
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

BLC302

Interoperability and bridging: Connecting blockchain networks

Rafia Tapia

Sr. Blockchain/Web3 Specialist Solutions Architect
AWS

Girish Dilip Patil

Head of Tech, DNB, ASEAN
AWS

Agenda

- What is blockchain interoperability?
- Interoperable solutions techniques
- Interoperability through bridges
- Scalability and interoperability
- Fabric & Ethereum interoperability via Amazon Managed Blockchain

What is blockchain interoperability?

Blockchain interoperability is the ability of two or more **blockchains to communicate and share data with each other.**

Interoperability is achieved through cross chain communication protocols.

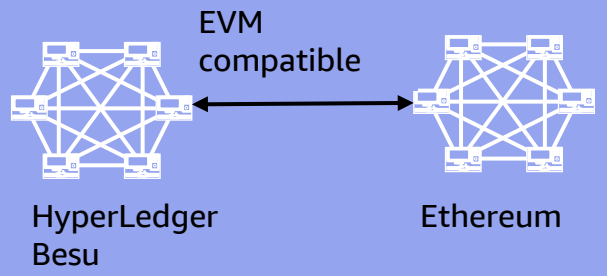
Two types of blockchain interoperability:

- Digital asset exchange
- Exchanging arbitrary data

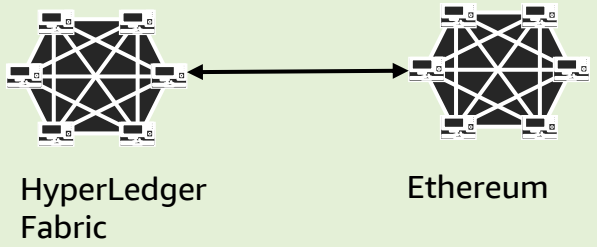
Blockchain interoperability can be between:

- Homogeneous blockchain
- Heterogeneous blockchain

Homogeneous blockchain



Heterogeneous blockchain



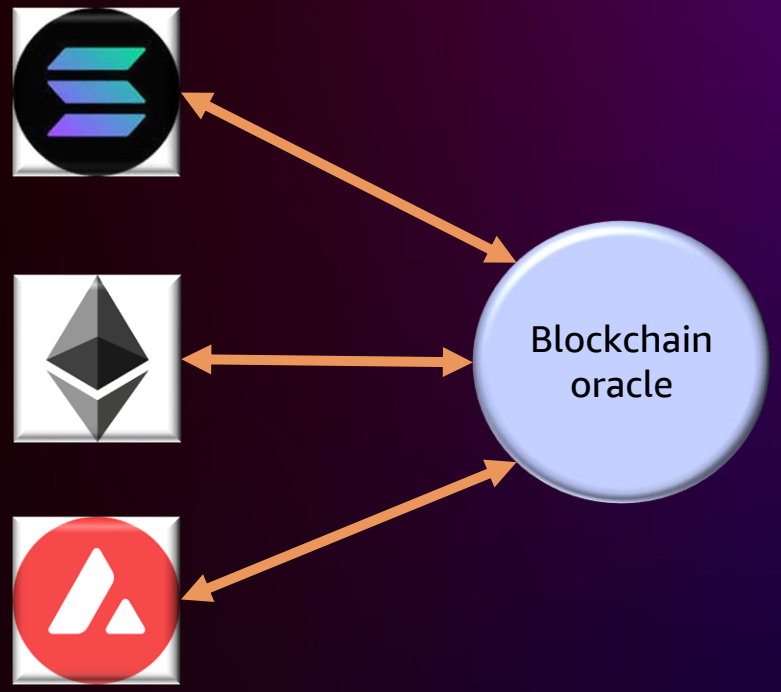
Interoperable solution techniques

- Oracles
- Notary schemes
- Atomic swaps/HTLC
- Sidechains/relays
- Blockchain of blockchains

Interoperability through oracles

Oracles connect smart contracts with off-chain data and services.

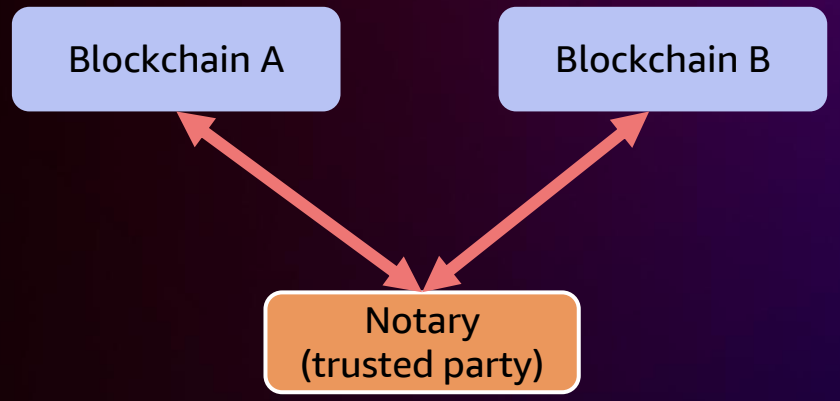
- Initial solution to blockchain interoperability was provided by oracles
- Interoperability solutions provided by oracles have several disadvantages
  a) Using centralized oracles removes the advantages of decentralization
  b) Security risks are associated with oracles



Interoperability through notary scheme

This technique involves a trusted central entity called notary that monitors multiple chains, triggering transaction in a chain upon an event taking place on another chain.

