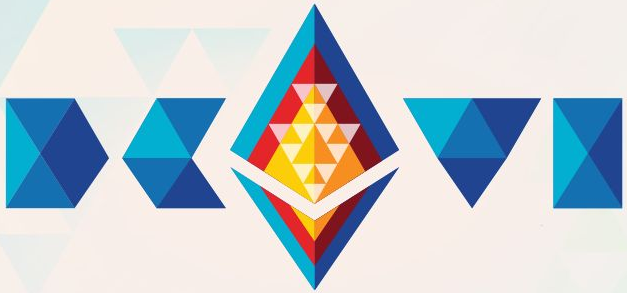


EthStorage

Scaling Ethereum Storage and Paving the Way to Future Web3

Qi Zhou
EthStorage.io

Qi Zhou: Self Introduction

- Founder of web3://, EthStorage, Web3 Buidl Group, QuarkChain

- Active Ethereum ecosystem contributor (ethresear.ch / magician), author/coauthor of EIPs-4804/4972/5018/5027/6150

- Working on Ethereum's technologies and received multiple grants from EF
  - DAS grant https://blog.ethereum.org/2022/12/07/esp-allocation-q3-22
  - Proof of Storage grant: Approved

@qc_qizhou

Outline

- Brief Introduction of Ethereum Layer 2
- EthStorage - A Storage Layer 2 on Ethereum
- Web3:// Access Protocol for Ethereum
- Conclusion

Ethereum Layer 2

- Very hot topic and a key role in Ethereum roadmap

- Definition
  - https://ethereum.org/en/layer-2
  - Inherit Ethereum security guarantee (e.g., smart contract)
  - Extend Ethereum
    - Scalability
    - New functionality such as privacy

- A lot of projects claim to be layer 2!
  - Sidechain? Validum? Rollup? Bnb Chain?
  - How to differentiate?

Ethereum Layer 2

- Ethereum security guarantee
  - Any additional trust assumption involved?
  - L2 nodes/validators <> L1 nodes/validators

- More specific
  - Safeness
    - 51% attack?
      - What if most of L2 nodes reverts a Tx?
    - Execution correctness?
      - What if most L2 nodes withdraw a balance of user from L2 to L1?
  - Liveness
    - Censorship resistant?
      - What if most L2 nodes refuse to include a Tx?
    - L2 world state availability?
      - What if most L2 nodes do not share their state?

