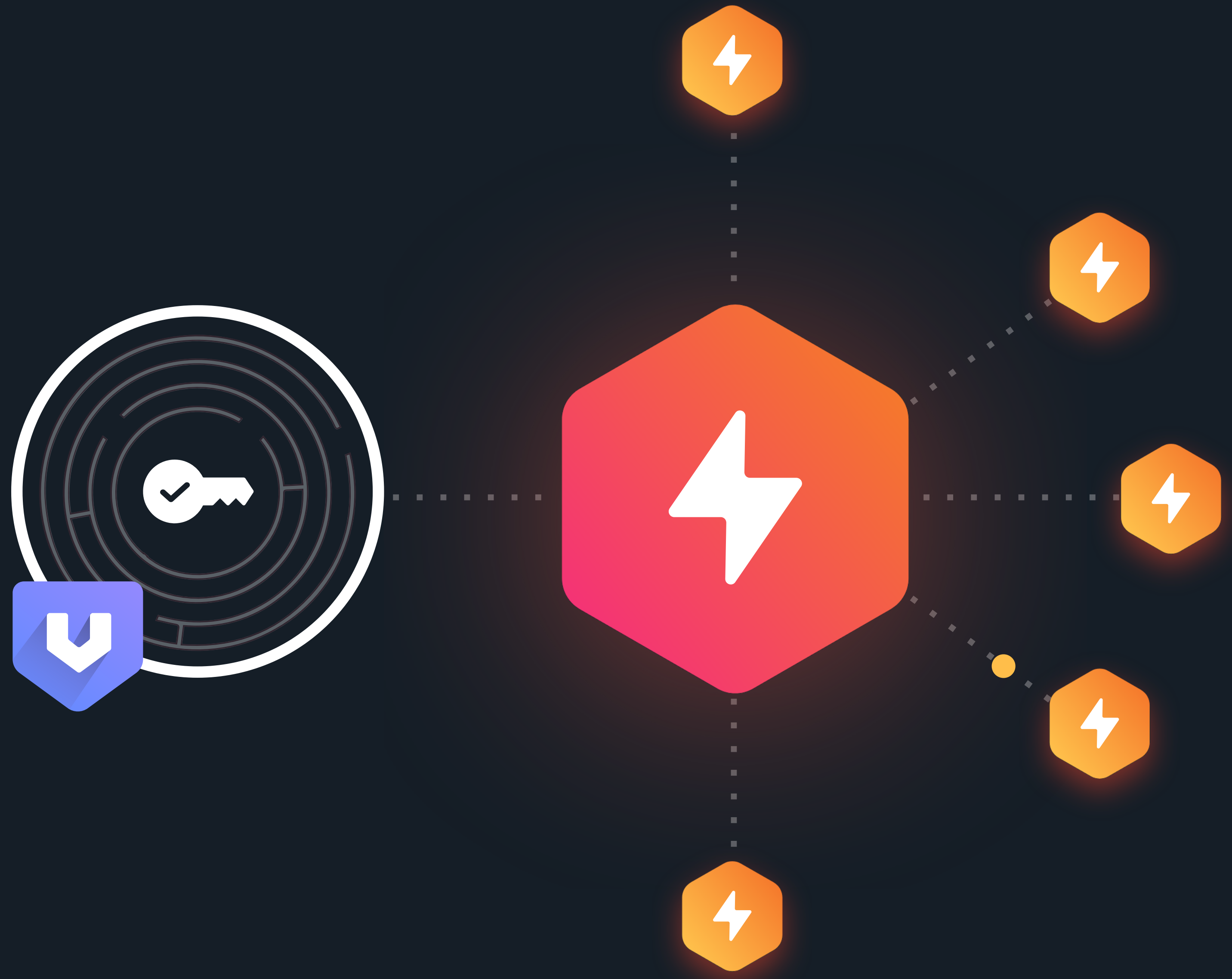
VLS

Improving Lightning node security



Bitcoin Lightning Network

Efficient Scaling: Lightning Network boosts Bitcoin's capacity and speed

Microtransactions: Enables small, low-fee transactions

Fast Payments: Delivers near-instant Bitcoin transactions

Bitcoin Lightning Network

On-chain multisig contracts between two channel peers, both need to stay online

Transactions between channel participants occur off-chain

If no direct route, payment routed via interconnected channels

Custody Challenges

