



ZK Proof Performance and Security Characteristics

Brian Wilkes CFA
Ethereum Foundation PSE Grantee

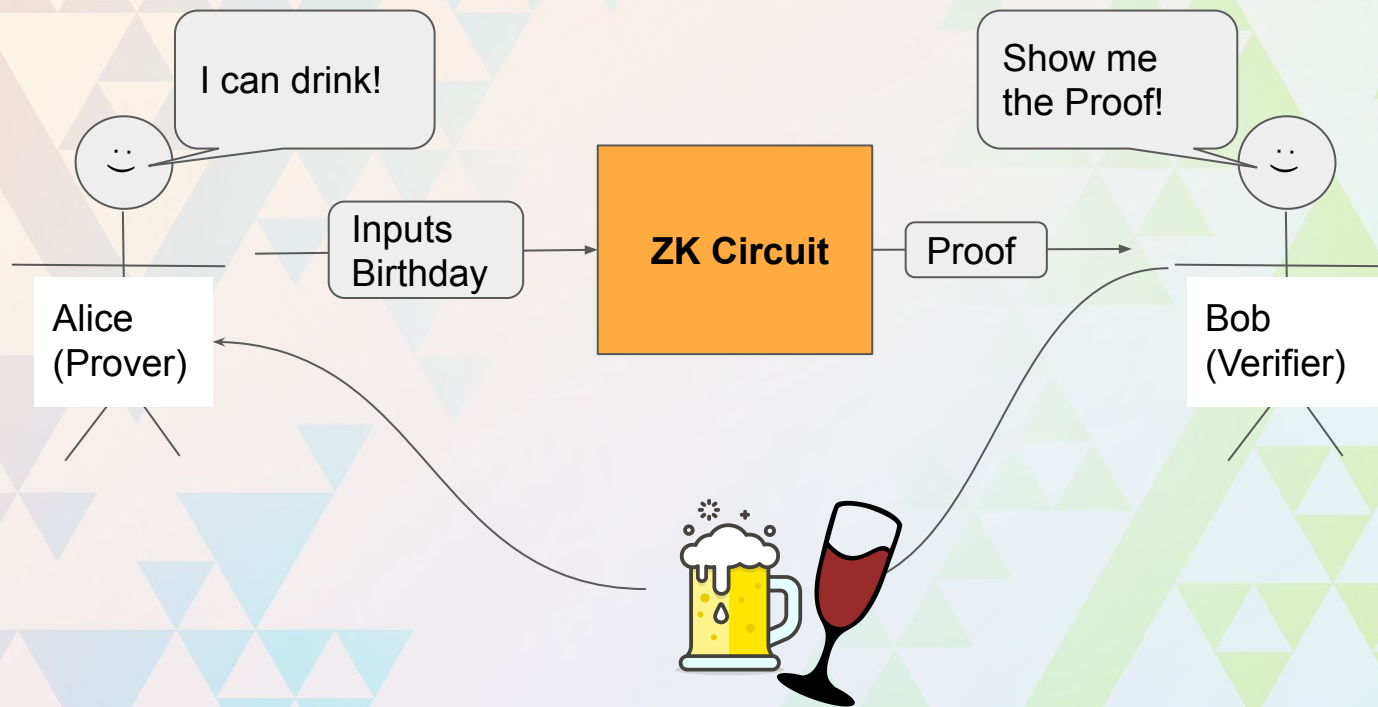
What's on the Docket?

- Background
- How to find ZKPs on and off chain
- Characteristics & what they mean





What are ZKPs?

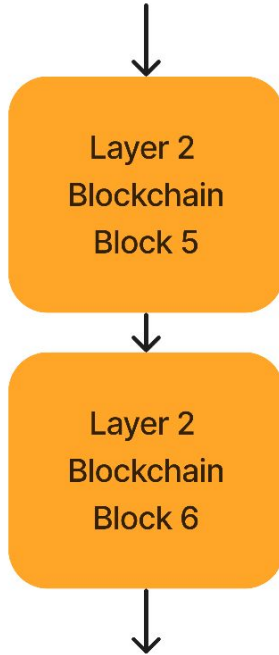


Why Zero-Knowledge Proofs?

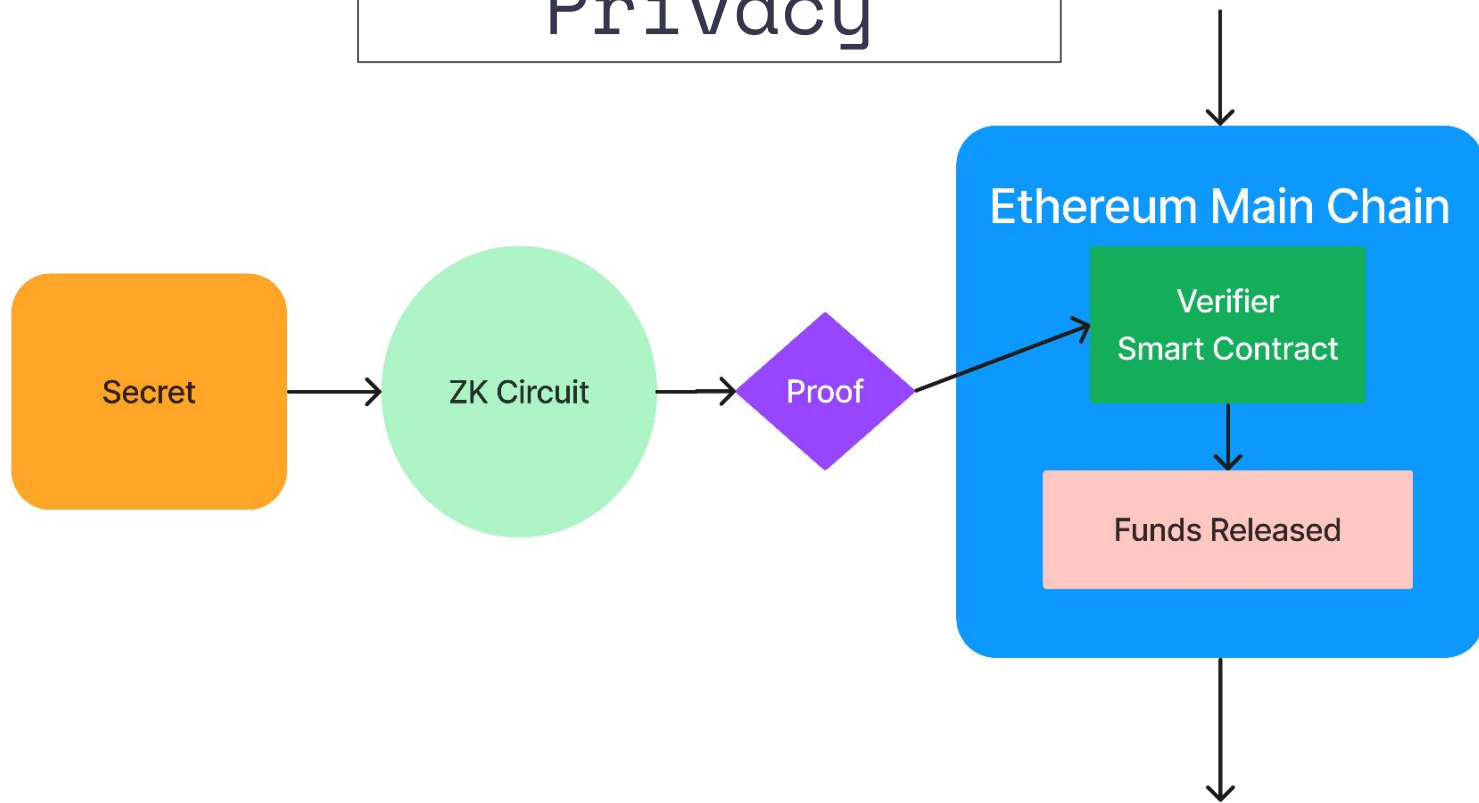
- Scalability
 - 13 TPS to 13K TPS
 - Separate Chains w/ Full Security of Ethereum
- Privacy
 - Ethereum is PUBLIC



