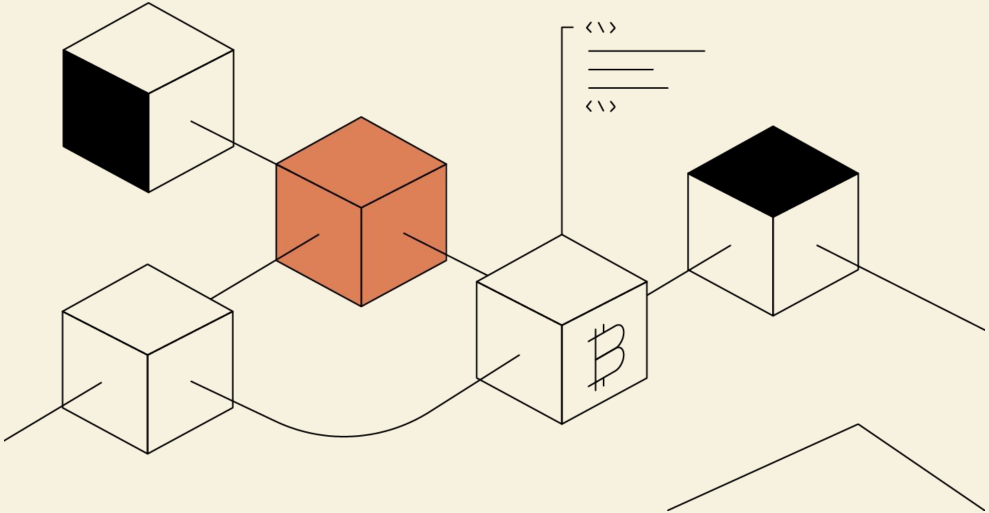
Scaling Ethereum with Zero-Knowledge Proofs

Tal Derei

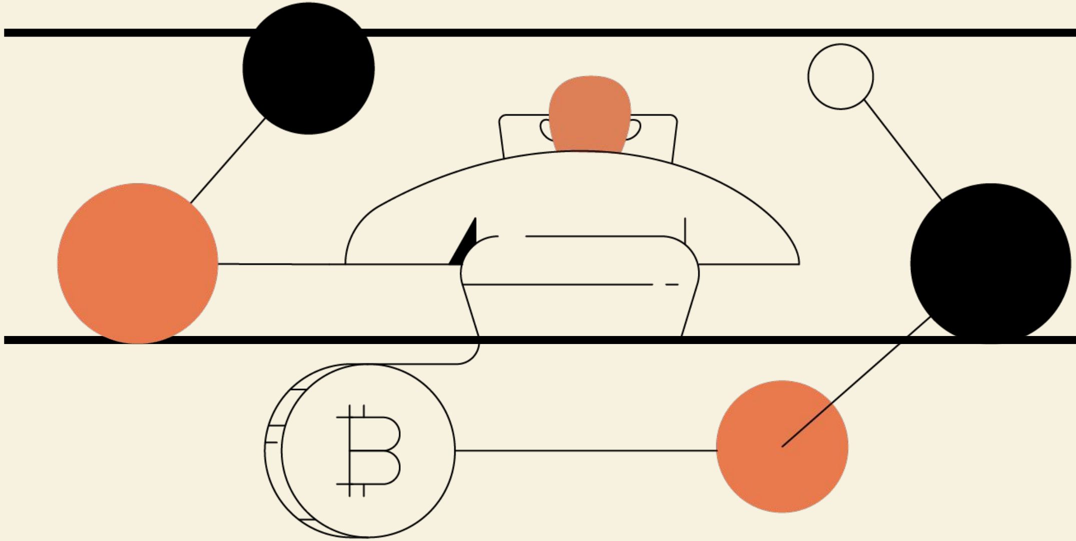
Agenda



1. What is a Blockchain?
2. Ethereum
3. Zero-Knowledge Scaling

Terms

- **L1** = Layer-1 (Ethereum Mainchain)
- **L2** = Layer-2 (ZK-Rollups)
- **ZK** = Zero-Knowledge
- **zk-SNARKs** = ZK Proofs
- **EVM** = Ethereum Virtual Machine
- **zkEVM** = Zero-Knowledge Ethereum Virtual Machine



Blockchain

What is a Blockchain?

Blockchain is a “*distributed*, *decentralized*, and *immutable* public ledger that exists across a peer-to-peer network.”

Blockchains store <u>transaction records</u> in a decentralized way!

Blockchains vs Databases?

