OST
Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

Ethereum Layer 2 Solutions

Thomas Bocek

25.11.2024

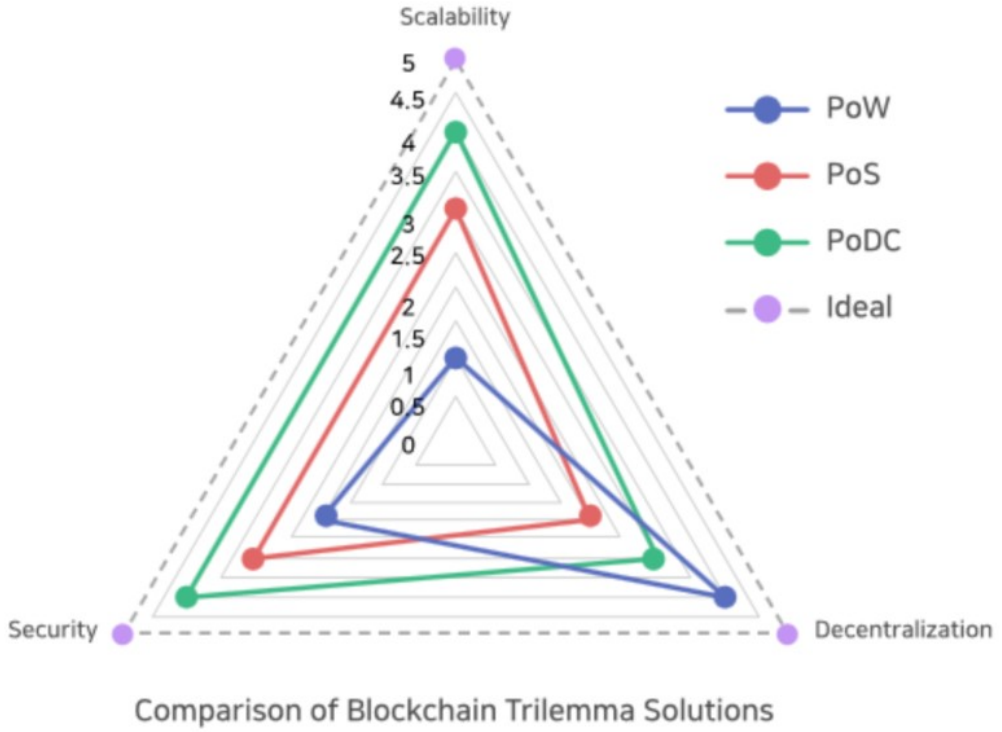
Layer 1 vs Layer 2: Basic Concepts

- Layer 1 (Base Chain)
  - Main Ethereum blockchain
  - Handles consensus, security, data availability
  - All nodes process all transactions
  - Limited by block size and time
- Layer 2 (Scaling Solutions)
  - Additional networks/protocols built on top of Ethereum
  - Inherit security from Layer 1
  - Process transactions externally
  - Post results back to mainnet
- Core Concepts
  - Secondary protocols built on top of Ethereum
  - Process transactions off the main chain
  - Inherit Ethereum's security guarantees
  - Significantly reduce gas fees
  - Increase transaction throughput
- Key Benefits
  - 10-100x lower fees (contracts, random)
  - Increased transactions per second (TPS)
  - Maintained decentralization

OST

Why Do We Need Layer 2?

