ETHTerakoya × Blockchain EXE

# What's Rollup?

2021/02/04

Shuhei Hiya@Cryptoeconomics Lab

Cryptoeconomics Lab

# Agenda

What's Rollup?

What's Optimistic Rollup？

What's ZK-Rollup？

ORU vs zkRU

# Products of ORU & zkRU

| Name | Highlights |
| --- | --- |
| Optimism (synthetix) | ORU that can write smart contracts with Solidity |
| FuelCore | UTXO-based ORU |
| Arbitrum | Unique VM called AVM. Dichotomous dispute resolution model |
| zkSync (curve, balancer) | zkRollup that aims for a smart contract platform |
| zkSwap | AMM using zkSync technology |
| Loopring | Currently has the highest L2 DEX trading volume ($10M volume) |
| StarkEx, StartNet | Validium, Rollup platform-type |

# Why learn about Rollup now?

Rollup is transitioning from research to practical use and is heading towards platforms. In other words, we are now reaching the stage where it is possible to actually develop applications on Rollup.

In this presentation, we will be introducing the basics of why Rollup improves the throughput of Ethereum.

As much as possible, we will explain the essential parts of the protocol rather than focus on specific products.

# Agenda

What's Rollup?

What's Optimistic Rollup？

What's ZK-Rollup？

ORU vs zkRU

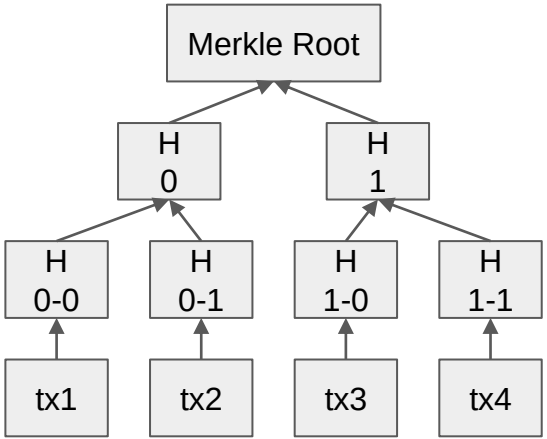
# Why Scaling?

To increase Ethereum capacity

Ethereum is currently at
approx. 15 tps

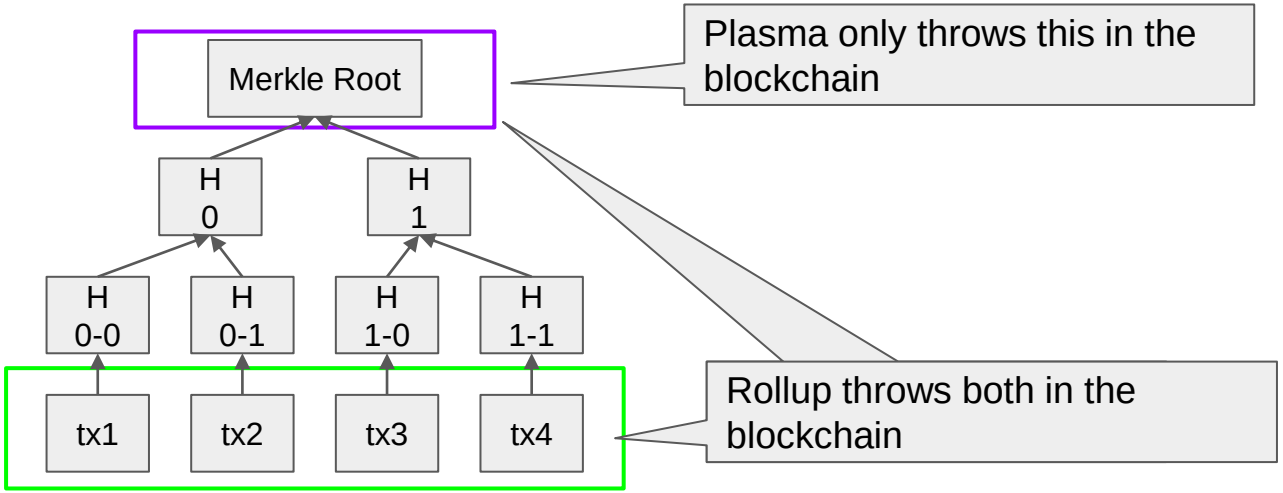
# Increasing capacity with Ethereum Layer 2

Reduces the time of sending transactions to the blockchain



# What's Rollup?

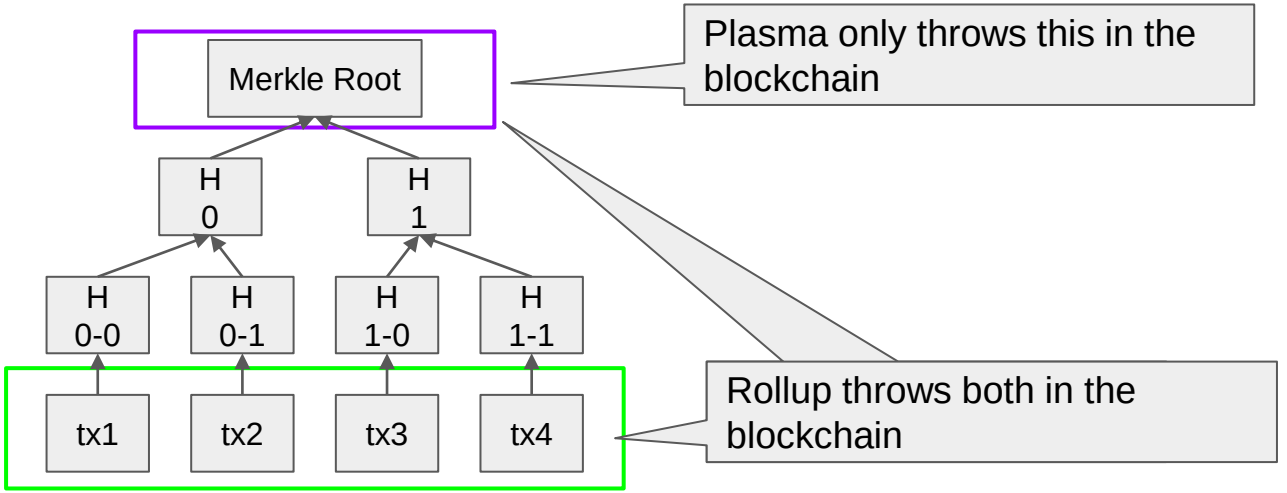
A technology that improves throughput while maintaining **data availability**
Throws transaction data in the blockchain as calldata but only saves the Merkle Root as state



