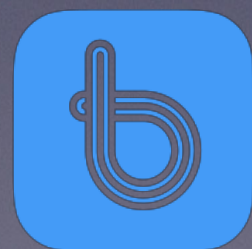


Lightning in Bitrefill

Justin Camarena

Chaincode Lightning Residency 2018



Bitrefill

Lightning Invoices

Lightning Payment Request Decoder

For decoding lightning network payment requests as defined in [BOLT #11](#).

Request String:

Inbc13370n1pdazz45pp5r4gk29vznylemn6dn5fyx2asnchdp7nzdur4fcempl7dfs8nn8aqdqagf5hgun9ve5kcmpqxyenxde3xvenwcqzysfnxd0qdp6wsmt5jw8z5mqawm4380w0la7m54kl7z7dk2gezu4zy4a7ugras9sez5s3k0sfn7u2me3wwf9z4tcv34t6m84lkj06qj5fsqkfkfmt

Decode

Payment Info:

Network	bitcoin mainnet
Amount	0.00001337 BTC
Date	Thu, 25 Oct 2018 00:13:40 GMT
Payment Hash	1d51651582993f9dcf4d9d12432bb09e2ed0fa626f0754e33b0ffcd4c0f399fa
Description	Bitrefill 13371337
Min Final CLTV Expiry	144
Expiration Time	3600 seconds
Signature	
<i>R value</i>	4cccd781a1d3a1b5d24e38a9b075dbac4ef73ffdf6e95b7fc2f36ca4645ca889
<i>S value</i>	5efb881f60586454846cf8267ee2b798b9c928aabc32355eb67afed27e812a26
<i>Recovery Flag</i>	0
Signing Data	6c6e62633133337306e0b7a2156810d0754594560a64fe773d3674490caec278bb43e989bc1d538cec3ff35303ce67e81a0ea134ba3932b334b636101899999b9899999bb001120
Checksum	kfkfmt

- Bolt 11
- Simple, extendable QR-code-ready protocol for requesting payments over Lightning
- Here is a decoded view of a bitcoin mainnet invoice

Lightning Invoices

```
Inbc13370n1pdazz45pp5r4gk29vznylemn6dn5fyx2asnchdp7nzdur4fcempl7  
dfs8nn8aqdqagf5hgun9ve5kcmpqxyenxde3xvenwcqzysfnxd0qdp6wsmt5jw  
8z5mqawm4380w0la7m54kl7z7dk2gezu4zy4a7ugras9sez5s3k0sfn7u2me3w  
wf9z4tcv34t6m84lkj06qj5fsqkfkfmt
```

Lightning Payment Request Decoder
For decoding lightning network payment requests as defined in [BOLT #11](#).

Request String:

```
Inbc13310n1pdazz45pp5r4gk29vznylemn6dn5fyx2asnchdp7nzdur4fcempl7dfs8nn8aqdqagf5hgun9ve5kcmpqxyenxde3xvenwcqzysfnxd0qdp6  
wsmt5jw8z5mqawm4380w0la7m54kl7z7dk2gezu4zy4a7ugras9sez5s3k0sfn7u2me3wwf9z4tcv34t6m84lkj06qj5fsqkfkfmt
```

Decode

Uh-Oh! Something is not quite right with this request.
Malformed request: checksum is incorrect

- Modification of an invoice will invalidate invoice due to checksum
- Similar to checksums for online addresses except more data is covered

Lightning Invoices

```
lnbc13370n1pdazz45pp5r4gk29vznylemn6dn5fyx2asnchdp7nzdur4fcempl7  
dfs8nn8aqdqagf5hgun9ve5kcmpqxyenxde3xvenwcqzysfnxd0qdp6wsmt5jw  
8z5mqawm4380w0la7m54kl7z7dk2gezu4zy4a7ugras9sez5s3k0sfn7u2me3w  
wf9z4tcv34t6m84lkj06qj5fsqkfkfmt
```

- A double click copies the entire invoice helping avoid users only copying some of the order information
- In comparison Bitcoin Cash for some reason includes the uri prefix in addresses making copying annoying

