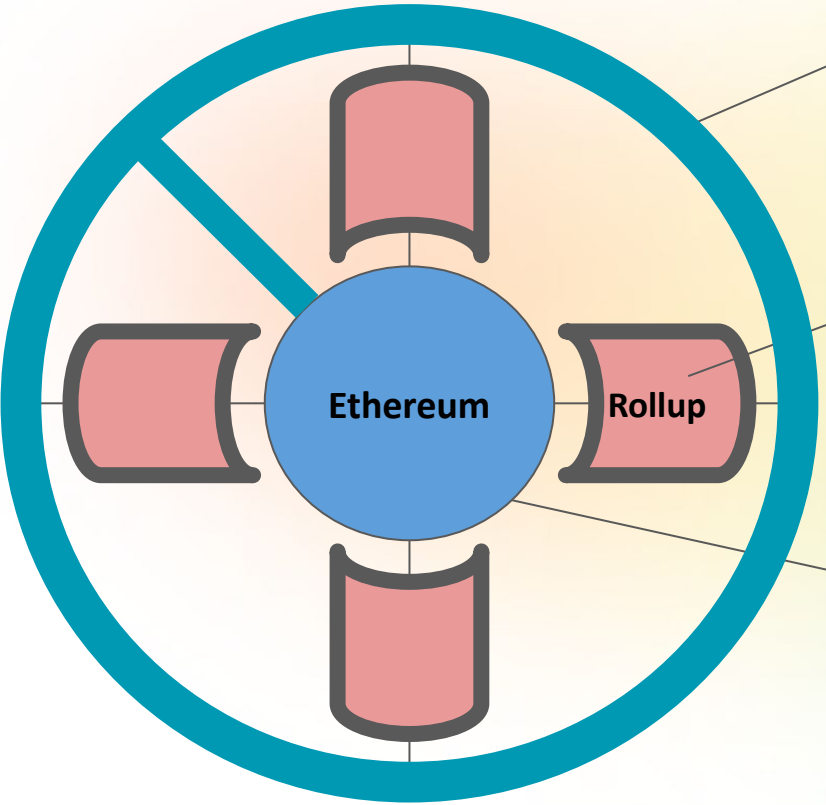

INTMAX
DC7
SEA

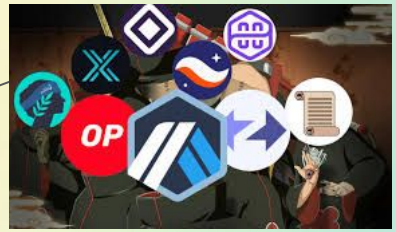
Transfer Layer of Ethereum
Stateless Layer of Ethereum

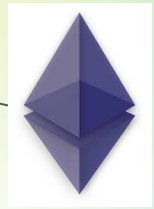
Stateless layer of Ethereum = Transfer Layer