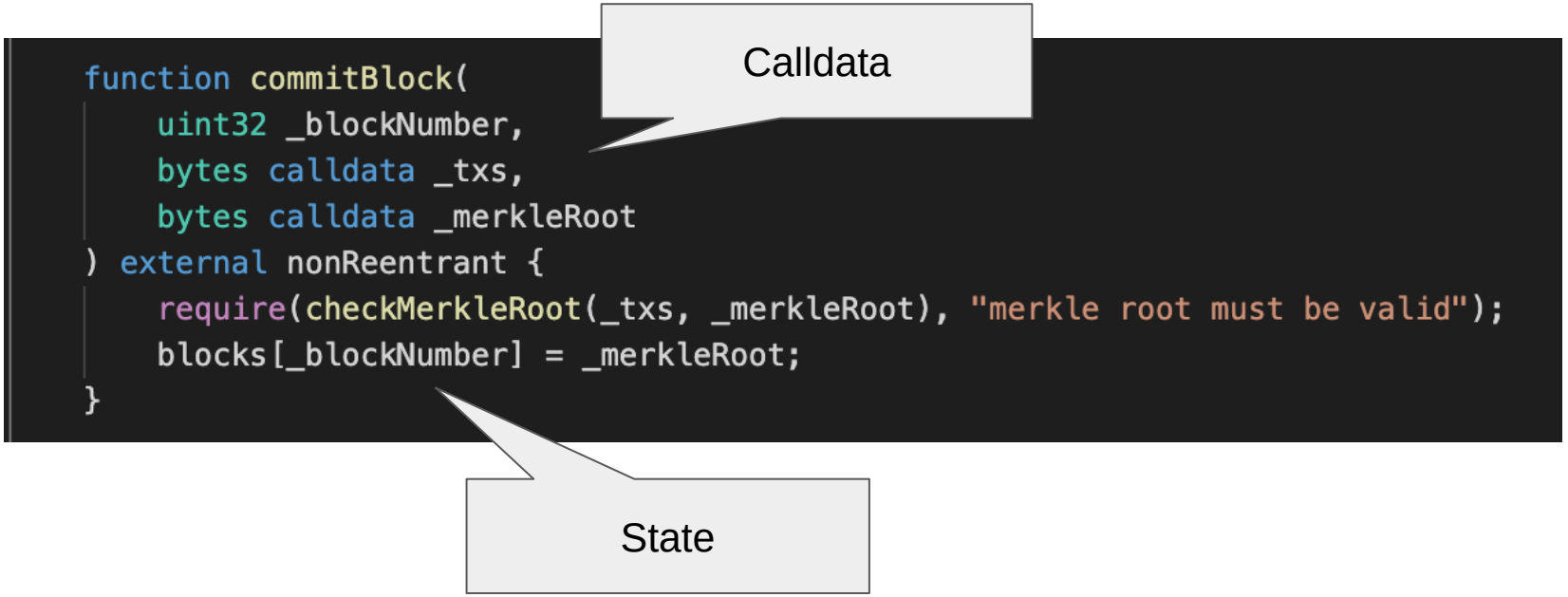
# What's Rollup?

No. of transactions processable per second

A technology that improves throughput while maintaining **data availability**
Throws transaction data in the blockchain as calldata but only saves the Merkle Root as state



# Difference between transaction calldata and state



# Difference between transaction calldata and state

- Ethereum currently has a state size of ~45GB and a chain size of 300GB.
- Unlike transactions, states cannot be truncated in full nodes.
- Validating transactions means a lot of random accesses to the state, meaning the state must be kept in the RAM.

To sum things up, **states are costly, transaction calldata are cheap.**

https://etherscan.io/chartsync/chaindefault

# What happens when there is no data availability?

Doesn't know whether tx is correct or not

?

h = Hash(tx)

tx content is currently unknown

i.e. Plasma's Exit Game

Knowing the original tx requires a **special mechanism,** and only a few of these can be realized. **Rollup is a general-purpose solution for this.**

# What’s Rollup

A technology that improves throughput while maintaining data availability

**Optimistic Rollup**

Validates transactions on the blockchain only if a problem occurs

**ZK-Rollup**

Validates transactions on the blockchain via (zk-)SNARKS every time

# A comparison from a gas-cost reduction perspective

In Ethereum, state, computation, and calldata rise proportionately to the number of transactions.
In Rollup and Plasma, gas consumption by states and computations is constant.

| | State | Computation | CallData |
|---|---|---|---|
| Ethereum | O(n) | O(n) | O(n) |
| zkRollup | C | C or log(n) | O(n) |
| Optimistic Rollup | C | C | O(n) |
| Plasma/Sidechain | C | C | C |

n is the no. of transactions, c is constant

# Gas cost comparison per transaction (approximate)

Around 10 times more effective for money transfers and great for complex transactions like DEX

| | Money Transfer | DEX swap |
|---|---|---|
| L1 | 22,000 gas | Approx. 80,000 gas |
| ORU | 2,576 gas | 3,600 gas |
| zkRU | 1,153 (833+320) gas | 4,406 (3750+656) gas |

zkRU is expected to store 360tx per block, with verification costs being 300,000 gas.

# Throughput Calculation

**The maximum no. of transactions per block** can be calculated by dividing the block gas limit by the previous slide's "gas per tx." However, in zkRU, circuit size and proof generation time are bottlenecks.
Assuming the maximum gas limit is 10M, **the maximum no. of transactions per block** will be as shown in the table below. Throughput is determined by how often this block is registered in L1.

| | Money Transfer | DEX swap |
|---|---|---|
| L1 | 30 tx per block | 8.3 tx per block |
| ORU | 258 tx per block | 185 tx per block |
| zkRU | 320 tx per block | 80 tx per block |

Note that zkRU's capacity still has room for improvement.

