Challenges of Building a Non-Custodial Lightning App

ek

STACKER NEWS

October 3, 2025

Agenda

1. Why Non-Custodial?
2. Custodial vs Non-Custodial Architecture
3. User Experience
4. Challenges

Why Non-Custodial?

Wallet of Satoshi stopped serving US customers

NEWS 1 MIN READ 24 NOV 2023

Wallet of Satoshi to Stop Serving Customers in the United States

"We've made the difficult decision to remove our app from the U.S. Apple and Google app stores, and will not serve U.S. customers going forward," announced Wallet of Satoshi.



- "For our existing users in the USA, rest assured that you have full access to your Bitcoin funds. You can seamlessly withdraw and transfer them to another wallet," was stated in the post.

Wallet of Satoshi is a custodial, closed-source Bitcoin and Lightning wallet and service provider based in Australia. The wallet became popular due to its ease of use and frictionless onboarding experience.

- "This decision doesn't come lightly. Our commitment to providing a secure, user-friendly, and compliant platform globally is unwavering. Our top priority is the safety and interests of our customers and our company."

https://www.nobsbitcoin.com/wallet-of-satoshi-stops-serving-us-customers/

Samourai Devs prosecuted



An official website of the United States government Here's how you know

DOJ Menu

United States Attorney's Office
Southern District of New York

About SDNY | Find Help | Contact Us

Search

About | Divisions | Priorities | News | Resources | Programs | Employment | Self-Reporting and Whistleblower Programs | Subscribe to SDNY News Alerts

Justice.gov > U.S. Attorneys > Southern District of New York > Press Releases > Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses

PRESS RELEASE

Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses

Wednesday, April 24, 2024

Share

For Immediate Release

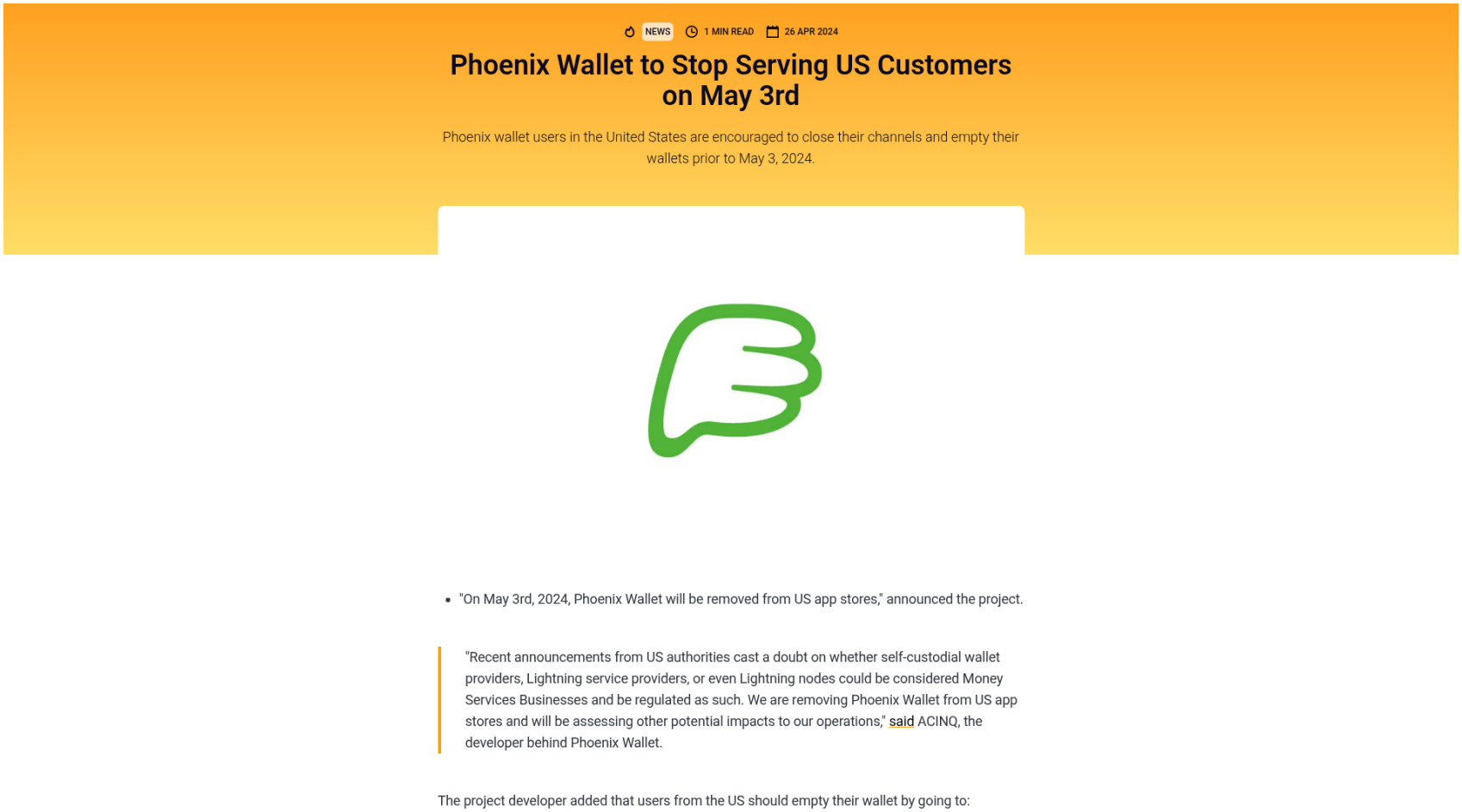
U.S. Attorney's Office, Southern District of New York

Keonne Rodriguez and William Lonergan Hill Are Charged with Operating Samourai Wallet, an Unlicensed Money Transmitting Business That Executed Over $2 Billion in Unlawful Transactions and Laundered Over $100 Million in Criminal Proceeds

Damian Williams, the United States Attorney for the Southern District of New York; Thomas Fattorusso, the Special Agent in Charge of the New York Field Office of the Internal Revenue Service, Criminal Investigation ("IRS-CI"); and James Smith, the Assistant Director in Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced today the unsealing of an Indictment charging KEONNE RODRIGUEZ, the Chief Executive Officer and a co-founder of Samourai Wallet ("Samourai"), and WILLIAM LONERGAN HILL, the Chief Technology Officer and also a co-founder of Samourai, with conspiracy to

https://www.justice.gov/usao-sdny/pr/founders-and-ceo-cryptocurrency-mixing-service-arrested-and-charged-money-laundering

Phoenix Wallet stopped serving US customers



NEWS 1 MIN READ 26 APR 2024

Phoenix Wallet to Stop Serving US Customers on May 3rd

Phoenix wallet users in the United States are encouraged to close their channels and empty their wallets prior to May 3, 2024.

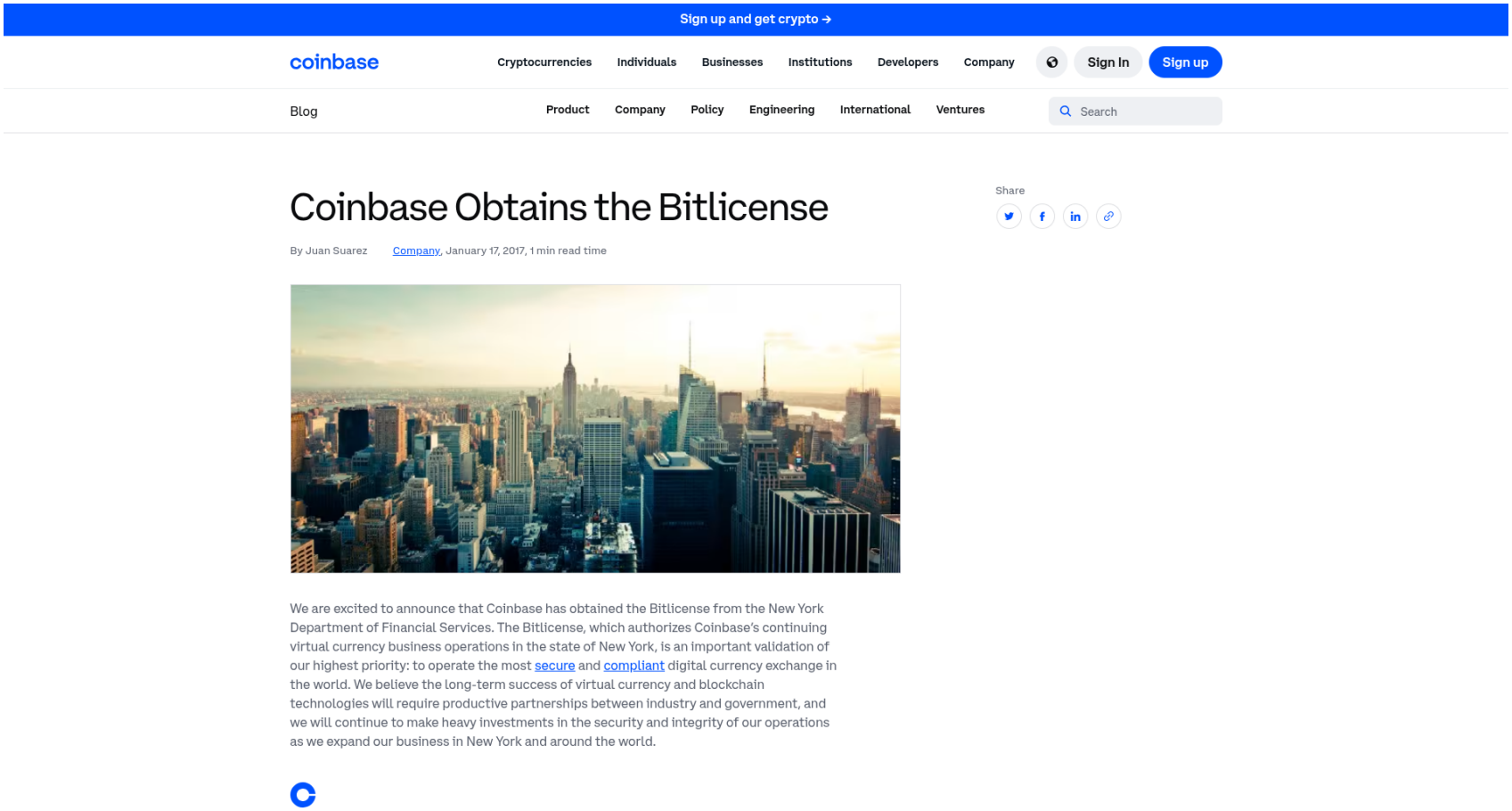
- "On May 3rd, 2024, Phoenix Wallet will be removed from US app stores," announced the project.