As Bitcoin Lightning Network grows, so do security concerns

Most Lightning Nodes running on cloud hosting providers

Most Lightning users are using custodial apps

Security Challenges

Non-custodial LN users store private keys on their LN node

If LN node is compromised, an attacker can steal user funds

Blind signers do not validate transactions, reducing security

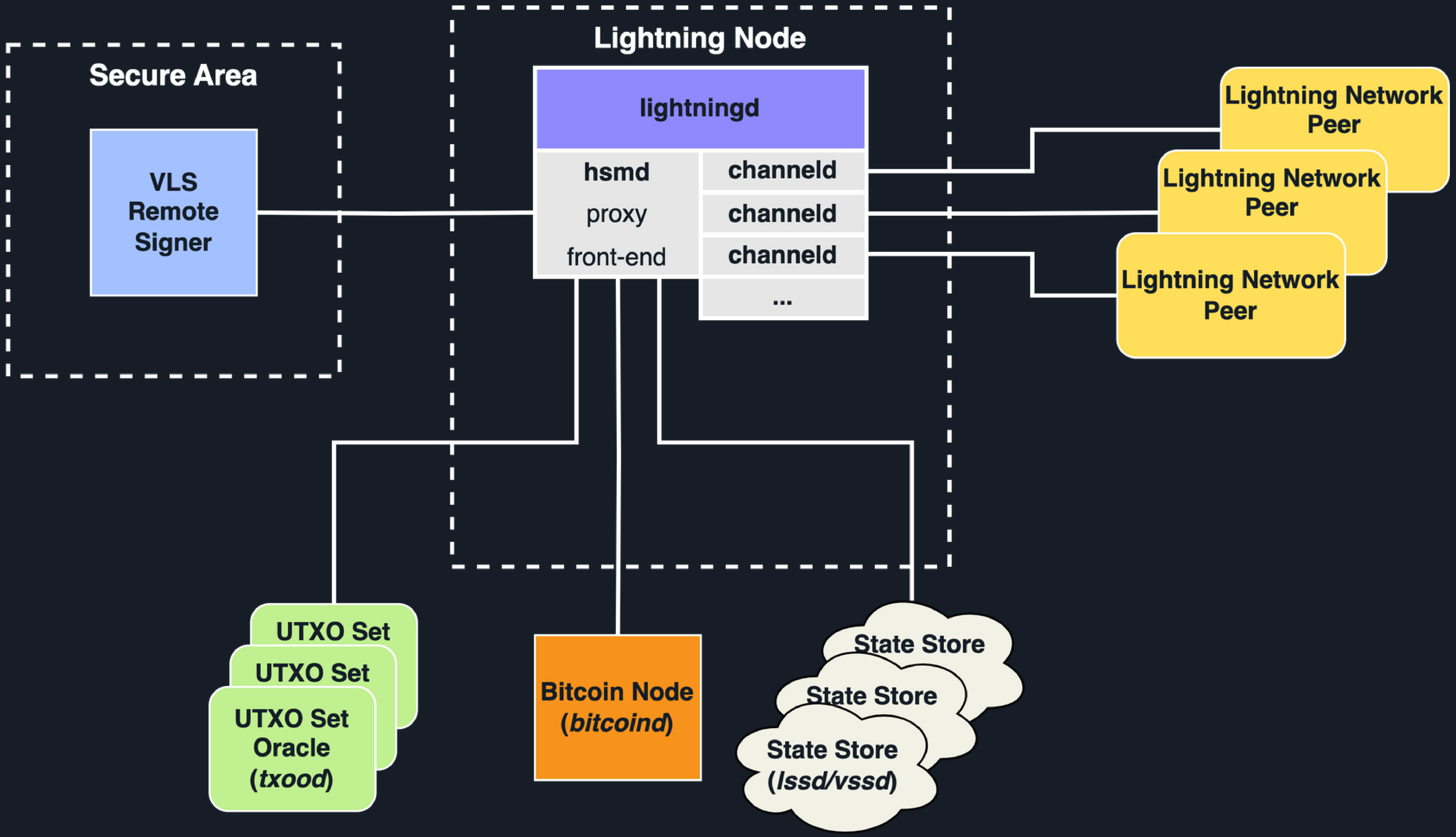
Enter VLS

Increases security by separating a user's private keys from their Lightning node, to hardened signing device