Suppose it takes 600 seconds to generate proof for a 320txx block. Ten machines will be needed to get a block time of 70 seconds (meaning tps=5.3).

# Why Rollup

Not sacrificing data availability has many benefits.

# Agenda

What’s Rollup?

What’s Optimistic Rollup？

What’s ZK-Rollup？

ORU vs zkRU

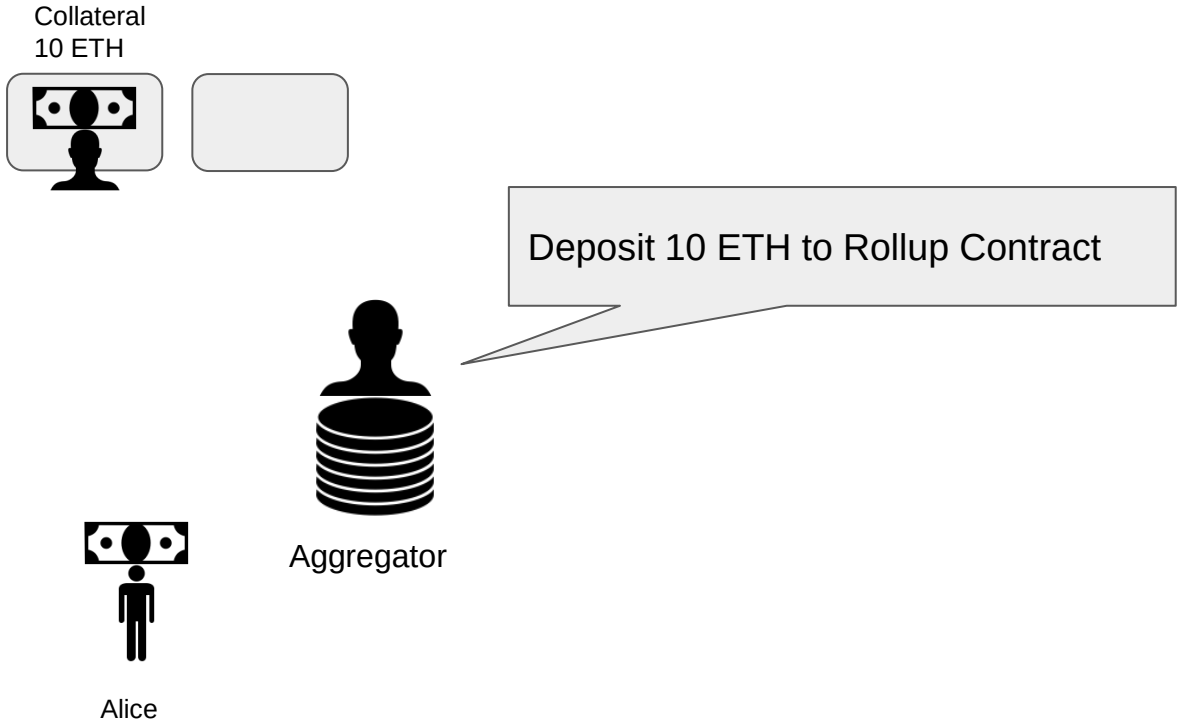
# What is Optimistic Rollup

Validates transactions on the blockchain only if a problem occurs

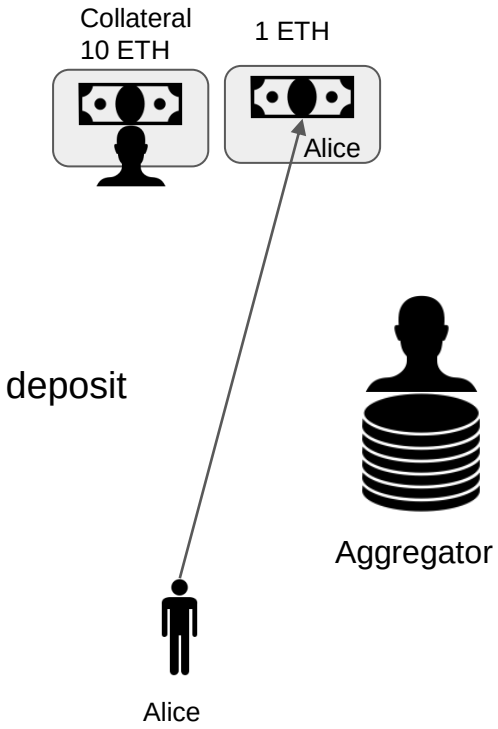
- Aggregator is permissionless
  - Anyone can validate transactions
- Easy EVM-compatibility
- Withdrawals to L1 take around a week
  - There is also a way to immediately exchange tokens between L1 and L2.