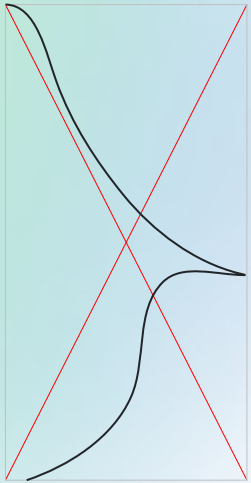


INTMAX

Stateless Layer
with Extreme Scalability
and Full Privacy



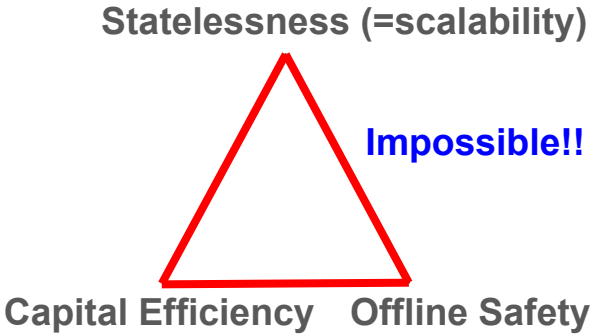


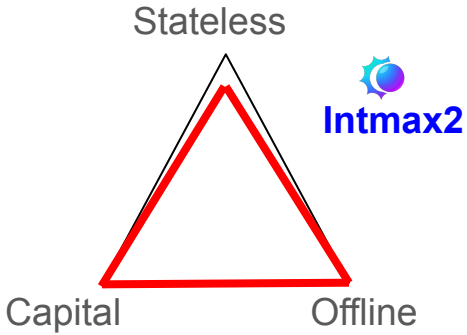


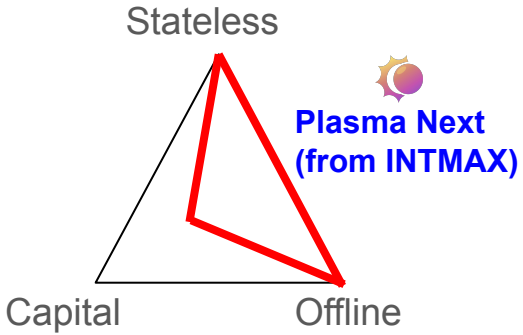
Stateful Layer
with a lot of
functionalities