Scalability



Privacy



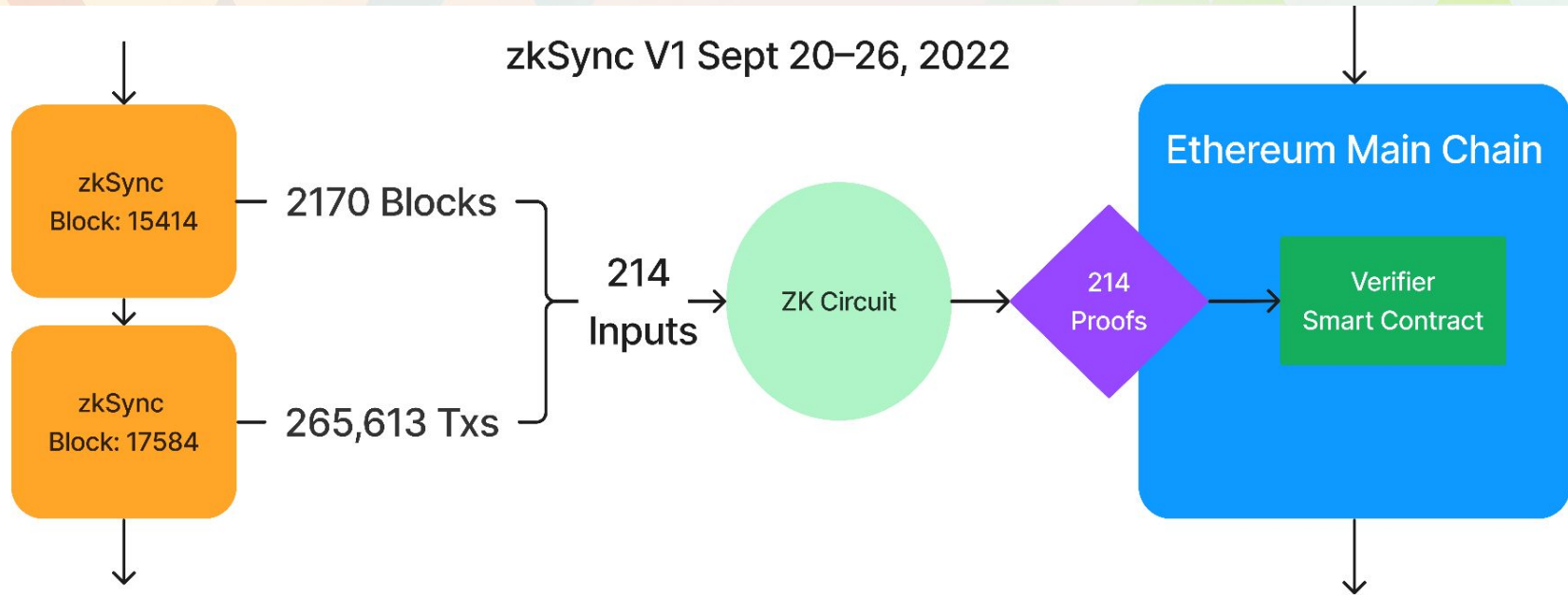
FANTASTIC ZK PROOFS

AND WHERE
TO FIND THEM™














The Search for Verifiers

zkSync V1 Sept 20–26, 2022



BigQuery

▼ bigquery-public-data	★	⋮
▼  crypto_ethereum	☆	⋮
 amended_tokens	☆	⋮
 balances	☆	⋮
 blocks	☆	⋮
 contracts	☆	⋮
 logs	☆	⋮
 sessions	☆	⋮
 token_transfers	☆	⋮
 tokens	☆	⋮
 traces	☆	⋮
 transactions	☆	⋮



Bytecode Search for Constants

? Other Attributes:

Txn Type: 0 (Legacy)

Nonce: 21

Position In Block: 18

? Input Data:

```
37382014b34303b00e01b90303b00f01b90303b014b4381614ad0303b01140130  
3f57600080fd5b614b4381614ad9565b614b4381614ae256fe30644e72e131a02  
9b85045b68181585d97816a916871ca8d3c208c16d87cfd4730644e72e131a029  
b85045b68181585d2833e84879b9709143e1f593f0000001a365627a7a7231582  
08d7221ab4e6a093b4d9762e3b9045849f85414fb85e1e53bc8c1ccd3adf63452  
6c6578706572696d656e74616cf564736f6c63430005100040
```