# How Optimistic Rollup works

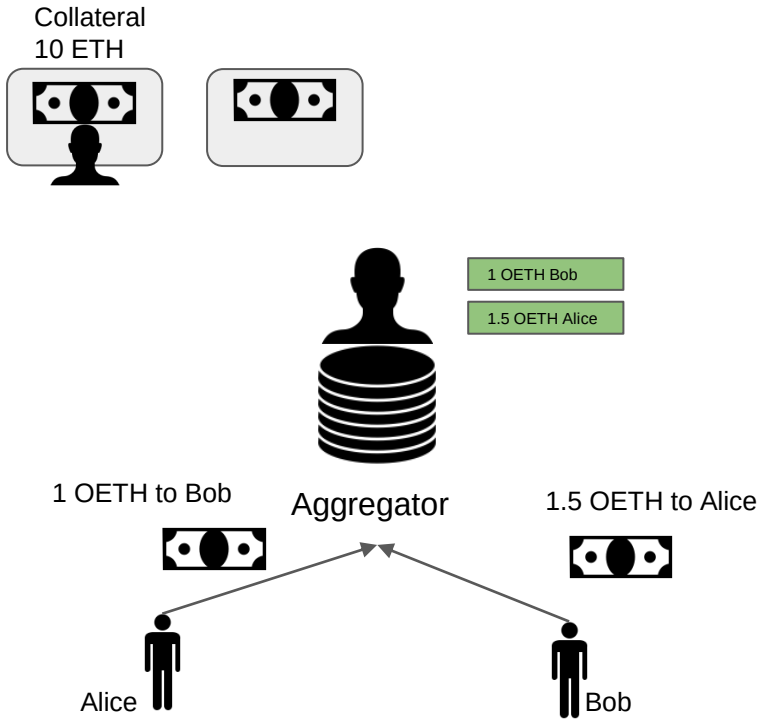
# How Optimistic Rollup works



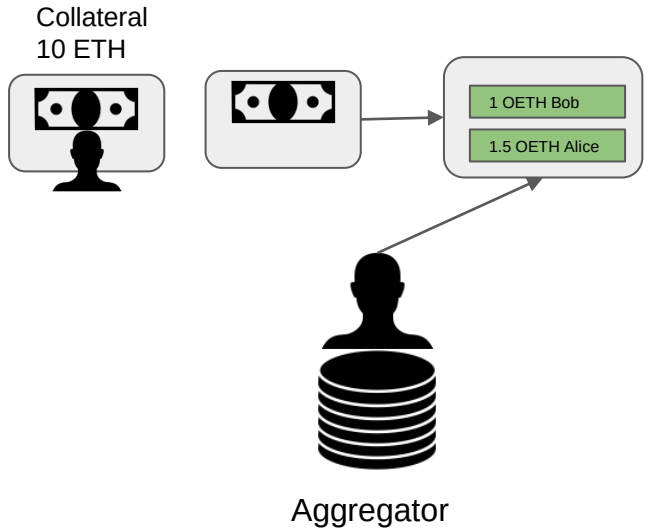
# Deposit



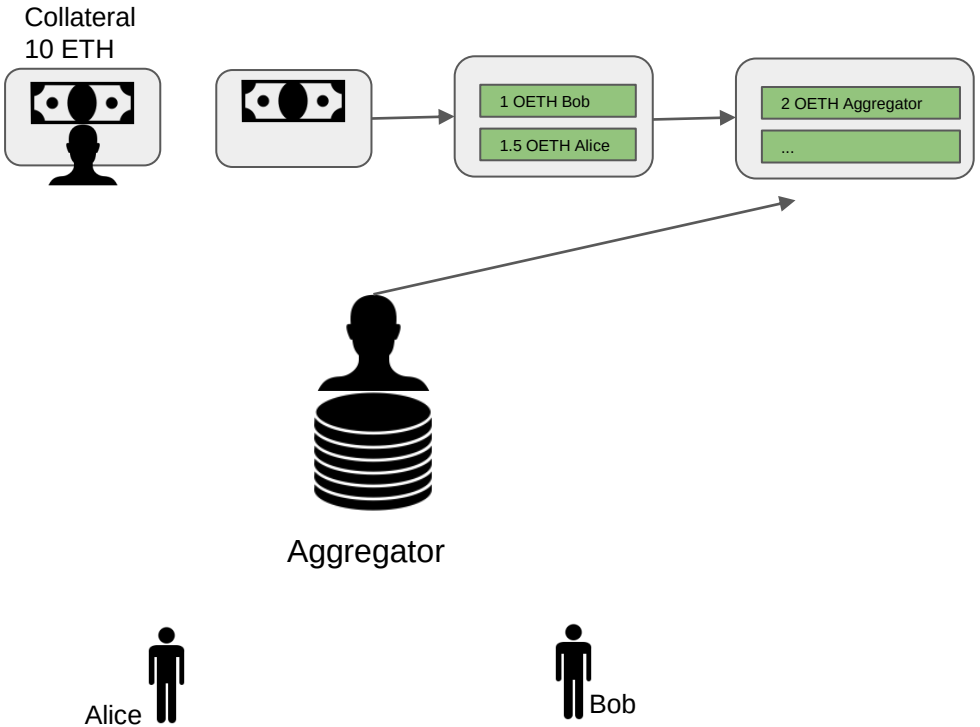
# Sending Transaction



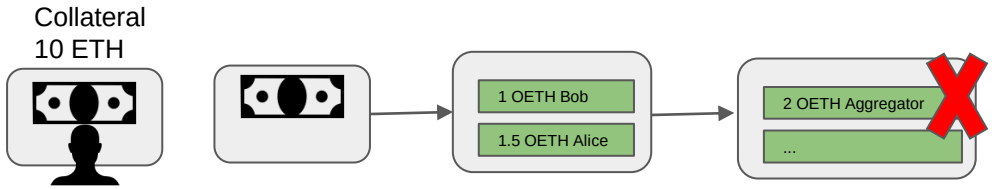
# Sending Transaction



# When a invalid block is created



# When a invalid block is created

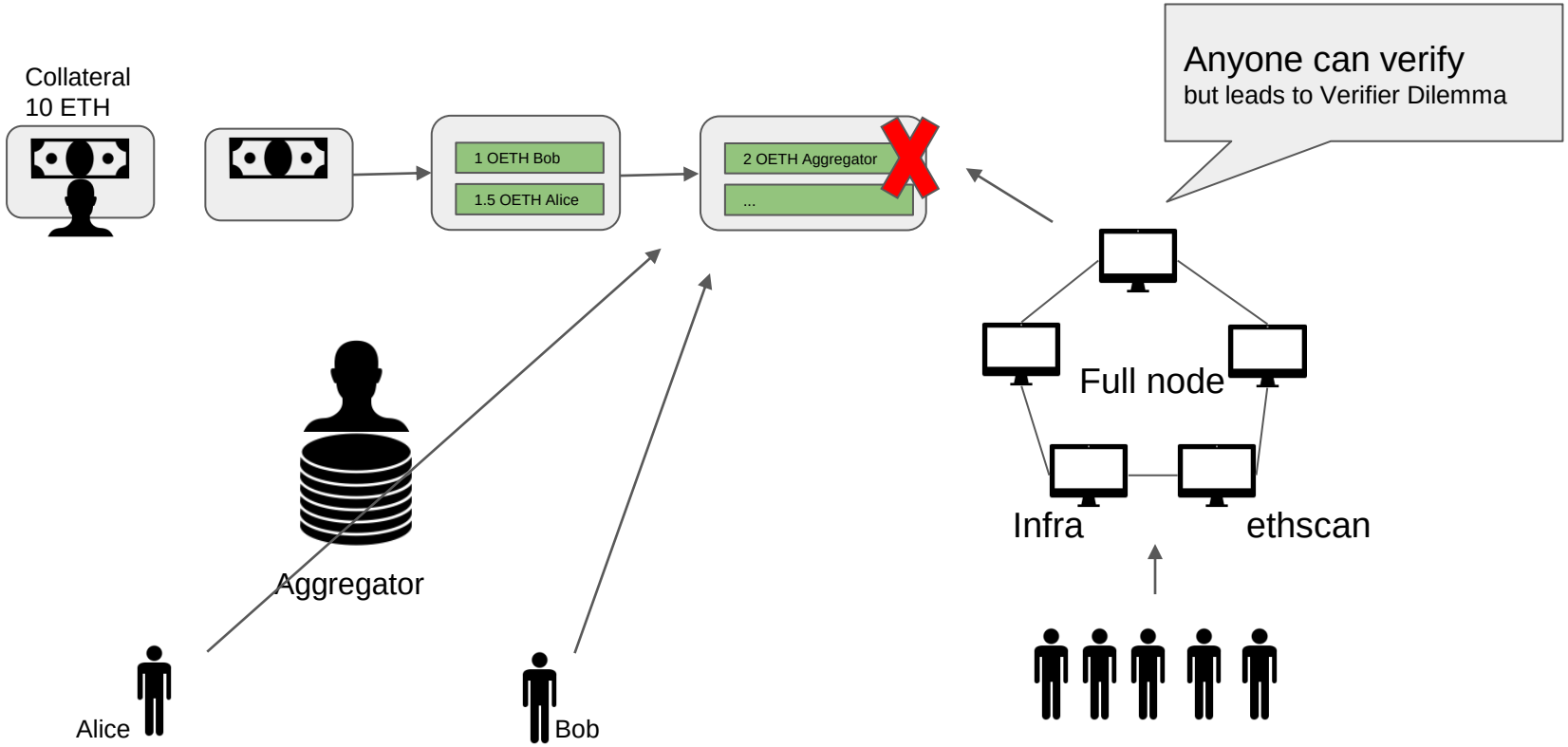



Aggregator

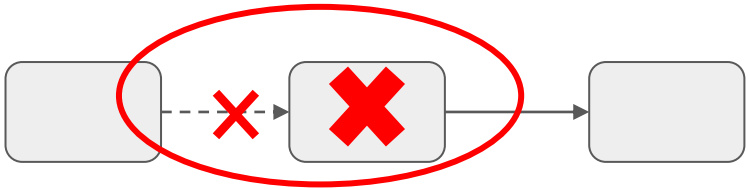
Alice

Bob

# When a invalid block is created



# Fraud Proof



Invalid block = block containing invalid state transitions
Fraud proof means proof of invalid state transitions

**OVM (Optimistic Virtual Machine)** is a mechanism that enables fraud proofs via EVM-compatible state transitions.

# Exploring ORU

Fraud proof validates blocks via EVM when a problem occurs. For this reason:

- Withdrawal to L1 takes about one week
- Applications can be EVM-compatible

Topics we won't be covering right now:

- How OVM works
- MEVAuction and Sequencer
- Further transaction cost reduction with BLS signature aggregation

# Agenda

What’s Rollup?

What’s Optimistic Rollup?

What’s ZK-Rollup?

ORU vs zkRU

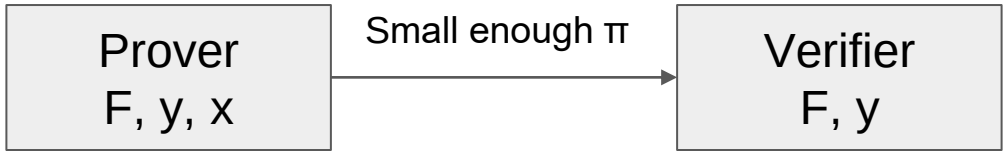
# How zkRollup works

In zkRollup, the correctness of the block is verified in L1 via (zk-)SNARK.

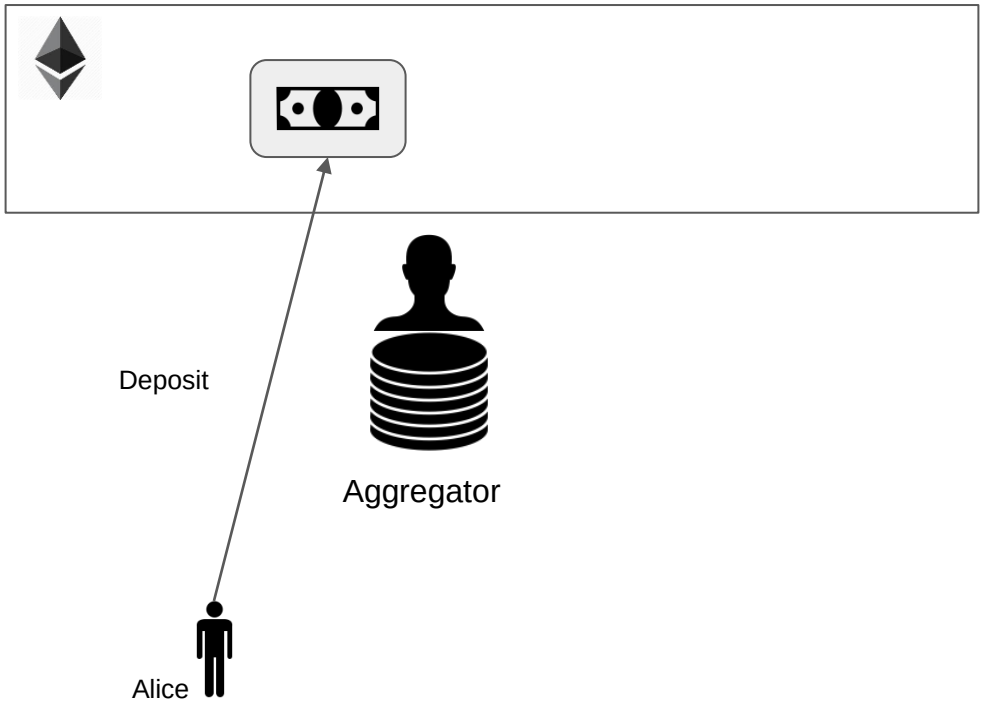
- Like ORU, aggregator is permissionless
- Withdrawal to L1 only takes a few minutes
- The block execution proof generation makes improving throughput a bottleneck
- Has restrictions on smart contract development
- Has a security advantage over ORU