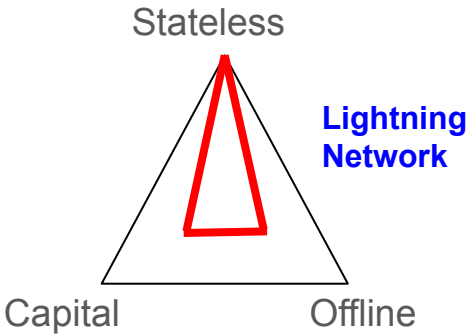
INTMAX

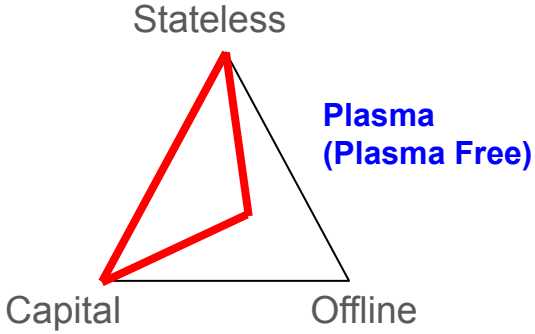
Stateless Trilemma

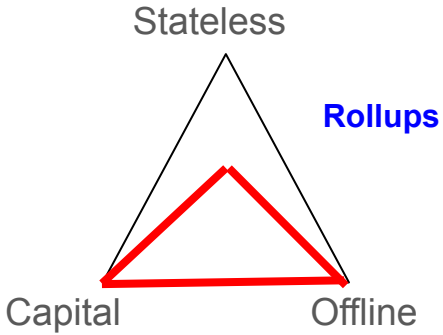




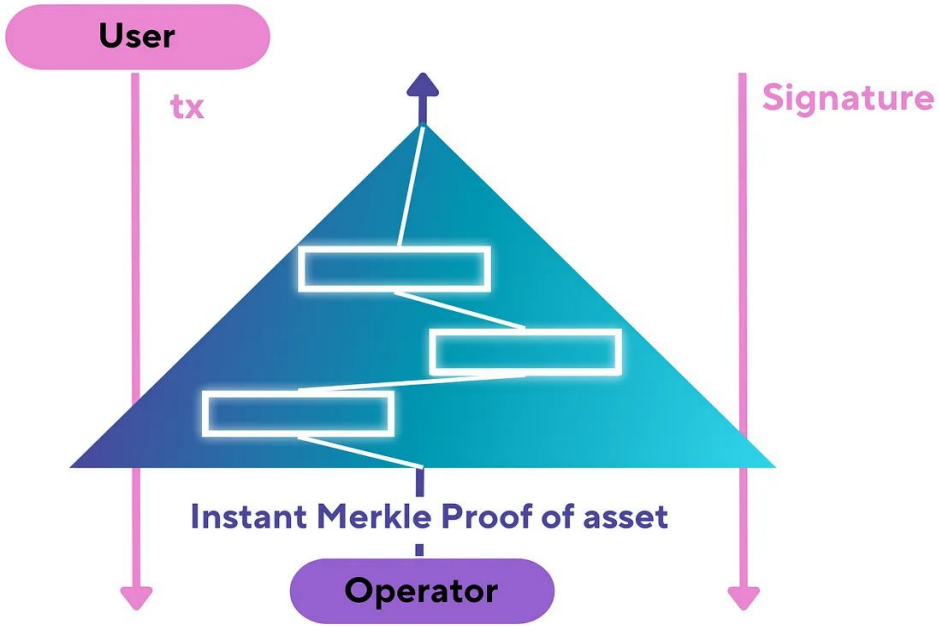








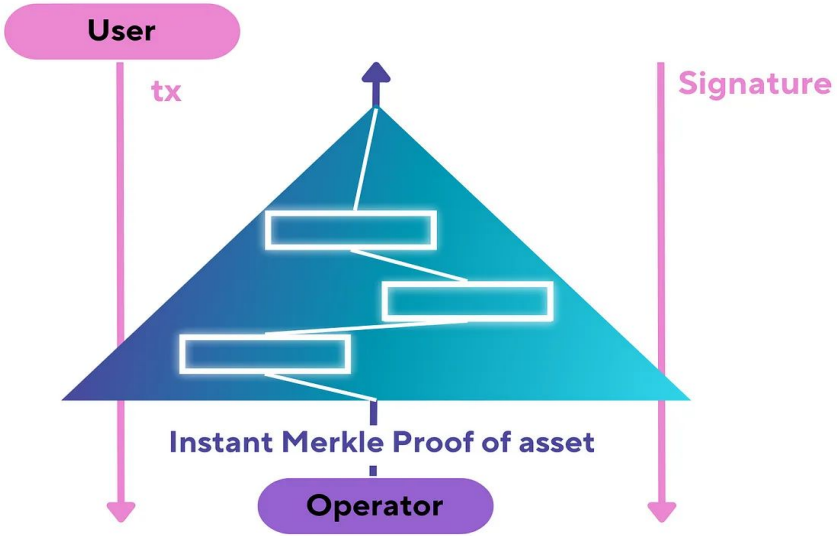
1. Safe proof (UTXO) distribution to avoid DA costs.
   Let's say the Merkle proof itself is UTXO.