Lightning Invoices

lnbc**13370n**1pdazz45pp5r4gk29vznylemn6dn5fyx2asnchdp7nzdur4fcempl7
dfs8nn8aqdqagf5hgun9ve5kcmpqxyenxde3xvenwcqzysfnxd0qdp6wsmt5jw
8z5mqawm4380w0la7m54kl7z7dk2gezu4zy4a7ugras9sez5s3k0sfn7u2me3w
wf9z4tcv34t6m84lkj06qj5fsqkfkfmt

- The network and amount are actually human readable but obscure enough for users to not try and manually set the amount for lightning payments
- One of the biggest problems on chain merchants have is users manually inputting amounts incorrectly or sending fiat amounts

Lightning Invoices Uses on Chain

- User errors with the system we have now
- Bitpay solution for this was BIP70 to force you to pay by scanning QR code or via a uri link
- Unless using a decoder most wallets cannot pay bitpay
- Many of those benefits provided with lightning invoices without the negative aspects
- Encode extra data for suggested fee rate for on chain usage
- Probably a big percentage exchange related subtracting withdrawal fee from sending amount causing issues
- Bitpay pretty much stopped most users using exchanges to send them that route

Lightning Invoices and BIP 21

- Thoughts on using BIP21 for lightning
- BIP21: backward-compatibility, URI Scheme, QR Codes
- Hard to select a BIP21 encoded string with two clicks
- bitcoin:**1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMH?**
amount=20.3&label=Foobar
- Lack of wallet support decoding when pasted, never intended to do this I think
- Preference to moving even bitcoin on chain send and receives to use lightning invoices, probably unpopular
- Worst case can encode information in bip21 and also incode it in the lightning invoice

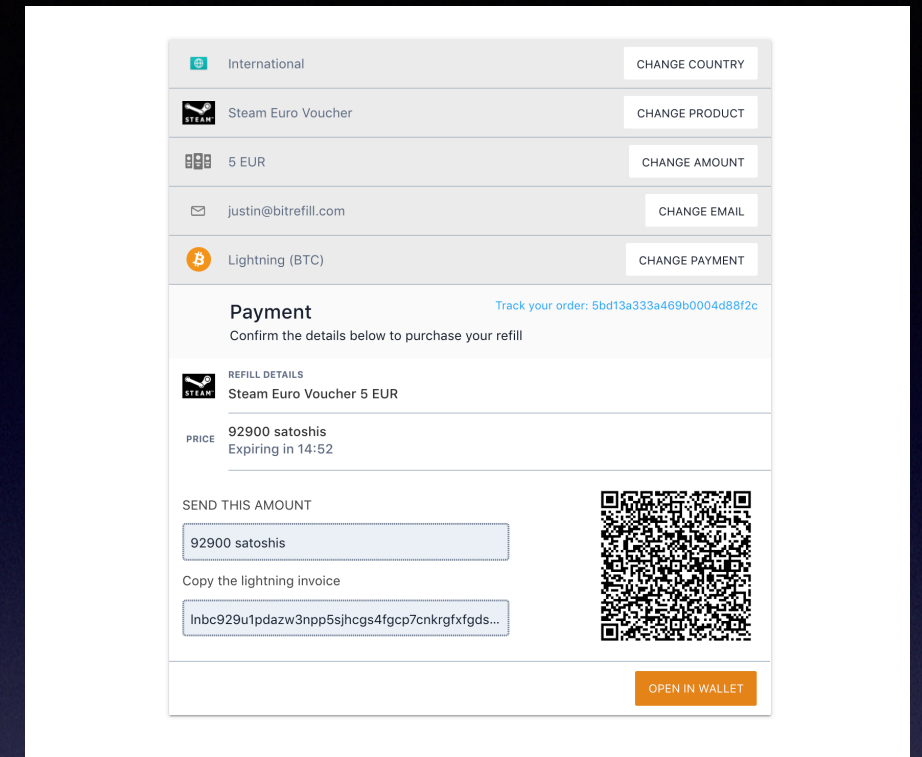
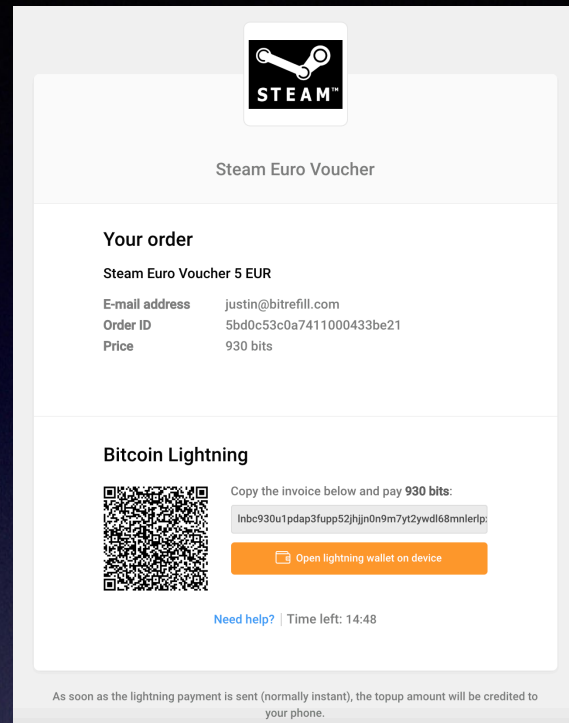
UX Improvements with lightning