> "Recent announcements from US authorities cast a doubt on whether self-custodial wallet providers, Lightning service providers, or even Lightning nodes could be considered Money Services Businesses and be regulated as such. We are removing Phoenix Wallet from US app stores and will be assessing other potential impacts to our operations," said ACINQ, the developer behind Phoenix Wallet.

The project developer added that users from the US should empty their wallet by going to:

https://www.nobsbitcoin.com/phoenix-wallet-to-be-removed-from-us-app-stores-on-may-3/

New York's BitLicense . . .



https://www.coinbase.com/en-de/blog/coinbase-obtains-the-bitlicense

. . . is not enough for the Lightning Network

BUSINESS

Coinbase Integrates Bitcoin Lightning Network for US Exchange Users

By **Vivek Sen** April 30, 2024



Bitcoin and crypto exchange Coinbase has integrated Bitcoin's Lightning Network, enabling faster and cheaper BTC transactions for its users in the United States (with the exception of New York).

As the largest Bitcoin exchange globally by users, trading volume, and custody of assets, Coinbase's adoption of Lightning is a major win for the Bitcoin scaling solution. Lightning allows near-instant Bitcoin payments with significantly lower fees by moving transactions off-chain.

Coinbase has been working to implement Lightning support for years to further its mission of building a payments network costing pennies per transaction. This integration finally unlocks the power of instant and affordable Bitcoin payments for the exchange's massive US user base.

https://bitcoinmagazine.com/business/coinbase-integrates-bitcoin-lightning-for-100-million-users

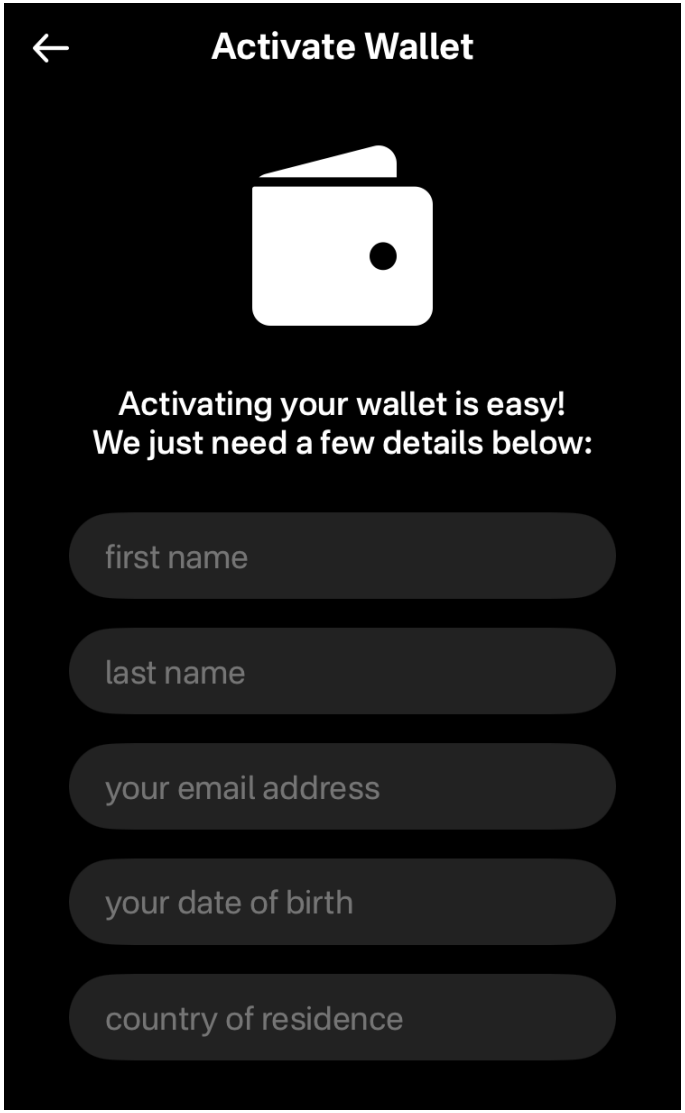
Alternatives

Paying $$$ for the privilege to:

- implement KYC
- monitor transactions
- report suspicious activity

Alternatives

“Soft KYC”



We said no.

OFAC

... but still had to comply with OFAC sanctions ...

OFAC

All U.S. persons must comply with OFAC sanctions, including all U.S. citizens and permanent residents regardless of where they are located, all individuals and entities within the United States, and all U.S. incorporated entities and their foreign branches.

https://ofac.treasury.gov/faqs/11

OFAC

api/resolvers/ofac.js

```
@@ -0,0 +1,24 @@
+ import { GraphQLError } from 'graphql'
+
+ // this function makes america more secure apparently
+ export default async function assertGofacYourself ({ models, headers }) {
+   const country = await gOFACYourself({ models, headers })
+   if (!country) return
+
+   throw new GraphQLError(
+     `Your IP address is in ${country}. We cannot provide financial services to residents of ${country}.`,
+     { extensions: { code: 'FORBIDDEN' } })
+ }
```

https://github.com/stackernews/stacker.news/commit/a5e50821b7e0dba0400a5f8ada6d3741a92de9d3

Custodial vs Non-Custodial Architecture

Custodial Architecture

- “zaps” are database transactions
- only deposits and withdrawals are lightning payments
- lightning node can go down and most users wouldn’t notice

Is this really a lightning app?

Non-Custodial Architecture

- (almost) every payment is over lightning
- senders now have to pay routing fees[1]
- zaps need to be forwarded to receiver

How to never take custody of funds while forwarding?

[1] if they don't have a channel with SN

Inproxy


↬ Inproxy.org
about
api
contact
Random relay
lnbc...
Wrap
more options ◀
dx7pn6ehykq6cadce4bjbxn5tf64z7e3fufpxgxce7n4f5eja476cpyd.onion