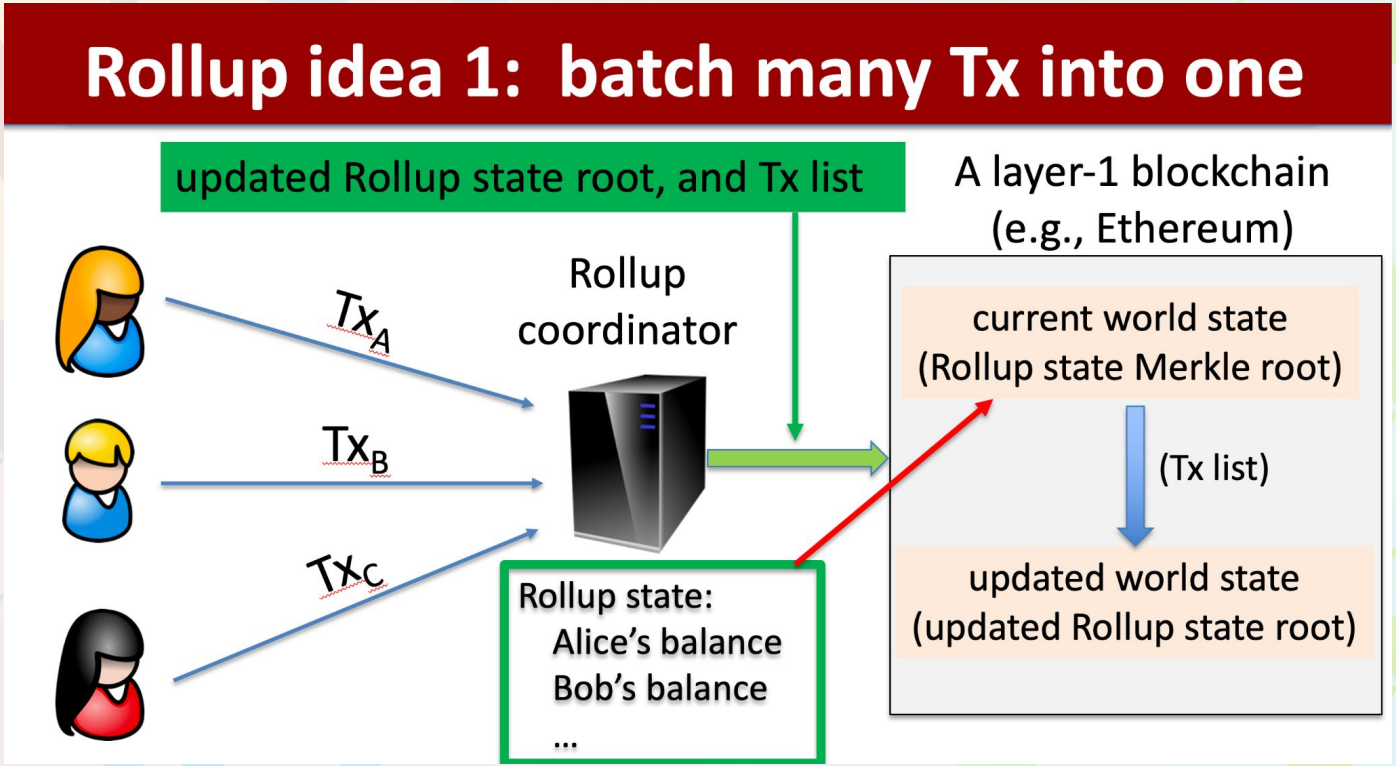
Comparison: Sidechain

- No L2
  - Polygon elects a list of L2 validators from L1
  - Update L2 world state to L1 periodically
  - Withdrawal of the L2 funds must be verified by L1 contract
- Safeness
  - 51% attack
    - Trust stakers
  - Execution correctness
    - Trust stakers
- Liveness
  - Censorship resistant
    - Trust stakers
  - L2 world state availability
    - Trust stakers

Rollup

- https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698
- https://research.paradigm.xyz/rollups
- https://cs251.stanford.edu/lectures/lecture17.pptx
- Main Idea:
  - Run transactions off-chain or L2
  - Periodically update batched execution results to L1
    - With actual **raw** L2 transactions
  - A batched L2 transaction forms a single L1
    - Correctness via proofs

Rollup


Rollup idea 1: batch many Tx into one
updated Rollup state root, and Tx list
A layer-1 blockchain
(e.g., Ethereum)
Rollup
coordinator
Tx_A
Tx_B
Tx_C
current world state
(Rollup state Merkle root)
(Tx list)
updated world state
(updated Rollup state root)
Rollup state:
Alice's balance
Bob's balance
...

Comparison: Optimistic Rollup

- Treated as L2
  - Arbitrum / Optimism
- Safeness
  - 51% attack
    - The L2 transactions settled on L1 after 7 days
  - Execution correctness
    - Fraud proof will be submitted on-chain
- Liveness
  - Censorship resistant
    - A user can forcibly execute a L2 Tx on L1
  - L2 world state availability
    - **At least one of the L2 node would like to share the L2 world state!**

Verifier's Dilemma

- Proposed by Professor Ed Felton from Arbitrum: (https://medium.com/offchainlabs/the-cheater-checking-problem-why-the-verifiers-dilemma-is-harder-than-you-think-9c7156505ca1)
  - If the system's incentives work as intended, nobody will cheat
  - If nobody cheats, then there's no point in running a verifier because you make no money from operating it
  - Since nobody runs a verifier, there's eventually an opportunity for a sequencer to cheat
  - The sequencer cheats, the system no longer functions as intended
- Essentially the liveness issue and the L2 world state availability issue!
  - **Liveness affects safety!**

EthStorage: Motivation

- Major goal: Reuse Ethereum security properties and extend Ethereum storage capabilities

- Key Idea: Build a **storage-specific** Rollup vs **EVM-specific** Rollup
  - Reduce Ethereum storage cost to 1/100x or 1/1000x (vs SSTORE)
  - Scale storage to PB (vs ~TB SSTORE)
  - Storage fee paid with ETH
  - Reuse Ethereum security properties

EthStorage v0: Multiple Rollups Approach

- Q: Why not run multiple Rollups with each Rollup having up to 4TB data!
  - E.g., running 100 Arbitrum-like Rollups with each having 4TB data
  - 100 * 4TB = 400TB storage on L2!