- Goal of removing Partial Order failures
- Funds not being sent after expiry, although some may settle after
- In practice at Bitrefill we have seen issues with lightning invoices being paid after expiry off chain
- No notification set, amount paid is not updated
- PR for invoices settled on chain updating amount paid is incoming for LND

Proof of Payment

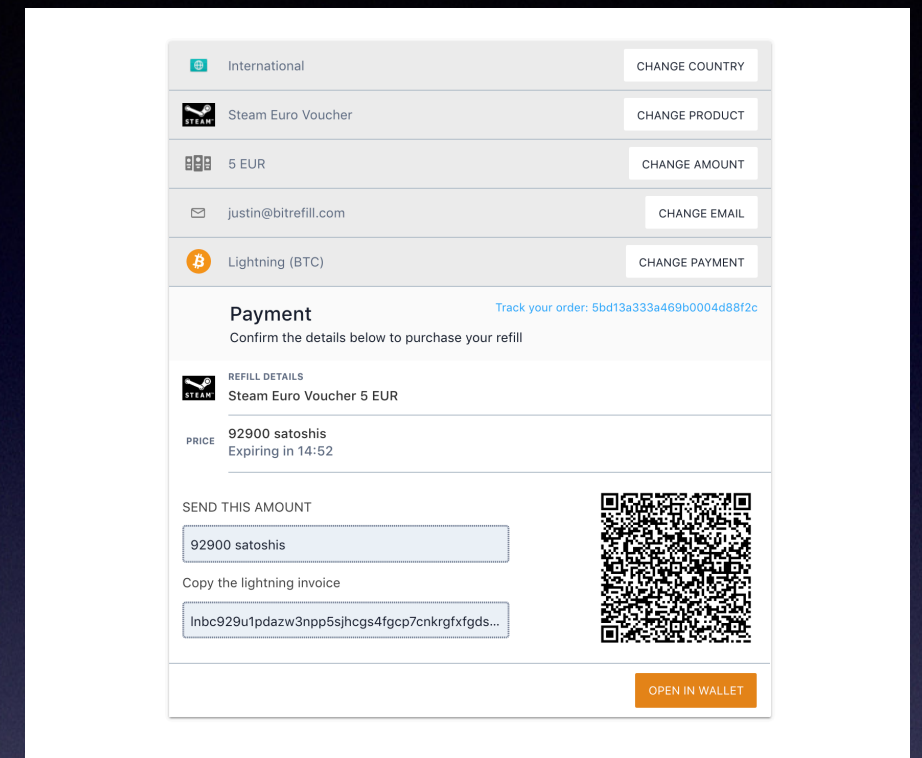
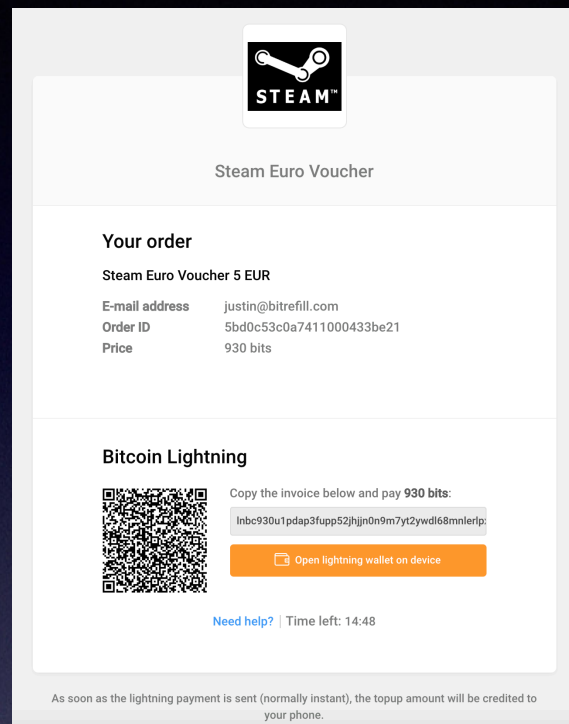
- What is proof of payment?
- Have had support issues remedied by user providing proof of payment
- Preimage Payment Hash