Inproxy

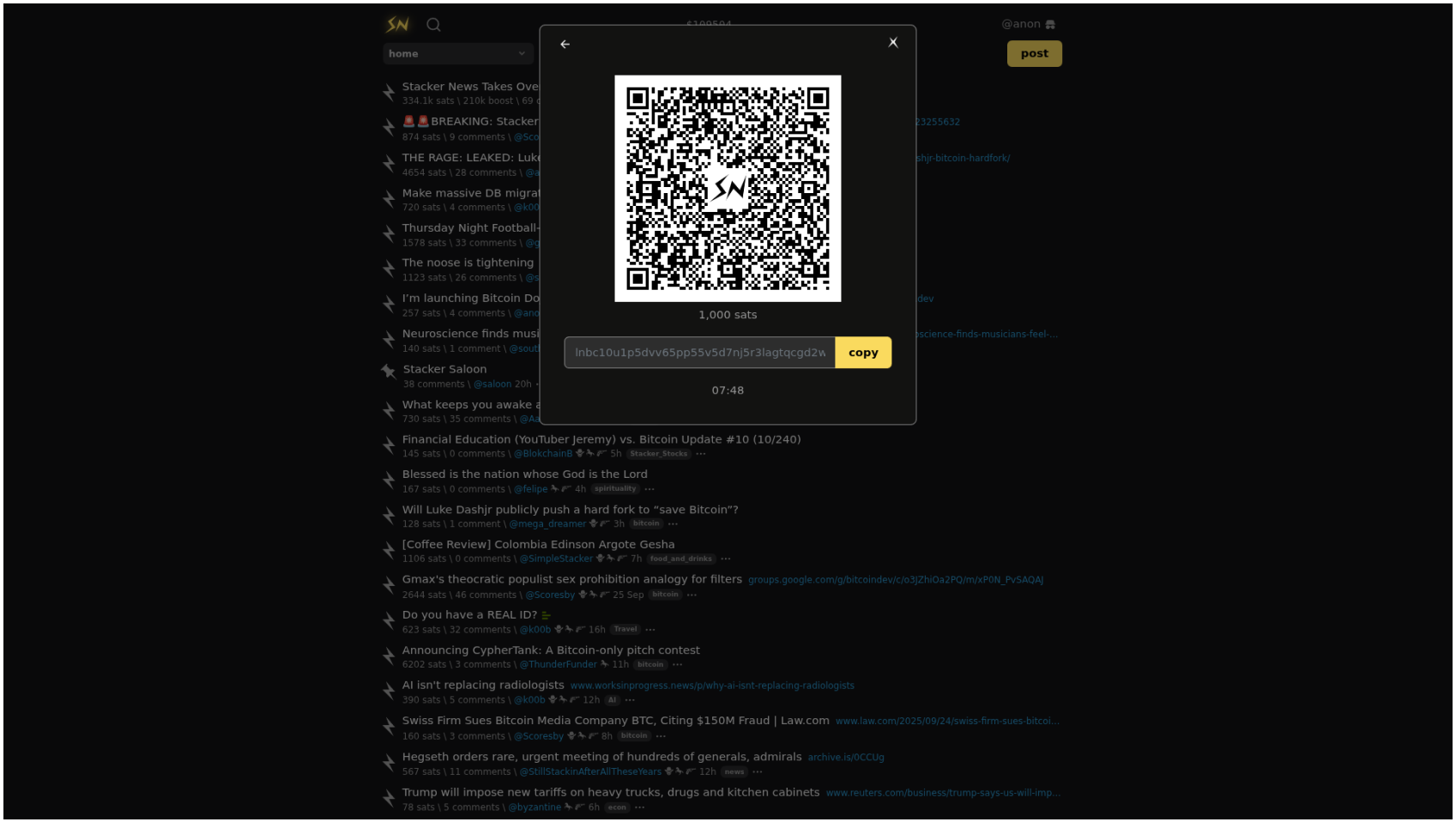
Demo

The End.

I wish ...

User experience

QR codes are not good UX

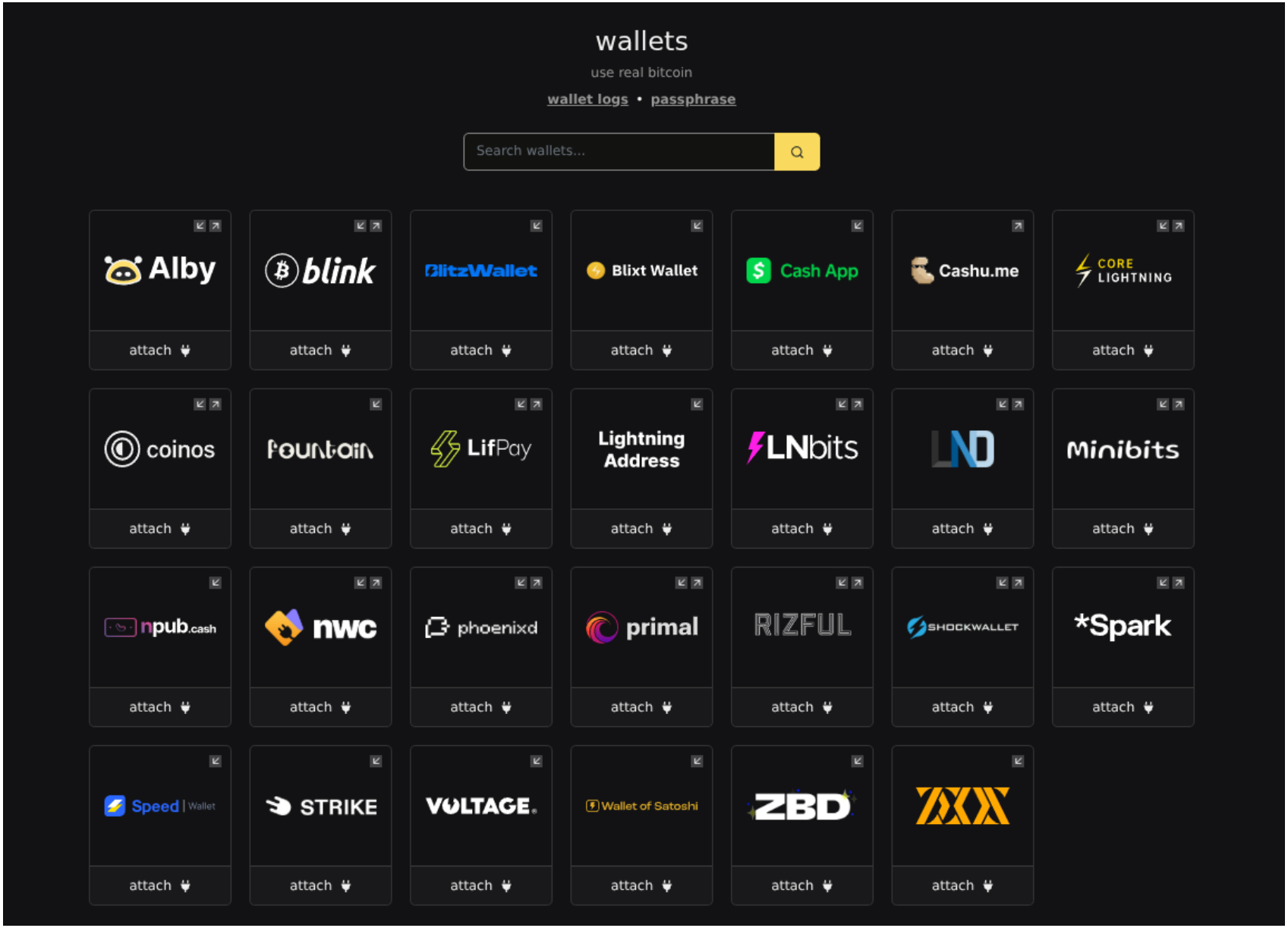


QR codes are not good UX

- desktop vs mobile
- everything about a payment can be slow

What if the payment fails?

Wallets


wallets
use real bitcoin
wallet logs • passphrase
Search wallets...
Alby
blink
BlitzWallet
Blixt Wallet
Cash App
Cashu.me
CORE LIGHTNING
coinos
FOUNTAIN
LifPay
Lightning Address
LNbits
LND
Minibits
npub.cash
nwc
phoenixd
primal
RIZFUL
SHOCKWALLET
*Spark
Speed | Wallet
STRIKE
VOLTAGE
Wallet of Satoshi
ZBD
attach

Wallets

Demo

Payment UX

- optimistic payments
- retry payments in the background
- notify user if a payment failed

should *feel* like custodial

Payment retries

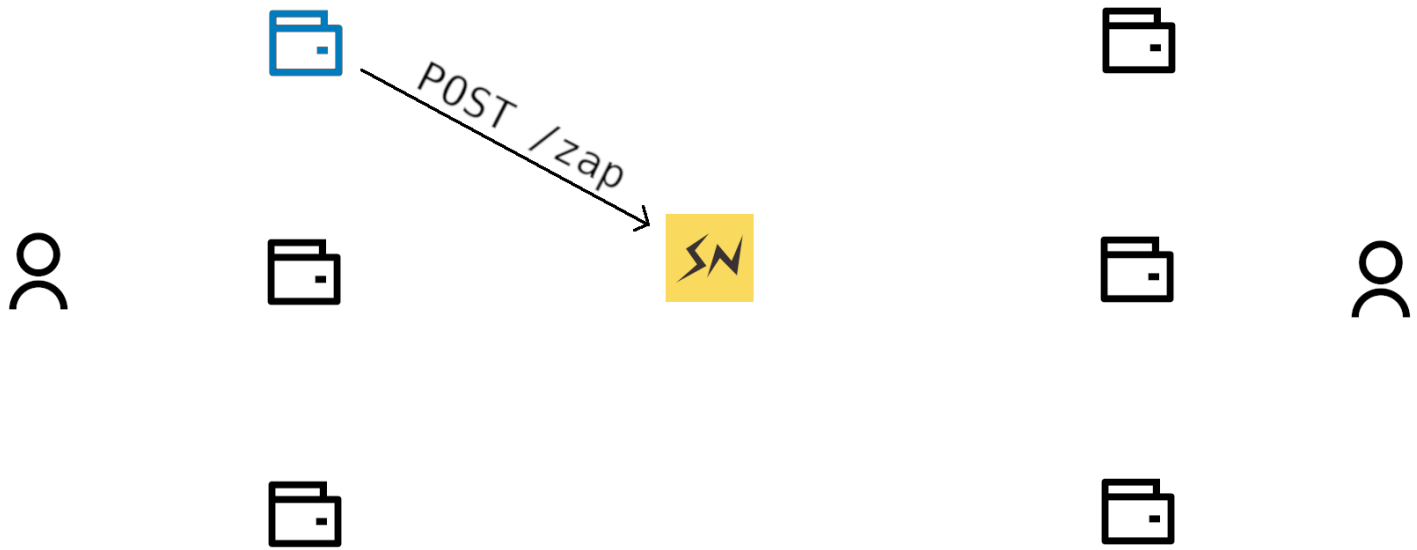
- payments are attempted three times
- users can attach multiple wallets as fallbacks
- did sender or receiver fail?