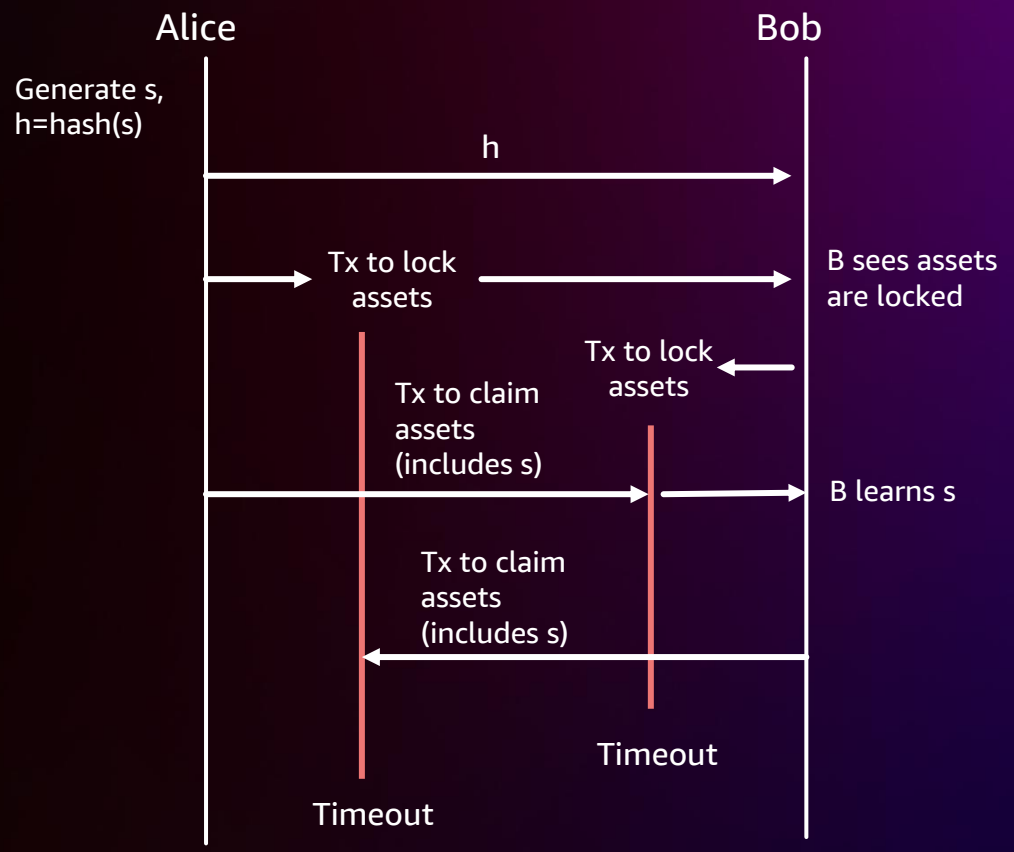
- Simple to implement
- Centralized exchanges like Coinbase are common examples of notary schemes
- A notary scheme is solely dependent on the honesty of the notary
- Interledger Protocol (ILP)



Interoperability through atomic swap/HTLC

An atomic swap allows exchange of assets from one blockchain to another without a third party.

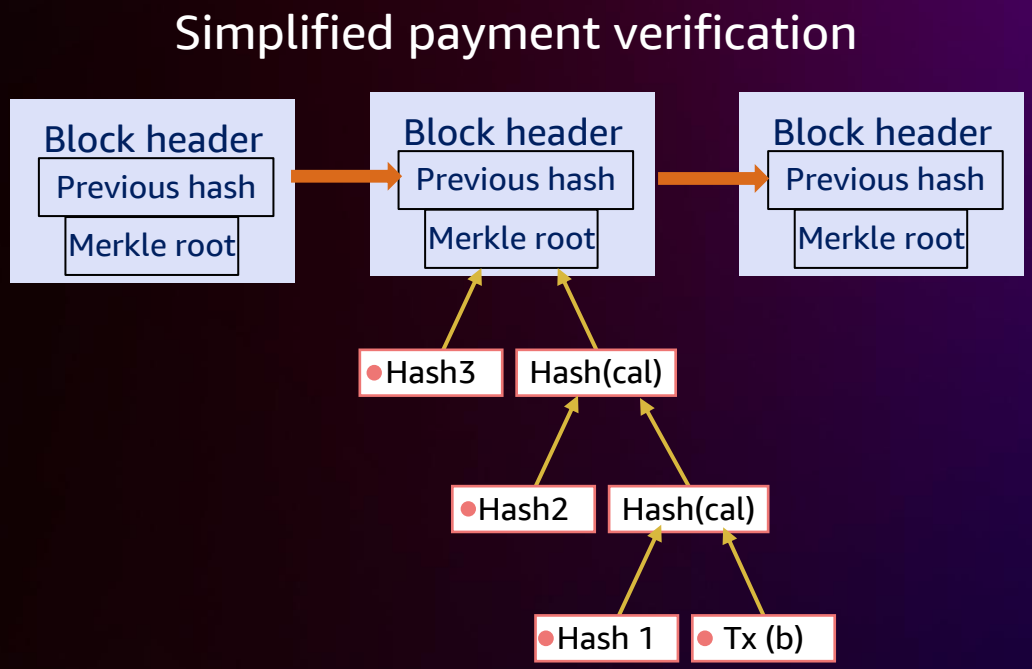
- An atomic swap gives control to token owner and removes centralized intermediaries' exchanges in transferring their tokens
- An atomic swap guarantees that either an exchange of assets happens completely or it does not happen at all
- Atomic swaps use hash time-lock contracts to automate the exchange



Interoperability through sidechains/relays

A sidechain is a blockchain that has the ability to read data from another blockchain, called mainchain, and is used to facilitate cross-chain asset portability.

