


Hardware Wallet + Lightning = 

Team 3



# Team

A large team of 13 people led by Stepan (@stepansnigirev) and Henrik (@hkjn)

- **Hardware:** Stepan, Stephanie, Akhilesh, Ivo
- **UI:** Justin, Gustavo, Michael, Nelson
- **Client:** Henrik, Sebastian<sup>2</sup>, Fabian, Kaspar

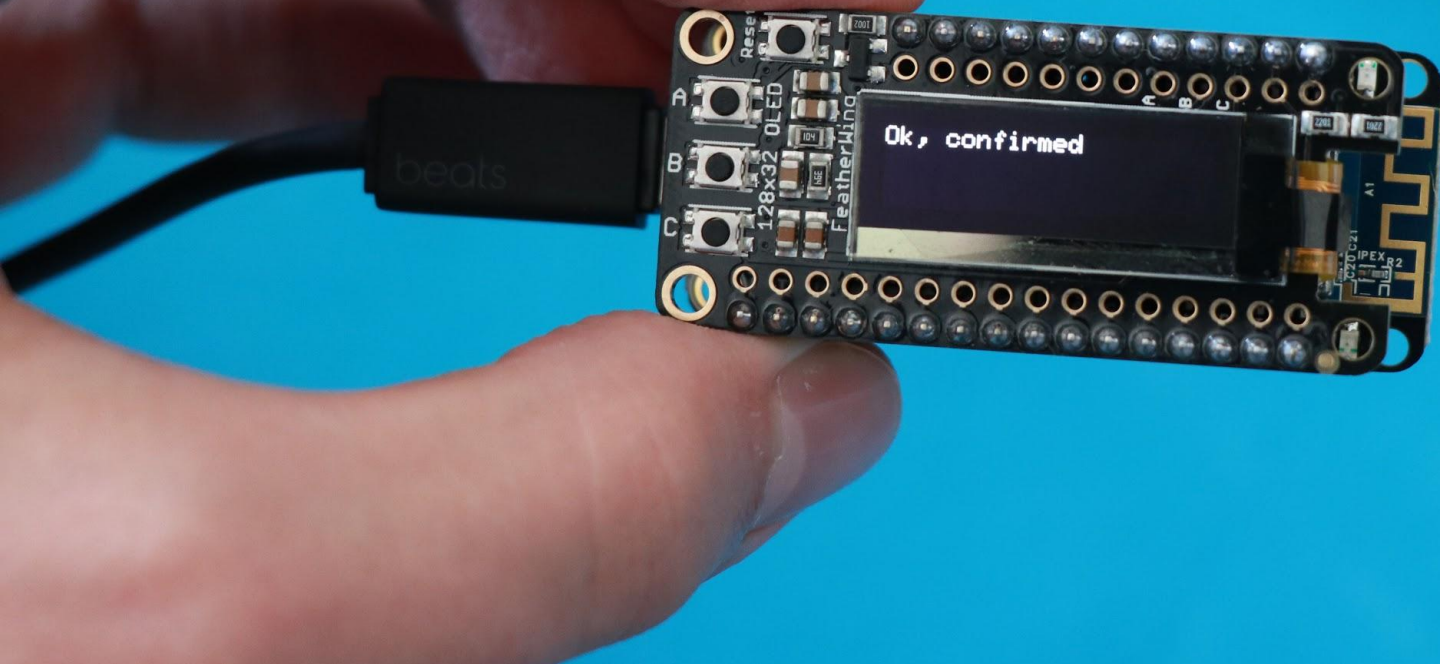
# The problem

Ledger, Trezor, BitBox etc. do not currently allow you to use their devices to securely open lightning channels, make lightning transactions and close lightning channels.

Lightning nodes hold your funds as “hot wallets” (private keys stored in a wallet connected to the internet)



The solution







Integration  
coming soon™!

Such GUI, much wow!

# Architecture

c-lightning - modular, daemons can be replaced, easy to hack

We started moving `hsm.c` functionality out

Runs on testnet and mainnet

Arduino hardware — user friendly, secure microcontroller

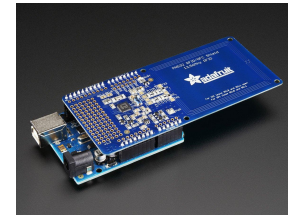
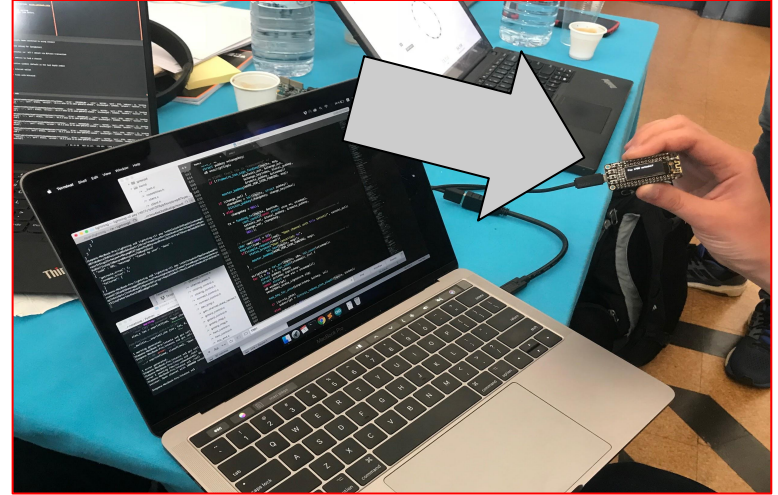
# Hardware wallet

Arduino board

Stores private key (`hsm_secret`)