No other solutions provide same level of security

Open-source Rust library & reference implementation

System Diagram



How VLS Works

Separates private keys in **hardened signing devices**

Node **substitutes internal signing** with calls to signer

Flexible policies to control payment flow

- Velocity control
- Approval settings
- React to events

Lightning Storage Server

Node and channel state can be stored in the cloud using LSS or VSS (coming in later release)

Disaster recovery using only a seed phrase

Cryptographically verified payment history and storage

Bitcoin UTXO Oracle

Signer must be aware of on-chain state (chain tip & UTXO set at the tip) to prevent the loss of funds

UTXO Oracle tracks on-chain Bitcoin transactions to prevent fund loss

Signer can get UTXO data from multiple sources

VLS Config

VLS can be used in several configurations:

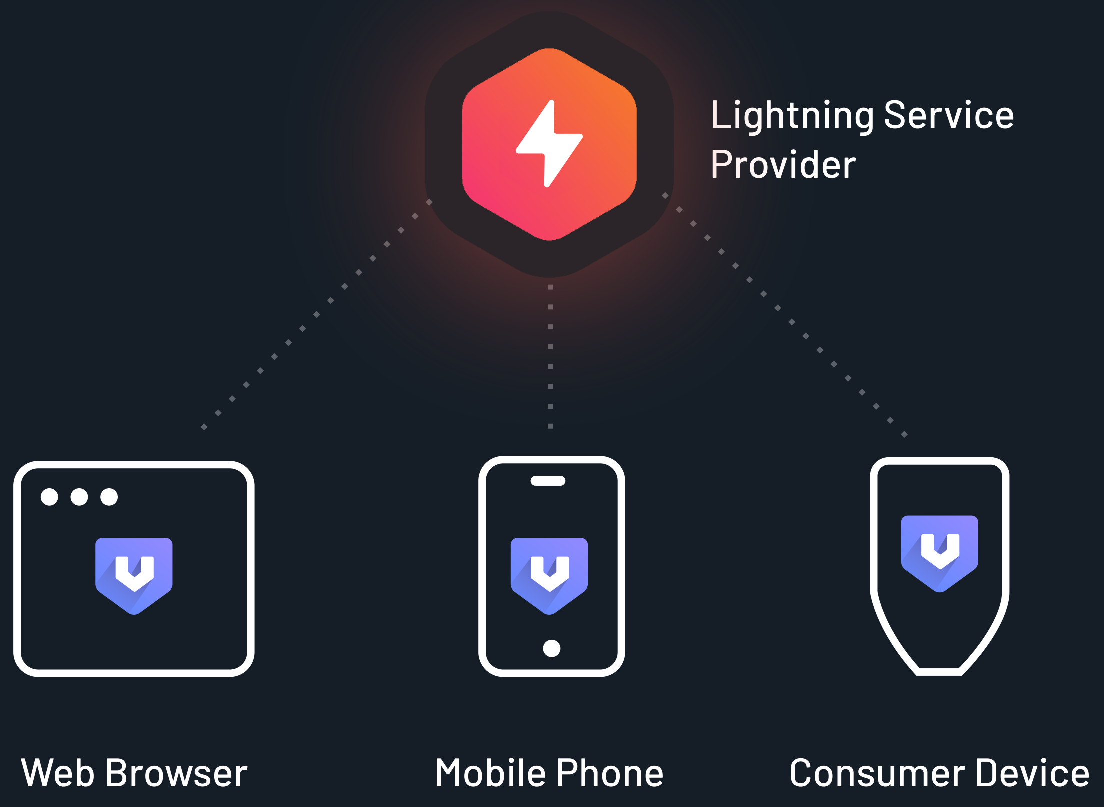
- CLN: Socket
- CLN: Serial
- LDK: Socket

