch to Jupyter and run Notebook B!

CEX vs DEX Dynamics

Centralized Exchanges (CEX)

Leading Centralized Exchanges (CEXs)

- Binance: The world's largest, handling over $50 billion in daily volume.
- Coinbase: A prominent US-based exchange known for its robust compliance.
- Kraken: An established player with a strong focus on security.
- OKX, Bybit, KuCoin: Significant global alternatives in the CEX market.

Centralized Exchanges (CEX)

Pros

- Deep liquidity for tight spreads
- Fast execution through off-chain matching and settlement
- Easy onboarding with fiat on/off-ramps
- Advanced features including margin, futures, and lending

Centralized Exchanges (CEX)

Custody Risk: "Not your keys, not your coins."

Other Risks:

- KYC requirements: Identity verification is mandatory.
- Withdrawal limitations: Restrictions on withdrawals may apply.
- Regulatory challenges: Potential for shutdowns or frozen assets due to regulatory actions.

Centralized Exchanges (CEX)

Market Share & Dominance

- Bitcoin: 98% CEX, 2% DEX
- Ethereum: 65% CEX, 35% DEX
- Solana: 75% CEX, 25% DEX

CEX dominance is driven by superior user experience (UX), high liquidity, and the absence of gas fees.

Decentralized Exchanges (DEX)

Major Decentralized Exchanges (DEXs)

- Uniswap (Ethereum): Handles over $4 billion in daily trading volume.
- Raydium (Solana): Operates as a hybrid automated market maker (AMM) and order-book exchange.
- PancakeSwap (Binance Smart Chain): A prominent DEX on the Binance Smart Chain.
- Curve (Ethereum): Specializes in stablecoin trading.

Decentralized Exchanges (DEX)

Advantages

- Self-Custody: You maintain control over your private keys.
- Anonymity: Trade without KYC (Know Your Customer) requirements.
- Composability: Seamless integration with other DeFi (Decentralized Finance) protocols.
- Permissionless: Open access for anyone to list tokens.

Decentralized Exchanges (DEX)

Here are the cons:

- Gas fees: Each trade incurs a cost on the blockchain.
- Slippage: Large orders can significantly alter the price.
- Impermanent loss: A risk faced by liquidity providers.
- UX complexity: Requires wallets, gas, and approvals.

Decentralized Exchanges (DEX)

How AMMs Work + Market Share

AMM Mechanics:

- Utilizes liquidity pools based on the $x * y = k$ formula.
- Unlike traditional exchanges, pricing is derived from the ratio within the pool, not an order book.
- Example: A pool containing 100 ETH and 200,000 USDC results in a price of $2,000/ETH (200,000 / 100).

Decentralized Exchanges (DEX)

Market Share:

- Decentralized Exchanges (DEXs) are experiencing significant growth, with market share ranging from 5-35% depending on the specific blockchain.
- Ethereum leads in DEX adoption, accounting for approximately 35% of the market.
- Bitcoin, lacking a smart-contract layer, has minimal DEX presence.

Trading Strategy Selection: CEX vs DEX

When to Use a Centralized Exchange (CEX)

- Large Trades: Benefit from deep liquidity and minimal slippage.
- Fiat On/Off-Ramp: Easily convert between fiat currencies (e.g., USD/EUR) and cryptocurrencies.
- Leverage Products: Access margin trading, futures, and perpetual contracts.
- High-Frequency Execution: Execute trades instantly and off-chain for speed and efficiency.

Trading Strategy Selection: CEX vs DEX

When to Use a DEX

- Privacy: Facilitates anonymous trading without Know Your Customer (KYC) requirements.
- DeFi Strategies: Enables various decentralized finance strategies through composability.
- Early Token Access: Provides access to new tokens, which often launch on DEXs first.
- Self-Custody: Allows users to maintain control of their assets, bypassing centralized custodians.

Trading Strategy Selection: CEX vs DEX

Hybrid Approach: Optimizing Trades with CEX and DEX

- Workflow Integration: Combine Centralized Exchanges (CEX) for large trades and fiat transactions with Decentralized Exchanges (DEX) for faster execution and access to new assets.

Gas Cost Impact on Trading Strategy

- Ethereum: High gas costs ($10–$100) limit viability to large trades.
- Arbitrum/Optimism: Moderate gas costs ($0.10–$1) make mid-sized trades feasible.
- Solana: Extremely low gas costs ($0.00025) enable even small trades.

Trading Strategy Selection: CEX vs DEX

Risk Management

- Centralized Exchange (CEX) Risks:
  - Counterparty risk
  - Freeze/shutdown risk
- Decentralized Exchange (DEX) Risks:
  - Smart contract bugs
  - Exploits
- Mitigation Strategy:
  - Diversify across multiple platforms; avoid relying on a single venue.

LIVE DEMO: Notebook C

Live Notebook Demo: CEX vs DEX Volume

Notebook C: 30-Day Volume Analysis

- Fetch 30-day trading volume history.
- Dynamically calculate CEX vs DEX splits.
- Generate over 9 visualizations (3 per blockchain).
- Identify trends and changes in market structure.