Lightning Payments



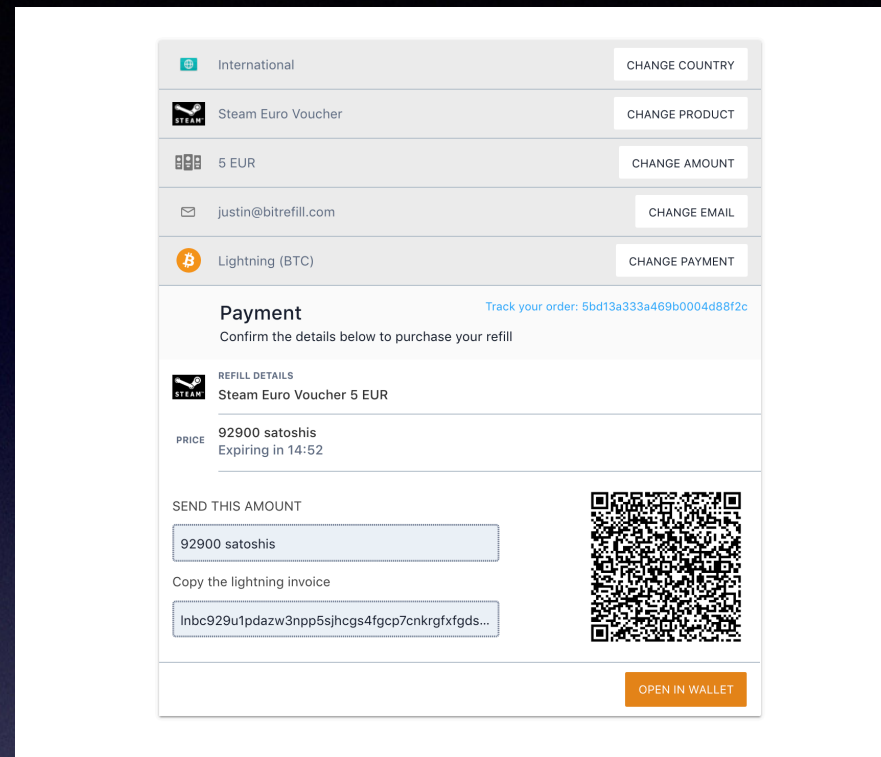
- Easy to integrate lightning basically reused bitcoin payments flow
- In a redesign we made QR codes bigger to be easier to scan
- Autocopy for important info
- Units: Bits vs Satoshis
- Doesn't really matter users will see their preferred unit in their wallet

