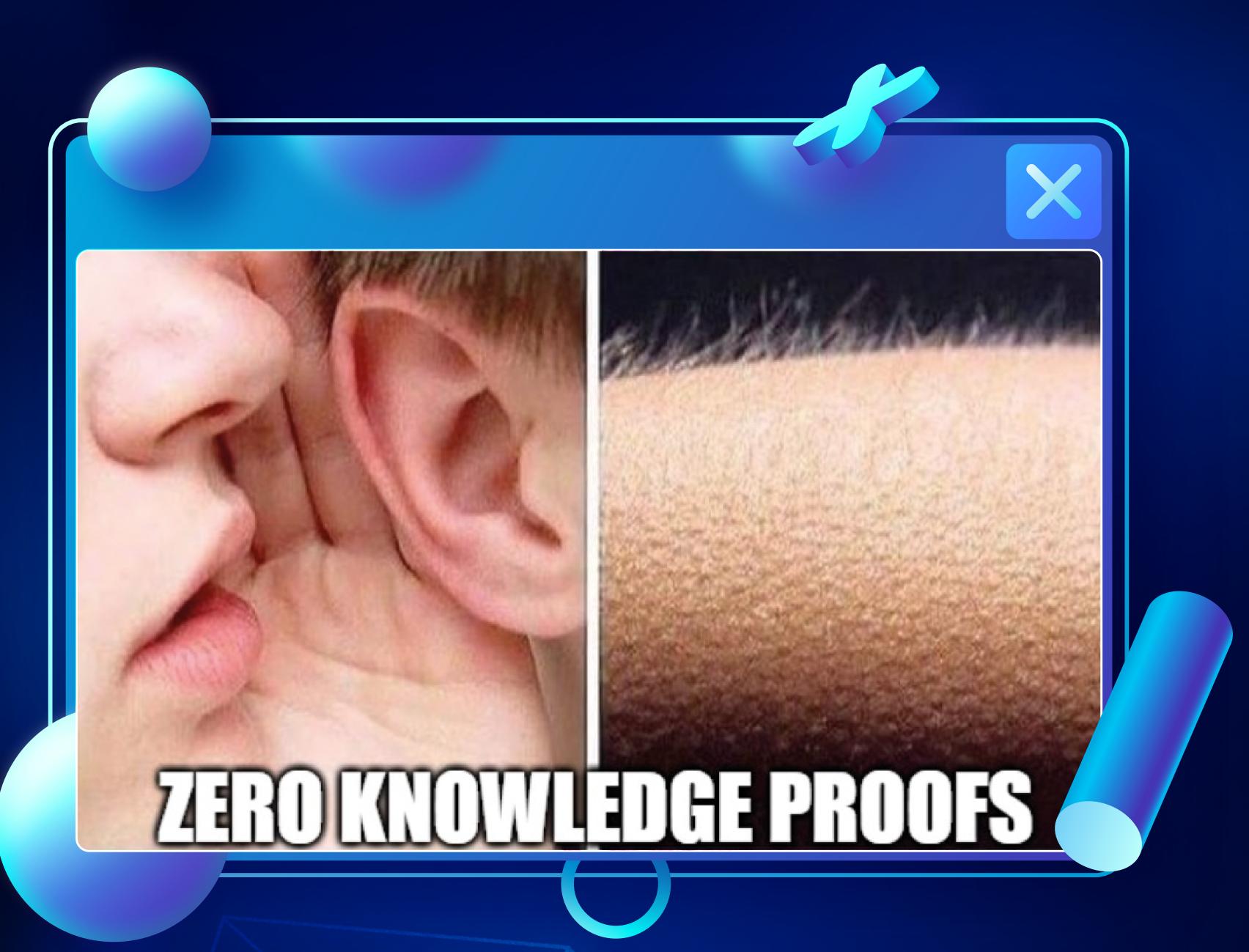


HYBRID ROLLUPS

A LOOK INTO THE FUTURE









BACK TO THE FUNDAMENTALS

Scalability



Blockchain Trilemma

Security







HOW TO SCALE: ROLLUPS



Rollups are Layer 2 scaling solutions for blockchains that perform transaction execution outside the main Ethereum chain (layer 1), but post transaction data on it