- Transfer of assets between mainchain and sidechain happens via two-way pegs
- Simplified payment verification (SPV) is used to implement two-way peg between sidechain and mainchain
- Relay is an SPV client for a source blockchain running on a target blockchain
- BTC Relays allow bitcoin transaction verification on Ethereum

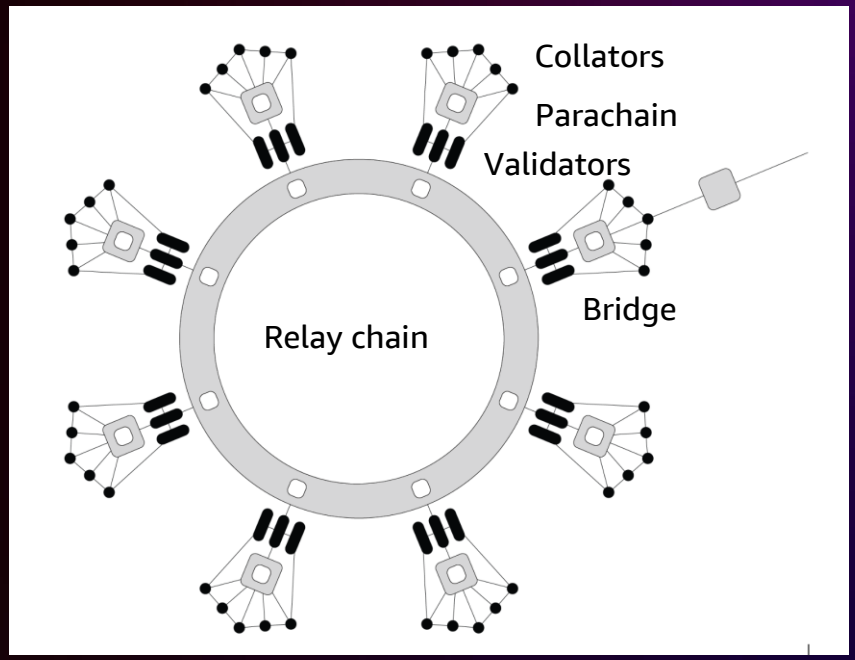


Interoperability through blockchain of blockchains

Blockchain of blockchains are frameworks that provide reusable data, network, consensus, incentive, and contract layers for the creation of application-specific blockchains that interoperate between each other.

- Blockchain of blockchains implementation is similar to relays and sidechain as there is a mainchain that application-specific sidechains connect to
- PolkaDot and Cosmos are two such implementations

PolkaDot design



Interoperability through bridges

A blockchain bridge is a connection between two blockchains that allows the transfer of arbitrary data and/or tokens from one chain to another.

Classification of bridges based on how they work

Trusted bridges: use a central authority for their operations

Trustless bridges: remove the role of the trusted third party through the use of smart contracts

Classification of bridges based on what they connect

L1 <> L1: connect different L1 blockchains with each other.

L1/L2 <> L2: connect the L1 with different L2 solutions and the L2s with each other

Interoperability through bridges

Classification of bridges based on how they move assets

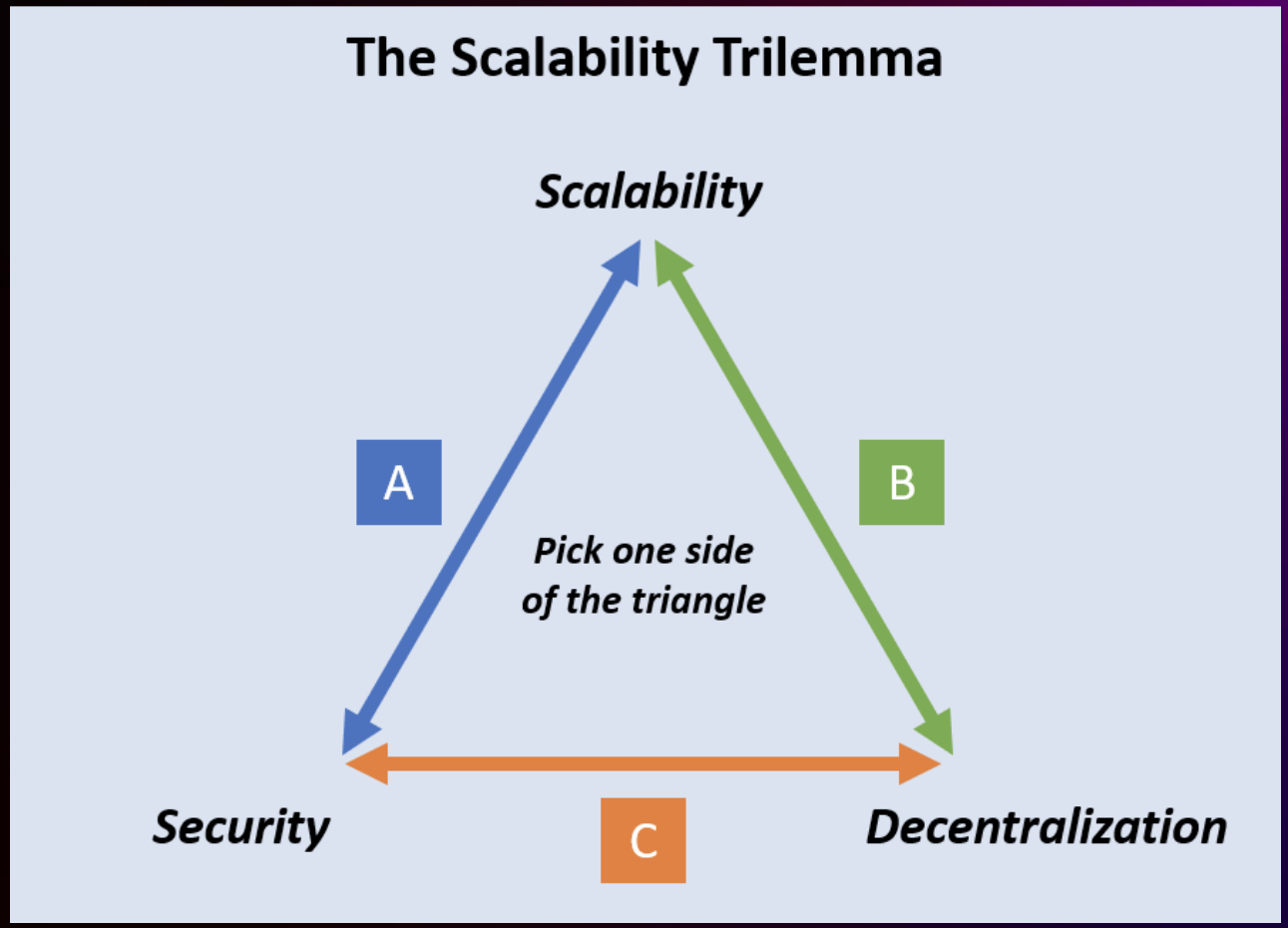
1. Lock & mint: Polygon's PoS bridge, Avalanche Bridge (AB)
2. Burn & mint: Hop, Across
3. Atomic swaps: cBridge, Connext