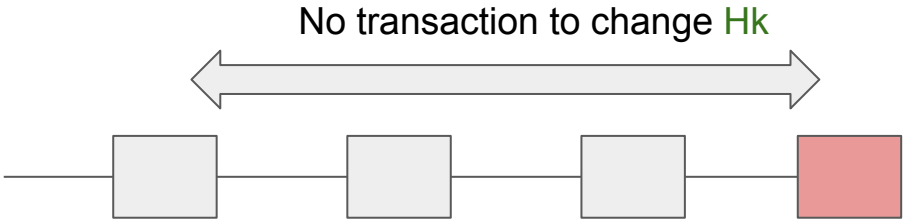


Intmax2 = Client-side UTXO with Infinite Recursive ZKP

Proof updates without online requirement

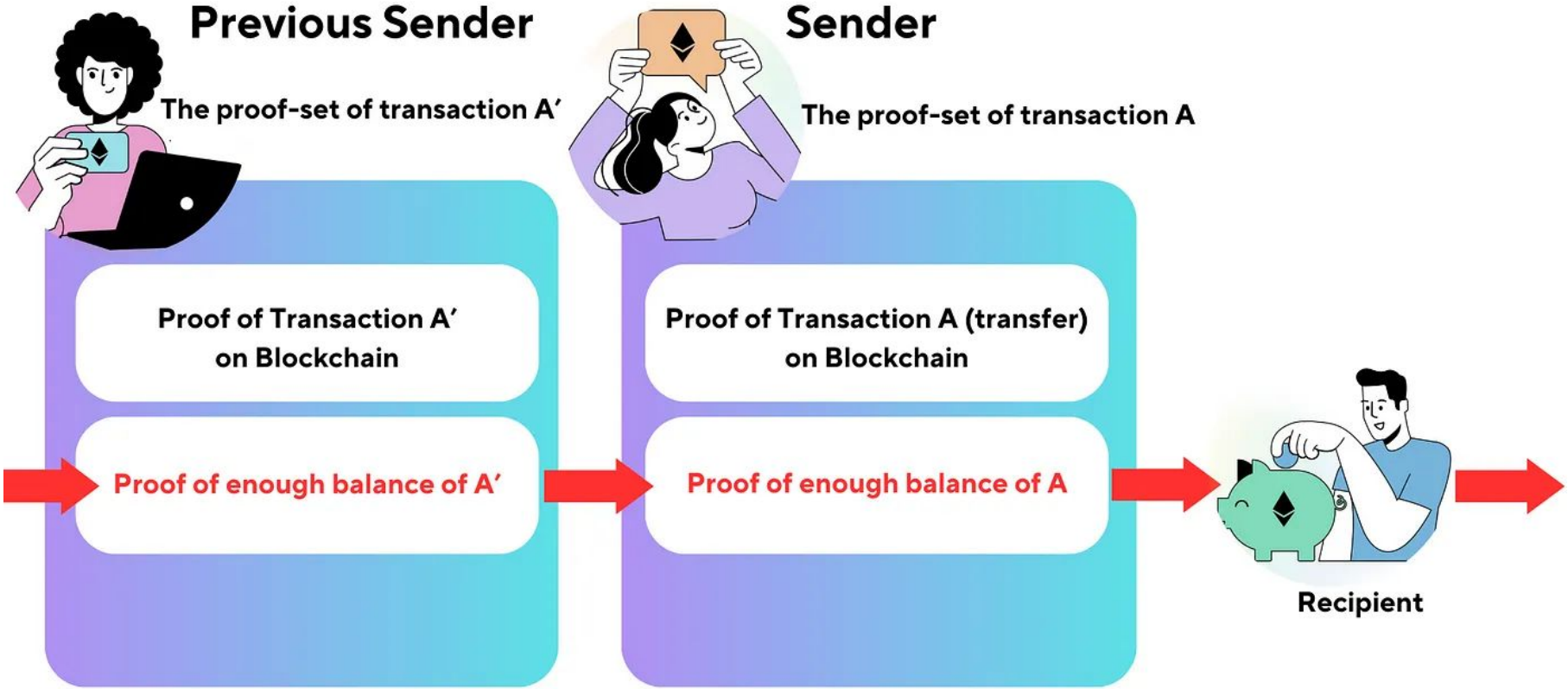
One example is signing back + proof of no transaction (by SMT)



