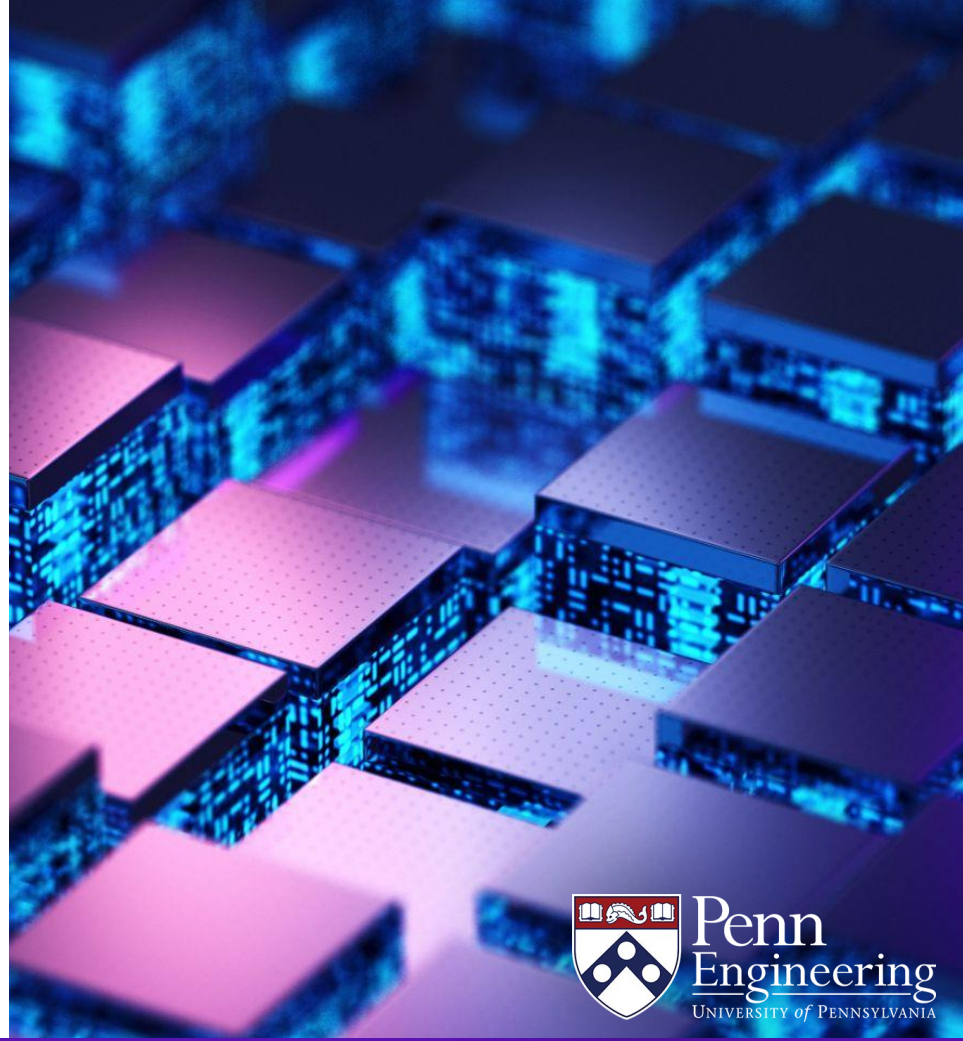
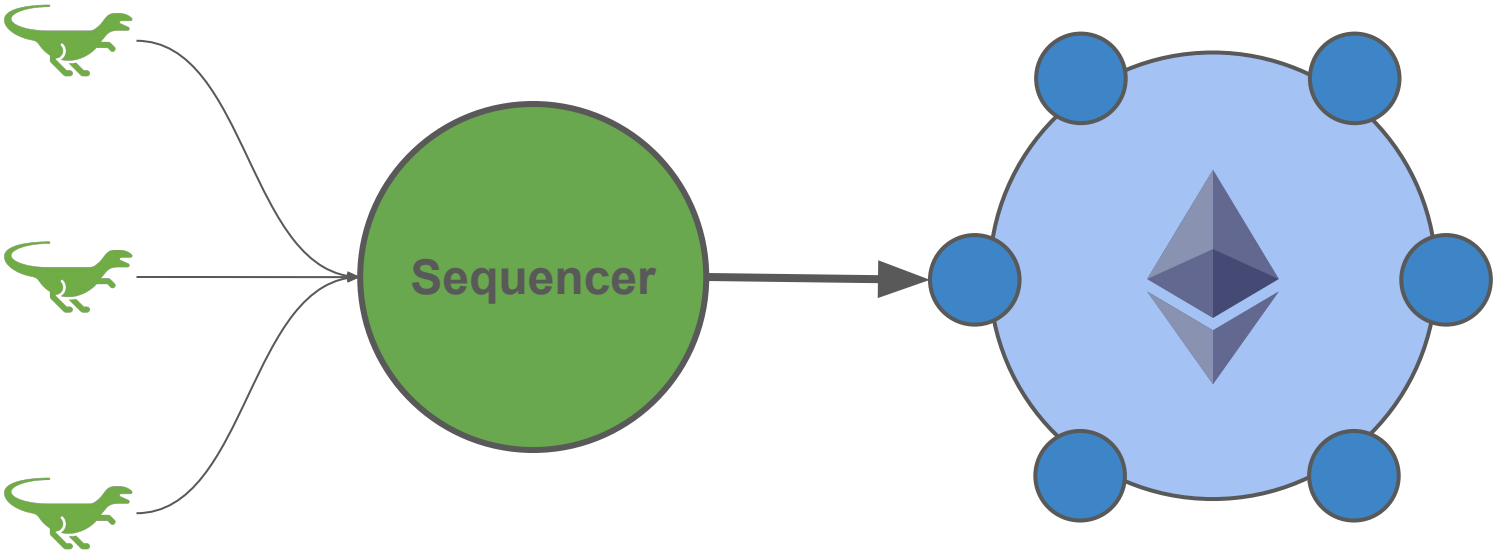
EAS 5830: BLOCKCHAINS

