Exploring different Etherium Layer 2 solutions for Academic Blockchain Network

Mihael Trajbarič[1]

[1]Faculty of Computer and Information Science
University of Ljubljana

Agenda

- Motivation
- Layer 2 solutions
- Blockchain bridges
- Bridge prototype
- Conclusions

Introduction

- Use case: Academic L2 Network
  - research testbed
  - students and researchers
  - low fees
  - high performance at small power consumption

Introduction

- Use case: Academic L2 Network
  - research testbed
  - students and researchers
  - low fees
  - high performance at small power consumption
- outside partners
  - a lot of interest for blockchain
  - no knowledge or infrastructure

Etherium Layer 2 solutions

- intended for scaling
  - higher volume of transactions
  - lower fees
  - retain (some) security guarantees

Etherium Layer 2 solutions

- intended for scaling
  - higher volume of transactions
  - lower fees
  - retain (some) security guarantees
- Different approaches
  - aggregate transactions, submit to L1
  - running parallel channels
  - separate chain, connected via bridge

Rollups

- off-chain transactions
  - greater volume
  - low transaction fees

Rollups

- off-chain transactions
  - greater volume
  - low transaction fees
- inherit security from L1
  - aggregate transactions
  - submit data/states/proofs back to L1

Rollups

- off-chain transactions
  - greater volume
  - low transaction fees
- inherit security from L1
  - aggregate transactions
  - submit data/states/proofs back to L1
- different approaches
  - submit transactions (Optimistic Rollups)
  - submit states and proofs (ZK-Rollups)

Optimistic Rollups

- batch transactions in a bundle
  - operator submits bundle to L1
  - submit details about all transactions
- optimistic
  - assume all submitted transactions are valid
  - challenge window (7 days)
  - fraud challenge
  - bonded operators

Optimistic Rollups

- batch transactions in a bundle
  - operator submits bundle to L1
  - submit details about all transactions
- optimistic
  - assume all submitted transactions are valid
  - challenge window (7 days)
  - fraud challenge
  - bonded operators
- pros
  - EVM-compatible
  - 100x decrease in gas fees
  - high levels of trustlesness
  - highly decentralised
  - cryptoeconomic incentives

Optimistic Rollups

- batch transactions in a bundle
  - operator submits bundle to L1
  - submit details about all transactions
- optimistic
  - assume all submitted transactions are valid
  - challenge window (7 days)
  - fraud challenge
  - bonded operators
- pros
  - EVM-compatible
  - 100x decrease in gas fees
  - high levels of trustlessness
  - highly decentralised
  - cryptoeconomic incentives
- cons
  - slow transaction finality (7 days)

Zero-Knowledge Rollups

- similar to optimistic
  - batch transactions
  - submit only last state
- cryptographic proofs
  - sequencer and proover
  - bypass (avoid censorship)
  - validity proofs

Zero-Knowledge Rollups

- similar to optimistic
  - batch transactions
  - submit only last state
- cryptographic proofs
  - sequencer and proover
  - bypass (avoid censorship)
  - validity proofs
- pros
  - fast transaction finality
  - transparent and resilient
  - cryptographic certainty

Zero-Knowledge Rollups

- similar to optimistic
  - batch transactions
  - submit only last state
- cryptographic proofs
  - sequencer and proover
  - bypass (avoid censorship)
  - validity proofs
- pros
  - fast transaction finality
  - transparent and resilient
  - cryptographic certainty
- cons
  - proving is costly, increased fees
  - specialized hardware
  - not EVM-compatible
  - some proofs require **trusted environment**

State channels

- p2p off-chain transactions
- **multisig contract**
- submit final state to L1
- finality after challenge period
- virtual state channels

State channels

- p2p off-chain transactions
- **multisig contract**
- submit final state to L1
- finality after challenge period
- virtual state channels
- pros
  - high volume of transactions
  - low fees
  - simple solution

State channels

- p2p off-chain transactions
- **multisig contract**
- submit final state to L1
- finality after challenge period
- virtual state channels
- pros
  - high volume of transactions
  - low fees
  - simple solution
- cons
  - users always online
  - grieving attacks
  - **not EVM-compatible**
  - p2p, user must have channel with every other user
  - pre-deposited funds

Side chains

- completely separate chain
  - different consensus algorithms (PoS, PoA, PoW,...)
  - different block parameters (block size, block times,...)
- connected via bridges

Side chains

- completely separate chain
  - different consensus algorithms (PoS, PoA, PoW,...)
  - different block parameters (block size, block times,...)
- connected via bridges
- pros
  - **EVM-compatible**
  - well established and tested tehnology
  - relatively simple solution
  - lower fees

Side chains

- completely separate chain
  - different consensus algorithms (PoS, PoA, PoW,...)
  - different block parameters (block size, block times,...)
- connected via bridges
- pros
  - **EVM-compatible**
  - well established and tested tehnology
  - relatively simple solution
  - lower fees
- cons
  - do not inherit security guarantees from L1
  - bridges are vulnerable