Lightning Payments



- User confusion by calling it Bitcoin Lightning
- There was actually an altcoin with that name I believe

Lightning Payments



The screenshot shows a web interface for purchasing a Steam Euro Voucher using Lightning payments. At the top, there are five configuration rows, each with a 'CHANGE' button: 'International' (country), 'Steam Euro Voucher' (product), '5 EUR' (amount), 'justin@bitrefill.com' (email), and 'Lightning (BTC)' (payment method). Below these is a 'Payment' section with a confirmation message and a tracking link. The 'REFILL DETAILS' section shows the product and price in satoshis. A 'SEND THIS AMOUNT' section contains a text input for the amount and a button to copy the invoice. A QR code is displayed on the right. At the bottom right is an 'OPEN IN WALLET' button.

International	CHANGE COUNTRY
Steam Euro Voucher	CHANGE PRODUCT
5 EUR	CHANGE AMOUNT
justin@bitrefill.com	CHANGE EMAIL
Lightning (BTC)	CHANGE PAYMENT

Payment [Track your order: 5bd13a333a469b0004d88f2c](#)
Confirm the details below to purchase your refill

REFILL DETAILS
Steam Euro Voucher 5 EUR

PRICE
92900 satoshis
Expiring in 14:52

SEND THIS AMOUNT

92900 satoshis

Copy the lightning invoice

lnbc929u1pdazw3npp5sjhcs4fgcp7cnkrxfxgds...

OPEN IN WALLET

- We do not actually publish our node info on our site but do separately
- Info is already in the invoice, wallets should be able to get connection details from gossip from other nodes
- We have channel minimums anyway so users may not open funds to us

Lightning Litecoin

- We currently also support litecoin lightning for orders
- A lot lower value due to no mobile wallets
- In the future we may phase it out when users can swap off chain easily

Lightning Invoices



- Uppercase lightning invoices when encoding in QR Codes
- 'All you need to get the better efficiency in QR is sequences of several characters of uppercase+digits in a row' - sipa
- Most wallets support even having the uri prefix capitalized as well but it is not a requirement

Wallets

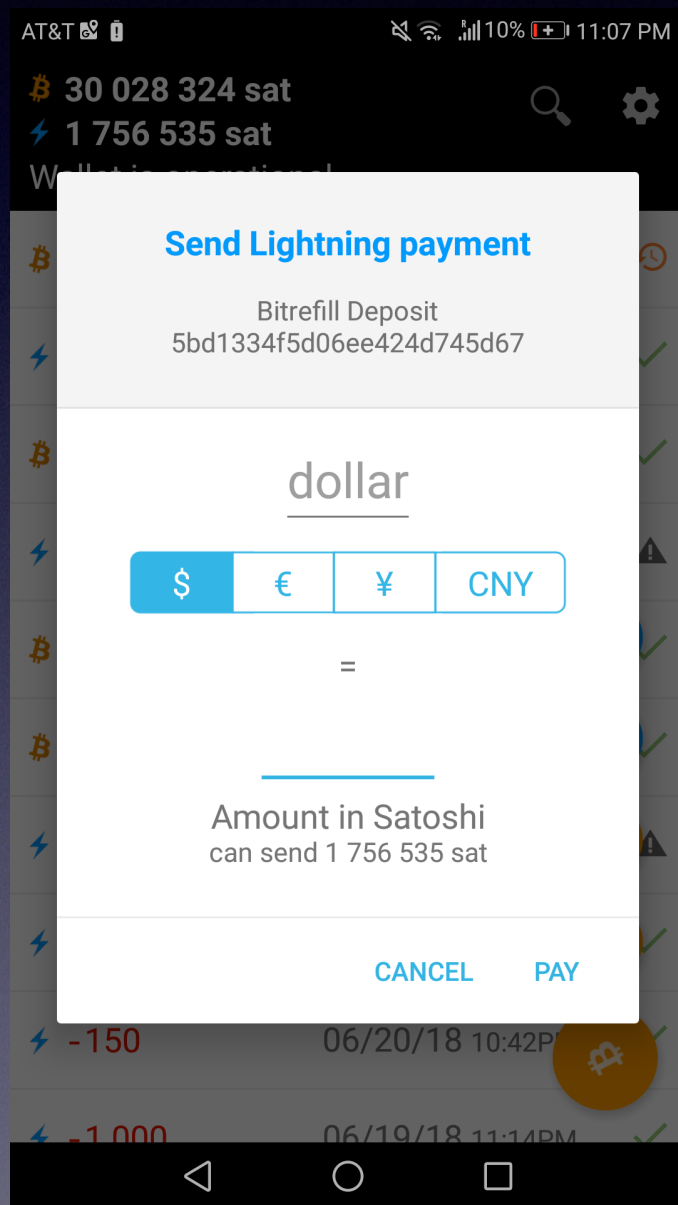
- Mobile Wallets in use
- Zap, Eclair, Bitcoin Lightning Wallet
- Zap with remote node feature and receive funds
- BLW can as well, but a bit more centralized
- Eclair is send only for now but may have receive functionality in the future