Never reuse a lightning invoice!

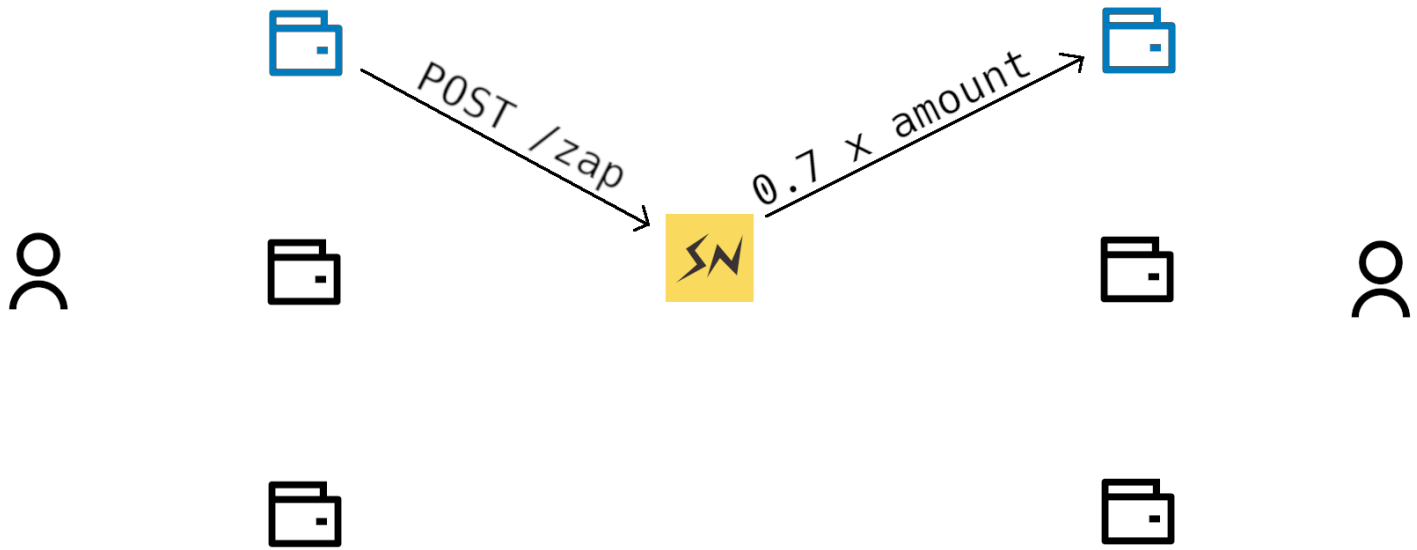
P2P zaps



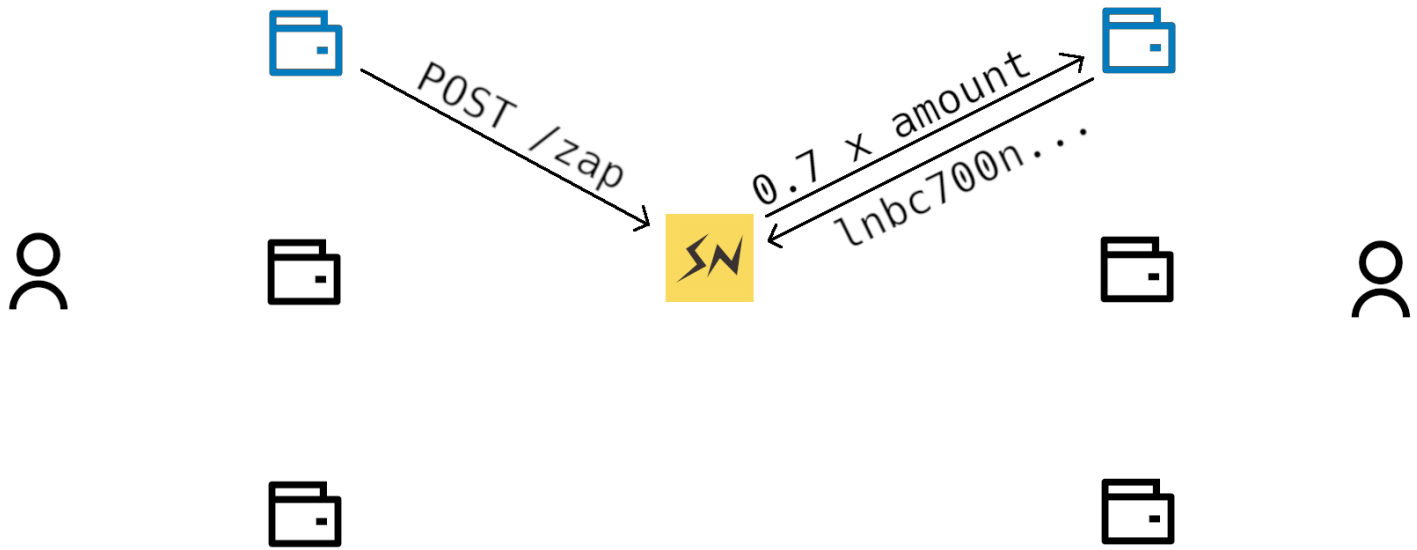
P2P zaps



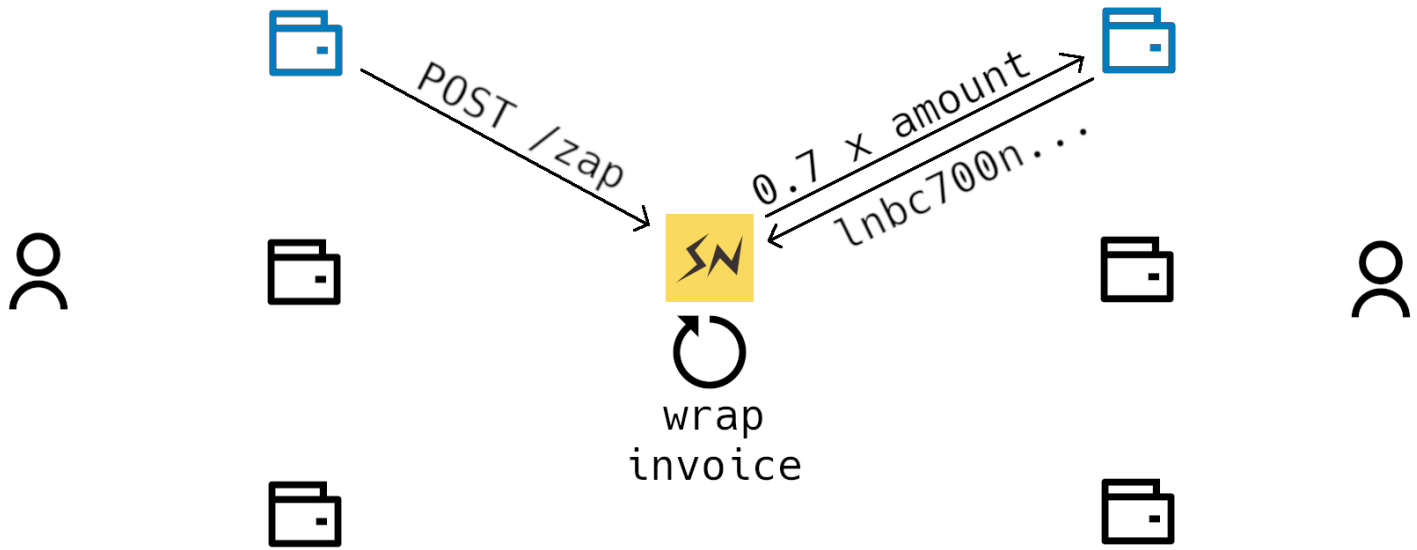
P2P zaps