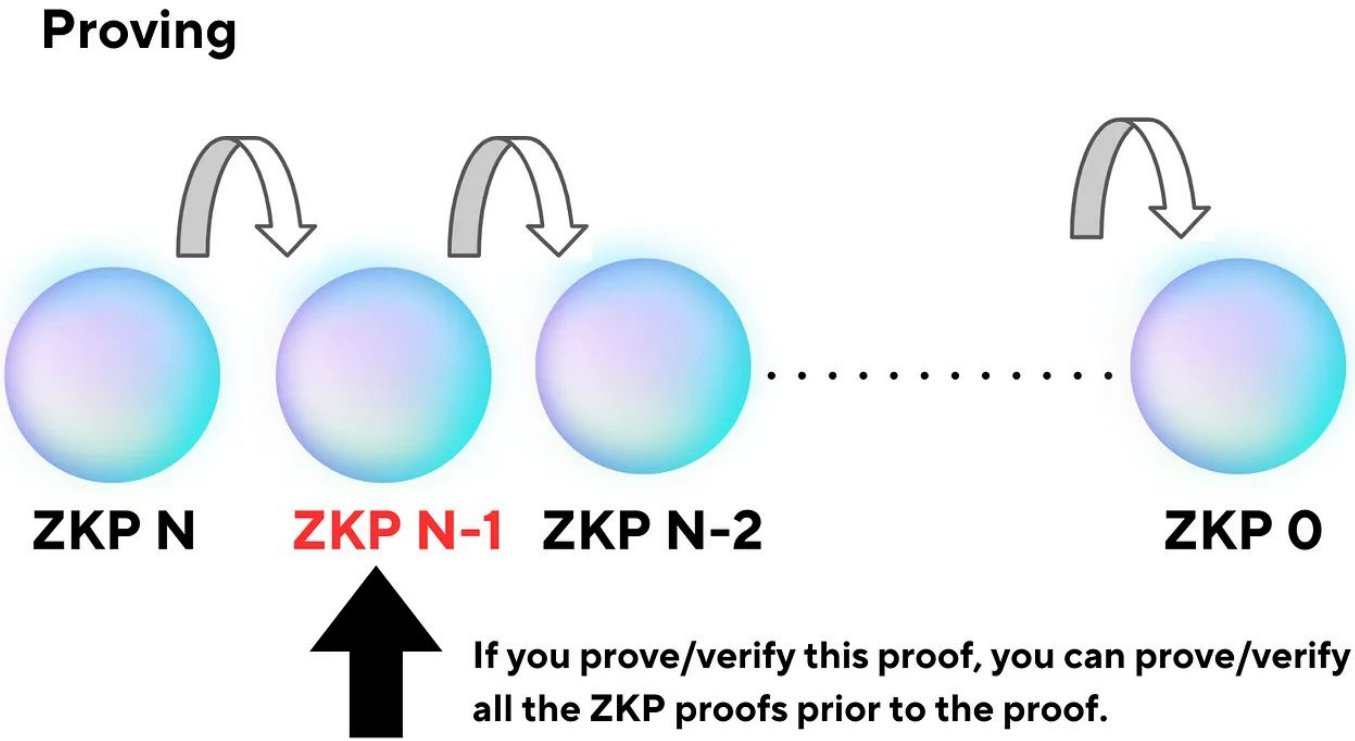


it consumes 5 bytes for each user.
But each user can put 10K transfers to one tx without additional bytes.

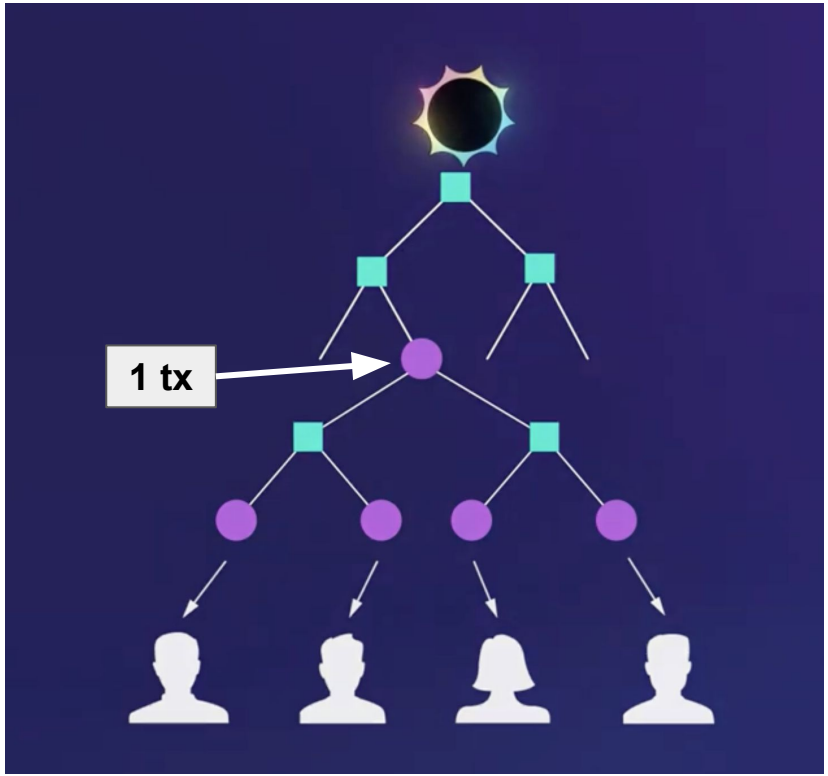
2. A sender sends ZKP & Merkle proof of a UTXO to recipients



3. Each client side UTXO gets Mina-style ZKP proving/verification



4. Each tx consumes 5 bytes onchain-cost, but it can include an unlimited number of transfers



If we set the sender of the aggregated transaction as a proxy.

Many senders can share the 5 bytes cost. It makes the complete statelessness.

5. Intmax2 is a Based Rollup

- Interoperable with other Rollups
- Helping all L2s to be one big L2

“Impossibility of Stateless Blockchain”

~Limits on revocable proof systems, with applications to stateless blockchains~

・What they stated is correct.

“the system must either have a linear-sized global state or require a near-linear rate of local proof updates”

Q: How do we avoid that problem?

A: Making local proof updates less critical.

Proof updates without online requirement or with less online requirement are the key.

Privacy Mining is a social experiment.
Please join this and Become a Miner.