- Problem solved? No!
  - How to ensure there are sufficient **honest** nodes would like to share the L2 world state data, especially the **storage cost is non-trivial**? (Verifier's Dilemma)

- Inspiration: Could we ensure **multiple physical replicas** of the L2 world state?
  - Proof of Storage from decentralized storage

EhStorage v1

- Single L1 storage contract runs multiple storage Rollups
  - Each storage Rollup contain up to 4TB (adjustable) data

- Simplified L2 transactional model and world state
  - Tx model: CRUD instead of EVM
  - World state: KV store instead of MPT

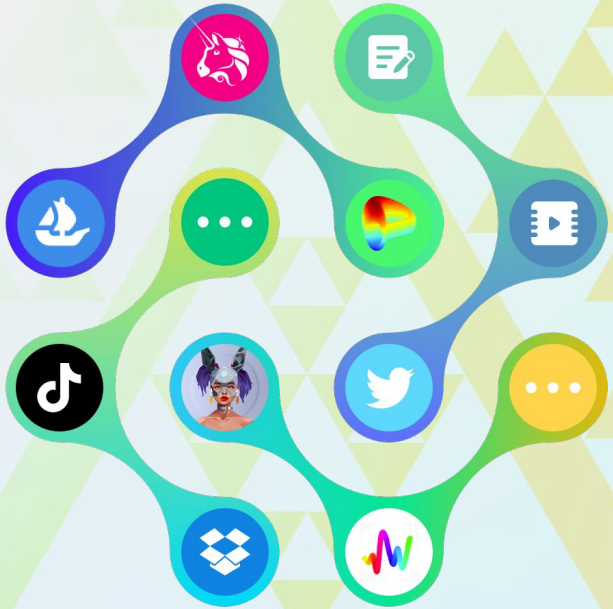
- Key contribution: **Proof of Storage on L2 Dynamic Datasets with an Ethereum L1 contract**
  - Supported by ESP grant
  - https://ethresear.ch/t/ethstorage-scaling-ethereum-storage-via-l2-and-da/14223

	EthStorage L2	EVM-Specific Rollups
Type of Off-Chain Tx	CRUD operation with a large-sized value	EVM Tx
L2 World State	A list of BLOBs written by off-chain Txs	MPT of the off-chain EVM
L1 Rollup Batch Data	List of CRUD operations with large-sized values (each value is a DA BLOG)	List of off-chain EVM Txs as DA BLOBs
L1 Rollup State Root	Hash of each value (BLOB)	Root Hash of the MPT
Require a sequencer?	No, a user can directly submit Tx to L1	Yes, a user must submit a Tx to a sequencer
How to pay the fee?	To the L1 storage contract	To the sequencer
How would L2 node collect the fee?	Storage providers collect the fee when generating a proof of storage and submitting it to L1.	The sequencer collects the fee after the L2 Txs are settled on L1
L2 World State Availability	At least one L2 node is honest	At least one L2 node is honest
Number of Physical Replicas of L2 World State	**m physical replicas**	No such enforcement

	Filecoin	Arweave	Ethereum SSTORE/SLOAD	EthStorage
Store Object	Static Files	Static Files	KV Store	
Semantics	CRD	CR	CRUD	
On-Chain Programmable	∅	∅	✓	✓
Proof of Storage	Proof of Space-Time with Challenge	Succinct Proof of Random Access	Fully Replicated	Dynamic Sharding with Proof of Random Access
Replication Guarantee	High	Median	Very High	High
Storage Cost	Very Low	Low	Very High	Low
Capacity	~ EB	~ 100 TB (Currnet)	~ 1 TB	~ PB
Access Protocol	ipfs://	N/A	web3://	
Wallet	Filecoin Wallet	ArWallet	ETH-Compatible	

