Monero + L2

HOW A SIMPLE LAYER TWO CAN BENEFIT MONERO AND ITS USERS

Seth For Privacy

@sethforprivacy

MONERO CONTRIBUTOR

Contributing to Monero for the past 2y in mostly non-dev roles

PRIVACY EDUCATOR

Building out pro-privacy education, guides, and resources, including the Opt Out podcast

Why does Monero need an L2?

03

Privacy via ephemerality

DEFEATS PASSIVE SURVEILLANCE

Surveillance can only be done actively, not via simple chain analysis.

REDUCES METADATA

Removes common metadata heuristics like transaction time, spend patterns, etc.

REDUCES FUTURE RISKS

As transactions are ephemeral, future tracing breakthroughs are less impactful.

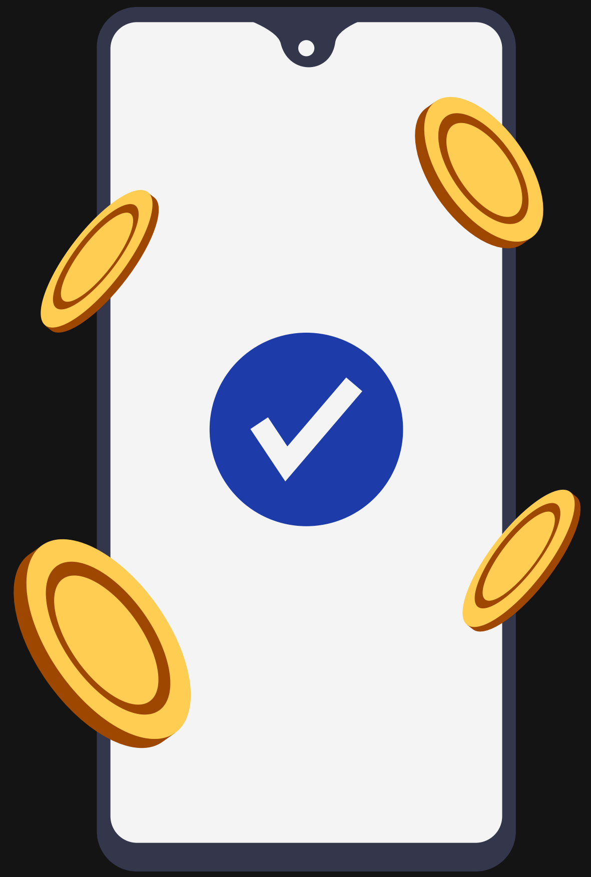
Improved payments

FURTHER ENABLE MONERO'S L1 SCALING

Leverage Monero's excellent L1 scaling to simplify L2 onboarding and UX.

REDUCED FRICTION FOR COMMERCE

Remove wait for confirmations and 10-block-lock.



Learning from Lightning

- LIGHTNING INHERITS PRIVACY AND SCALING ISSUES
- OVER-RELIANCE ON LN TO SOLVE SCALING + PRIVACY PROBLEMS
- NEED FOR LIGHTNING TO SUPPORT MAJORITY OF PAYMENTS LEADS TO OVERLY COMPLEX SYSTEM
- ON-CHAIN FEES + COMPLEX NETWORK LEAD TO CENTRALIZED ROUTING HUBS

Monero's unique benefits for L2s

On-chain privacy leads to far greater node-level privacy in a layer 2

Discovered payment channels reveal no extra information.

Social consensus enables enforcing fungible channel open/close TXs.

Base-layer is not reliant on fees, so we can move as much (or as little) off-chain as is helpful.

How we should differ from the Lightning Network

SIMPLE DIRECT-CHANNEL APPROACH

No need for all payments to be off-chain, so can focus on direct channels and not cross-network routing

ONLY USE L2 FOR TRUSTED PEOPLE OR FREQUENT SPENDS

Users can easily use L1 w/ low fees and strong privacy

IMPLEMENT STRONG RECEIVER PRIVACY FROM DAY 1

Leverage improvements like BOLT12, alias SCIDs, and route blinding

Current Approaches

- “PayMo: Payment Channels For Monero”
- “Sleepy Channels: Bitcoin-Compatible Bi-directional Payment Channels without Watchtowers”
- Universal Atomic Swaps: Secure Exchange of Coins Across All Blockchains
- "AuxChannel: Enabling Efficient Bi-Directional Channel for Scriptless Blockchains"
- MoNet: A Fast Payment Channel Network for Scriptless Cryptocurrency Monero

Conclusion

A simple payment-channel layer two network for Monero can be an important improvement that uniquely benefits from Monero's L1 approach.

Get in touch

EMAIL

seth@sethforprivacy.com

SIGNAL

616-326-4079

BLOG

sethforprivacy.com

TWITTER

@sethforprivacy