Lightning Deposits

- 0 amount invoices can be an option for deposits
- Possible use case being send all feature
- Sendable balance meaning balance minus the reserve with amount being sent reduced for routing fees until successful routed
- Amounts can also be set as not all lightning wallets support sending payments without amounts set unfortunately
- Downside being a user may try to send an amount our node may not have capacity to receive
- When crediting deposits credit amount paid and not invoice amount when dealing with deposits as many implementation pay more than invoice amount, LND

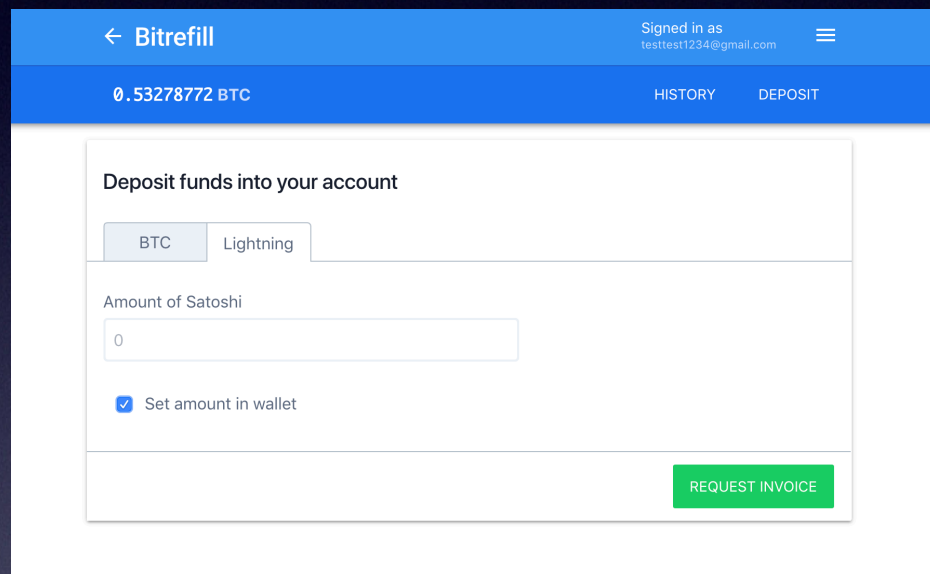
The screenshot shows the Bitrefill web interface for depositing funds. At the top, a blue header bar contains a back arrow, the text 'Bitrefill', the user's balance '0.53278772 BTC', and a 'Signed in as' status with an email address. Below the header, there are tabs for 'HISTORY' and 'DEPOSIT'. The main content area is titled 'Deposit funds into your account'. It features two tabs: 'BTC' (selected) and 'Lightning'. Under the 'Lightning' tab, there is a text input field labeled 'Amount of Satoshi' with the value '0'. Below this is a checkbox labeled 'Set amount in wallet' which is checked. A green button labeled 'REQUEST INVOICE' is positioned at the bottom right of the form.