# SNARK Properties

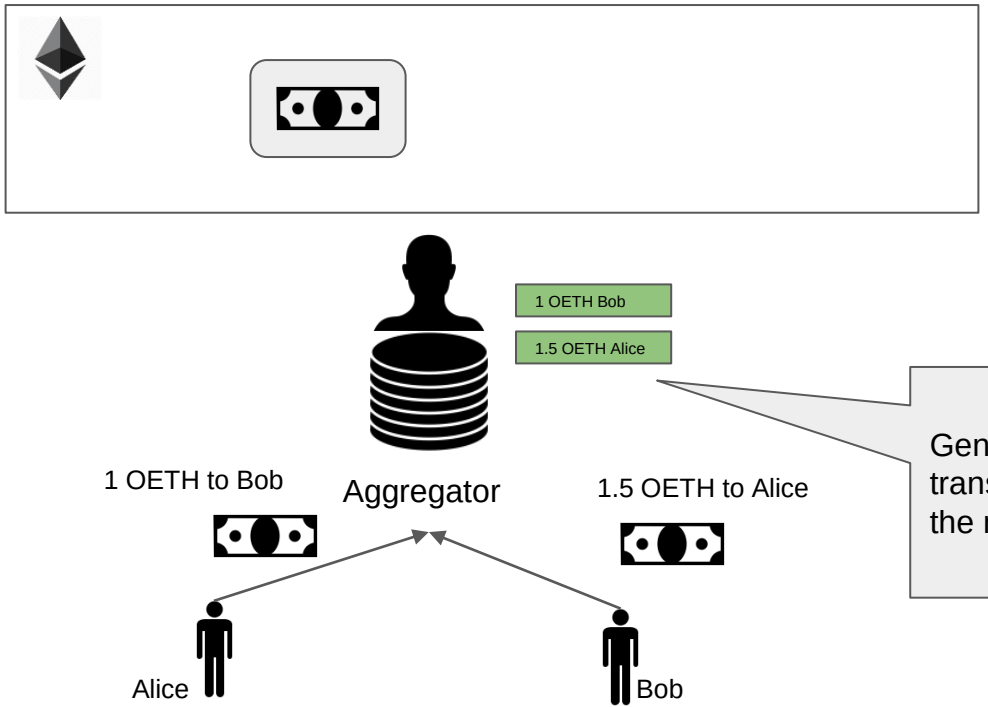
$$F(x) = y$$



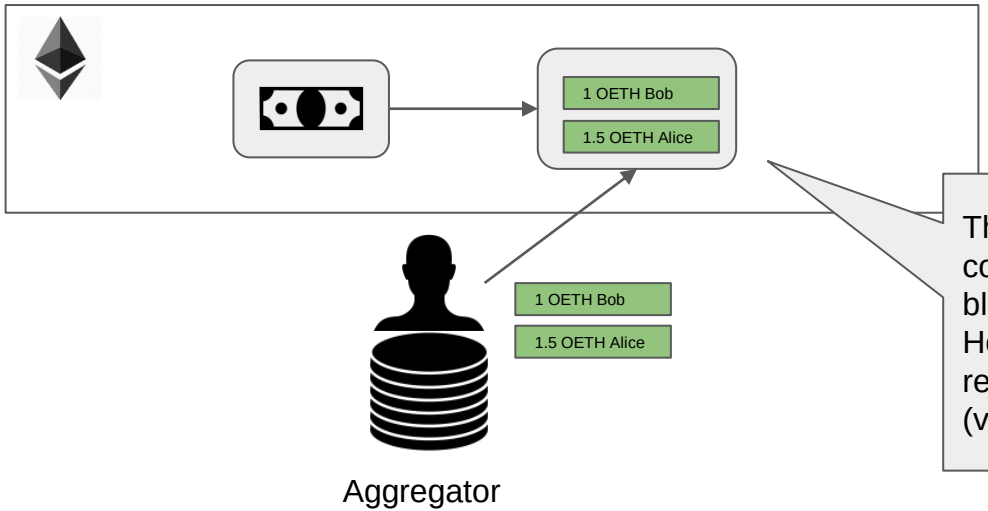
# How zkRollup works



# How zkRollup works

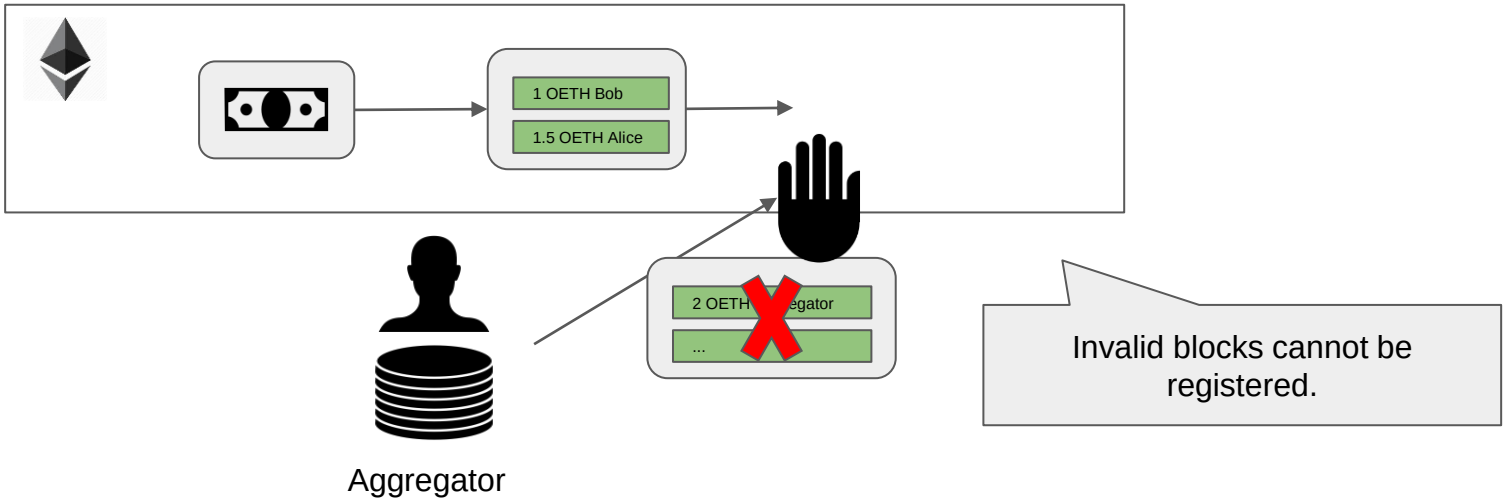


# How zkRollup works

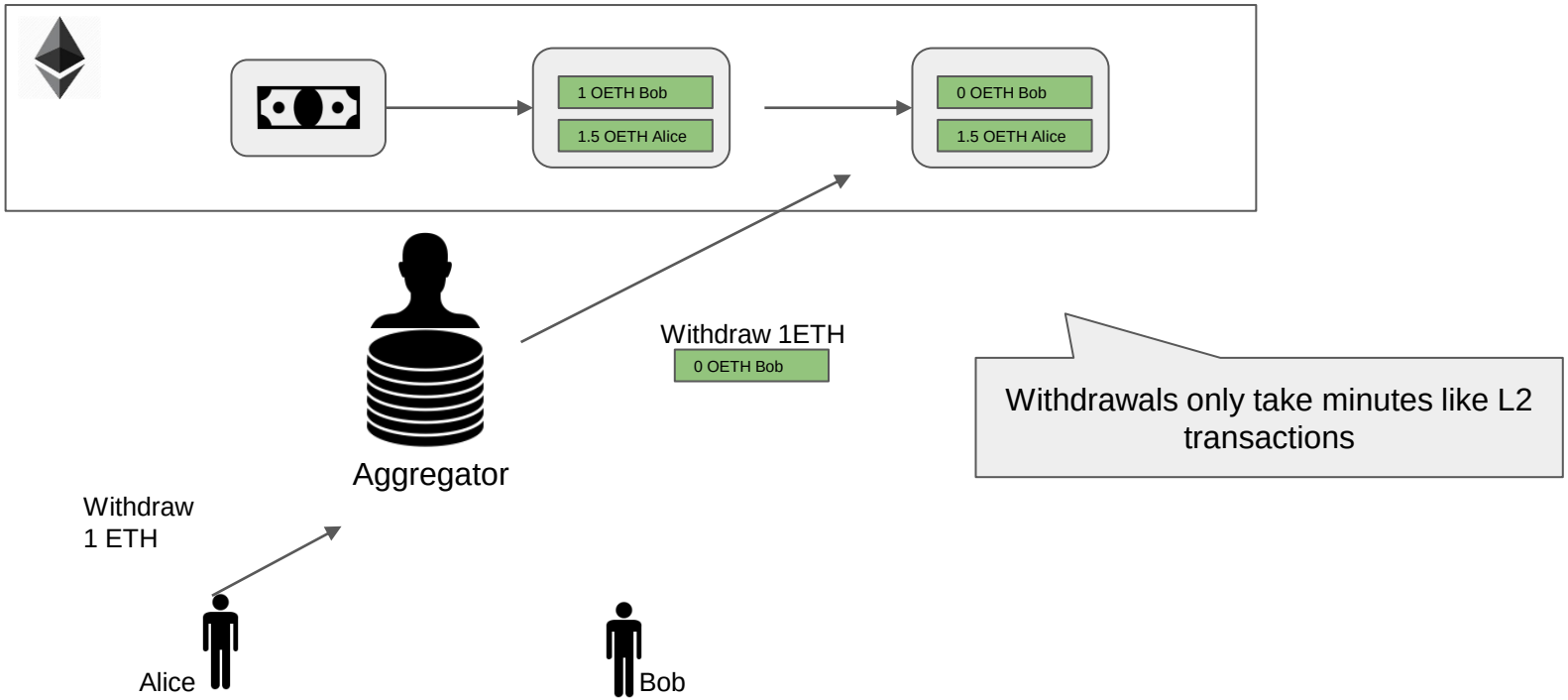



The L2 block is always correct because the smart contract validates the transaction every time via block execution proof (zk proof).
However, there is a delay between transaction registration (commitBlock) and verification (verifyBlock).