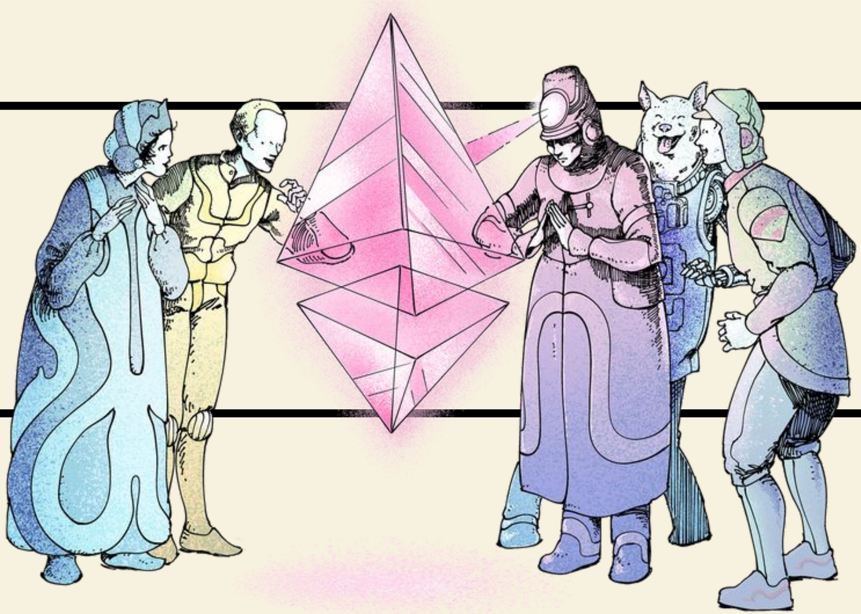
Q. Do blockchains REPLACE databases?

NO! You need BOTH!

It's expensive to store data on a blockchain…As per the price of Ethereum (Feb. 2020), storing 1MB of data will cost you up approx. **$17,100** USD…Probably **10x+** more expensive in Jan. 2022.

As a result…

- Blockchains mainly store **transaction history**
- Databases store **account addresses and balances**



Ethereum

- **General Background**
- **Smart Contracts**
- **Consensus Mechanism**

General Background

Ethereum was launched in 2015 by **Vitalik Butertin**

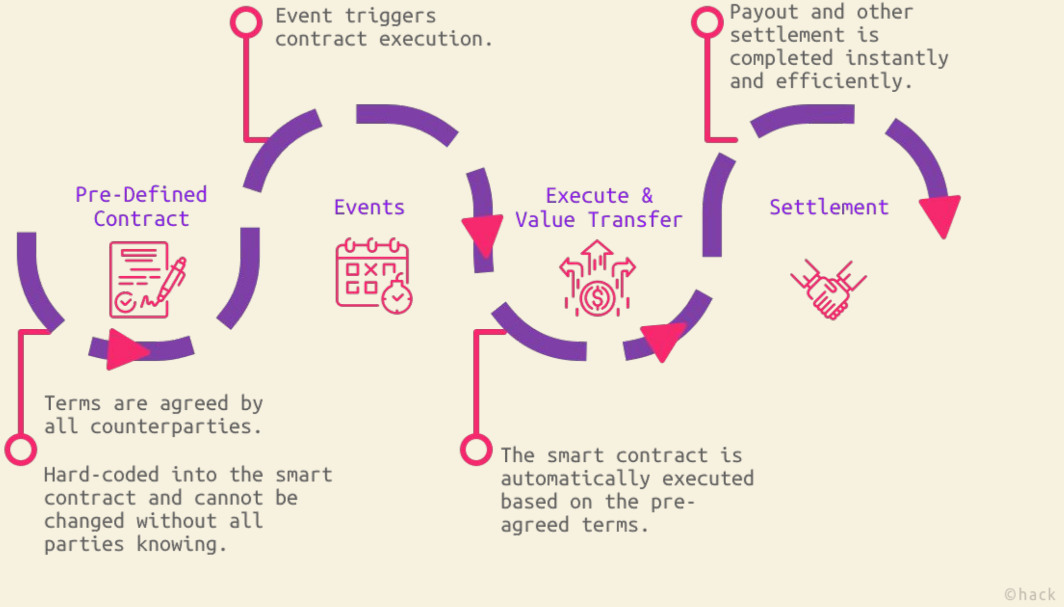
→ **Decentralized** blockchain platform

→ **Smart Contracts** are digital contracts on Ethereum

Allow participants to transact with each other
without a central authority

These transactions are *immutable*, *verifiable*,
and securely *distributed* across the network

Smart Contracts


Event triggers contract execution.
Payout and other settlement is completed instantly and efficiently.
Pre-Defined Contract
Events
Execute & Value Transfer
Settlement
Terms are agreed by all counterparties.
Hard-coded into the smart contract and cannot be changed without all parties knowing.
The smart contract is automatically executed based on the pre-agreed terms.
©hack

__Solidity Smart Contract__

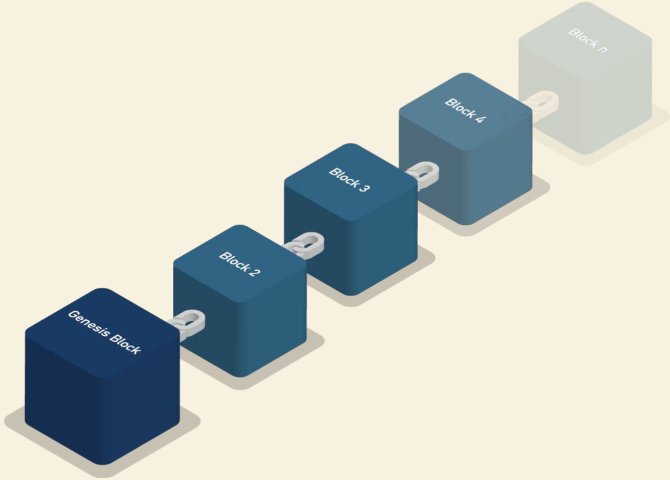
Smart Contracts

→ Tokens (ERC-20)
→ NFTs (ERC-721)
→ DeFi
→ DAPPs
→ DAOs
→ Asset transfers
→ Transactions
→ DEXs

SOLIDITY

Consensus Mechanism

Consensus: how the ***state*** of the Ethereum network is maintained in a blockchain. This makes the blockchain secure! Currently running **Proof-of-Work (PoW)** scheme



State Transitions!