Feature	ZK Rollups	Optimistic Rollups
Core Technology	Zero-Knowledge Proofs (zk-SNARKs or zk-STARKs)	Fraud Proofs
Transaction Processing	Off-chain with a cryptographic proof of correctness	Off-chain, assumed correct unless challenged
Data Availability	Data necesary for reconstructing transactions is posted on chain	State changes are posted on-chain, allowing for later verification
Finality	Immediate upon proof verification	Delayed, contingent on a challenge period
Security Model	Cryptographic proof ensures all transactions are valid	Transactions are considered valid if no fraud proof is submitted during the challenge period
Challenge Period	Not applicable (no challenges due to upfront proof)	Exists, typically ranging from several hours to a week
Computational Intensity	High (due to the complexity of generating ZK proofs)	Lower (no complex proofs required)
Privacy	Enhanced (transaction details are not disclosed)	Standard (details are not disclosed, but no enhanced privacy compared to ZK Rollups)
Scalability Impact	High (efficient use of blockchain space and quick finality)	Moderate (efficient, but finality delay reduces throughput)
Use Cases	High-value transactions, privacy- centric applications	General applications where immediate finality is not critical

TYPES OF ROLLUPS



WHAT ARE HYBRID ROLLUPS?

Scalability & Efficiency

Optimistic Rollups

Assumed Validity

Hybrid Rollup

Integrates
Optimistic &
ZK Rollups
Features

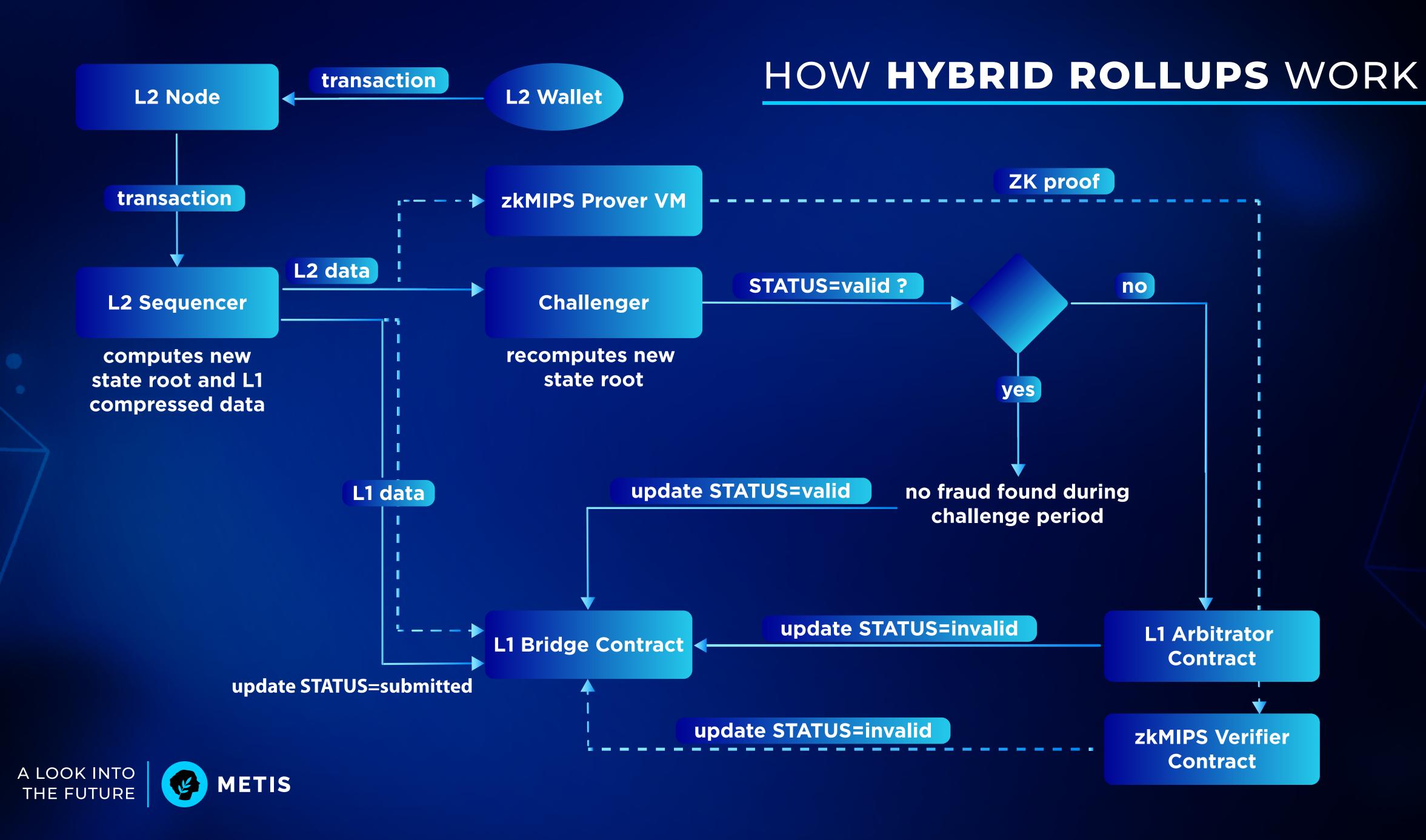
ZK Rollups

Immdiate Finality

Blockchain

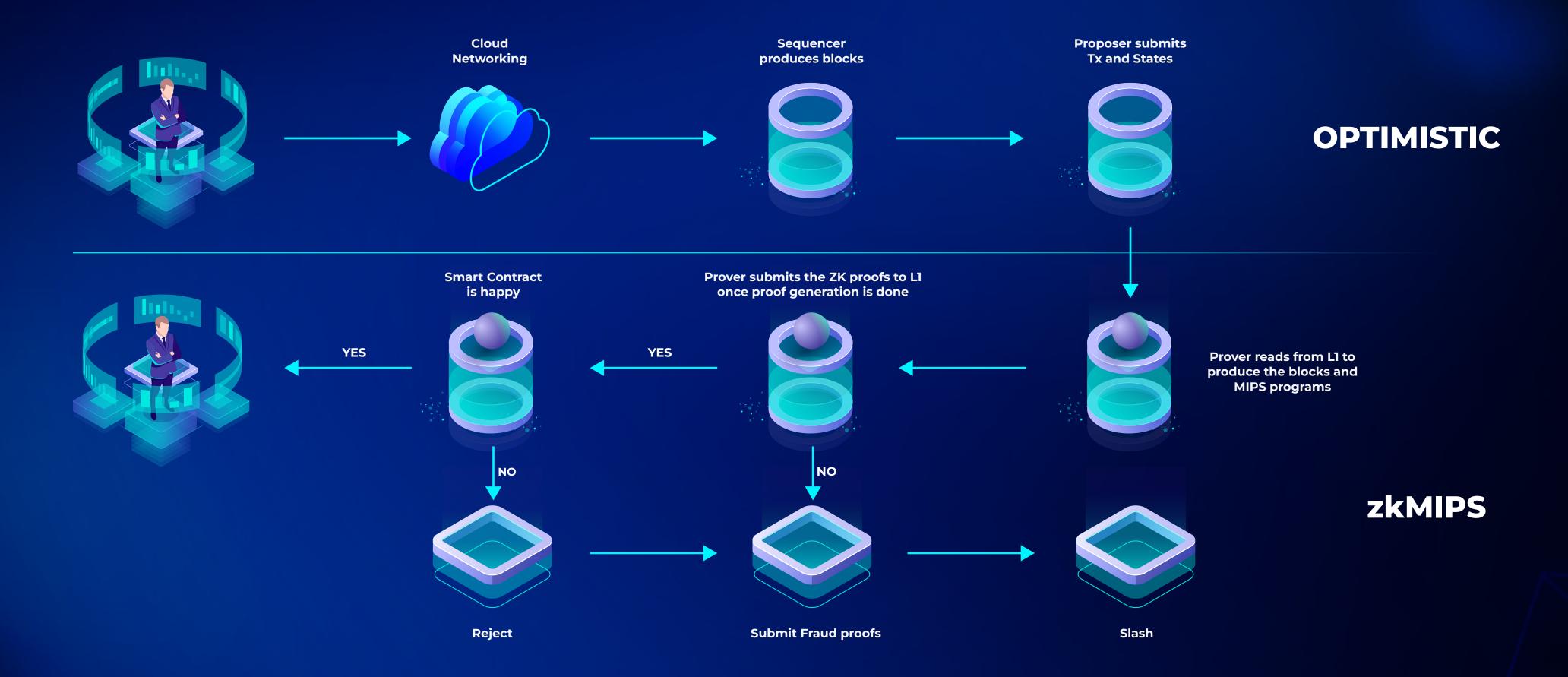
Layer (Layer 1)





HYBRID ROLLUPS IN PRACTICE





Improving the optimistic rollup architecture to expedite the process of withdrawals and dispute processes between verifier and the sequencer. In practice, that means changing the challenger contract to ZK Interactive Circuit

CURRENT OUTLOOK









IMPROVED EFFICIENCY



(HARD TO PREDICT)



BEYOND LAYER 2 AND BLOCKCHAIN



Alt L1s (BNB, Celo, etc.)



loT security (tamper-proof loT devices)



Cloud Computing



THANK YOU!