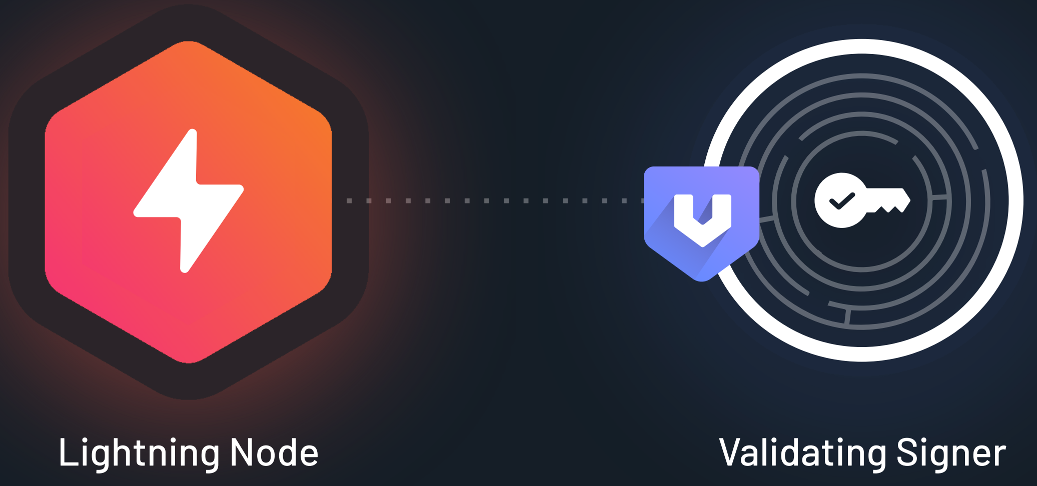
Signing device can be hardened as needed for the specific use case

Use Cases

Home user running VLS on their **mobile device**

Small merchant using a **inexpensive consumer device** (e.g. ESP32 / STM32)





Large enterprise running VLS on an **HSM or hardened server**

Lightning Service Providers

VLS users control their private keys, even if their node is hosted by an LSP

Users can unilaterally close their channels and recover coins without involvement from LSP

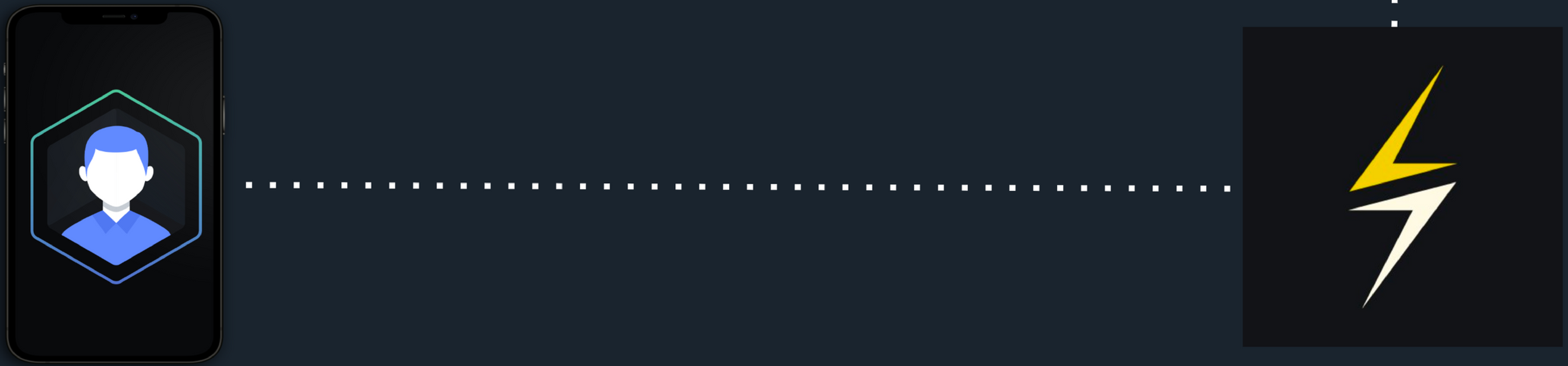
Sphinx Chat

Integrated VLS for **wifi-connected hardware signer** (ESP32)