Consensus Mechanism

Q. What are these **blocks** and how do they get **added** to the blockchain?

- 1. There's a collection of transactions in the ***memepool*** (pool where valid transactions are waiting to be confirmed)

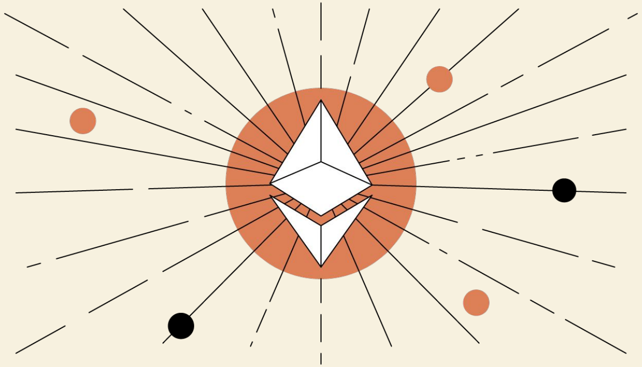
- 2. Batch of transactions are packaged into a block (miners choose which transactions to execute, based on ***gasprice***)

- 3. Miner try to **mine** that block by solving a hard cryptographic puzzle (Proof of Work) and collect the transaction fees

Consensus Mechanism

- The blockchain state is updated as new blocks are added to the blockchain (i.e. **mined and validated**) by network participants (**miners**) at regular intervals

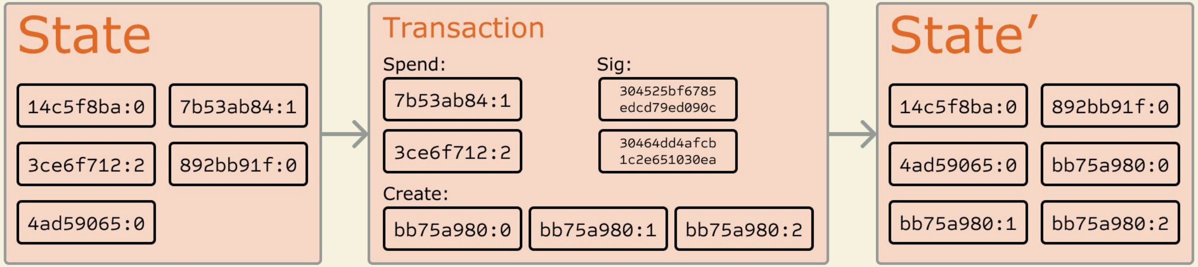
- Block creation mints new ETH tokens
  - As an incentive for mining blocks (validating transactions), miners are rewarded with ETH



CS Explanation

- **Ethereum** = Transaction-Based State Machine
  - EVM traverses blockchain starting from genesis block

- **Ethereum Virtual Machine (EVM)** = Stack Machine
  - Processes transactions



State

14c5f8ba:0 7b53ab84:1
3ce6f712:2 892bb91f:0
4ad59065:0

Transaction

Spend:
7b53ab84:1
3ce6f712:2

Sig:
304525bf6785 edcd79ed090c
30464dd4afcb 1c2e651030ea

Create:
bb75a980:0 bb75a980:1 bb75a980:2

State’

14c5f8ba:0 892bb91f:0
4ad59065:0 bb75a980:0
bb75a980:1 bb75a980:2

What’s the Problem?