View Input As ▾

Finite Field Results

- 558 Contracts with FF Constant
- Checked Every Contract on Etherscan
- Most were not Verifier Contracts

Transaction Decoder



Eth: \$1,326.87 (+0.05%) | 24 Gwei

All Filters

Search by Address / Txn Hash / Block / Token / Ens



Home

Blockchain

Tokens

Resources

More

Sign In



Transaction Details

Buy

Exchange

Earn

Gaming

Overview

Internal Txns

State

Comments



Transaction Hash:

0x47d6331796efecf8b72379331c0701188f1e11b9be4aa88f668824b66eb6769b

Status:

Success

Block:

15710594 109 Block Confirmations

Timestamp:

21 mins ago (Oct-09-2022 12:39:35 PM +UTC) | Confirmed within 20 secs

From:

0x01c3a1a6890a146ac187a019f9863b3ab2bff91e (zkSync: L2 Operator V1)

To:

Contract 0xabea9132b05a70803a4e85094fd0e1800777fbef (zkSync)

Validate Transaction

Geth Debug Trace

Parity Trace

Transaction Decoder

Get Raw Tx Hex

Execution Trace

Execution Trace

Contract Code

▼ Proxy  **.83981808()** => ()


▼ ZkSync  **.proveBlocks**

```
(_committedBlocks=, _proof=[{name:recursiveInput, type:uint256[], order:1, index:  
449943031429362}, {"name:recursiveInput, type:uint256[], order:1, index:  
88698348431398146506, 269414076969748101691, 701963316730518, 142065530193881289682,  
250941787329182719118, 156988162341172272777, 5108525806615991377, 449943031429362}],  
=> ())
```

▼ Proxy  **.a830bd60()** => ()

▼ Verifier  **.verifyAggregatedBlockProof**

```
(_recursiveInput=[187320679881025715674887764611697255150022732444785640491512,  
404423317004003200003331140479370737127307404227919355376651142631719263767007,  
123853929344511249591126680326281724285748493020433, 48698706597565120418809007615,  
994084721963906214892710367327053470764953311744126,  
147462495627716885842, 448845074513113, 2105333460,  
142065530193881289682, 52927000072333905701, 415197,  
5108525806615991377, 449943031429362]),  
=> (True))
```

Null Address: 0x000...002  **.1ffdc7eb()** => ()

Null Address: 0x000...005.**00000000()** => ()

Null Address: 0x000...005.**00000000()** => ()

Method IDs

② Input Data:

```
0xe85a6a28000000000000000000000000
000000000000000000000000000000d2
00000000000000000000000000000000
```

File 3 of 9: FriStatementContract.sol

```
36      /* NOTE: This function is used
37      */
38      function verifyFRI(
39          uint256[] memory proof,
40          uint256[] memory friQueue,
41          uint256 evaluationPoint,
42          uint256 friStepSize,
43          uint256 expectedRoot
44      ) public {
```

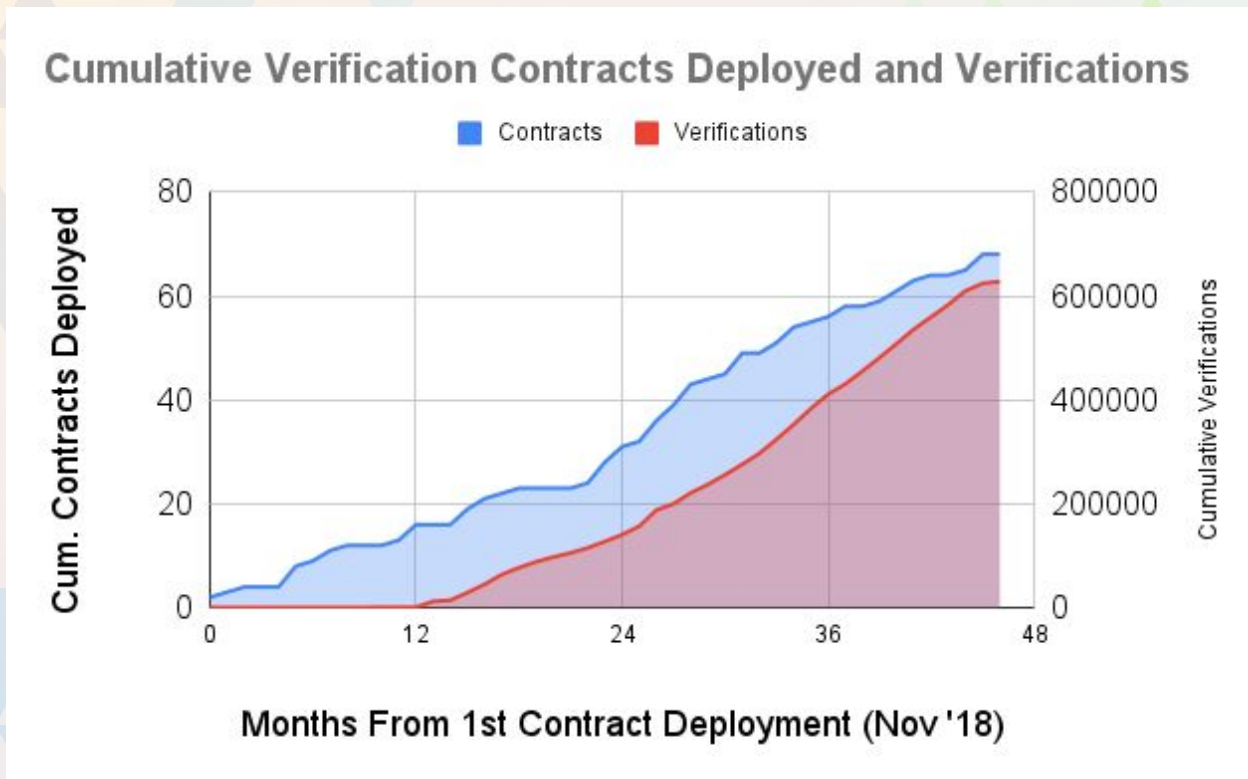
- Keccak-256(verifyFRI(uint256[],uint256[],uint256,uint256,uint256))
- **(0x)e85a6a28**47c217651cfe25e4e2df6637ce6c010a99bbf00918...