Sphinx app stores **seed phrase backup**, controls VLS policies remotely

VLS enables Sphinx users to have **self-custody** of their funds, even while using hosted Sphinx nodes

Hardware Signer

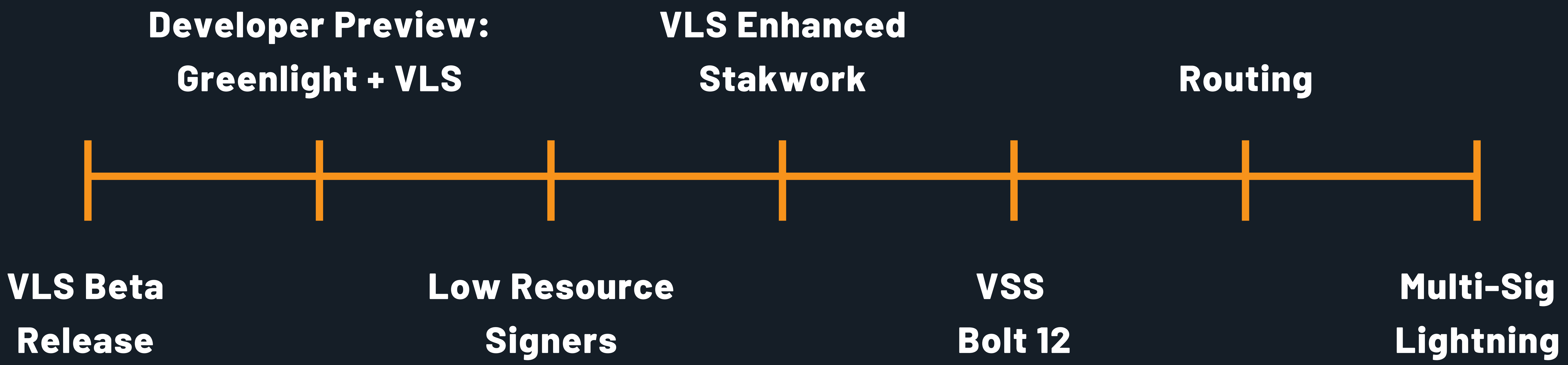


Demo

VLS Beta Release

- Works with CLN and LDK
- Encrypted cloud state backup
- Disaster recovery from signer and node failure
- Complete set of layer-2 validation rules
- Optional validation rules (e.g. velocity, approval)
- A complete set of layer-1 validation rules (on-chain channel state tracking)
- Heartbeat generation
- Allowlist for approved destinations
- UTXO set oracle guarantees safe on-chain state