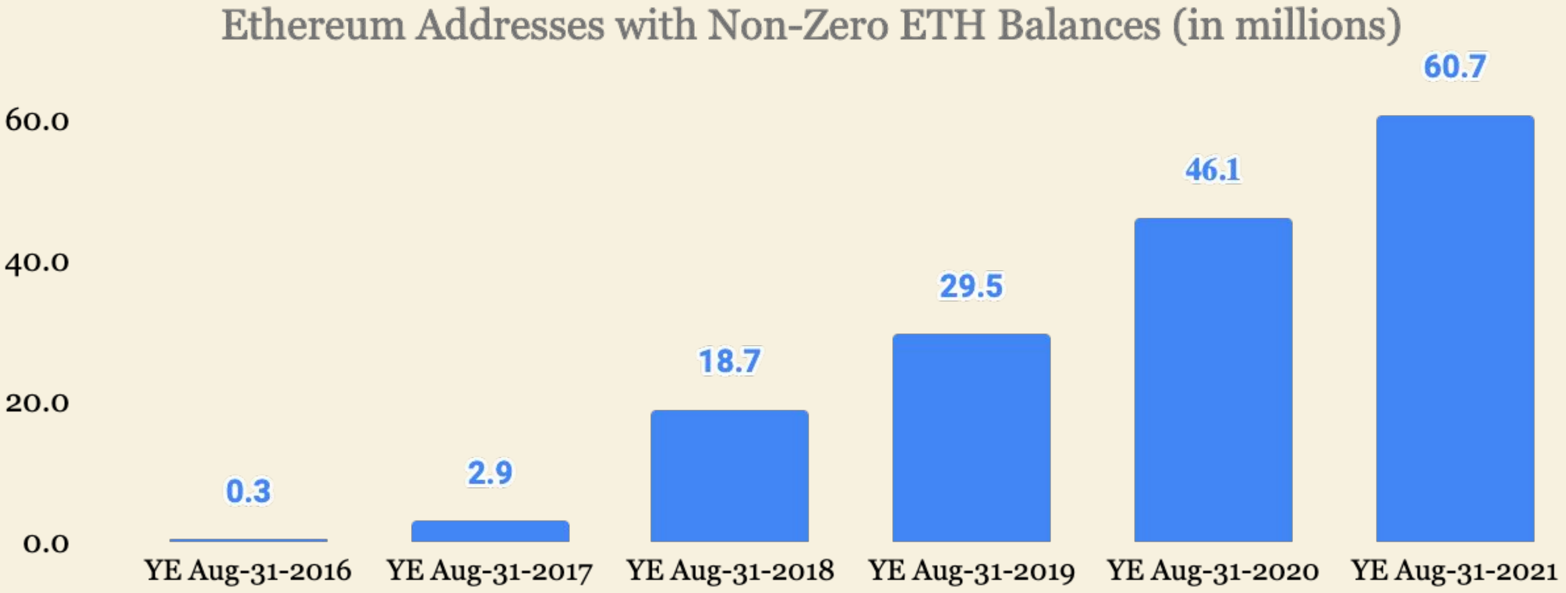
Sacrificing scalability for decentralization!

Centralized blockchains are usually faster? Lower Latency?

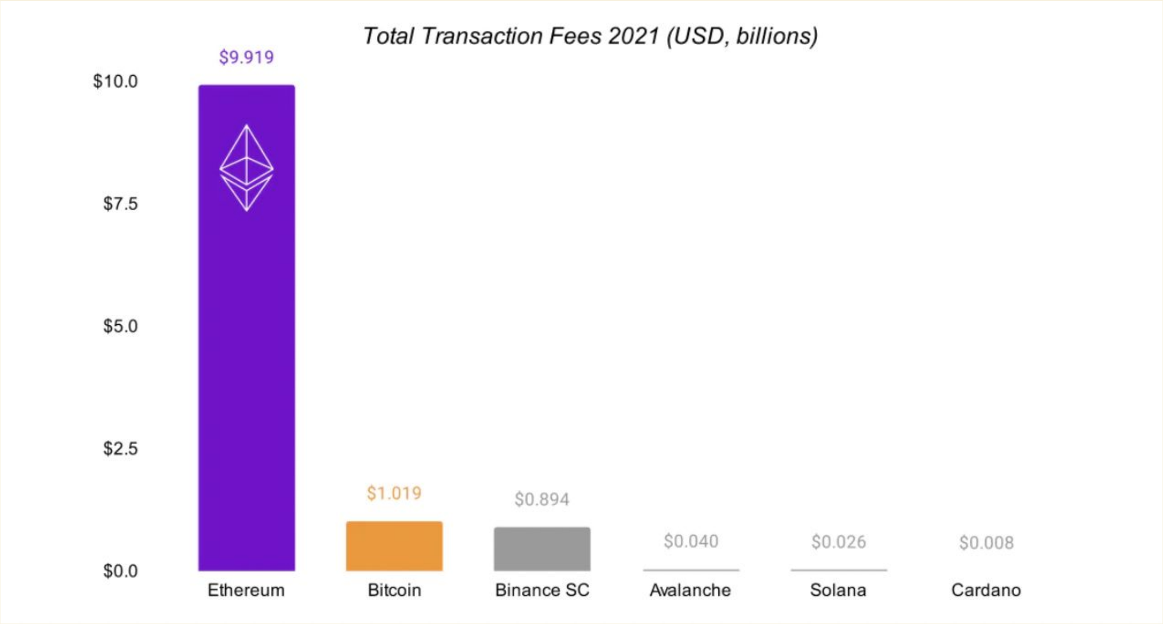
Low Scalability

→ ~15 transactions per second (TPS) vs network demand of 1.355 million TPS/day
→ Network congestion
→ High *gas* fees