Listens to serial port

User confirms digital signatures on screen



# Hardware wallet client

Monitors ports

Sends pairing request to hardware device

Runs the c-lightning daemon

Flask web server sends RPCs to lightningd

React frontend





## My channels

[Open new channel](#)[Pay invoice](#)

5ed8fc952bff5772a8e5e0b8d8aaf23d2d002738b1af30e2cd79973bcd37f39

Connected with: 030f0b260acd3edcad84d7588ec7c5df471e87e6a230f6989b8d3a4147230

Current state

NORMAL

0.01000 BTC  
63.53 USD



f56f744c65e564b599fedbbc53706695d01cdd9326d51aaf03345579eae96ae8

Connected with: 03933884aaf0d6b108397e5efe5c86bc12d8ca8d2f700eda99db9214fc2712b134

Current state

NORMAL

0.09965 BTC  
633.11 USD



0b7ba48057442c6766147eff4450b0660059b1a5cf5980cd4af86e7c99dd87

Connected with: 038863cf8ab91046230f561cd5b386cbf8309fa02a3f0c3ecd161a3aeb64a643b9

Current state

NORMAL

0.10000 BTC  
635.34 USD



ff19b9da3489d8af03afcdf647dcd90ffc7ebf50b80d622732a133136c8d570

Connected with: 02212d3ec887188b284d4bb7b2e6eb40629a6e14fb049673f22d2a0aa05f902090e

Current state

ONCHAIN

0.01000 BTC  
63.53 USD



6ea173a55ea0c5e38323a543060067fd01901820d0ff26da70071b2fdb2443c8

Connected with: 02212d3ec887188b284d4bb7b2e6eb40629a6e14fb049673f22d2a0aa05f902090e

Current state

ONCHAIN

0.01000 BTC  
63.53 USD



3c7b3e5afede7a6ef875f35a61908fa25ba04d06ade8c8a0c65d0c9fdb69877

Connected with: 02212d3ec887188b284d4bb7b2e6eb40629a6e14fb049673f22d2a0aa05f902090e

Current state

ONCHAIN

0.01235 BTC  
78.44 USD



cf9c4614bbd17c4fb1fdf310591dfb7fb0945d0cddf8dff2b7c5e42bc8015a4

Connected with: 02212d3ec887188b284d4bb7b2e6eb40629a6e14fb049673f22d2a0aa05f902090e

Current state

ONCHAIN

0.01000 BTC  
63.53 USD



697beea1d83cf0679570a1f639ccff1e2cc174869d8726d3a139a55d3031c21b

Connected with: 02212d3ec887188b284d4bb7b2e6eb40629a6e14fb049673f22d2a0aa05f902090e

Current state

ONCHAIN

0.01000 BTC  
63.53 USD



32bc4d21ed59064119fc767ef240c8cecf665995d703c6d824bfb7f02841423e

Connected with: 037ea3a8984c2eae56766b45a528e924c10944b211fd5c19a2ca96962ea380496a

Current state

ONCHAIN

0.01000 BTC  
63.53 USD



47b4e68a7de8d46788769d26d0b3f8a5c8595481c937b991b3271114c8495970

Connected with: 037ea3a8984c2eae56766b45a528e924c10944b211fd5c19a2ca96962ea380496a

Current state

CLOSINGD\_CONFIRM

0.01000 BTC  
63.53 USD

## Payments



b64190b640e488c98c6d873c187560f8cf3fa60647b910f5edd745d8b6302f55

Datetime: 18:07:34 GMT+0100 (Western European Standard Time)

Payment status

COMPLETE

1200.000 sat



Home

Device

Connected

Balance

฿ 12.00

⚡ 0.002

My Channels

Transaction history

My bitcoin address



OPEN NEW CHANNEL



1 Scala Chip Frappuccino

Connected with: 03933884aaf1d6b1108397e5efe5c86bcfe5c86b

CURRENT STATE

NORMAL

1.2960948653 BTC

6239,00 USD



1 Scala Chip Frappuccino

Connected with: 03933884aaf1d6b1108397e5efe5c86bcfe5c86b

0.4660443645 BTC

2909,00 USD

## Payment request

INVOICE REFERENCE

*Insert invoice reference*

Pay



Home



Device

Connected

Balance

฿ 12.00

⚡ 0.002

My Channels

Transaction history

My bitcoin address



OPEN NEW CHANNEL



1 Scala Chip Frappuccino

Connected with: 03933884aaf1d6b1108397e5efe5c86bcfe5c86b

CURRENT STATE

NORMAL

1.2960948653 BTC

6239,00 USD



1 Scala Chip Frappuccino

Connected with: 03933884aaf1d6b1108397e5efe5c86bcfe5c86b

Payment request



0.002 BTC paid

0.4660443645 BTC

2909,00 USD

# Learnings

It is possible to build a working prototype in a weekend

This is only a proof of concept — it is not secure against various attack vectors.....

...but it is a feasible project going forward

# Future Work

## **Added Features**

Routing transactions for others without user interaction

Machine to Machine (M2M) Payments

## **Hardware**

More secure and faster microcontrollers, hardened against different attacks (e.g. side-channel)

## **Contributing to c-lightning**

Better separation of private key handling

Separation of hardware wallet and controller — define a standard that all wallets can use



Visit the Team 3 table for a demo!

[github.com/hkjin/lnhw](https://github.com/hkjin/lnhw)



# 101 on Lightning Network

A user can join the lightning network by opening up a payment channel with a lightning node.

Funding the payment channel requires the sending of funds to a 2-of-2 multi-signature address (requires private key to sign)

Each commitment transaction between the two parties sends funds to a hashed time locked multi-signature address (requires private key to sign)

Closing the payment channel requires signing and broadcasting the latest commitment transaction to the blockchain (requires private key to sign)