Method IDs

<https://www.4byte.directory/>

ID	Text Signature	Bytes Signature
614653	verifyFRI(uint256[],uint256[],uint256,uint256,uint256)	0xe85a6a28

65 Confirmed Verifiers on Main Chain



16 Active Contracts on Main Chain

Project	Latest Deployed Verifie	Proving Sys	First txn	Last Txn	Number of Verificat	Avg gas Per Verification	Libraries	Language	Hashes Used	Purpose	L2?	Rollup or Va
Element Finance	0xd0abdb2175ef925a3f378c	PLONK	2022-04-12 02:31:56 UTC	2022-09-20 00:53:47 UTC	507	258689	circom, snarkjs	circom	Pedersen	Private Airdrop	No	
zkSync V1	0xf7bd436a05678b647d74a	PLONK	2021-12-17 06:21:35 UTC	2022-10-02 15:46:35 UTC	7899	470407	bellman, franklin	RUST	Rescue, Sha256	Token Transfer	Yes	Rollup
Aztec Connect	0x07528c46a34d16e4fb7cfa	PLONK	2022-06-08 18:41:50 UTC	2022-10-02 13:10:59 UTC	2654	270461	barretenberg	C++	Blake2, Pedersen	Private Defi	Yes	Rollup
StarkEx (DYDX)	0xf6b83ccadeee478fc372af	STARK/FRI	2021-02-21 21:35:10 UTC	2022-10-02 14:15:59 UTC	90928	268430	cairo	C++, Cairo	Pedersen	Perpetual and Ti	Yes	Rollup
Messier 10 Ether	0x39e5b71535cc98fddcd8b	Groth16	2022-07-08 21:47:02 UTC	2022-09-15 02:42:33 UTC	20	219023				Mixer	No	
Messier .1 Ether	0x04f94e0bf3b30b0ce53288	Groth16	2022-06-30 21:23:19 UTC	2022-09-15 03:17:08 UTC	130	242996				Mixer	No	
Messier 1 Ether	0x1a7578ce0a6225cce8140	Groth16	2022-06-30 20:32:47 UTC	2022-09-15 02:52:17 UTC	110	242993				Mixer	No	
ZK Space	0x44deda2c824458a5dfe1e	PLONK	2022-04-20 08:25:15 UTC	2022-10-02 15:14:59 UTC	3057	480766	bellman, franklin	RUST	Rescue	Bridge to L2?	Yes	Rollup
Aztec	0xd3a6d9de4cbc2cc752936	TurboPLONK	2021-12-12 19:50:49 UTC	2022-10-02 10:01:59 UTC	2380	631297	barretenberg	C++	Blake2, Pedersen	Privacy	Yes	Rollup
StarkEx (IMX, Rinofi, Sorare	0x932457426841dc45ca4ab	STARK/FRI	2022-08-02 01:19:04 UTC	2022-10-02 07:20:59 UTC	1038	257416	cairo	C++, Cairo	Pedersen	App Specific Val	Yes	Both
Loopring	0x6150343e0f43a17519c03	Groth16	2020-11-24 01:57:51 UTC	2022-10-02 15:53:47 UTC	30035	420389	ethsnarks, libsnark	C++	Poseidon	Orderbook	Yes	Rollup
ZK Swap V2	0x94b9401945a9bc06ce5b6	PLONK	2021-07-12 13:24:43 UTC	2022-09-28 08:39:35 UTC	7283	512626	bellman, franklin	RUST	Rescue, Sha256	Token Transfer	Yes	Rollup
Polygon Hermez	0x1dc4b451dfcd0e848881e	Groth16	2021-05-13 08:20:21 UTC	2021-05-13 08:20:21 UTC	4932	202593	circom, snarkjs	circom	Poseidon	Token Transfer	Yes	Rollup
Polygon Hermez Withdrawal	0x4464a1e499cf5443541da	Groth16	2021-09-10 08:15:58 UTC	2022-09-22 18:05:35 UTC	266	202593	circom, snarkjs	circom	Poseidon	Withdrawal for H	Yes	Rollup
WanChain	0x84271540f80e8879826c3		2020-11-02 06:46:24 UTC	2022-10-01 20:22:59 UTC	5829	16811						
Tornado.Cash	0xce172ce1f20ec0b3728c9	Groth16	2020-05-13 06:38:49 UTC	2022-10-02 15:45:59 UTC	302984	242621	circom, snarkjs	circom	Pedersen	Mixer	No	



Section 3

Characteristics

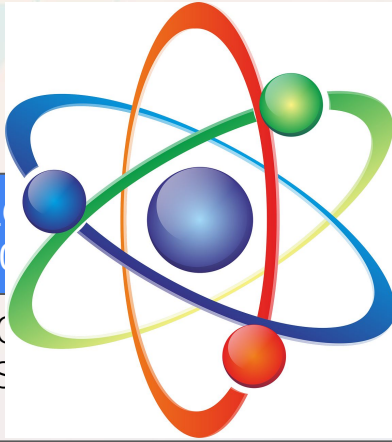
Proving Systems

GROTH16
(2016)

TC, Hermez,
Loopring

PLONK
(2019)

Aztec Circuits
zkSync



PLONK
(2019)

etc

Halo2
(2020)