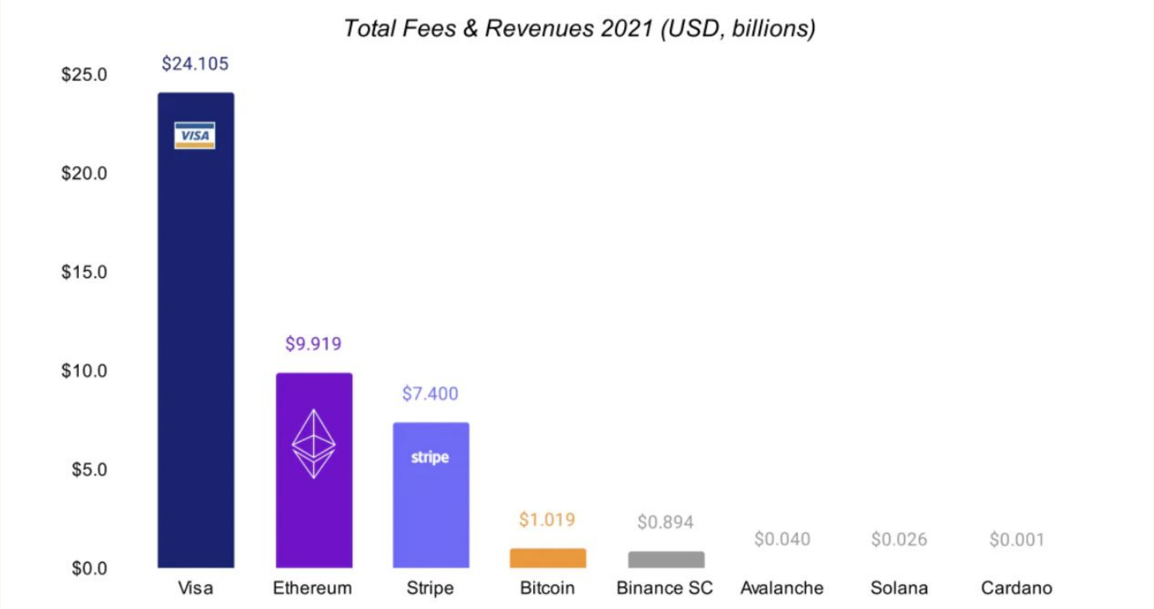
Wallet Addresses



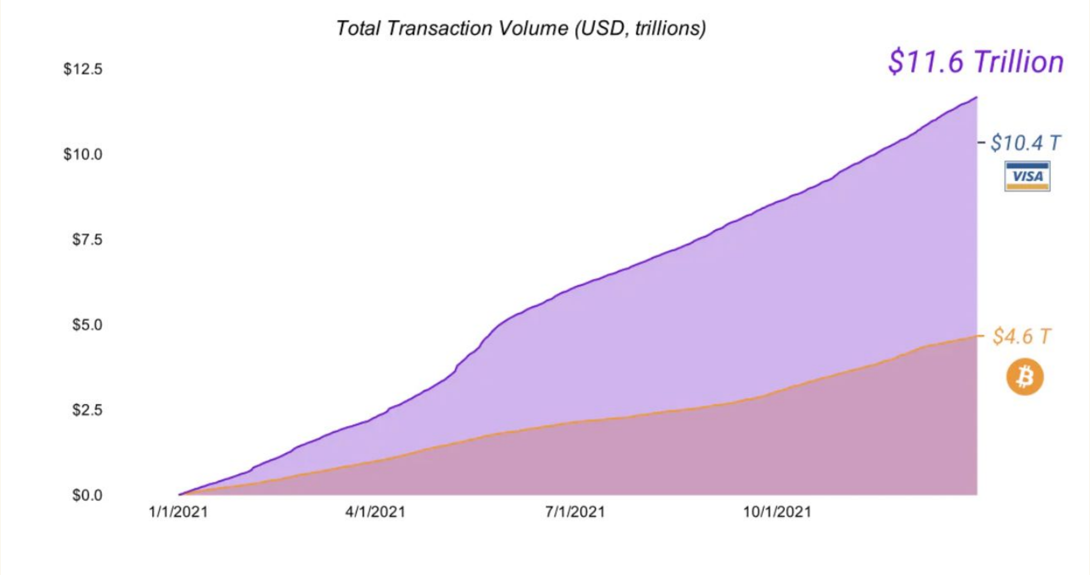
Transaction Fees



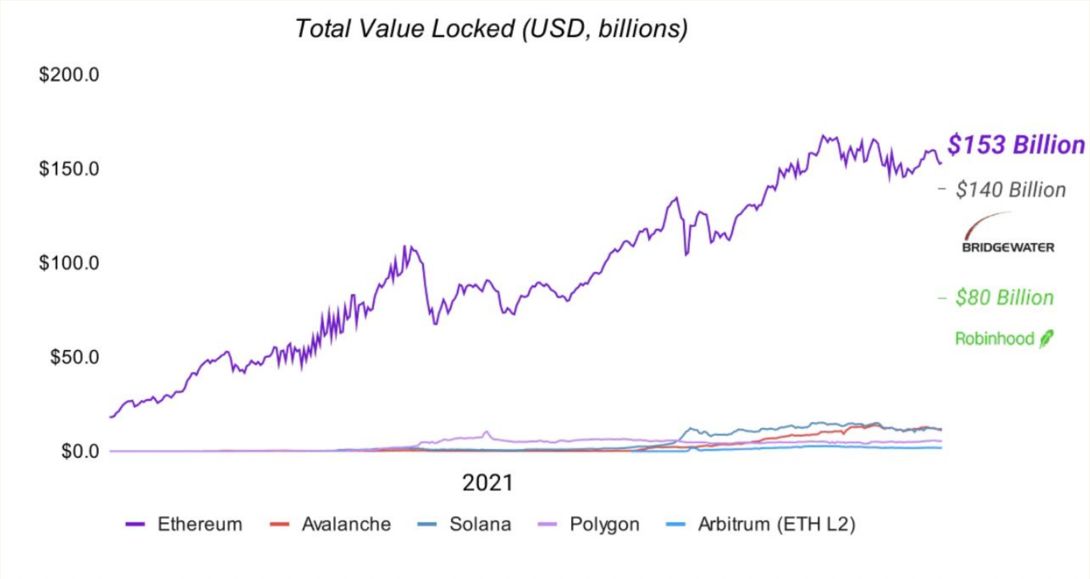
Transaction Revenues