Key components to most bridge designs

1. Monitoring
2. Message passing/relaying
3. Consensus
4. Signing

Scalability and interoperability

Since scaling L1s is hard, L2s and sidechains are operated to move assets and conduct transactions with low transaction speeds and fast confirmations



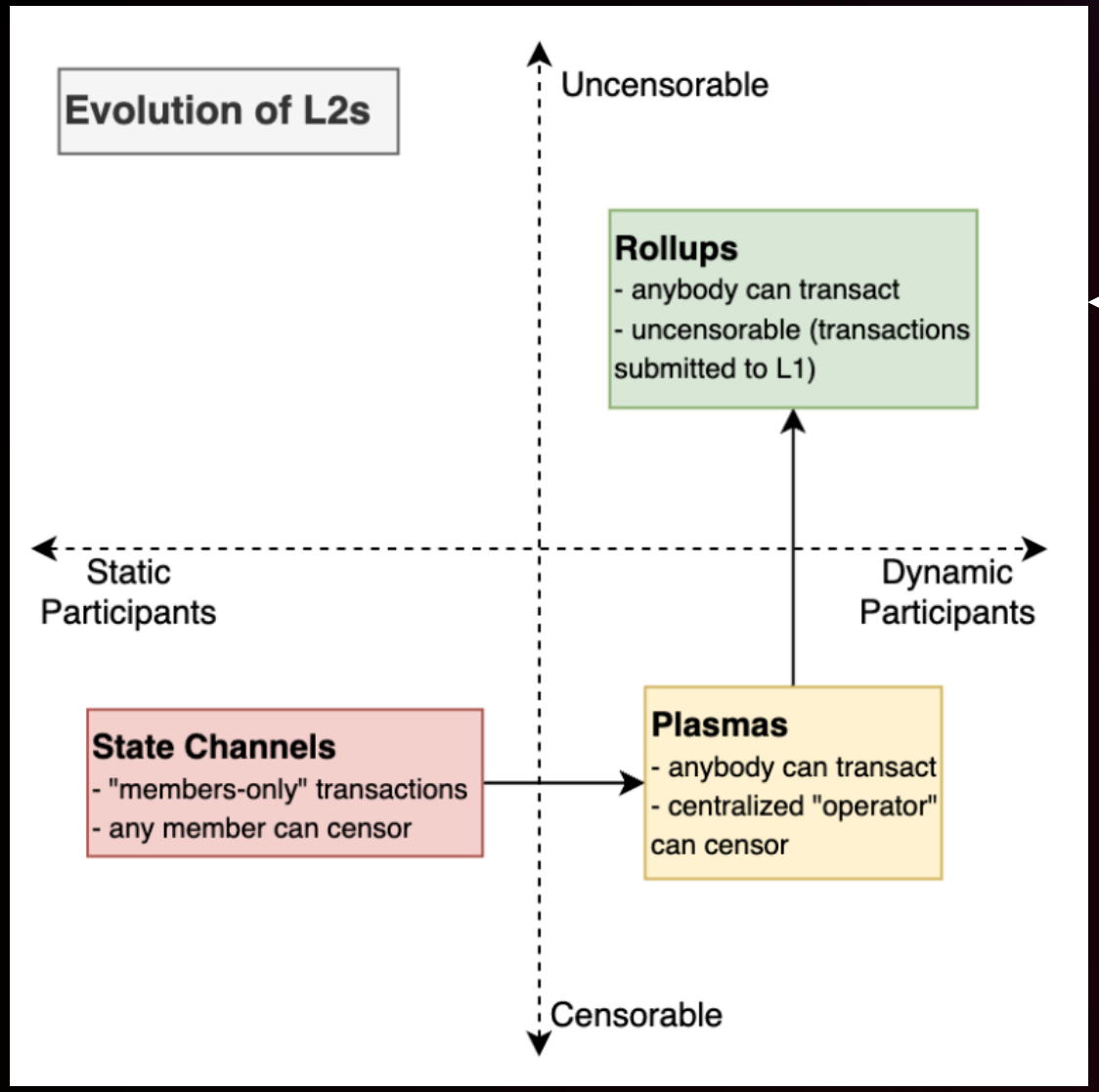
Sidechain vs. L2s

Sidechains have their own security mechanism

L2s depend on parent chain's security mechanism, hence are more secure

In general, sidechains like **Polygon** typically have more throughput than **L2s like Optimism, Arbitrum, ZKSync, StarkNet**