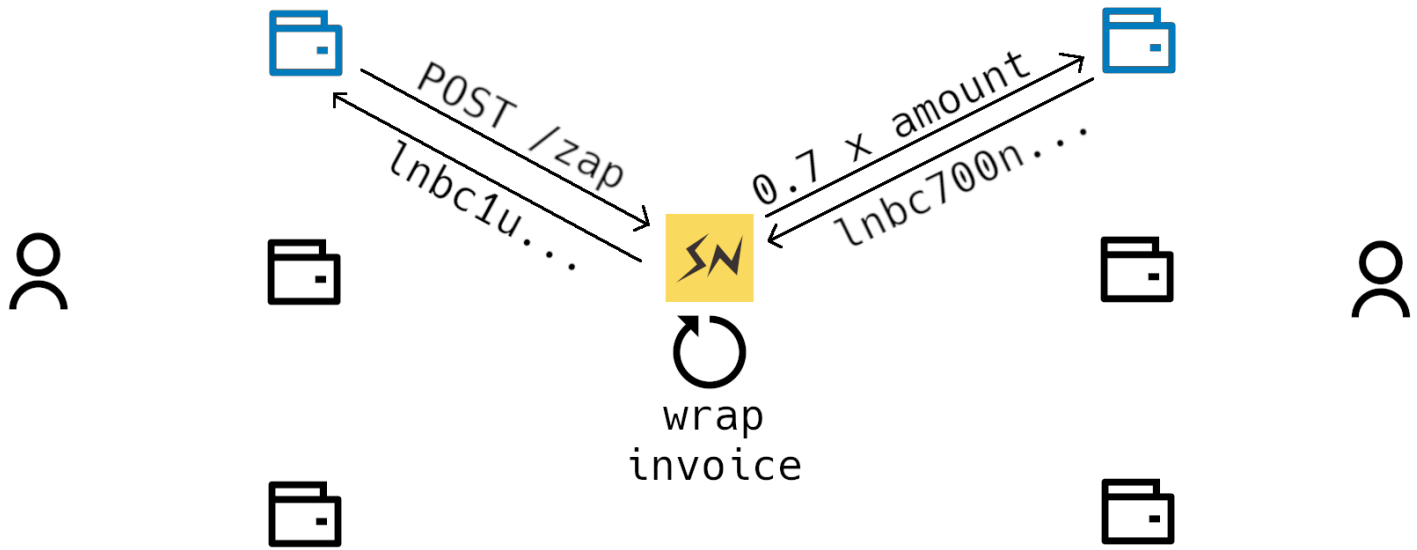
P2P zaps



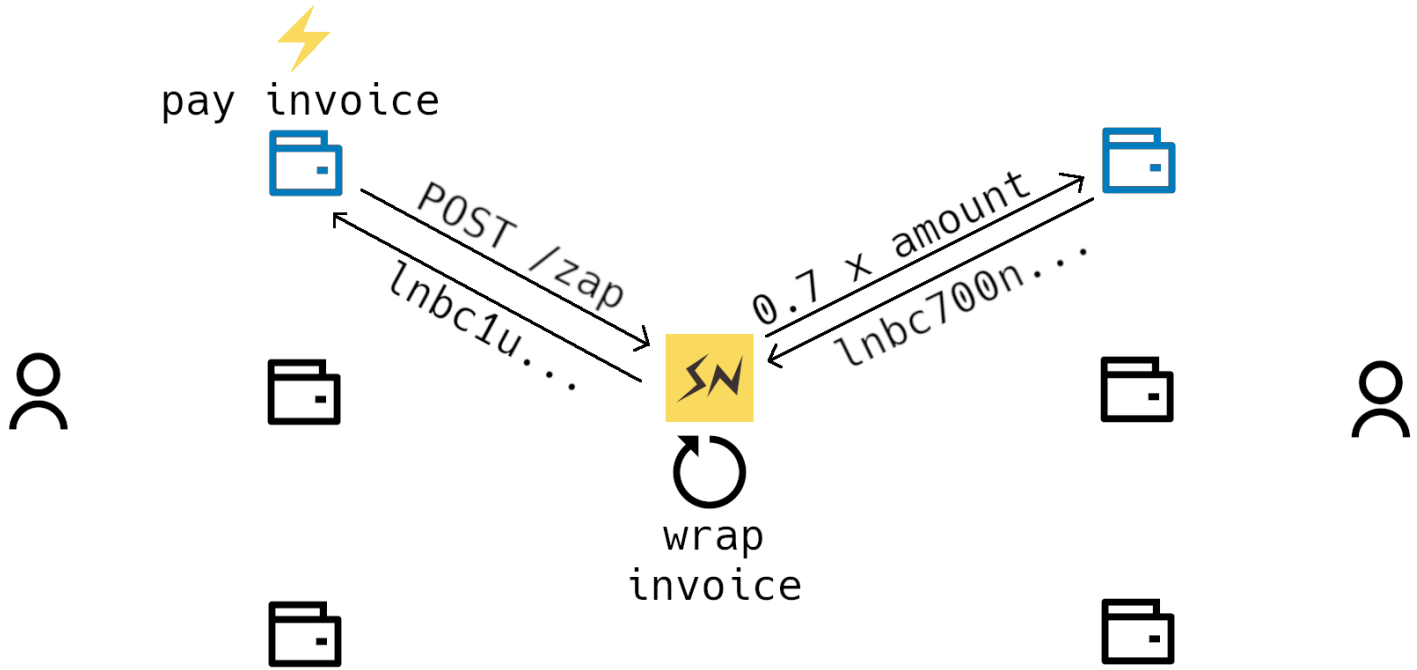
P2P zaps



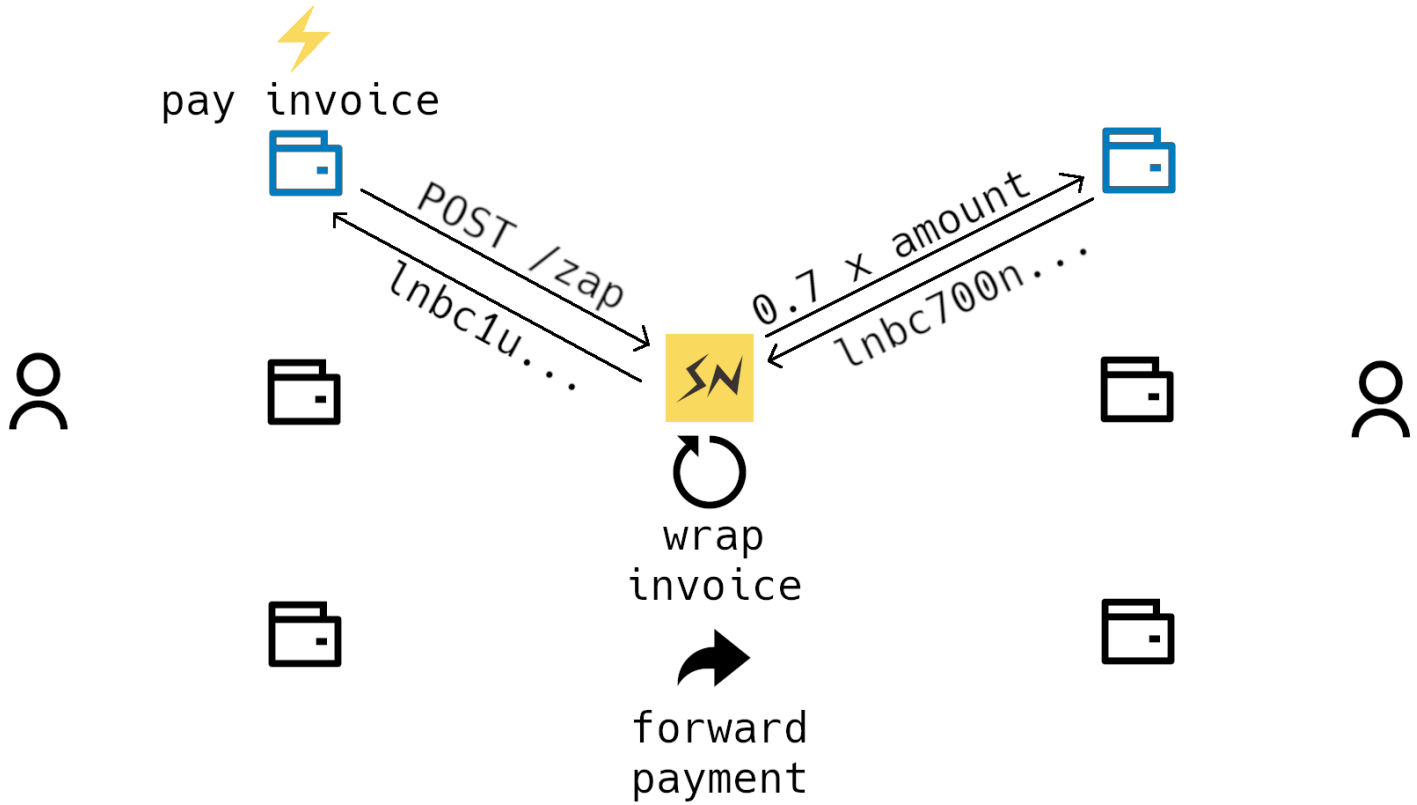
P2P zaps



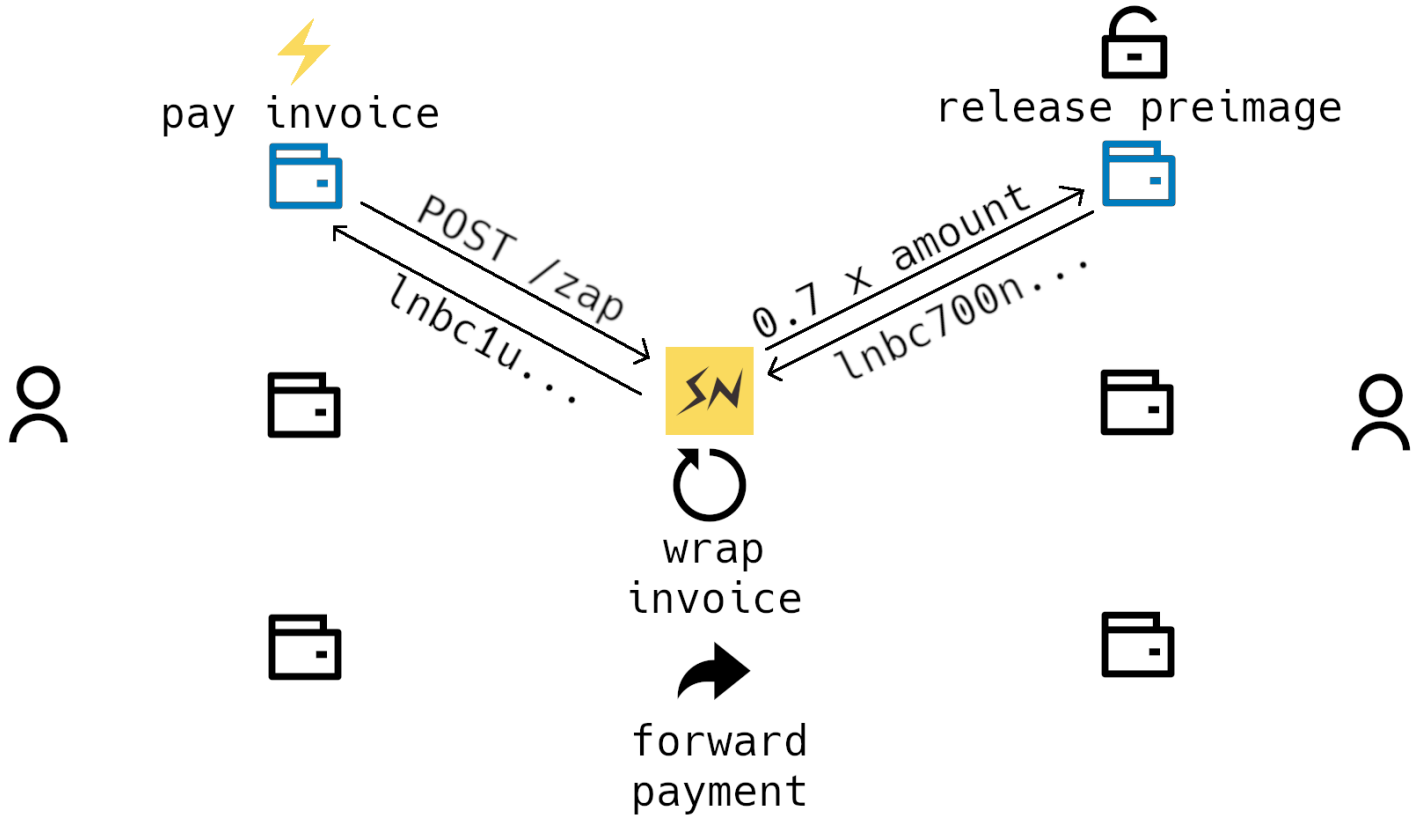
P2P zaps


pay invoice