Total Transaction Volume



Total Value Locked (TVL)

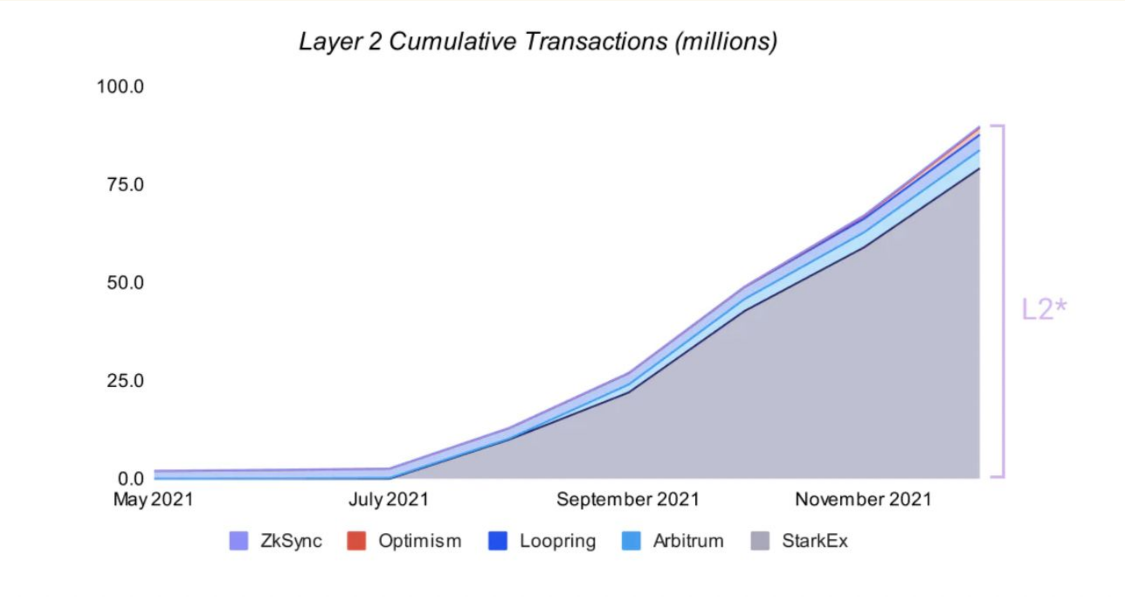


So How Do You Scale Ethereum?

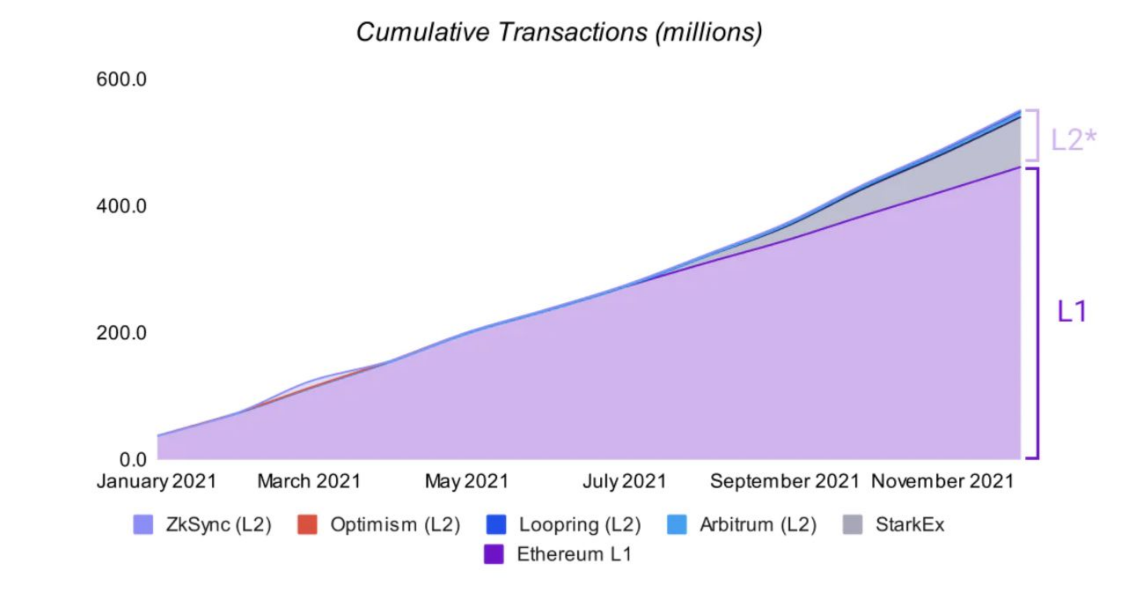
Two Ways...