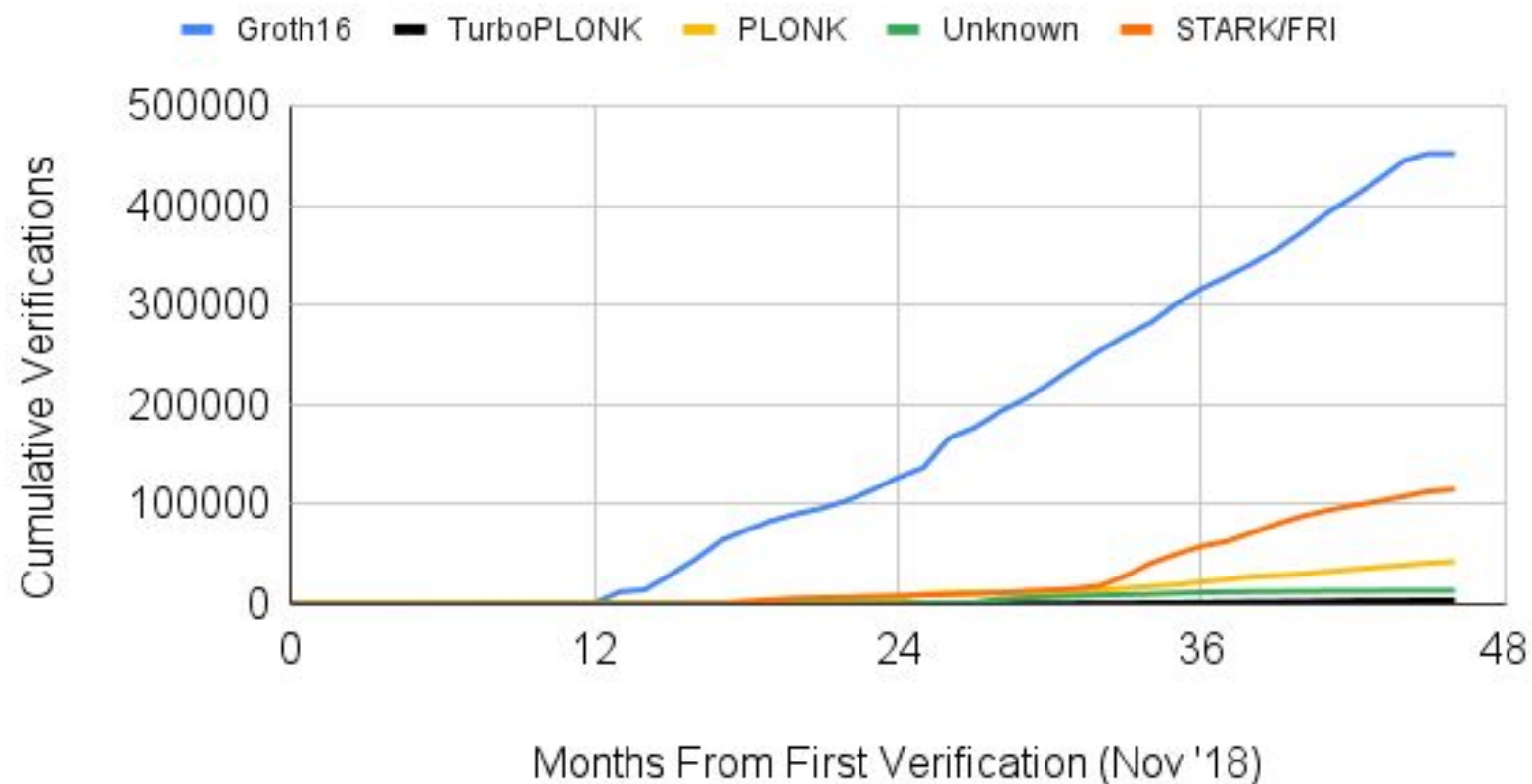
Scroll

STARKs

STARK
(2018)

Starkware
Projects

Cumulative Verifications by Proving System



Trusted Setups (CRS)



Trusted Setup

SNARKs

GROTH16
(2016)

TC, Hermez,
Loopring

PLONK
(2019)

Aztec Connect,
zkSync

TurboPLONK
(2019)

Aztec

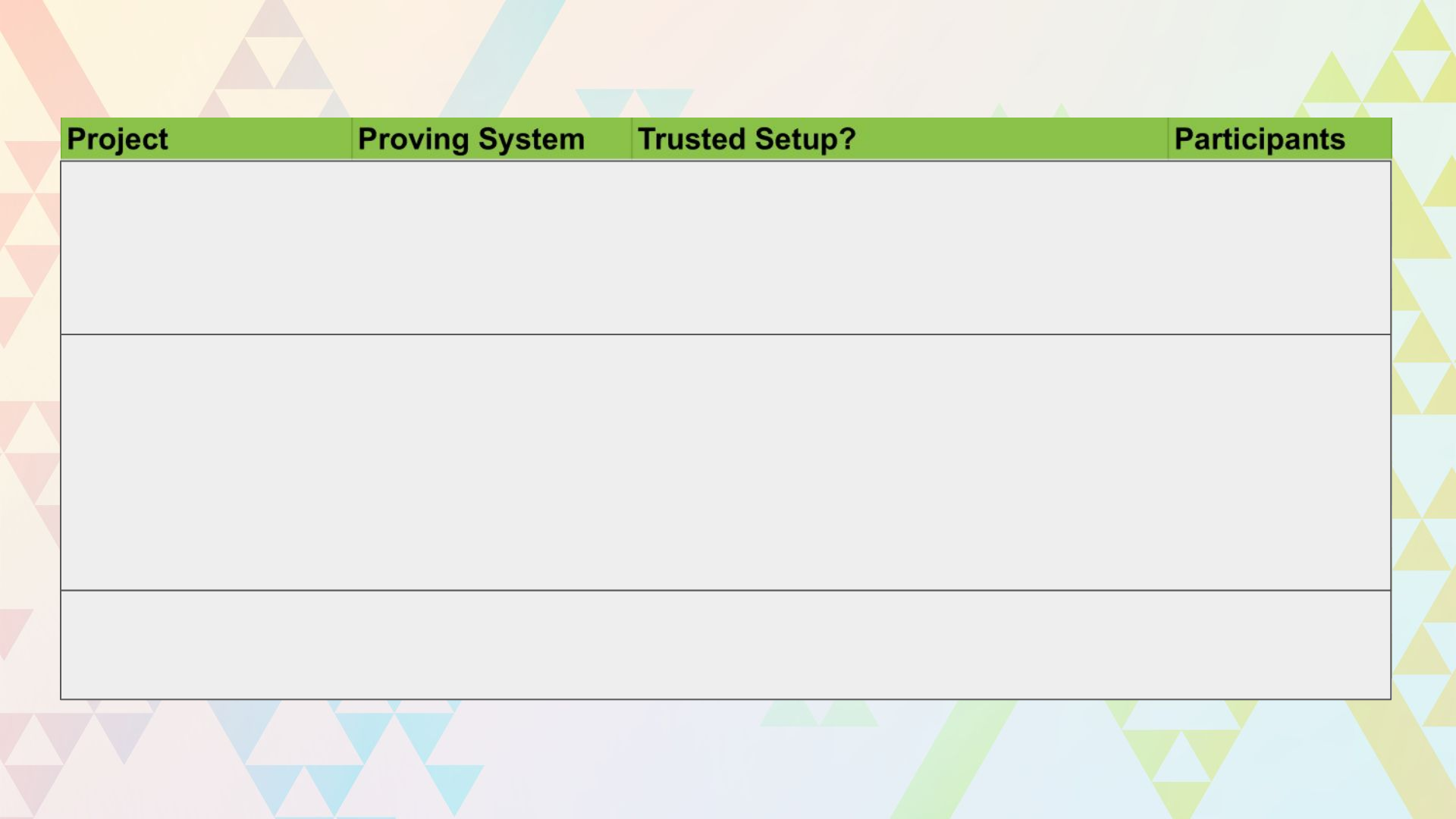
Halo2
(2020)