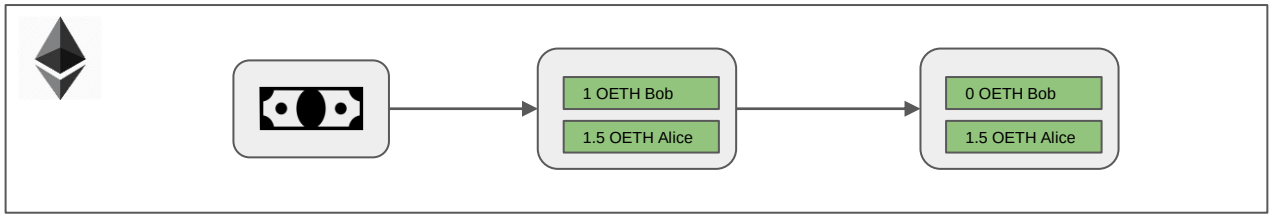
# How zkRollup works



# How zkRollup works



# How zkRollup works





Can theoretically assume multiple full nodes

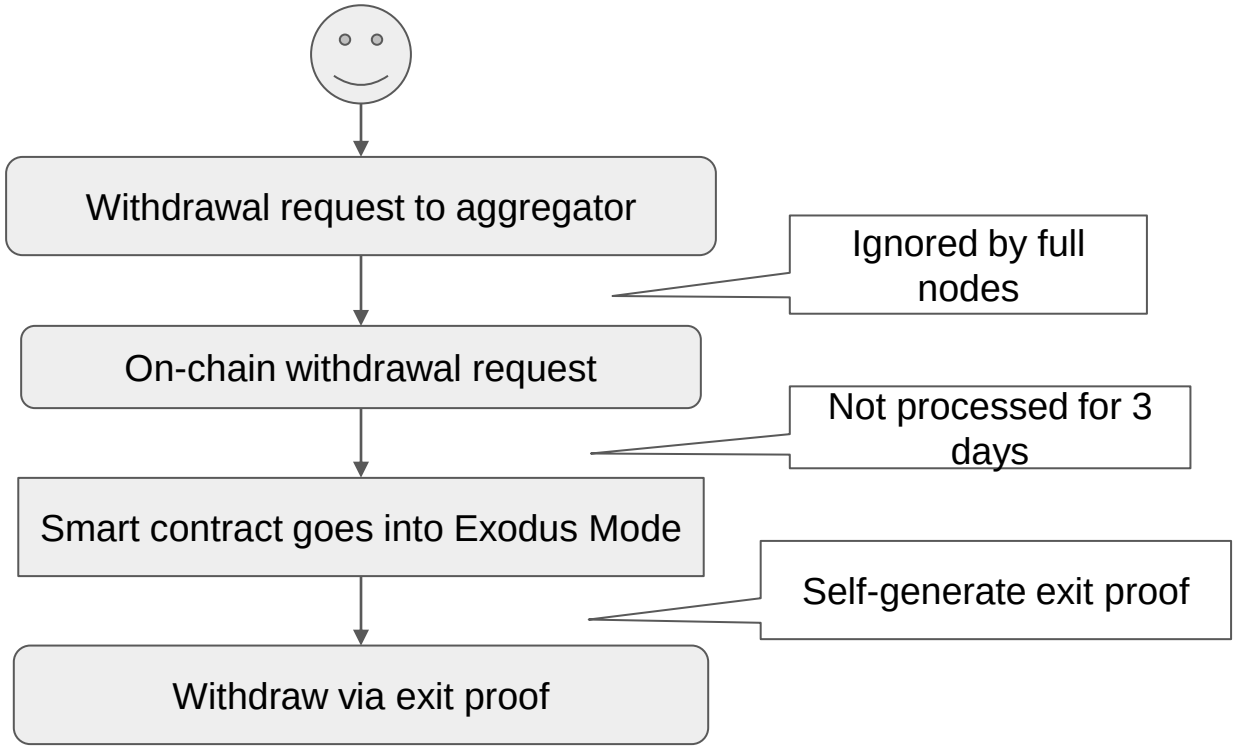
Withdraw
1 ETH

Alice

# Exodus mode

A withdrawal request can be thrown directly on-chain if the withdrawal request is ignored by all full nodes. If the withdrawal request is not processed, it goes into an emergency mode called **Exodus Mode**.

# Emergency fund withdrawal procedure



# zk-SNARK protocol comparison

| | Proof size | Verification cost | Proving Time | |
|---|---|---|---|---|
| Groth16 | 188 bytes | Approx. 200k gas | quasiliner | Trusted setup is required. |
| Plonk | 500 bytes | Approx. 300k gas | quasiliner | Universal trusted setup = increase the number of participants in the setup to gradually make it more secure. The same setup can be used with different programs. |
| Redshift | 96-234kb (2^20-2^28 constraint) | | quasiliner | Trusted setup is not required. |
| Stark | 80kb- (786k hash invocations) | Approx. 1M- gas | quasiliner | Trusted setup is not required. |

Practically speaking, the lower you go, the faster it gets.

# Conclusion zkRU

Since zkRollup has verified that the block is correct, it is no longer necessary to assume a sufficient number of validators for safety. This means assets can be immediately withdrawn to L1.

Topics we won't be covering right now:

- Development of zk-SNARK protocols
- Zk Programming (Zinc, Cairo)
- zk-SNARK protocol proof generation time improvements
    - Improvements using AWS F1 instances: https://medium.com/matter-labs/worlds-first-practical-hardware-for-zero-knowledge-proofs-acceleration-72bf974f8d6e

# Agenda

What’s Rollup?

What’s Optimistic Rollup?

What’s ZK-Rollup?

ORU vs zkRU

# ORU vs zkRU (user-side)

**Latency (time it takes for tx to be verifiable)**

- ORU gets immediate economic finality, L1 finality after challenge period (around 1-7 days)
- zkRU gets immediate economic finality, L1 finality after block proof generation (around 1-10 mins.)

**Withrawal to L1**

- Withdrawals take a week for ORU
- Withdrawals are immediate for zkRU

https://vitalik.ca/general/2020/08/20/trust.html

# ORU vs zkRU (developer, node admin-side）

**Programmability**

- ORU is EVM-compatible
- zkRU has some quirks in programmability but has seen significant improvements with Cairo and Zinc.

**Cost**

- ORU can be operated on cheap machines but needs to be distributed across multiple validators.
- zkRU requires high-spec machines to generate proofs and multiple machines to improve throughput.

https://vitalik.ca/general/2020/08/20/trust.html

# ORU vs zkRU, which is safer？

Unsafe = defined by an invalid block getting finality at L1

| | Assumptions required for safety |
|---|---|
| ORU | Assumes that many miners are honest |
| zkRU | None |

ORU must assume that L1 has a certain level of censorship resistance. As for zkRU, assets are safe even if the withdrawal is censored. On the other hand, depending on the zk-SNARKS protocol, there may be situations that rely on the trustworthiness of the person who set it up.

https://vitalik.ca/general/2020/08/20/trust.html

# Products of ORU & zkRU

| Name | Feature |
| --- | --- |
| Optimism (synthetix) | ORU that can write smart contracts with Solidity |
| FuelCore | UTXO-based ORU |
| Arbtrum | Unique VM called AVM. Dichotomous dispute resolution model |
| zkSync (curve, balancer) | zkRollup that aims for a smart contract platform |
| zkSwap | AMM using zkSync technology |
| loopring | Currently has the highest L2 DEX trading volume ($10M volume) |
| StarkEx, StartNet | Validium, Rollup platform-type |

# Interesting fields not covered by today's presentation

- Economics surrounding Aggregators (MEVAuction)
- Private Transactions (opzkru, zkzkru)
- Frontrunning (MEV-Geth)

# Conclusion

Discussed Rollup, an Ethereum scaling technology

- Rollup can improve throughput while maintaining Ethereum's safety and decentralization as much as possible.
- Increases throughput tens to hundreds of times
- ORU can execute EVM-compatible smart contracts. zkRU is also rapidly fixing its smart contract development bottleneck.
- zkRU is more secure, and withdrawals to L1 only take minutes.