ZK Rollups

Professor Brett Hemenway Falk



ZK Rollups



Rollup users

Optimistic Vs ZK Rollups

Optimistic Rollups

- Sequencer pushes new state to the L1
- If the state is invalid users can challenge the update by issuing a “fraud proof”

ZK Rollups

- Sequencer pushes new state to the L1
- Sequencer “proves” that the state update was valid
- L1 Contract verifies the proof

ZK Rollups are a misnomer

Most ZK rollups do **not** implement any Zero-Knowledge technology

Succinctness

- The goal is **not** to hide the L2 transactions from the L1
- The goal is to allow the L1 to verify the validity of a state transition **succinctly**

SNARKs

Succinct

Non-interactive

ARgument of

Knowledge

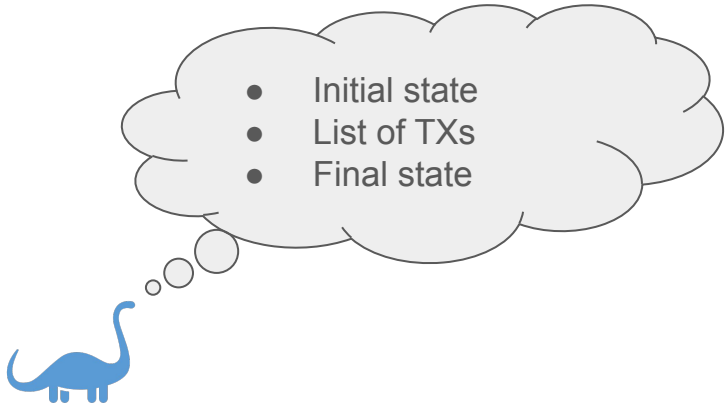
ZK-SNARKs

Most SNARKs can be transformed into ZK-SNARKs

ZK-SNARKs

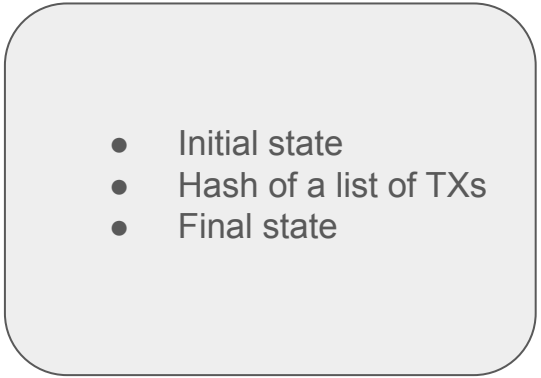
Most SNARKs can be transformed into ZK-SNARKs

But most rollups only use regular SNARKs



Prover

Proof:
If you executed this list of TXs (under the rules of the EVM) Then it would transform the initial state to the final state



Verifier
(Contract)

Active projects 11 | Upcoming projects 6 | Archived projects 6

#	NAME	RISKS	TECHNOLOGY	STAGE	PURPOSE	TOTAL	MKT SHARE
1	zkSync Era		ZK Rollup	STAGE 0	Universal	$430M ▼ 4.43%	3.43%
2	dYdX		ZK Rollup	STAGE 1	Exchange	$359M ▼ 0.85%	2.86%
3	Starknet		ZK Rollup	STAGE 0	Universal	$131M ▲ 0.68%	1.04%
4	Loopring		ZK Rollup	STAGE 0	Tokens, NFTs, AMM	$102M ▲ 10.03%	0.82%
5	Polygon zkEVM		ZK Rollup	STAGE 0	Universal	$84.12M ▲ 17.76%	0.67%
6	Linea		ZK Rollup	STAGE 0	Universal	$77.86M ▼ 2.16%	0.62%
7	zkSync Lite		ZK Rollup	STAGE 1	Payments, Tokens	$73.82M ▲ 2.34%	0.59%
8	Scroll		ZK Rollup	STAGE 0	Universal	$35.56M ▲ 29.05%	0.28%
9	ZKSpace		ZK Rollup	STAGE 0	Tokens, NFTs, AMM	$22.99M ▲ 3.63%	0.18%
10	DeGate V1		ZK Rollup	STAGE 2	Exchange	$3.54M ▼ 2.50%	0.03%
11	Paradex		ZK Rollup	STAGE 0	Exchange	$2.18M ▲ 3.86%	0.02%

Where does the data live?

On the L1

- L2 TXs are stored on the L1 as “calldata”
- Not executed on the L1
- But still expensive
- ZKSync Era stores data on Ethereum L1

On a “data-availability layer”

- Celestia
- Avail
- ZKPorter “guardians”

Proving complexity

- ZKSync proof generation time is 10 minutes
- Starkware's dy/dx prover took hours