Scroll

STARKs

STARK
(2018)

Starkware
Projects



Project	Proving System	Trusted Setup?	Participants

Recursion

- Parallelization of Proof Generation
- Proof Chaining



Recursion

SNARKs

GROTH16
(2016)

TC, Hermez,
Loopring

PLONK
(2019)

Aztec Connect,
zkSync

TurboPLONK
(2019)

Aztec

Halo2
(2020)

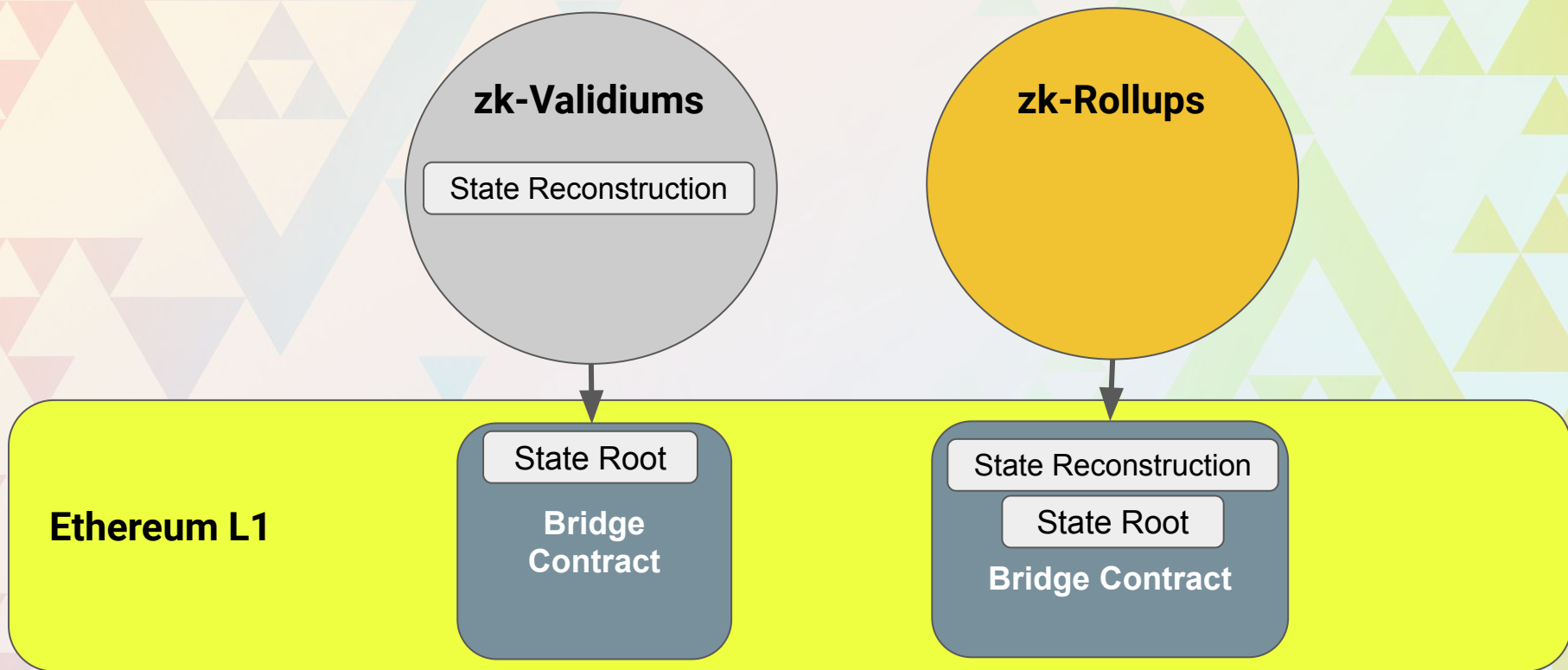
Scroll

STARKs

STARK
(2018)