Lightning Deposits



- BLW is one wallet that can pay invoices without an amount set with user setting the amount to send
- Can also set amount in the cli with Ind
- Useful for exchanges for users wanting to pay an invoice and have that amount known only when the node receives payment for trades
- Ideally invoices for tips and other use cases will not use invoices in the future

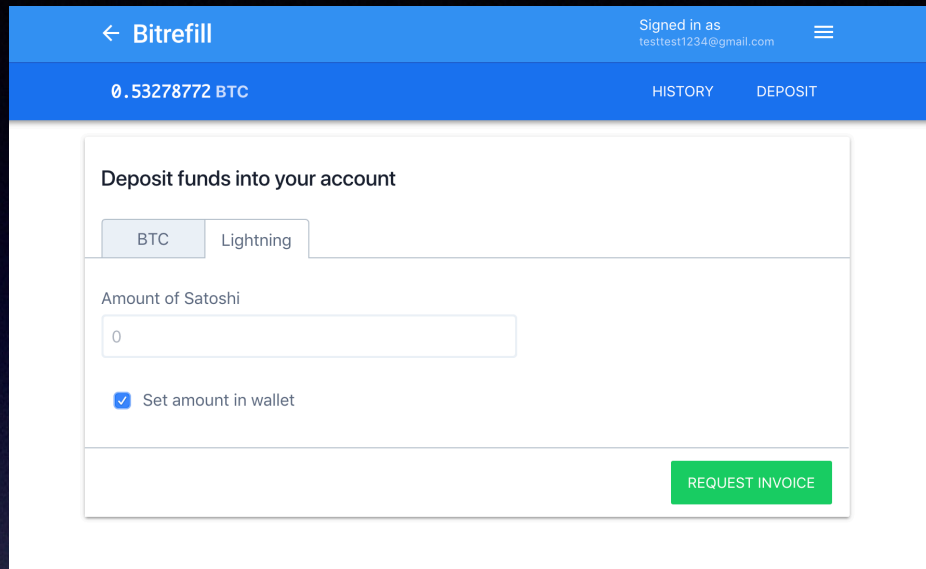
Lightning Deposits



The screenshot shows the Bitrefill web interface for depositing funds. At the top, a blue header bar contains a back arrow, the 'Bitrefill' logo, the user's login status ('Signed in as testtest1234@gmail.com'), and a menu icon. Below the header, a blue bar displays the current balance '0.53278772 BTC' and navigation links for 'HISTORY' and 'DEPOSIT'. The main content area is titled 'Deposit funds into your account'. It features two tabs: 'BTC' (selected) and 'Lightning'. Under the 'Lightning' tab, there is a text input field labeled 'Amount of Satoshi' with the value '0'. Below this, a checkbox labeled 'Set amount in wallet' is checked. A green button labeled 'REQUEST INVOICE' is positioned at the bottom right of the form.

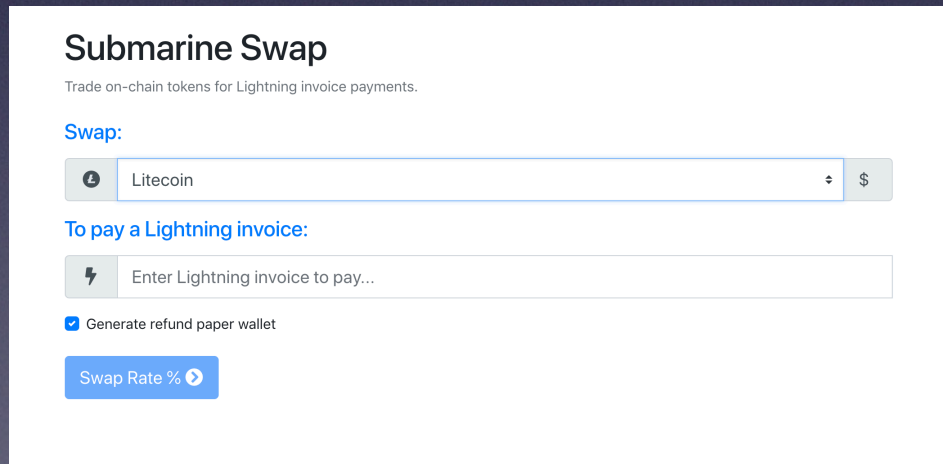
- Deposit are live in production!
- Can deposit as low as 1 satoshi or up to payment limit which is currently around 0.04 BTC

