DeFi Talents

Organized by

Frankfurt School Blockchain Center

Web3 Talents

Powered by

KFW

INNO LAB

Deka

DATENSERVICE

dwpbank

Supported by

DEC INSTITUTE

DCA

MAMA

ECOTA

Assignment 7

Feb 3, 2025

By

Manjiri Birajdar

Software Developer

Scaling solutions

Scaling solutions based on Ethereum: Create a typology of scaling solutions.

Type	Solution	Description	Example
Layer 1	Ethereum 2.0 (PoS)	Transition to PoS to improve scalability and energy efficiency.	Ethereum 2.0
Layer 2	Optimistic Rollups	Off-chain execution with fraud-proof mechanisms.	Optimism, Arbitrum
	ZK Rollups	Uses zk-SNARKs to validate transactions off-chain.	zkSync, StarkWare
	Plasma	Child chains to offload computation from the Ethereum main chain.	Matic, OmiseGo
	Validium	Similar to ZK Rollups but with off-chain data availability.	StarkEx
	Sidechains	Independent blockchains with periodic data anchoring to Ethereum.	Polygon, xDai
Hybrid	Ethereum + Layer 2	Combining Layer 1 and Layer 2 solutions.	Polygon
Off-chain	State Channels	Off-chain channels for faster, cheaper transactions.	Raiden Network
Data Availability	Celestia	Off-chain data availability for Layer 2.	Celestia

Scaling solutions

What is a second layer? How do they differ from L1s in terms of execution and consensus? What are some examples you know of?

A **Second Layer (L2)** refers to a set of protocols built on top of a base blockchain (Layer 1, such as Ethereum) to improve scalability, reduce transaction costs, and increase speed without altering the underlying Layer 1 blockchain. L2 solutions enable the handling of more transactions off-chain or through different methods, while still relying on the security of the Layer 1 blockchain.

Feature	Layer 1 (L1)	Layer 2 (L2)
Execution	Executes transactions and smart contracts directly on the main chain (e.g., Ethereum).	Executes transactions off-chain or partially off-chain, processing data outside the L1 blockchain.
Consensus	Consensus is achieved through the main chain's mechanism (e.g., Proof of Work or Proof of Stake).	Relies on the L1's security and finality but has its own consensus for handling transactions off-chain (e.g., Optimistic Rollups, ZK Rollups).
Scalability	Limited by block size, throughput, and network congestion.	Can handle more transactions by moving the workload off the main chain.
Security	Security is inherent and directly enforced by the main chain.	Security is guaranteed by L1, but L2s may have additional challenges, like fraud proofs or data availability.
Transaction Costs	Higher fees due to network congestion and block space competition.	Reduced fees due to off-chain processing or more efficient mechanisms.

Examples of Layer 2 solutions

Optimistic Rollups: Off-chain execution with fraud-proof mechanisms.
Example: **Optimism**, **Arbitrum**.

ZK Rollups: Use cryptographic proofs (zk-SNARKs or zk-STARKs) for off-chain transaction validation.
Example: **zkSync**, **StarkWare**.

State Channels: Off-chain transactions with only final states submitted on-chain.
Example: **Raiden Network**, **Lightning Network**.

Plasma: Child chains that offload computation and submit critical data to the main chain.
Example: **Matic** (now Polygon), **OmiseGo**.

Sidechains: Independent blockchains with their own consensus mechanisms.
Example: **Polygon**, **xDai**.

Scaling solutions

Explore the risks associated with different Layer 2 solutions (e.g., L2Beat).

Layer 2 Solution	Risks	Mitigation Strategies
Optimistic Rollups	Fraudulent transactions (if not challenged)	Fraud proofs and time delays
ZK Rollups	High cost and complexity of zk-proof generation	Optimizations in zk-rollup technology
State Channels	Counterparty risk (inactive or malicious parties)	Timeout periods and dispute resolution
Plasma	Exit scams and data availability issues	Layer 1 anchors and challenge mechanisms
Sidechains	Security risks of custom consensus mechanisms	Use of secure consensus protocols
General L2 Risks	Centralization, exit liquidity issues	Decentralization efforts and liquidity support

DYOR

Scaling solutions

What is the business model of L2s?

1. **Transaction Fees**: L2s charge lower fees than L1, earning revenue from off-chain transactions.
2. **Transaction Volume**: More transactions mean more fees, driving adoption and usage.
3. **Staking and Liquidity**: L2s may require staking or liquidity provision, generating revenue for stakers and liquidity providers.

These models focus on reducing costs, increasing transaction throughput, and enhancing scalability.

DYOR

Scaling solutions

How do they work “under the hood”?

Layer 2 Solution	How It Works	Mechanism
Optimistic Rollups	Transactions are processed off-chain, with only a summary (state root) posted on Layer 1.	Assumes transactions are valid unless proven otherwise through **fraud proofs** when challenged.
ZK Rollups	Off-chain transactions are bundled, and cryptographic proofs (zk-SNARKs or zk-STARKs) are generated to prove validity.	**Zero-knowledge proofs** are submitted to Layer 1 to ensure the correctness of off-chain batches.
State Channels	A private, off-chain communication channel is opened for multiple transactions, and only the final state is recorded on-chain.	Participants interact off-chain, reducing fees and latency. Dispute resolution happens on Layer 1.
Plasma	Creates child chains that process transactions off-chain, committing data (state roots) periodically to the main chain.	Transactions are executed off-chain on Plasma chains, and only essential data is posted back to L1.
Sidechains	Independent blockchains with their own consensus mechanisms, periodically anchored to the main chain for data validation.	Transactions are handled on the sidechain and periodically verified on Ethereum.