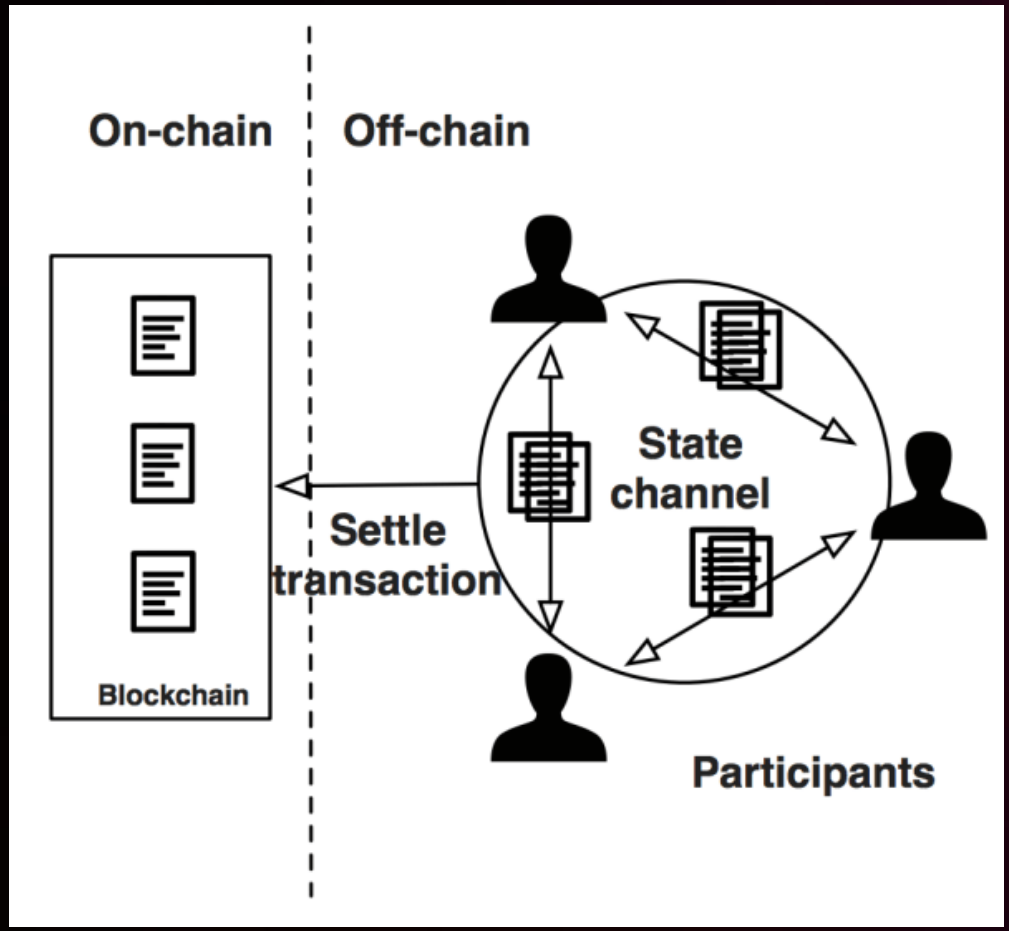
Evolution of L2s



← Best of both worlds!