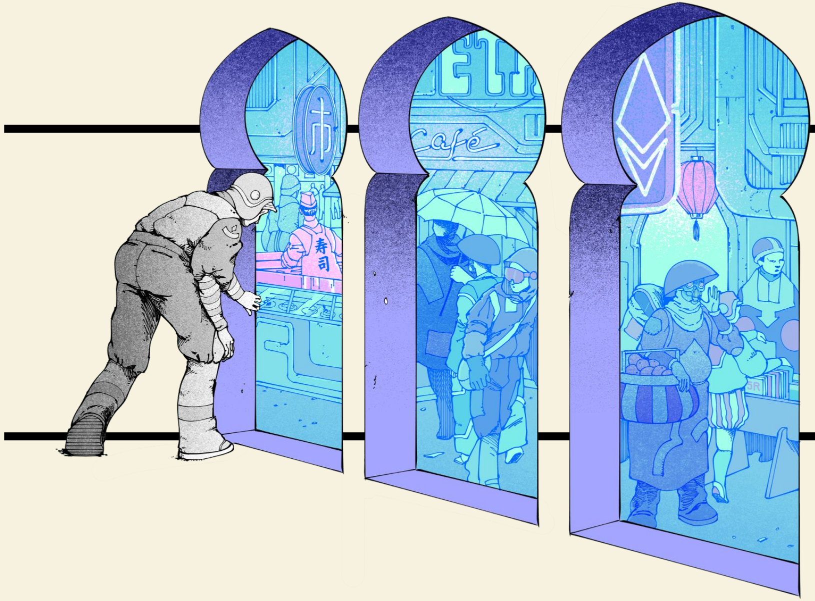
- **Layer-1 (L1)**
  - ETH2 (Proof-of-Stake (PoS) + Sharding)
- **Layer-2 (L2)**
  - Separate blockchains on top of an L1 blockchain
  - E.g. *ZK Rollups*

Layer 2 (L2) Cumulative Transactions



Cumulative Transactions (L1 + L2)





Zero Knowledge Scaling

Zero Knowledge

Zero Knowledge: “It’s a way for a <u>prover</u> to convince <u>verifier</u> that something is true without revealing anything about why it's true.”

Rooted in advanced mathematics and cryptography!

Example

Where’s Waldo?

What's the Point?

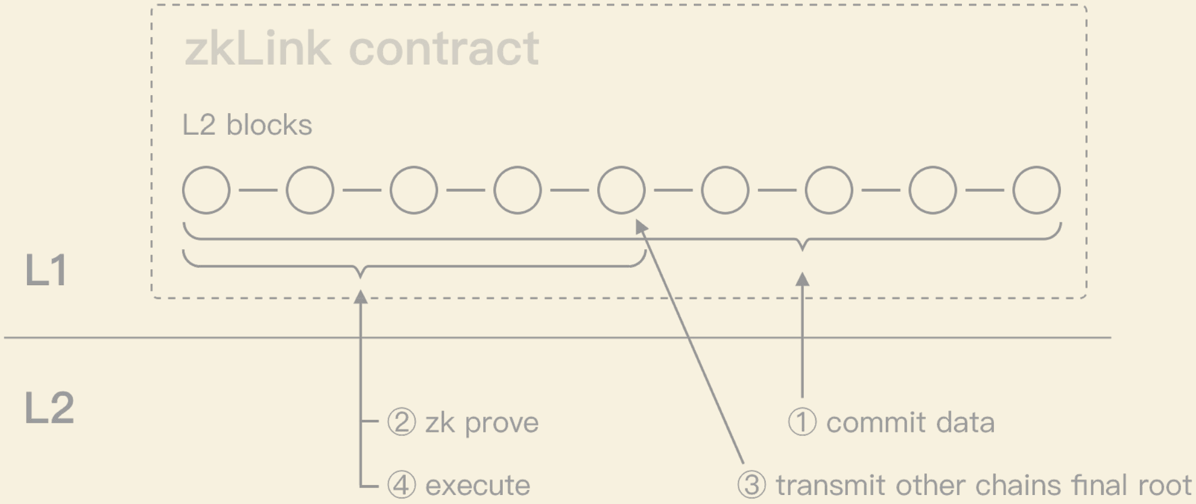
What if we can move the execution of transactions onto layer-2 (**separate blockchains**) and prove to the Ethereum that they are correct?

Can we provide a **PROOF** of some sorts to Ethereum?

YES! … Zero knowledge provides **privacy/security** + **scalability**!

