

The Fiat Standard – Lecture 14 (Bitcoin Scaling) • Study Notes

Overview

- Global digital payments today: **2–3 billion non-cash transactions per day**.
 - Bitcoin's on-chain peak: **~500,000 transactions/day** (~0.017% of global volume).
 - To process all digital payments on-chain, Bitcoin would need a **6,000× capacity increase**.
 - Naïve solution: bigger blocks = more transactions.
 - Problem: larger blocks undermine **decentralization**, which is Bitcoin's core value.
-

1. The Naïve Scaling Approach: Bigger Blocks

- **Idea:** Increase block size → more transactions per block.
 - **Reality:**
 - Larger blocks → harder to download & sync → fewer nodes can participate.
 - Leads to **centralization** (only powerful computers can keep up).
 - Example: To handle global non-cash transactions, Bitcoin would need **5 TB blocks every 10 minutes**.
 - No consumer hardware can support this.
 - Would shrink the network to a handful of operators.
 - **Trade-off:**
 - **Efficiency vs. decentralization.**
 - Centralized systems (e.g., PayPal, Visa) are already efficient.
 - Bitcoin's value lies in being **decentralized and uncapturable**.
-

2. Why On-Chain Scaling Won't Happen

- **Decentralization is non-negotiable:**
 - Bitcoiners resisted block size wars; preserving small blocks preserves sovereignty.
 - Running a node must remain possible for anyone (~\$100–700 hardware).
 - **On-chain = cash settlement:**
 - Bitcoin transactions are **final settlement**, not retail payments.
 - More comparable to interbank transfers than buying coffee.
 - Consumer payments can run on **second layers**.
-

3. Market for Scarce Block Space

- Bitcoin block space = scarce resource.
 - Analogy: **shuttle bus** leaving every 10 minutes, limited seats, auction for entry.
 - Result:
 - Transaction **count** has plateaued since ~2016 (~200–300k/day).
 - **Value per transaction** has skyrocketed (from ~\$10 avg in 2011 → ~\$30–40k avg today).
 - Total **settlement volume** continues to grow (billions daily).
 - **Economic pattern:**
 - Low-value uses get priced out → off-chain.
 - High-value uses dominate on-chain.
 - Just as cows don't graze in Manhattan, trivial transactions won't live on Bitcoin's blockchain.
-

4. Second-Layer Scaling

- **Already happening:**
- Exchanges, casinos, and services settle internally off-chain.

- On-chain only for deposits/withdrawals.
 - **Lightning Network:**
 - Based on **multisig channels**.
 - Two parties lock coins → update balances off-chain infinitely.
 - Closing channel = one on-chain settlement.
 - Routing through other nodes allows global connectivity.
 - Lightning = cheap (fractions of a cent) but limited by **liquidity**.
 - **Other second-layer models:**
 - Custodial systems (exchanges, apps).
 - Physical Bitcoin tools (e.g., OpenDime).
 - Multisig arrangements.
-

5. Liquidity and Investment in Lightning

- Putting Bitcoin into channels = **investment**, not cash holding.
 - Similar to investing in a payments company.
 - Provides liquidity for routing payments in exchange for fees.
 - This specialization → emergence of **professional liquidity providers**.
 - Likely outcome: **hub-and-spoke model**:
 - Tens of thousands of large, well-connected nodes.
 - Individuals open a few channels to these hubs.
 - More centralized than coffee-on-chain dream, but far more decentralized than fiat.
-

6. Risks and Trade-Offs

- **Censorship:**
- A node operator can refuse to serve you, but cannot prevent you from opening your own channel or going elsewhere.
- **Centralization of liquidity:**
- Hubs may form, but unlike fiat banks, they:

- Cannot inflate supply.
 - Cannot control protocol rules.
 - Cannot unilaterally censor the entire network.
 - **Key point:**
 - Bitcoin doesn't need to be decentralized enough to process every coffee purchase.
 - It only needs to be decentralized enough to resist **monetary capture**.
-

Key Takeaways

1. **On-chain scaling is impossible** without sacrificing decentralization.
 2. Bitcoin's on-chain layer = **final settlement**, not everyday payments.
 3. Block space scarcity leads to prioritization of **high-value transactions**.
 4. **Second layers (Lightning, exchanges, multisig)** handle small, high-frequency payments.
 5. Providing liquidity = **investment industry**, leading to specialization and efficiency.
 6. Even with some centralization of payment routing, Bitcoin remains **fundamentally uncensorable, non-inflatable, and decentralized enough** to preserve its value proposition.
-