We shall focus more on rollups

State channels

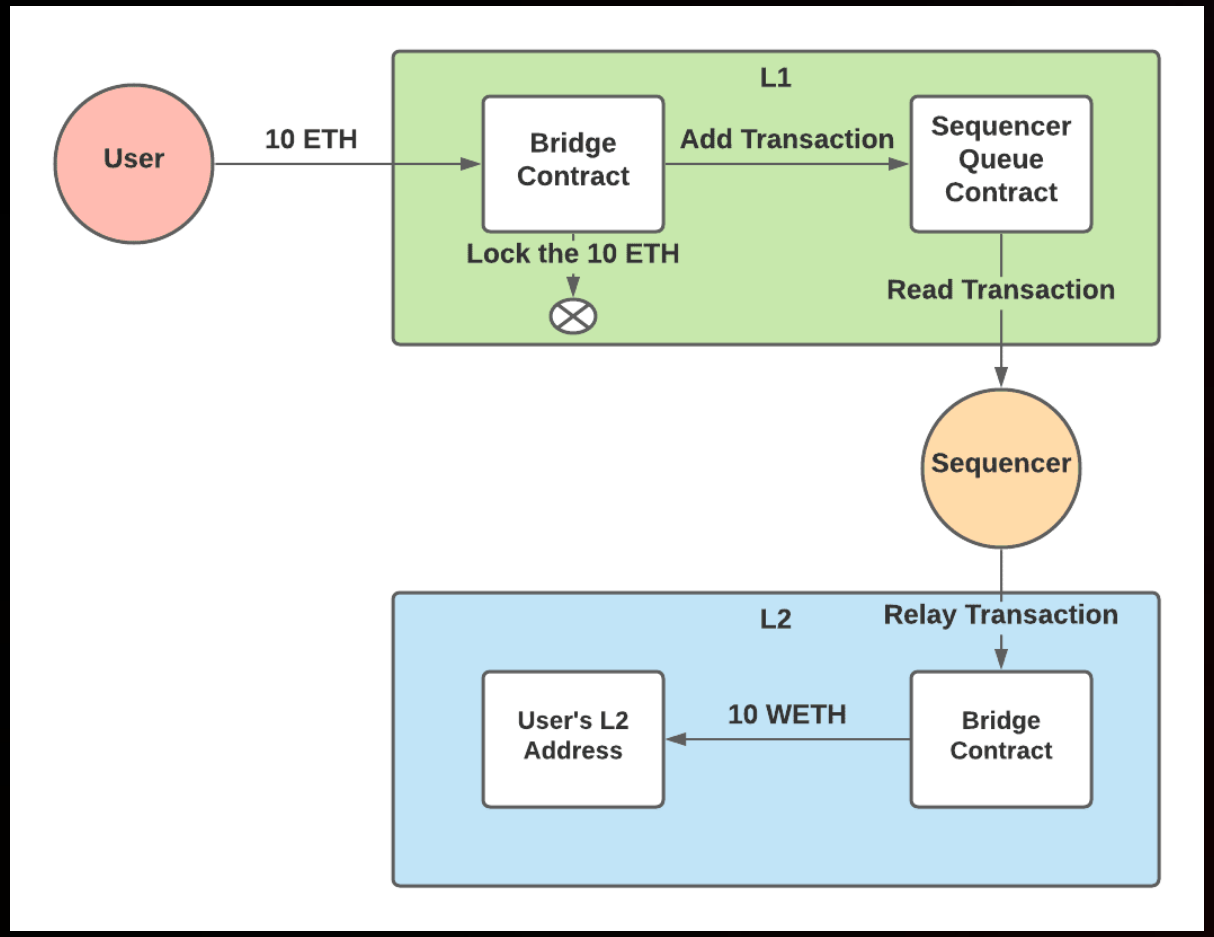


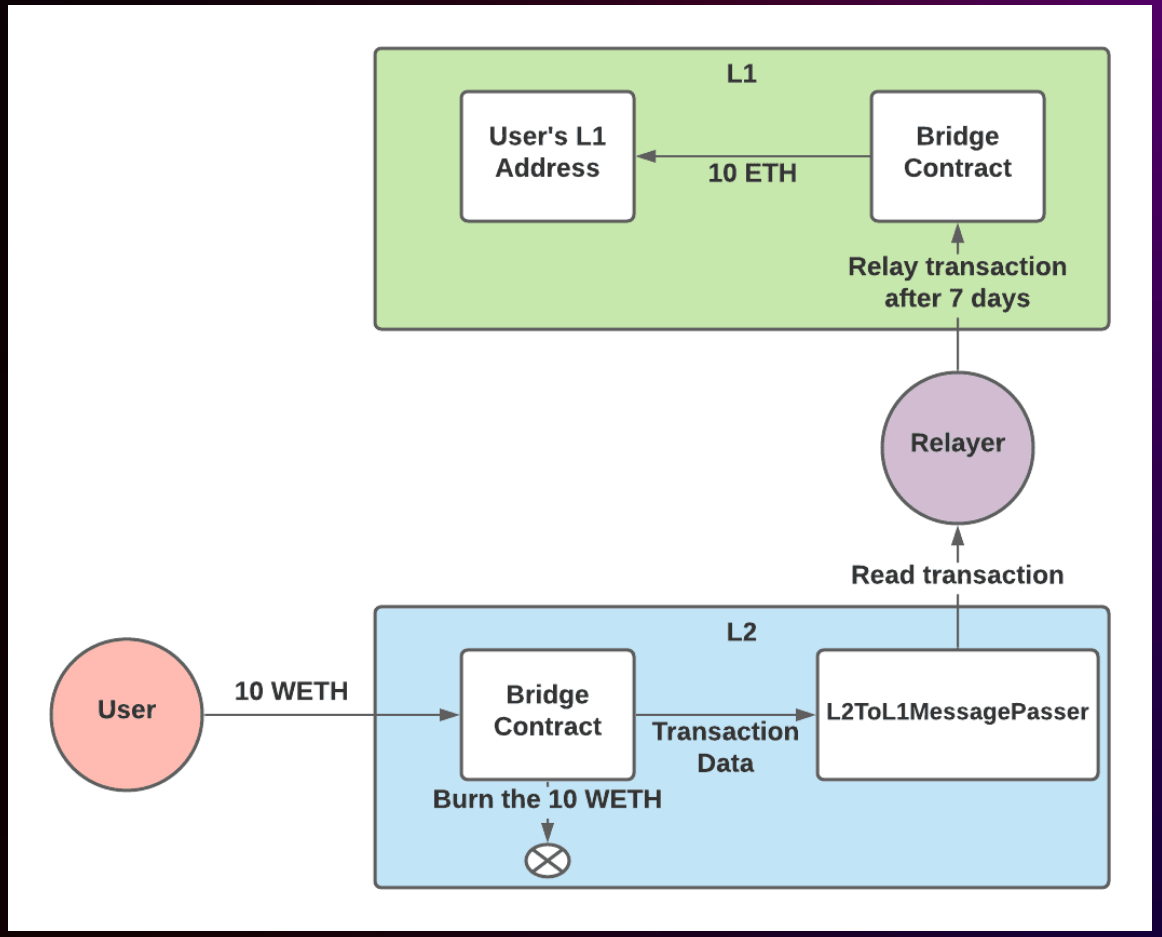
Plasma

A plasma chain is a separate blockchain that is anchored to the main Ethereum chain and uses fraud proofs (like optimistic rollups) to arbitrate disputes.

We shall discuss fraud proof later.

Rollups: L1 <-> L2 value movement





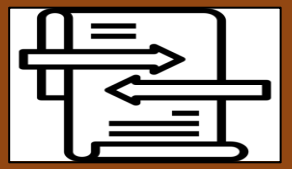
Naïve scheme

How to represent large datasets efficiently

L1

Merkle Root: Hash ABCDEFGH

Cheap logs



Smarter scheme

L2

Data A	Data B	Data C	Data D	Data E	Data F	Data G	Data H

Rollup types

1. Optimistic rollups
2. Zero knowledge (ZK) rollups

Optimistic rollups (fraud proofs)

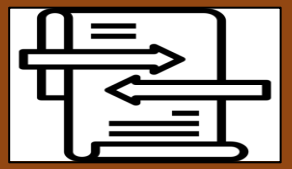
“Assume everyone is honest until proven otherwise.”