Plasma chains

- off-chain transactions
- still derive security from mainnet
  - periodically post *state commitments*
  - without revealing actual transactions
  - challenge period

Plasma chains

- off-chain transactions
- still derive security from mainnet
  - periodically post *state commitments*
  - without revealing actual transactions
  - challenge period
- pros
  - higher throughput
  - low transaction fees

Plasma chains

- off-chain transactions
- still derive security from mainnet
  - periodically post *state commitments*
  - without revealing actual transactions
  - challenge period
- pros
  - higher throughput
  - low transaction fees
- cons
  - not EVM-compatible
  - users must be always online
  - slow transaction finality (1 week)
  - single operator
  - data is not available on L1
  - *mass exit*

Validium

- off-chain transactions
- still derive security from mainnet
  - validity proofs
  - proovers and operators
  - similar to zk-proofs

Validium

- off-chain transactions
- still derive security from mainnet
  - validity proofs
  - proovers and operators
  - similar to zk-proofs
- pros
  - much higher throughput
  - low transaction fees
  - near instantaneous transaction finality

Validium

- off-chain transactions
- still derive security from mainnet
  - validity proofs
  - proovers and operators
  - similar to zk-proofs
- pros
  - much higher throughput
  - low transaction fees
  - near instantaneous transaction finality
- cons
  - not EVM-compatible
  - data not available on L1

Approach for Academic Blockchain Network

- requirements
  - full EVM-compatibility
  - low transaction cost

Approach for Academic Blockchain Network

- requirements
  - full EVM-compatibility
  - low transaction cost
- zk-proof based are out (zk-rollups, Validium)

Approach for Academic Blockchain Network

- requirements
  - full EVM-compatibility
  - low transaction cost
- zk-proof based are out (zk-rollups, Validium)
- neither state channels nor Plasma have full EVM-compatibility

Approach for Academic Blockchain Network

- requirements
  - full EVM-compatibility
  - low transaction cost
- zk-proof based are out (zk-rollups, Validium)
- neither state channels nor Plasma have full EVM-compatibility
- Optimistic rollups complicated and have long transaction finality

Approach for Academic Blockchain Network

- requirements
  - full EVM-compatibility
  - low transaction cost
- zk-proof based are out (zk-rollups, Validium)
- neither state channels nor Plasma have full EVM-compatibility
- Optimistic rollups complicated and have long transaction finality
- winner: **sidechain**

Approach for Academic Blockchain Network

- requirements
  - full EVM-compatibility
  - low transaction cost
- zk-proof based are out (zk-rollups, Validium)
- neither state channels nor Plasma have full EVM-compatibility
- Optimistic rollups complicated and have long transaction finality
- winner: **sidechain**
- deployment is simple, bridge is the difficult part

Blockchain bridges

- essential to L2
- facilitate cross-chain transfer of funds

Blockchain bridges

- essential to L2
- facilitate cross-chain transfer of funds
- Methods
  - **Lock and mint**
  - **Burn and mint**
  - **Atomic swaps**

Blockchain bridges

- essential to L2
- facilitate cross-chain transfer of funds
- Methods
  - **Lock and mint**
  - **Burn and mint**
  - **Atomic swaps**
- Types of bridges
  - **Native bridges**
  - **Validator / oracle based bridges**
  - **Message-passing bridges**
  - **Liquidity networks**

Blockchain bridges

- essential to L2
- facilitate cross-chain transfer of funds
- Methods
  - **Lock and mint**
  - **Burn and mint**
  - **Atomic swaps**
- Types of bridges
  - **Native bridges**
  - **Validator / oracle based bridges**
  - **Message-passing bridges**
  - **Liquidity networks**
- security
  - **trusted**
  - **trustless**
  - smart contract risk
  - open issues

Our blockchain bridge

- essential to Academic network
- proof of concept
- transfer of tokens between two test networks

Our blockchain bridge

- essential to Academic network
- proof of concept
- transfer of tokens between two test networks
- Main parts
  - Token-defining smart contracts
  - Bridge smart contracts
  - Bridge server function (Moralis)
  - Event listeners

Conclusions

- This project is a research into Etherium Layer 2 solutions for Academic research network as a **sidechain** and blockchain bridge as the most crucial part.

Conclusions

- This project is a research into Etherium Layer 2 solutions for Academic research network as a **sidechain** and blockchain bridge as the most crucial part.
- We used public testnets, did not dive into deploying private net. This should not be difficult, the most difficult is **bridge**.

Conclusions

- This project is a research into Etherium Layer 2 solutions for Academic research network as a **sidechain** and blockchain bridge as the most crucial part.
- We used public testnets, did not dive into deploying private net. This should not be difficult, the most difficult is **bridge**.
- Future work includes support of other chains, production-grading prototype, implementing Academic research DAO smart contracts etc.