Scaling solutions

What are the cheapest scaling solutions? Is it worth the trade-off?

1. **State Channels**: Minimal fees as transactions happen off-chain; only final states are posted on-chain.
2. **Plasma**: Low costs by processing transactions on child chains and only committing essential data to Layer 1.
3. **Optimistic Rollups**: Low fees with off-chain execution, but with potential delays due to fraud-proof challenges.

Is it worth the trade-off?

- **Yes**, if you prioritize low costs and can accept minor trade-offs in terms of latency, complexity, and security risks. However, the cost-saving benefits are balanced by factors like potential security issues or slower finality.

DYOR

Scaling solutions

What are the differences between Optimistic Rollups and ZK-Rollups? Compare transaction fees and security tradeoffs.

Factors	Optimistic rollups	ZK rollups
Proof type	Uses fraud proofs to dispute invalid transactions	Uses ZK proofs to prove the validity of transactions
Latency	Settlement finality is delayed due to dispute-resolution period on Layer 1	Faster finality, reducing settlement times and improving user experience
Security	Rely on honest participants and economic incentives for detecting fraudulent transactions	Provide cryptographic certainty of the validity of transactions, eliminating the reliance on trust
Complexity	Simpler to implement but require a robust monitoring system for fraud detection	More complex due to the need to generate and verify ZK proofs
Withdrawal time	Withdrawal times take longer due to potentially delayed finality	Quicker access to funds because finality is nearly-instant

https://starkware.co/blog/zk-rollups-explained/zk-rollups-vs-optimistic-rollups/

Assignment for next session (deadline: session 8)

REMINDER:

Practical: Interview a DeFi expert (2/2)

A. Get in contact with an expert within your chosen domain and prepare and conduct a 15-minute interview. No recording is required. As a fall-back alternative, you can also interview a Talent or a Mentor from the DeFi Talents program (in an emergency, we can assist with expert contact).
B. Reflect on the interview you did, and revisit it. How can the outcomes of the interview be matched with your learnings so far and the current situation in the DeFi ecosystem?
C. Summarize the key insights in a 3-5-minute video and upload it to YouTube as an “unlisted link” (not publicly available).
D. Next session, each participant will present their interview for 3 minutes.

DYOR

Practical Interview

Reviewed interview: https://www.defipulse.com/blog/ama-with-cryptex-founder-preston-van-loon

AMA with Cryptex founder Preston Van Loon : Key Insights

1. **Cryptex Mission**: Provides liquidity and transparency in DeFi through synthetic assets, enabling exposure to various assets like indexes and commodities.
2. **TCAP Token**: Cryptex's flagship synthetic asset, representing the total market cap of cryptocurrencies, allowing decentralized exposure to the entire crypto market.
3. **Partnerships**: Emphasizes the importance of partnerships for ecosystem growth and product integration.
4. **Future Plans**: Expanding beyond crypto to include synthetic assets for traditional real-world assets and enhancing scalability and decentralized governance.
5. **Challenges**: Security and risk management are key challenges in creating synthetic assets.
6. **Education**: Building user awareness on synthetic assets to ensure safe use in DeFi.
7. **Vision for DeFi**: Aims to make DeFi globally accessible, providing financial tools without traditional intermediaries.

References

Layer 2 Solutions Overview:

- https://ethereum.org/en/layer-2/
- https://www.coindesk.com/learn/what-are-layer-2-scaling-solutions-and-how-do-they-work
- https://www.polygon.technology/

Layer 2 Scaling Solutions (Optimistic Rollups, ZK Rollups, etc.):

- https://ethereum.org/en/layer-2/optimistic-rollups/
- https://ethereum.org/en/layer-2/zk-rollups/
- https://arbitrum.io/
- https://zk-sync.io/

Risks of Layer 2 Solutions:

- https://www.l2beat.com/
- https://www.coindesk.com/learn/understanding-layer-2-ethereum
- https://www.coindesk.com/learn/risks-layer-2-scaling-solutions

Layer 2 Business Model:

- https://www.coindesk.com/learn/how-ethereum-layer-2-solutions-make-money
- https://www.polygon.technology/solutions
- https://www.optimism.io/

Smart Contract Auditing:

- https://blog.trailofbits.com/2020/10/21/the-art-of-smart-contract-auditing/
- https://consensys.github.io/smart-contract-best-practices/
- https://www.coindesk.com/learn/how-to-audit-smart-contracts

Risks in Blockchain (Smart Contracts, Layer 2):

- https://www.coindesk.com/learn/blockchain-security-risks
- https://medium.com/coinmonks/blockchain-security-risks-explained-7f6504a5d538
- https://www.consensys.net/blog/blockchain-security/how-to-secure-smart-contracts/