L1

Merkle Root: Hash ABCDEFGH

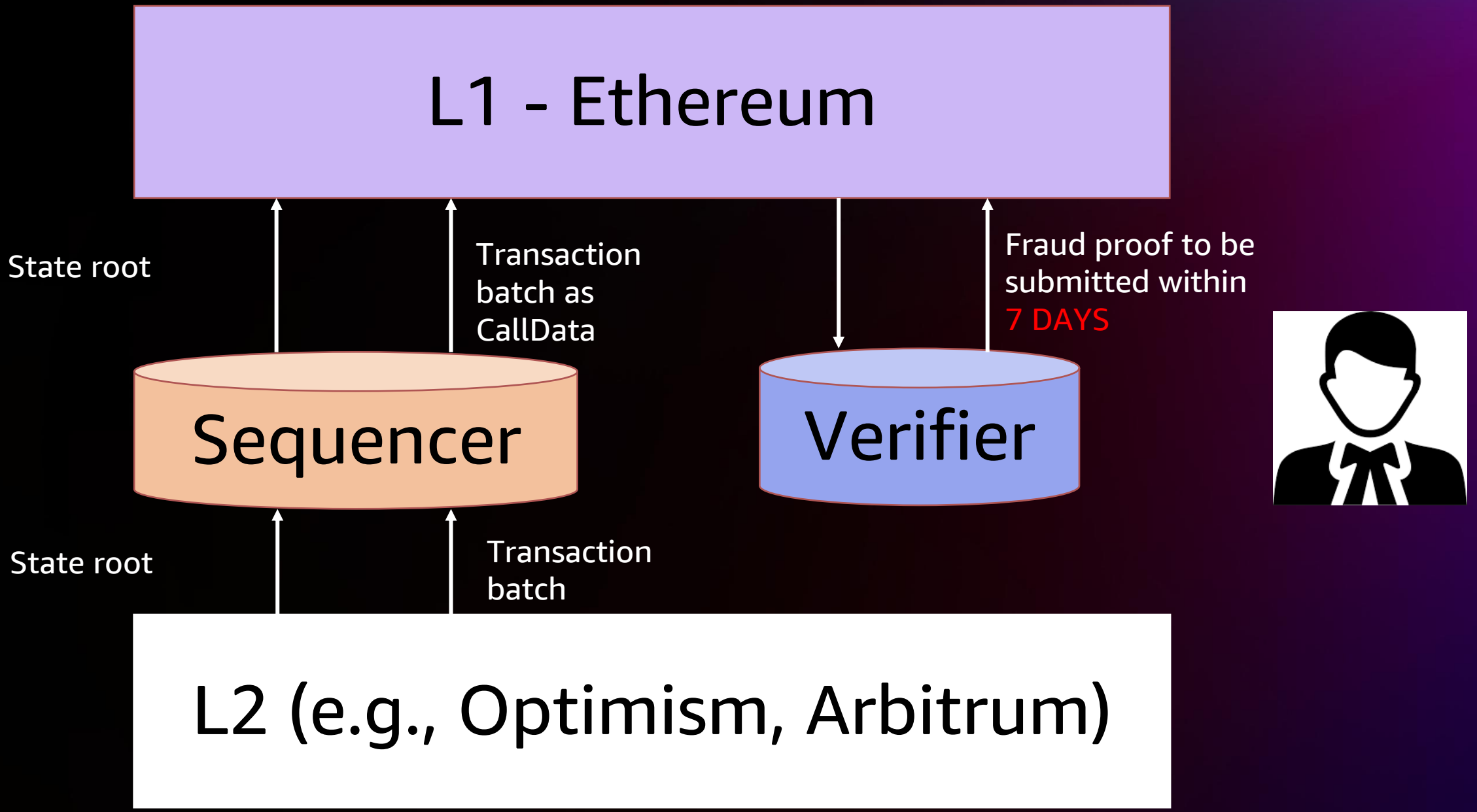
Verification through fraud proofs (7 days)

Cheap logs



L2

Data A	Data B	Data C	Data D	Data E	Data F	Data G	Data H



Zero knowledge rollups (validity proofs)

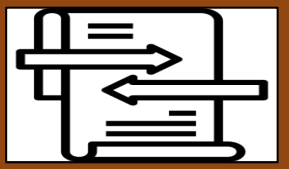
“Assume everyone can be dishonest, trust no one but maths!”

L1

Merkle Root: Hash ABCDEFGH

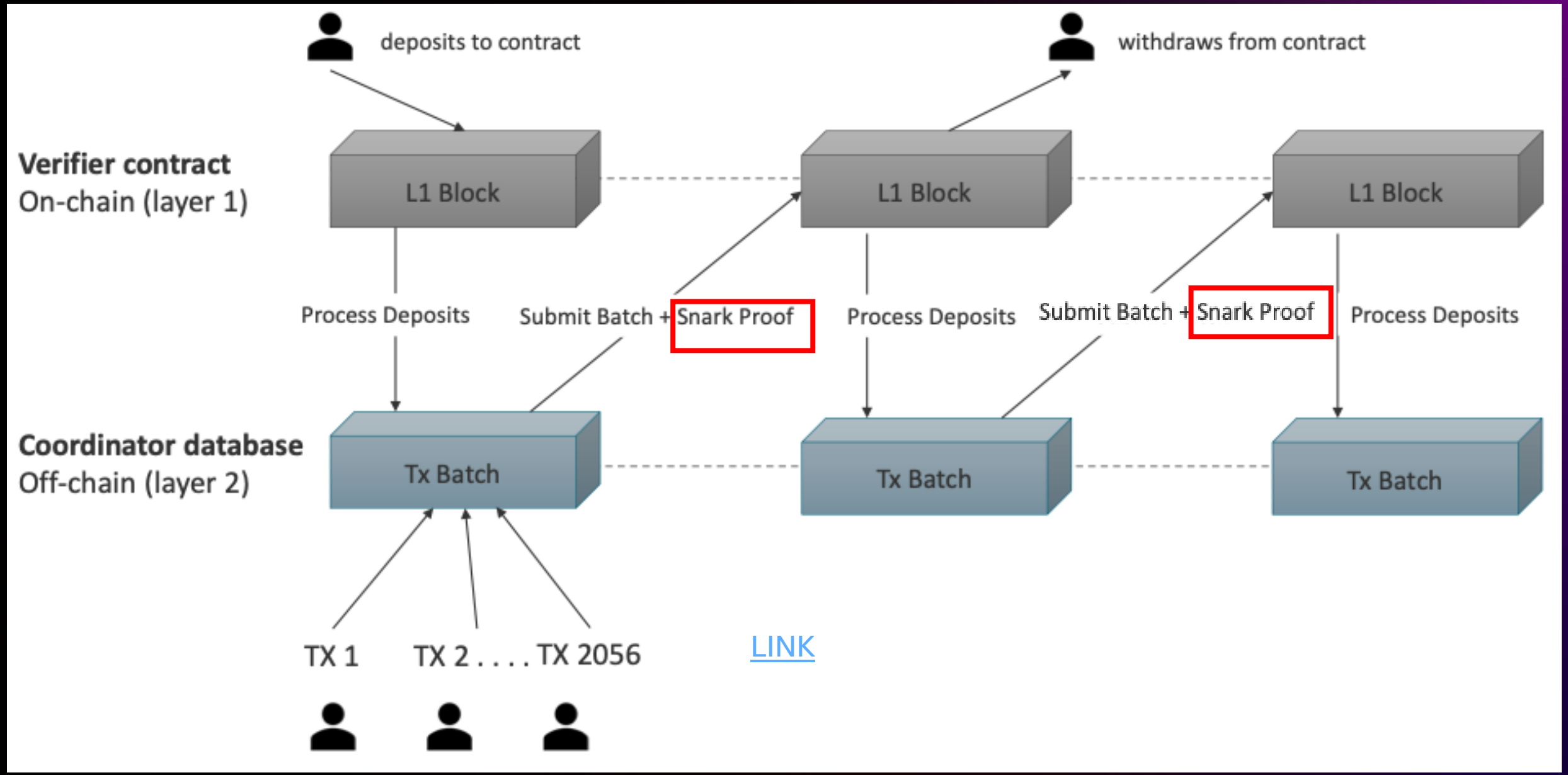
Instant verification through validity proofs