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
wrap
invoice

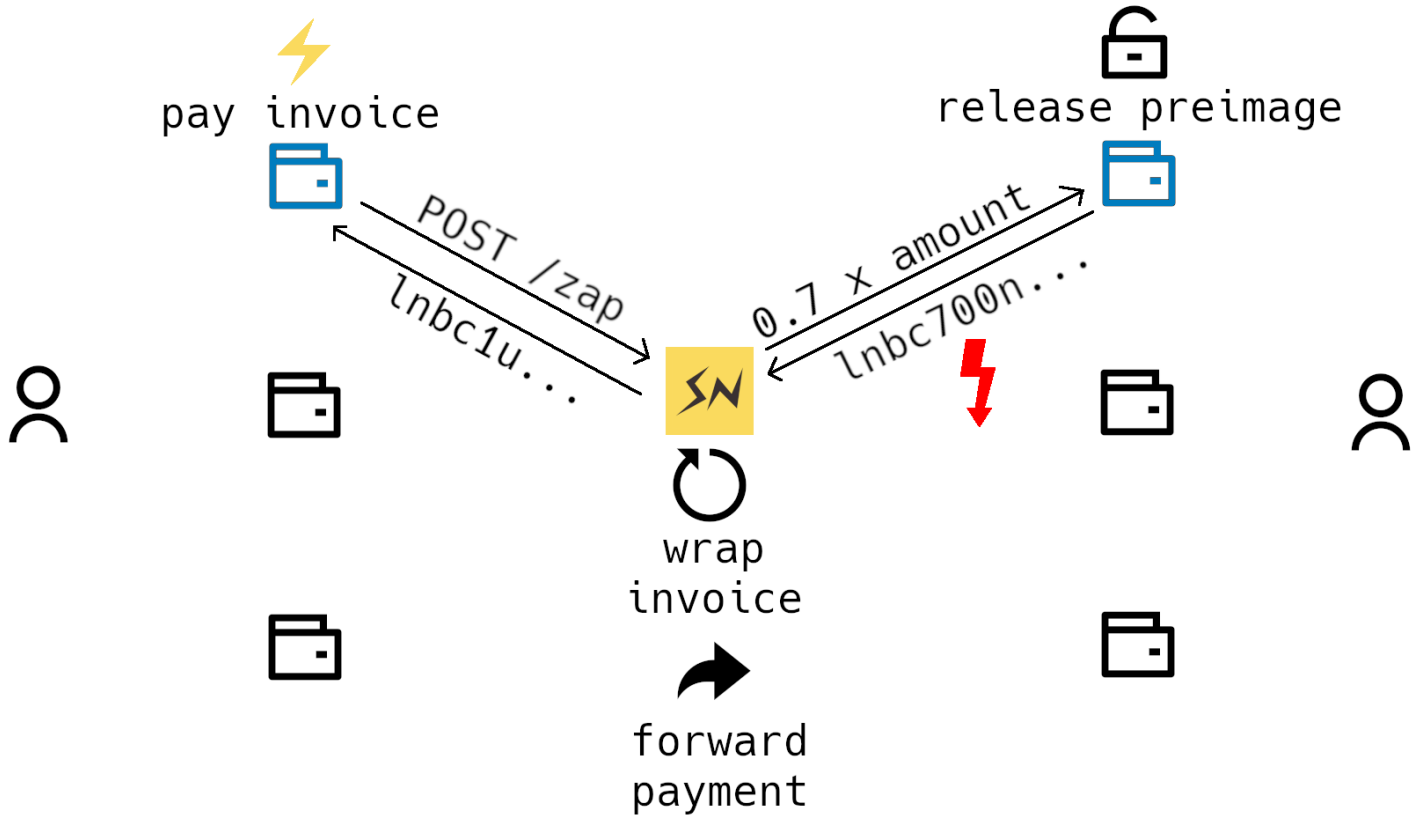
P2P zaps


pay invoice
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
wrap
invoice
forward
payment