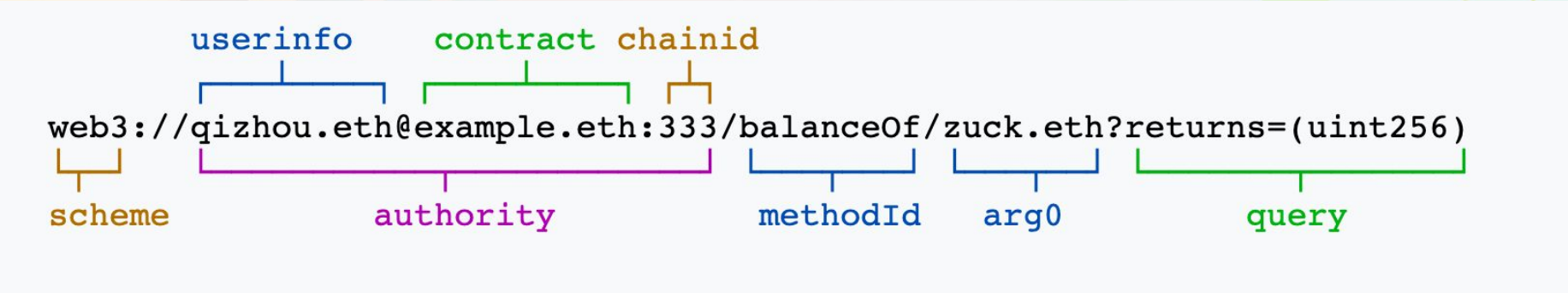
Applications

- Long-term storage solution for other Rollups
  - OR, ZKP
- Decentralized frontend with dynamic websites
  - FILECOIN/AR can only do static ones
- Native storage for NFTs



web3:// Access Protocol

- ERC-4804: Web3 URL Standard - an IANA Registered Scheme
- Render Web Objects Hosted by Smart Contracts (or hash linked to EthStorage)



Early Experiments and Community Ideas

- Vitalik's blog uploaded to Arbitrum Nova with 0.13ETH
  - https://www.reddit.com/r/ethereum/comments/107ok8e/upload_40mb_vitaliks_blog_to_a_smart_contract_on/

- Decentralized Reddit pixel war
  - https://twitter.com/qc_qizhou/status/1615233757207990272

- git3 (decentralized git), w3box (decentralized dropbox), w3mail (decentralized email), ...

Summary of Technologies

Proof of Publication via Data Availability

Increase Data Upload Speed Using KZG Commitment and Reed-Solomon Code

DA Research Grant from EF

EthStorage: External Data Retention L2 Network

Proof of Storage on Large Dynamic Datasets

~ PB Capacity with CRUD

Proof of Storage Grant from EF

web3:// Access Protocol

Decentralized Access to Dynamic Web Objects Hosted by Smart Contracts

Future Web3 Vision

Rich Storage Semantics

Create/Read/Update/Delete BLOBs on Large Dynamic Datasets

Programmable by Smart Contracts

Simple User Onboarding

Just Use ETH-Compatible Wallet such as Metamask

Inherit Ethereum Security

End-to-End Fully Decentralized

No Centralized Identity From Frontend to Blockchain to Storage

Timeline of EthStorage

2022
PoC Testnet

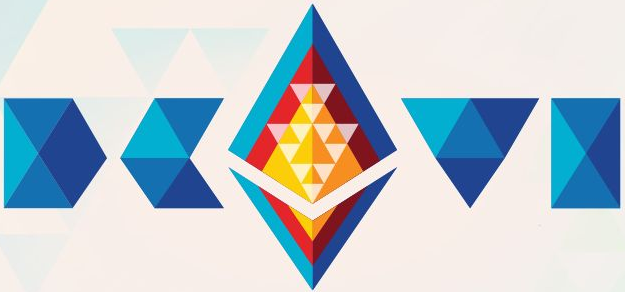
- ERC-4804: Web3 URL Standard
- Technical White Paper
- web3:// Gateway
- BFT + PoS Sidechain Consensus
- Devcon Talk

2023
Full Functional Testnet

- Storage Contacts
- Data Retention Network
- Permissionless Staking and Validator Change
- BLOB Libraries
- 2-3 Community Projects
- Verifiable Gateway

2024
Pre-Launch*

- Full Integration with Danksharding
- EthStorage CL + EL Clients
- web3:// Browser Native Integration



Thank you!

Website : ethstorage.io
Twitter: twitter.com/EthStorage
Medium: ethstorage.medium.com/
Telegram: t.me/ethstorage
Discord: discord.gg/mZqqUZxjed