- Ethereum's current limitations
  - ~15-30 transactions per second
  - Average gas fees: $2-$50+ (highly variable)
  - Block space competition
  - Growing demand for DeFi and NFTs
- The Blockchain Trilemma
  - Decentralization: Network participants and control
  - Security: Protection against attacks
  - Scalability: Transaction throughput and costs
  - Why we can't have all three on L1



Comparison of Blockchain Trilemma Solutions

https://www.halborn.com/blog/post/what-is-sharding

OST

Main Types of Layer 2 Solutions

- Rollups
  - Bundle multiple transactions into one
  - Submit transaction data to Ethereum mainnet
  - Two main types:
    - Optimistic Rollups
    - Zero-Knowledge (ZK) Rollups
- State Channels
  - Private payment channels between parties
  - We covered this in lecture 8

- Difference to Sidechains?
  - Store their own data independently
  - Own security mechanism (separate from Ethereum), independent consensus mechanism (e.g., Proof of Stake)
  - If sidechain is compromised, assets on that chain can be lost
  - But
    - Protocol-level connection to the parent chain
    - Regularly commits/anchors state to the parent chain

OST

Optimistic vs. Zero-Knowledge Rollups

- Optimistic Rollups
  - Post transactions without proofs
  - Assume transactions are valid by default
  - Use fraud proofs to challenge invalid transactions
  - 7-day withdrawal period for security
  - Pros: EVM compatible, simpler technology
  - Cons: Longer withdrawal times
  - Examples: Optimism, Arbitrum
- ZK Rollups
  - ZKP: “A Zero-Knowledge Proof (ZKP) is a cryptographic method that allows one party to prove they know or possess specific information without revealing the information itself.”
  - Generate validity proofs for each batch
  - Use mathematical proofs to verify transactions
  - Immediate finality once proven
  - Pros: Faster withdrawals, more efficient
  - Cons: More complex technology, limited EVM compatibility, compute intensive
  - Examples: zkSync, StarkNet

OST

Technical Details

- Key Components
  - Smart Contracts on L1
    - Handle deposits/withdrawals
    - Store transaction batches
    - Verify proofs
  - Off-chain Infrastructure
    - Sequencers for transaction ordering
    - Provers/Validators for verification
  - State Management
    - Maintain current state off-chain
    - Regular state roots posted to L1
- Flow
  - User initiate transaction on e.g., Arbitrum
  - Arbitrum sequencer (orders transactions), operated by Offchain Labs (centralized)
  - Batch transactions together, post batch to Ethereum
  - Transaction considered "confirmed" on Arbitrum
- Security levels:
  - L2 confirmation from sequencer: immediate
  - L1 Batch Confirmation: ~10-15 minutes
  - Full Security: 7 days

OST

Sequencer / Arbitrum Node

- Sequencer malicious or down
  - Users can force-include transactions directly through L1
  - Alternative sequencers can take over
  - Worst case: delays, but funds remain safe
- Data availability
  - ALL transaction data is posted to Ethereum
  - Posted in compressed calldata ~ratio 1:10
  - Anyone can reconstruct the entire Arbitrum state, not just summaries - full transaction data
- Arbitrum node
  - Anyone can run an Arbitrum node
    - validate all transactions
    - Challengers are rewarded for finding fraud
    - Can challenge incorrect state transitions within 7 days
    - Faster?
      - Run your own trusted Arbitrum node
      - Use ZKP to check proof
- ZK proof for Sui: 1-2v cores: 20-30sec
  - Threadripper 2990WX 32-Core Processor, 2sec

OST

Bridges / Future of L2

- For L1 to L2: ETH on L1
  - → ETH locked in Bridge contract
  - → Message to L2 to mint WETH
  - → Auto-unwrapped to ETH on L2
- For L2 to L1: ETH on L2
  - → Initiate withdrawal
  - → Wait 7 days
  - → Claim on L1
  - → ETH released from bridge contract
- You need on both chains ETH for fees!
  - Or use exchanges / fast bridges (fee vs risk)

- L2 Ecosystem Growth
  - Total Value Locked (TVL) trends
  - Major DApps deploying on L2s
  - User adoption metrics
  - Cost comparisons with L1
  - L2 vs. fast L1
- Future
  - Layer 3s and application-specific chains
  - Cross-L2 communication protocols
  - Protocol standardization, Proto-Danksharding
  - Role in Ethereum's scalability roadmap

OST