Live Notebook Demo: CEX vs DEX Volume

Key Visuals & Learning Points

- Charts & Trends
  - Line charts: Volume trends over time
  - Stacked area charts: CEX vs. DEX market share
  - Pie + bar charts: Comparative market dominance
- Decentralized Exchange (DEX) Insights
  - Why Ethereum leads DEX adoption
  - How architecture affects DEX viability
  - Volume behavior during volatility spikes

Let's switch to Jupyter and run Notebook C!

Architecture Performance Scoring

Multi-Dimensional Comparison

Trading: Beyond Just Speed

While speed is crucial, it's not the only factor in successful trading. Consider:

- Security: Is the finality of your trades trustworthy?
- Liquidity: Can you execute large orders efficiently?
- Cost: Are transaction fees eating into your profits?

Multi-Dimensional Comparison

10 Key Comparison Dimensions

1. Speed (finality): How quickly transactions are finalized.
2. Throughput (TPS): The number of transactions processed per second.
3. Security (track record): The historical security performance of the network.
4. Decentralization (validators): The degree of decentralization based on the number of validators.
5. DeFi Capability (smart contracts): The ability to support decentralized finance applications through smart contracts.
6. Liquidity Depth (volume/TVL): The extent of liquidity, measured by trading volume and total value locked.
7. Trading Venues Available: The number of platforms where the asset can be traded.
8. Bridge Availability: The presence of bridges for cross-chain transfers.
9. Network Stability (uptime): The reliability and consistent operation of the network.
10. Transaction Cost (fees): The fees associated with each transaction.

LIVE DEMO: Notebook D

Live Notebook Demo: Architecture Scoring

Notebook D: Multi-Dimensional Scoring

- Scores blockchains across 10 performance dimensions
- Uses real, dynamic data (not assumptions)
- Generates radar charts and comparative visuals
- Computes trading suitability per strategy

Live Notebook Demo: Architecture Scoring

Key Visuals & Learning Points

- Radar charts: Illustrate 10-dimensional profiles.
- Bar charts: Rank dimensions individually.
- Heatmaps: Show suitability between strategy and blockchain.
- Learn to apply weighting methods for priorities.
- Understand that data-driven scoring is goal-dependent, with no single "best" approach.

Let's transition to Jupyter and execute Notebook D!

Architecture Evolution: The Future

Architecture Evolution: The Future

Bitcoin: Layer 2 Focus

- Lightning Network: Enables instant and low-cost payments.
- Taproot: Lays the groundwork for enhanced privacy and smart contracts.
- Ordinals/NFTs: A controversial area of growth on the Bitcoin network.

Ethereum: Scaling with Layer 2s and Sharding

- Rollups: Key solutions include Arbitrum, Optimism, and zkSync.
- Proto-danksharding: Aims to reduce data costs for Layer 2 solutions.
- Long-term Target: Achieve over 100,000 transactions per second (TPS).

Solana: Stability and Performance

- Firedancer Validator Client: Developed by Jump Crypto.
- Target: Reach over 1 million TPS through parallel execution.
- Goal: Enhance decentralization and resilience of the network.

Wrap-Up & Next Steps

Key Takeaways

Architecture Determines Performance

Different blockchain architectures offer varying performance characteristics:

- UTXO (Unspent Transaction Output): Known for its security and simplicity, but offers lower transaction throughput (e.g., Bitcoin).
- EVM (Ethereum Virtual Machine): Provides programmability and moderate scalability (e.g., Ethereum).
- Parallel Execution: A newer technology enabling high-speed transactions (e.g., Solana).

Key Takeaways

Performance Dictates Strategy

- Bitcoin: Approximately 60-minute finality, preventing fast arbitrage.
- Ethereum: Approximately 6.4-minute finality, enabling decentralized finance (DeFi).
- Solana: Approximately 13-second finality, facilitating high-frequency trading (HFT) and arbitrage.

Key Takeaways

No Single "Best" Blockchain

The optimal blockchain choice is dictated by its intended use:

- Bitcoin: Prioritizes security and serves as a store of value.
- Ethereum: Excels in decentralized finance (DeFi) and composability.
- Solana: Offers high speed and low transaction fees.

Key Takeaways

Prioritize Real Data Over Assumptions

- Disregard marketing claims (e.g., "65k TPS!").
- Verify actual performance: fees, transactions per second (TPS), and finality.
- Utilize explorers, RPCs, and measurement tools for verification.

Key Takeaways

Tools Matter

- Jupyter notebooks for live data analysis
- RPC queries for real-time chain insights
- Visualizations to reveal trends and patterns

Architecture drives trading outcomes!

Next Steps & Homework

Next Steps & Homework

Homework Assignment

- Run all 4 notebooks independently.
- Modify parameters to explore different blockchains.
- Analyze behavior during high volatility periods.
- Determine which blockchain best suits your trading strategy.

Next Steps & Homework

Stablecoins, Risk Management & Trading Psychology

- Stablecoins: USDT, USDC, DAI mechanisms
- Other on-chain tradable instruments:
  - Perpetual futures
  - Leveraged tokens
  - Liquid staking tokens (stETH, mSOL)
  - RWAs (tokenized treasuries, commodities)
  - Options / structured vault products
- Risk: position sizing, stop losses, leverage
- Psychology: emotions, discipline, journaling

Next Steps & Homework

Resources

- Block explorers: blockchain.info, etherscan.io, solscan.io
- APIs: CoinGecko, Alchemy, Helius
- Community: Discord, Twitter, GitHub