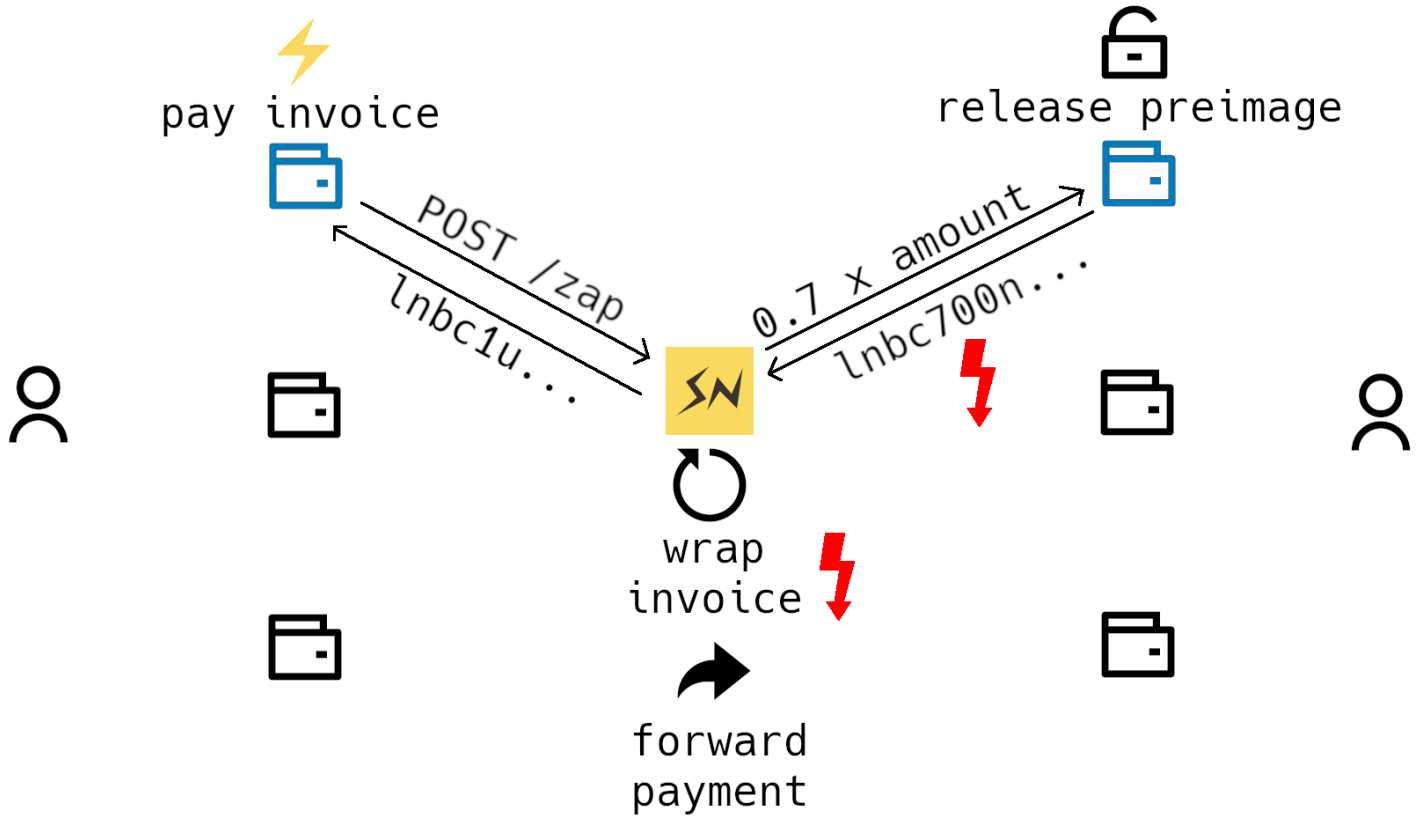
P2P zaps


pay invoice
release preimage
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
wrap
invoice
forward
payment

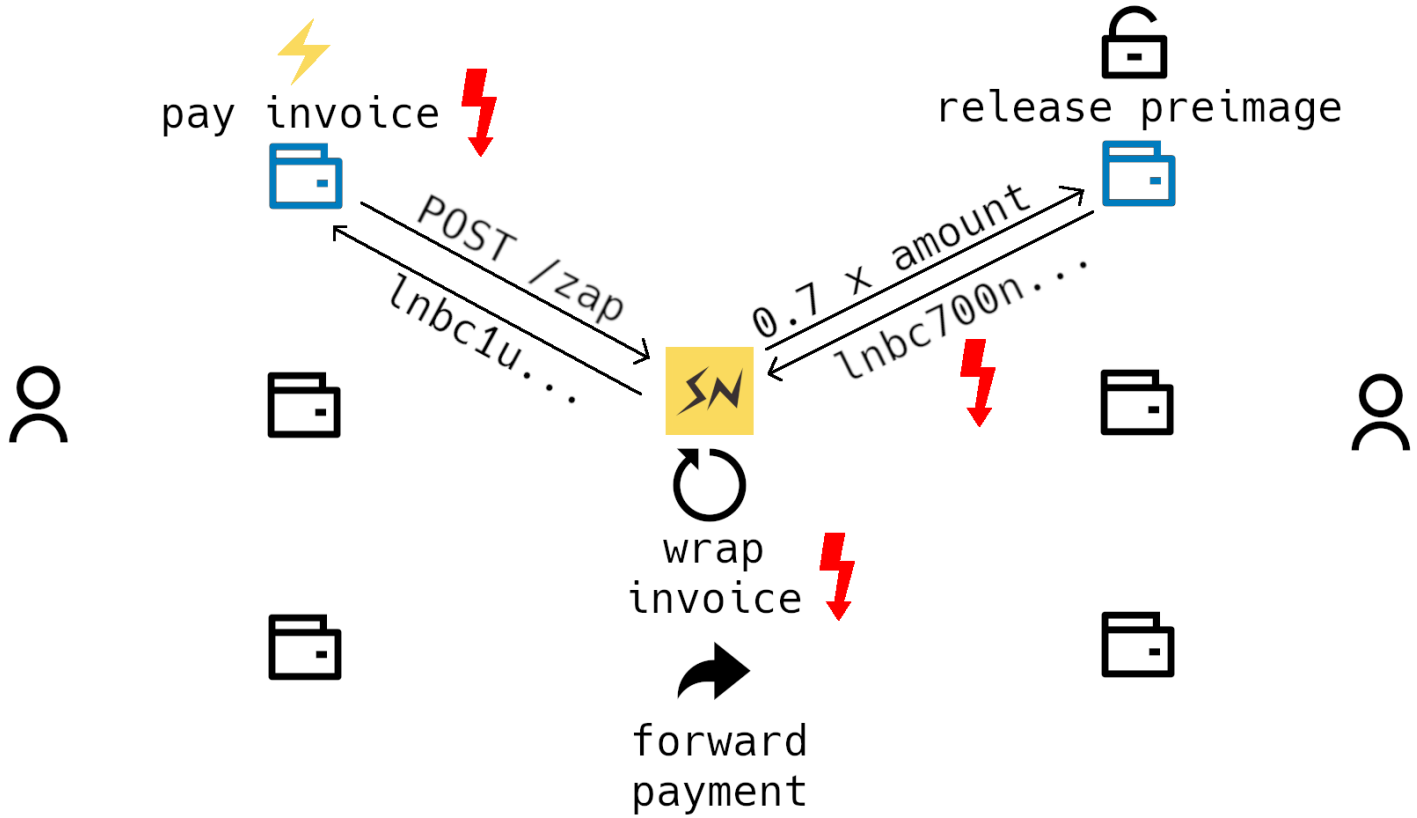
P2P zaps


pay invoice
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
release preimage
wrap invoice
forward payment

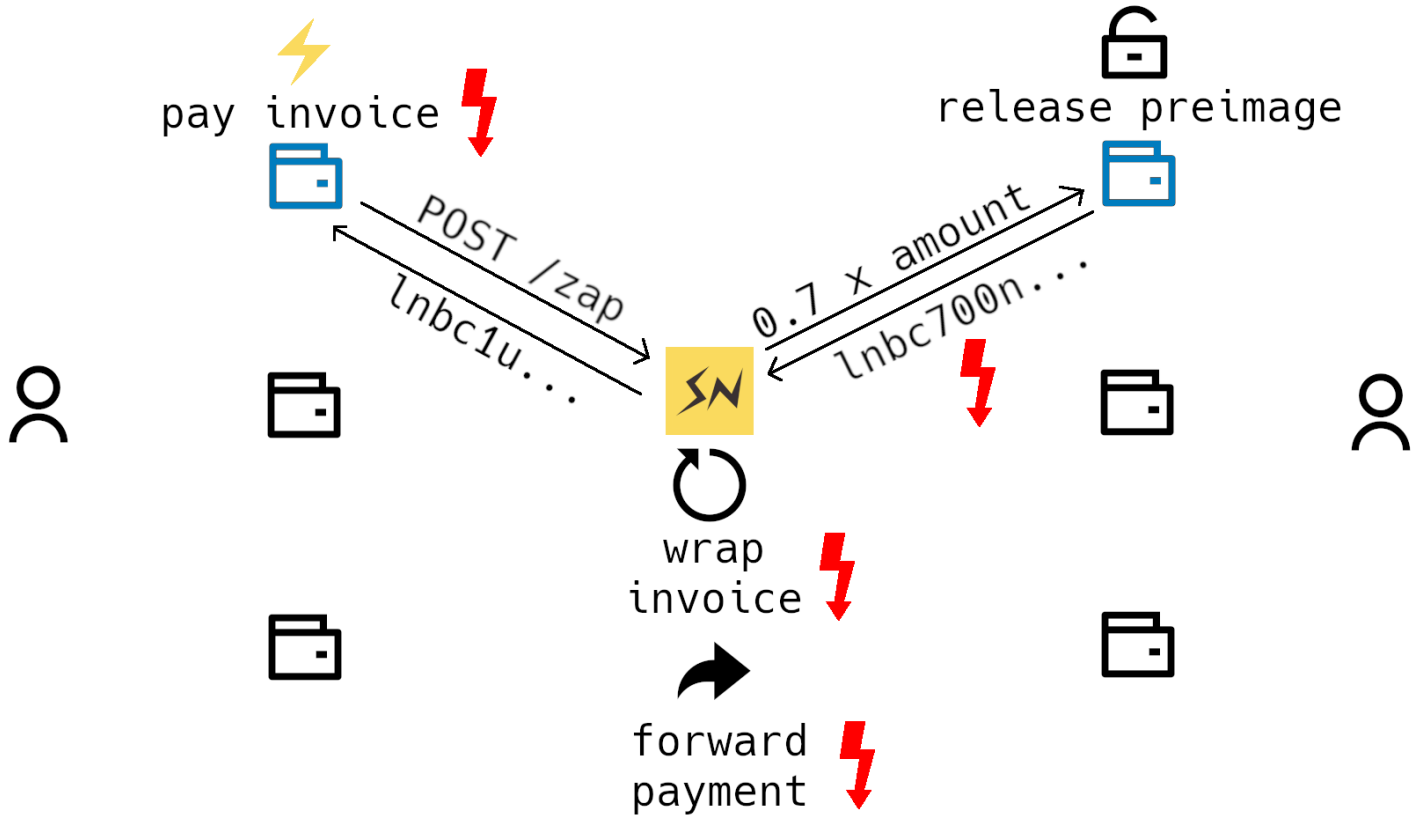
P2P zaps


pay invoice
release preimage
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
wrap invoice
forward payment