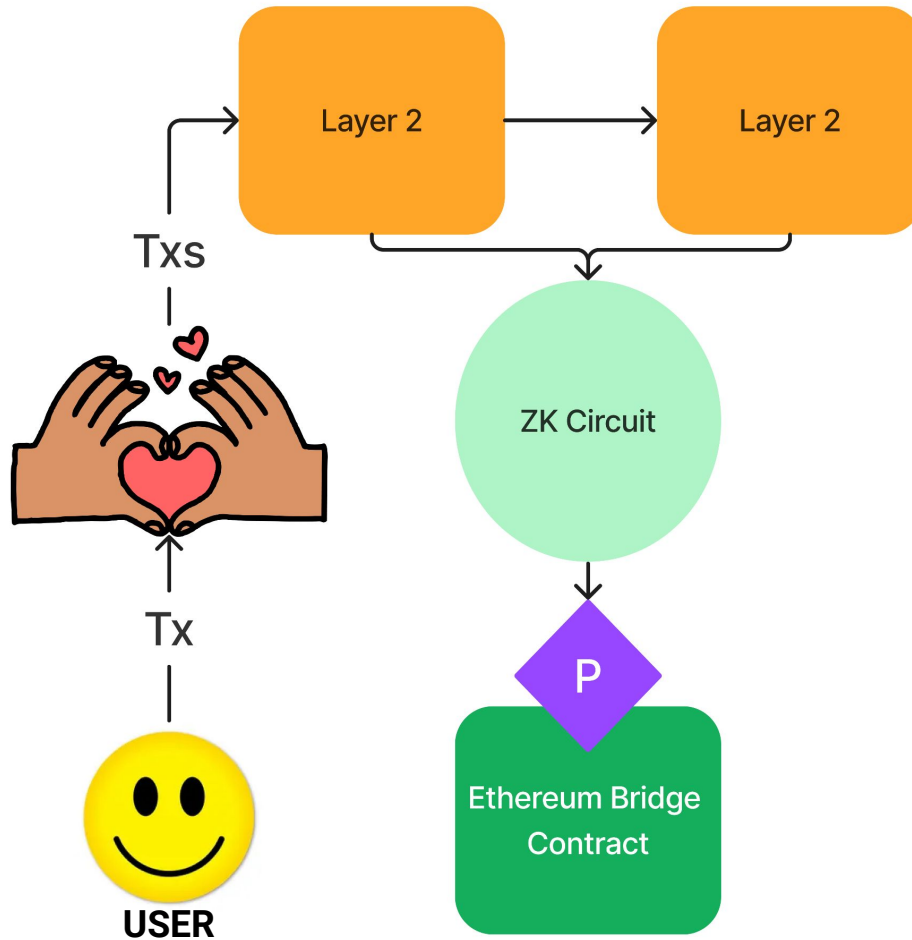
Starkware
Projects

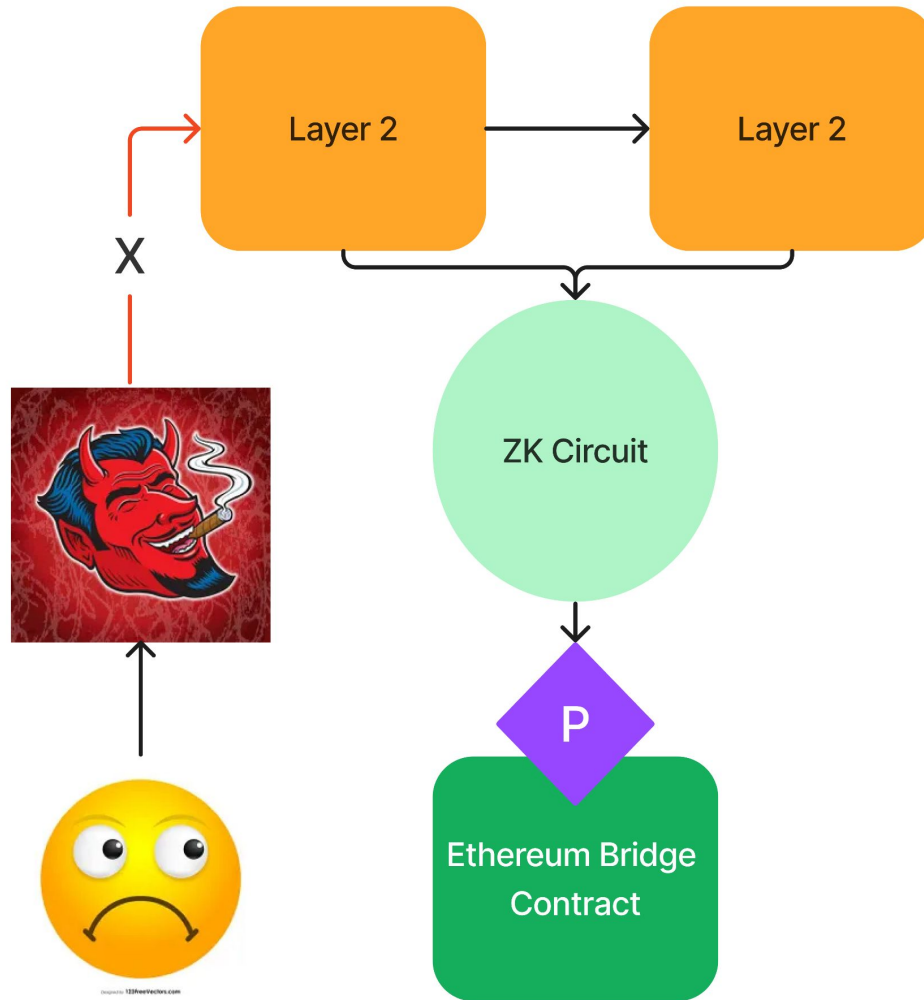
Data Availability

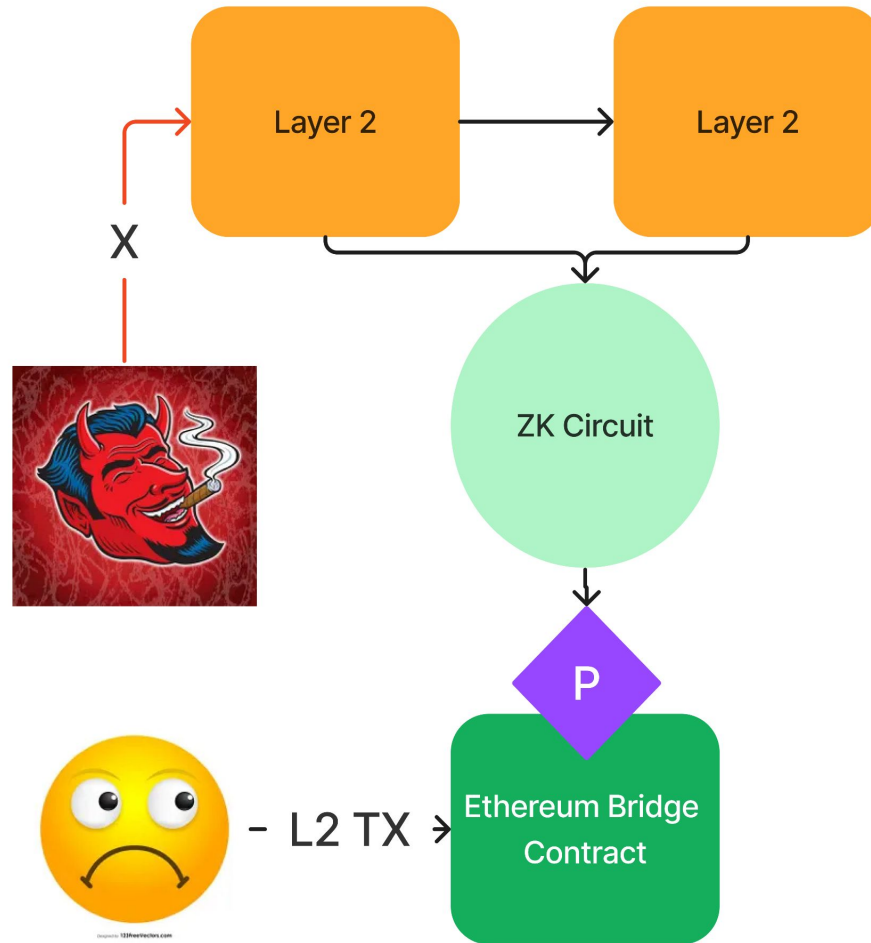


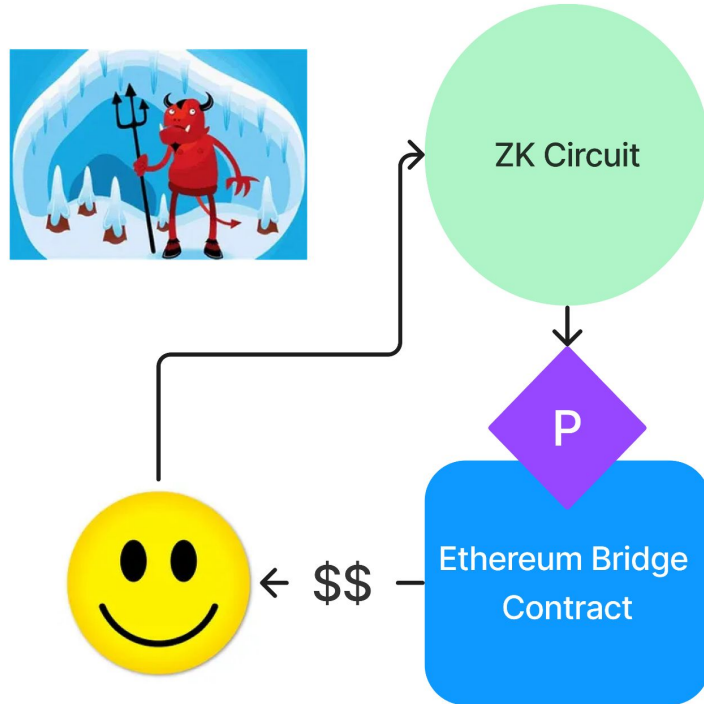
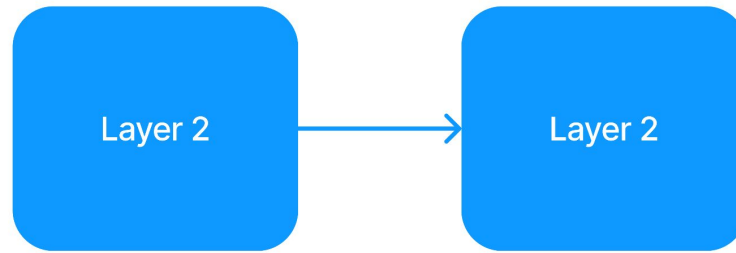
Data Availability

- Validiums
 - StarkEx (IMX, Rinofi, Sorare, Apex...)
 - zkPorter
- Rollups
 - zkSync V2
 - Borel
 - Polygon V2, Miden, zkEvm, Zero
 - zkSpace
 - StarkNet







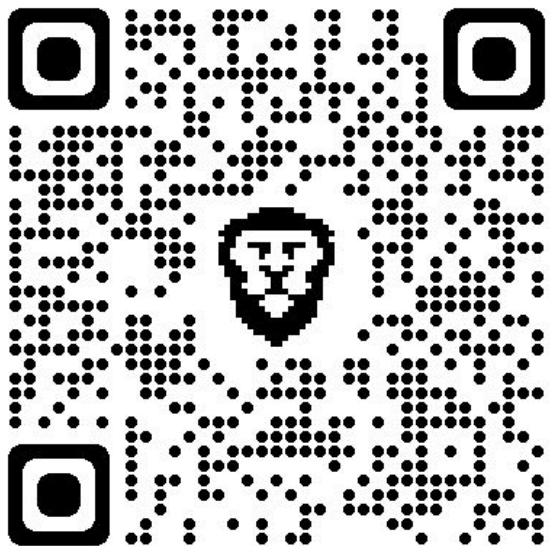


To Inherit Full Ethereum Security A Rollup Must Have:

- Available Data on L1
- Functional, Accessible Force Exits
- Time Delays for L1 Updates
- L1 Locked Funds = Market Value on L2

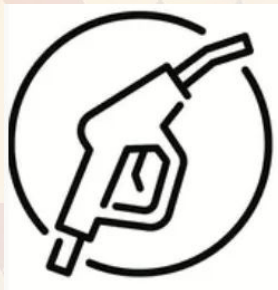


Get into the Data



- Big Query (& Dune)
- Project Github
- L2 BEAT
- Layer 2s

Thank You!



Justin Martin
(@thefrozenfire)



Mark Roddy (@mroddy5280)



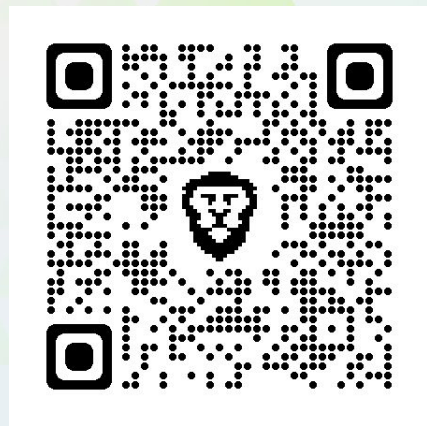
Thank you!

Brian Wilkes

Your title, your organization

email@emailaddress.com

@outsideranalytics



Project Github