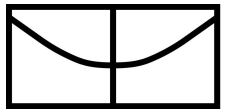


MIT Digital Currency Initiative and the University of Brasilia presents

Cryptocurrency Design and Engineering

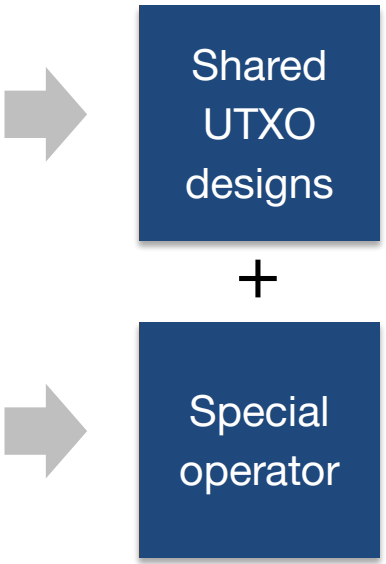
Lecture 13: Scalability Continued
Taught by: Neha Narula
October 21st, 2025
MAS.S62

Payment channel pattern

- If we're the only ones who care about our payments, do that **cooperatively** off-chain, with the ability to always litigate on-chain
- This concept is called *unilateral exit* – a user can always get their funds out
  - Very cool that we can broaden it to work in a network of off-chain transactions!

Technical, economic, and usability challenges of Lightning

- UTXO set capacity
  - Lightning still relies on at least one UTXO per user
  - Unclear how to safely increase the UTXO set by an order of magnitude and we may run into limits
- Rebalancing liquidity
  - Economic relationships are not balanced
  - Requires going back on chain
- Interactivity (online requirements)
  - Mobile phones aren't always online to sign new states



Shared UTXO designs

- Ark
- Rollups

Coinpool

- Multiple users share a UTXO with a multisig
- Continuously sign transactions which change the distribution (payouts) of the funds
- Requires everyone online to sign

Ark

- Idea: Coinpool, but special operator coordinates payments between Ark users, who have exit transactions
- Operator maintains and updates regular on-chain commitments to trees of exit transactions
- Way to atomically revoke old exit paths
- Only spending/receiving users need to be online to sign

nehanarula.org/2025/05/20/ark.html

Ark pros/cons

Pros

- Very good off-chain scalability with more users in one Ark
- No user liquidity management
- Doesn’t require routing (but interoperates with Lightning)

Cons

- Requires a special operator
- Lots of interactivity (spenders and receivers have to sign multiple times)
- No latency improvement
- Operator requires 2X liquidity

Rollups

- Idea: move work to another blockchain!
- L1 (main chain) *validates* what happens on the L2 (rollup)
- L1 and L2 can have different:
  - Data models
  - Smart contracting languages
  - Consensus protocols

Easier to do in Ethereum, harder in Bitcoin

Rollup architecture

- Coordinator / sequencer
- Two key questions:
  - Where is the data for the rollup stored?
  - How does the L1 validate execution on the rollup?

Data availability (DA)

Optimistic vs. ZK

Proof of execution

- Optimistic rollups
  - Assume rollup operator is operating correctly
  - Fraud proof game on L1 to *challenge* execution in the event of incorrect operation
  - Who can trigger the fraud proof game?
- ZK rollups
  - Rollup operator has to provide a valid proof of execution to commit to L1
  - Who can become an operator?

This prevents the rollup operator from stealing funds

Rollup nomenclature

Limited storage improvement (state diffs)

	ZK proofs	Fraud proofs
Data on L1	ZK rollup (Linea, Starknet, ZKSync)	Optimistic rollup (Optimism, Base, Arbitrum)
Data somewhere else	Validium (Sophon)	Plasma

Different trust model

l2beat.com

Before rollups: sidechains (2014)

- Move funds back-and-forth with a federated set of signers
  - The federation has custody
- Need a majority (or super majority) of k of n signers to move the funds
  - n-k can freeze the funds
- Example: Blockstream's Liquid has 11 of 15 signers

Fundamentally different trust model: No DA, no validating, no exit

Relying on exit

Challenges:

- Online requirements: requires watching what's happening and being ready to act if needed (liveness)
- Non-cooperative exit often less efficient
- Having to choose fees ahead of time
- Block space □ minimum securable amounts

There is some "minimum securable wallet size"

Average vs. worst case

Beware super optimistic scaling numbers that assume optimal batching and perfect cooperation!

- With cooperative operators, the on-chain footprint can be low. But the non-cooperative case can be much worse than just transacting on-chain
- There are many normal reasons why one might end up looking “non-cooperative”
  - Users on mobile phones not always online
  - Operators fail thundering herd
  - People just want to go back on chain sometimes, it makes them feel safer

Next week: smart contracts

- Ethereum Virtual Machine
- Smart contract development
- Security and exploits
- Common applications

But first: guest lecture on BitVM and Bitcoin rollups!