Cheap logs

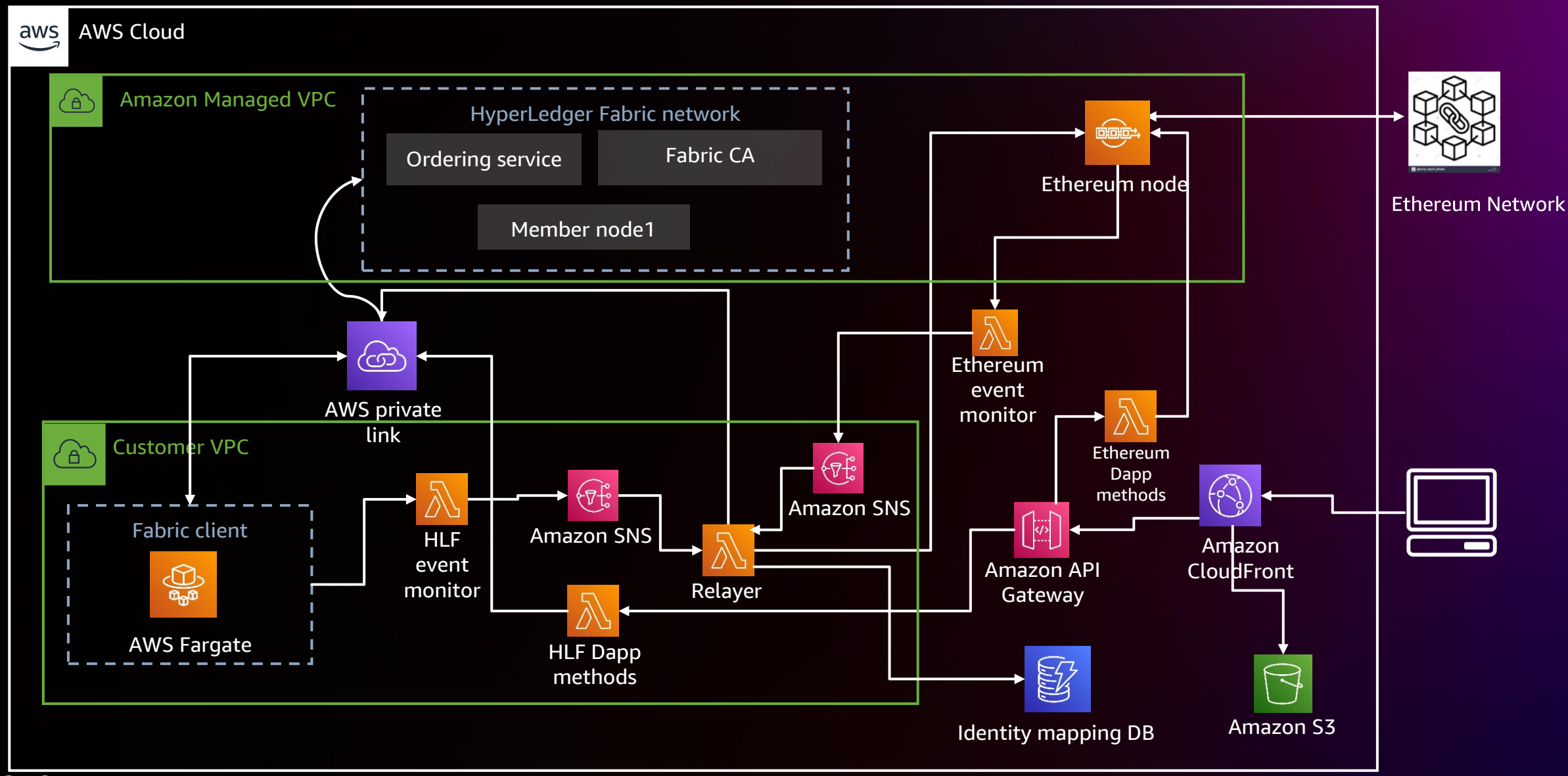


L2

Data A	Data B	Data C	Data D	Data E	Data F	Data G	Data H



Reference architecture: Fabric & Ethereum bridge via Amazon Managed Blockchain



Thank you!

Rafia Tapia
taprafia@amazon.com

Girish Dilip Patil
girpatil@amazon.com

Please complete the session survey in the **mobile app**