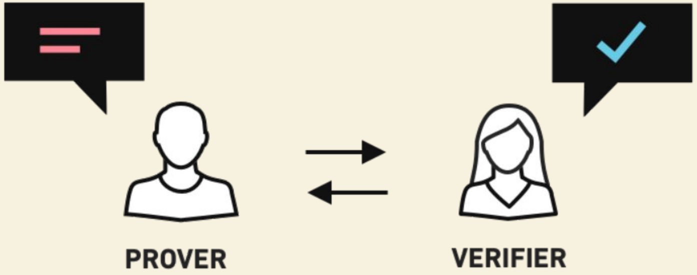
zk-Rollups

- **zk-Rollups** = Layer 2 scaling solutions that move the execution of transactions **off-chain**. Then a "**validity proof**" is posted back onto Ethereum verifying these transactions were executed correctly.



zk-SNARKs

- **SNARKs** = cryptographic **proof**
    - Enables a prover to prove a mathematical statement to a verifier with a *short proof* and *succinct verification* using zero knowledge techniques



zk-Rollups

BUT…

Generating proofs is resource and computationally <u>expensive</u>!

Control Flow:

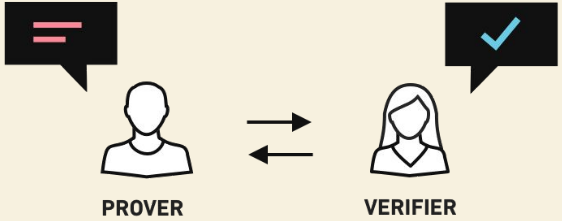
Computation → Algebraic Circuit → R1CS → QAP → zk-SNARK

Problem?

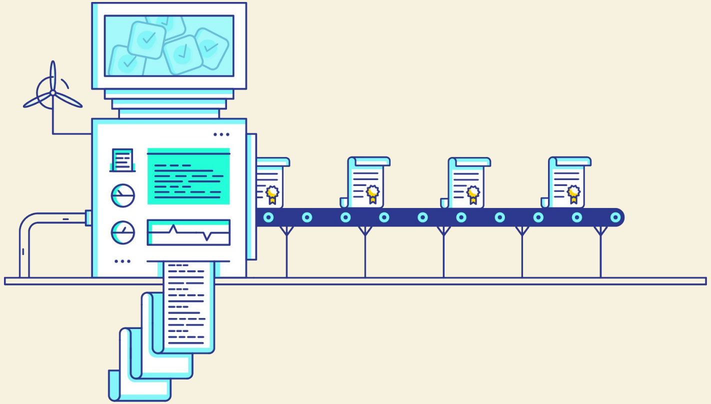
ZK-Rollups:

- Generate zero knowledge-proofs on L2
- Pass back proof on L1 for verification
- ZK proofs (and the EVM) need to conform to zk-circuit proof specifications

…And the problem is the EVM wasn't designed with zero-knowledge in mind!



What is zkEVM?



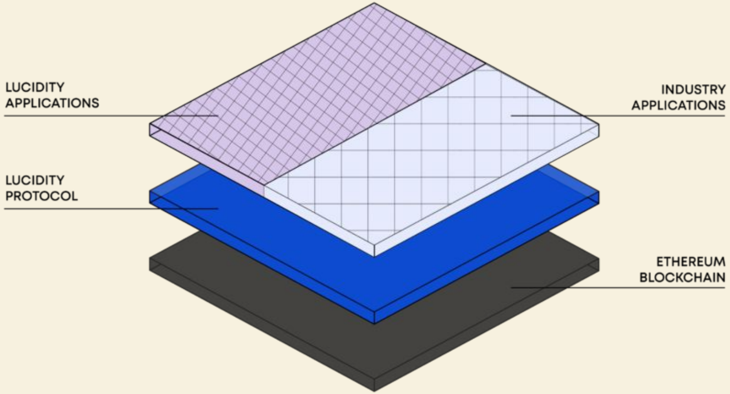
zkEVM is the ***key*** to scaling Ethereum blockchain in the future!

Vitalek Buterin: “In the medium to long term, zk-rollups will win out in all use cases over Optimistic Rollups as ZK-SNARK technology improves”

What is zkEVM?

L2 ZK-Rollup for Payments and **Generic Smart Contracts**!

L2 + EVM!



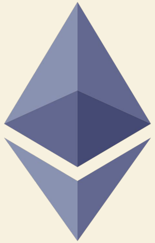
What is zkEVM?

zkEVM is a “**A turing-complete virtual machine that executes smart contracts on a zk-Rollup (Layer-2) network, is EVM-compatible and zero-knowledge (SNARK) friendly**””

- Key to building ZK-Rollups compatible with the EVM
  - Easily port DAPs and DAOs written in solidity on L2

- zkEVM keeps EVM semantics (e.g. gas fee structure and security properties of the main-chain)

- Based on traditional CPU architectures



References

https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

https://stark.mirror.xyz/q3OnsK7mvfGtTQ72nfoxLyEV5lfYOqUfJIoKBx7BG1I

https://medium.com/degate/an-article-to-understand-zkevm-the-key-to-ethereum-scaling-ff0d83c417cc

https://medium.com/fcats-blockchain-incubator/how-zk-rollups-work-8ac4d7155b0e

Thank you!

SCALABLE SYSTEMS
& SOFTWARE
RESEARCH GROUP

https://sss.cse.lehigh.edu/