Roadmap



VLS Beta Release

Developer Preview: Greenlight + VLS

Low Resource Signers

VLS Enhanced Stakwork

VSS Bolt 12

Routing

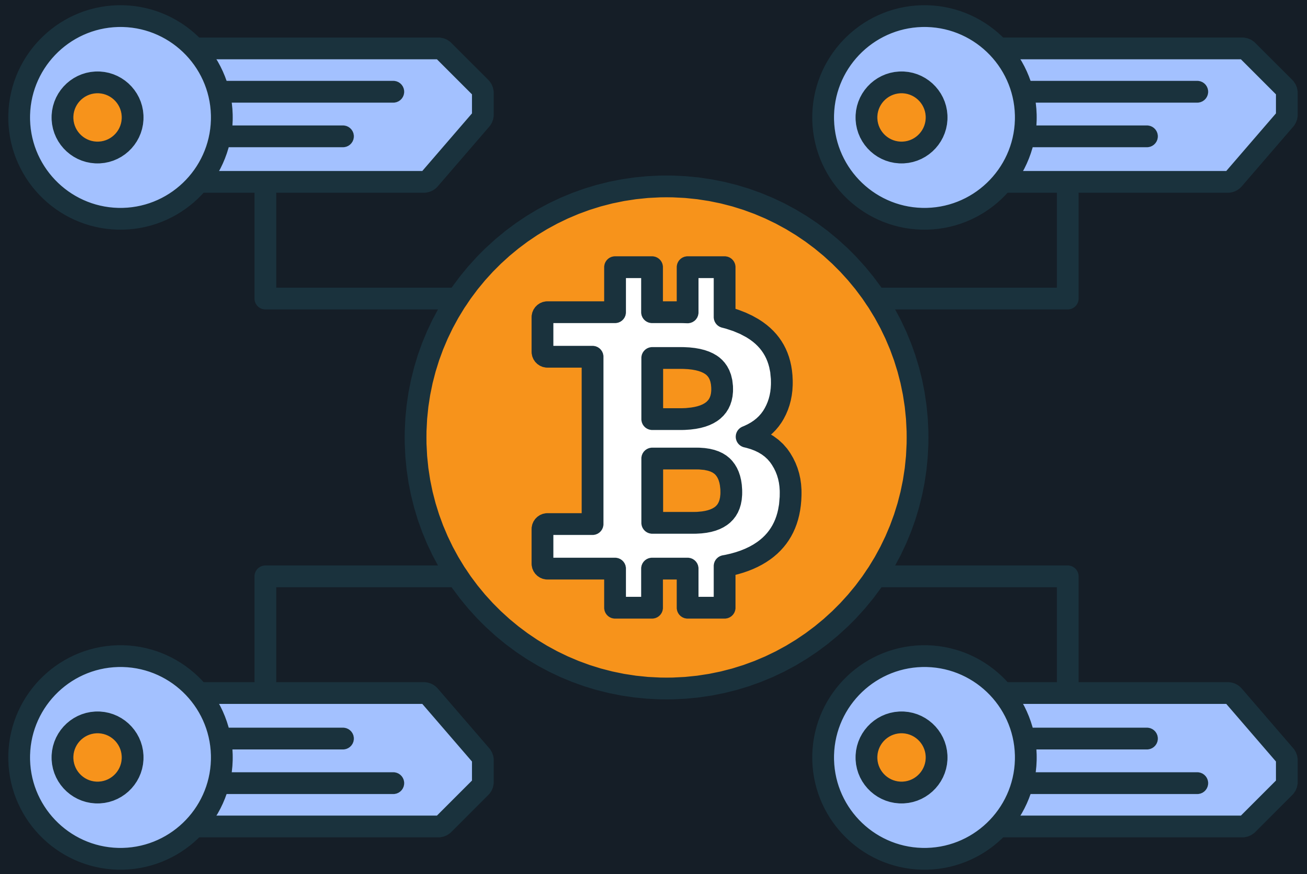
Multi-Sig Lightning

Multisig Lightning

Taproot (Schnorr signatures) has enabled new, more flexible multisig

FROST (Fast Round-Optimized Schnorr Signature Thresholds)

- No limit to size of quorum
- Signatories can change on the fly



Take VLS for a Spin

Matrix Chat

Ask us anything on Matrix

Feature Request

Submit a feature request on GitLab

Core Lightning

See VLS in action on a sample CLN Node

LDK

See VLS in action on a sample LDK node

Thank you!

vls.tech

sphinx.chat

@vlsproject

@sphinx_chat

Disclaimer

This presentation is for The Canadian Bitcoin Conference use only

This material is the property of the presenter and all uses, modifications, and distributions are subject to Speakers approval and otherwise expressly prohibited.

This material is intended for general information purposes only and should not be considered specific or personal investment or legal advice. Examples given are for illustration purposes only, and the specific facts and circumstances of each case will differ from client to client.

This material may contain information obtained from third-party sources. While reasonable efforts have been made at the time of publication to ensure that the contents of this material have been derived from reliable and accurate sources, including third party sources, we provide the information “AS IS” and we do not warrant the accuracy, completeness, usefulness, or timeliness of the information contained herein. The views and opinions of the invited speakers to The Canadian Bitcoin Conference are not those of MC Event Management. MC Event Management does not constitute or imply endorsement or recommendation by MC Event Management of the speaker’s business.
NEITHER MC EVENT MANAGEMENT NOR ITS AFFILIATES, OFFICERS, EMPLOYEES OR ANY OTHER PERSON ACCEPTS ANY LIABILITY WHATSOEVER FOR ANY DIRECT, INDIRECT OR CONSEQUENTIAL LOSS ARISING FROM ANY USE OR RELIANCE ON THE INFORMATION, GENERAL STRATEGIES OR OPINIONS CONTAINED HEREIN.