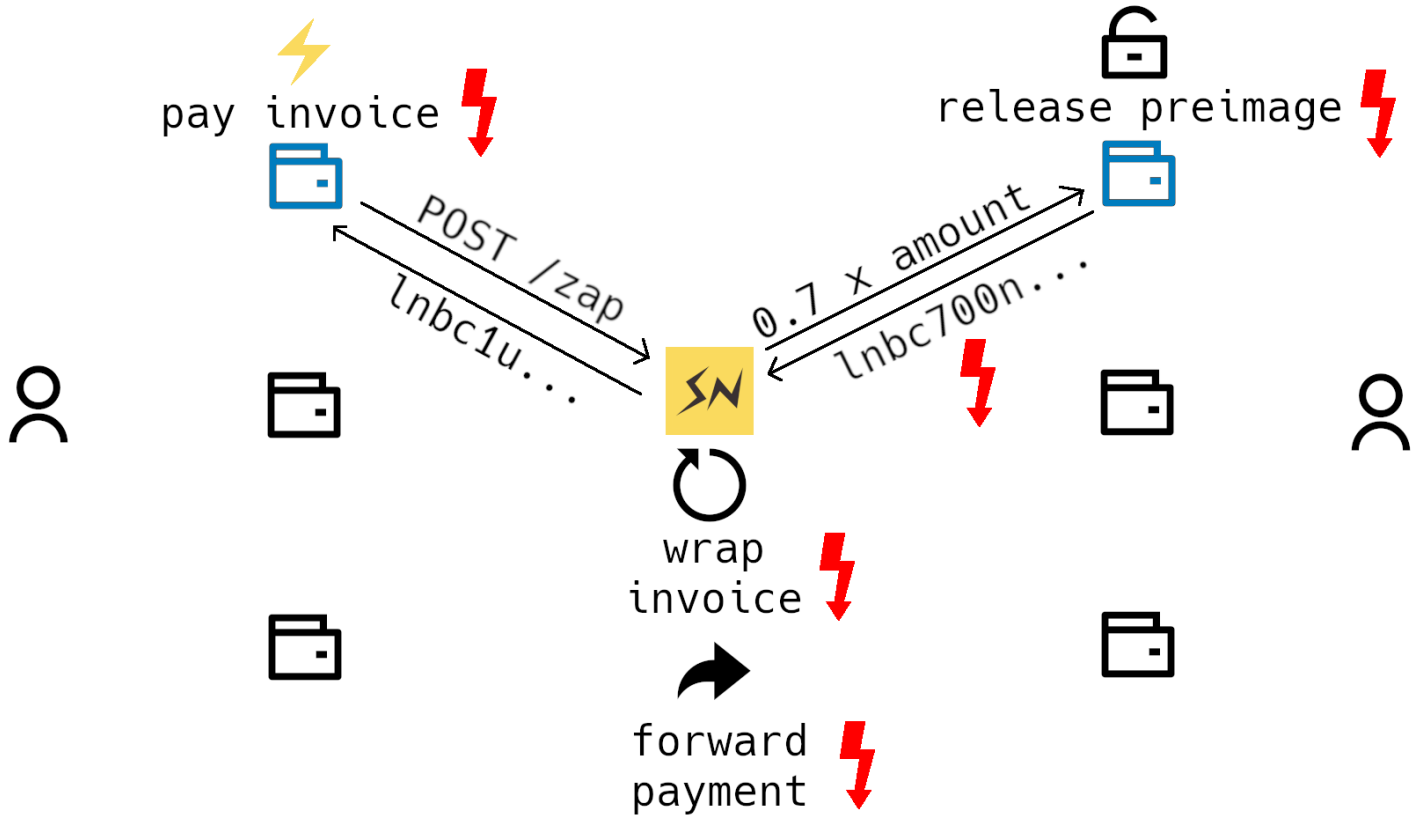
P2P zaps


pay invoice
release preimage
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
wrap
invoice
forward
payment

P2P zaps


pay invoice
POST /zap
lnbc1u...
release preimage
0.7 x amount
lnbc700n...
wrap invoice
forward payment

P2P zaps


pay invoice
release preimage
POST /zap
lnbc1u...
0.7 x amount
lnbc700n...
wrap invoice
forward payment

P2P zaps

Summary:

Lightning on the Application layer

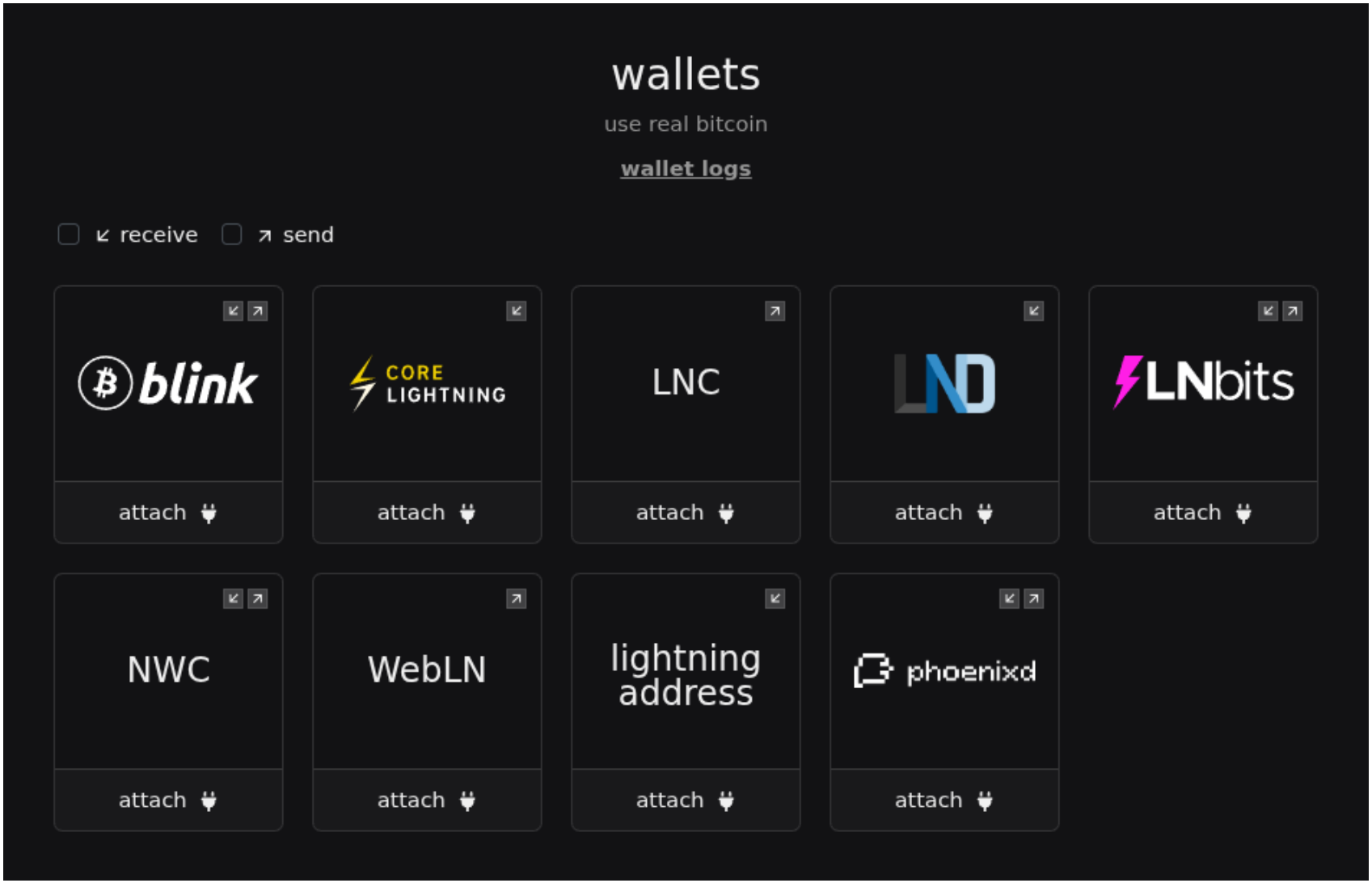
Reminder to show notifications

Challenges

Challenges

- zaps must include forwarding fee
- wallets vs protocols

Challenges


wallets
use real bitcoin
wallet logs
receive
send
blink
CORE LIGHTNING
LNC
LND
LNbits
NWC
WebLN
lightning address
phoenixd
attach
attach
attach
attach
attach
attach
attach
attach
attach

Challenges

- share wallets between multiple devices
- encrypted send credentials vs plaintext receive credentials
- how to test send credentials?

Challenges

- user education
- high availability lightning node
- liquidity issues
- forwarding to multiple receivers

What if somebody has no lightning wallet?

Cowboy Credits

Cowboy Credits exist to smooth over UX issues:

- new users do not have a wallet
- receiving sats can fail for many reasons
- some users prefer UX over sats

CCs are non-withdrawable

Cowboy Credits

Also:

- used first to pay SN instead of sats
- backup for lightning network issues
- 30% of a zap go to territory founders and rewards **as sats**

Half-life of a CC is two zaps

The End



special thanks to

plebpoet