Lightning Deposits



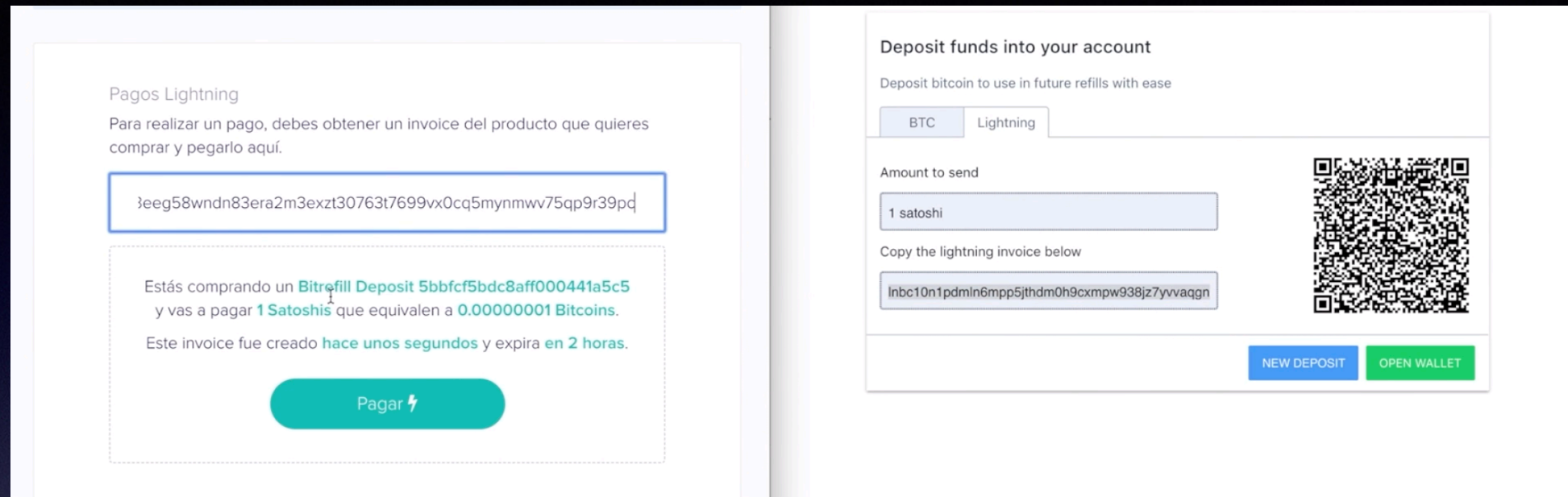
The screenshot shows the Bitrefill Lightning deposit interface. At the top, there's a blue header with a back arrow, the text "Bitrefill", and a "Signed in as" section showing "testtest1234@gmail.com". Below the header, a blue bar displays "0.53278772 BTC" and navigation links for "HISTORY" and "DEPOSIT". The main content area is titled "Deposit funds into your account" and features two tabs: "BTC" and "Lightning". The "Lightning" tab is active, showing a form with a label "Amount of Satoshi" and a text input field containing "0". Below the input field is a checked checkbox labeled "Set amount in wallet". A green "REQUEST INVOICE" button is positioned at the bottom right of the form.

- Submarine swaps allows us to simplify deposit flow
- Altcoiners can send credit to a swap provider which sends us bitcoin over lightning



The screenshot displays the "Submarine Swap" interface. It starts with the title "Submarine Swap" and a subtitle "Trade on-chain tokens for Lightning invoice payments." Below this, there's a "Swap:" section with a dropdown menu currently set to "Litecoin" and a currency selector showing "\$". The "To pay a Lightning invoice:" section includes a text input field with a lightning bolt icon and the placeholder text "Enter Lightning invoice to pay...". A checked checkbox labeled "Generate refund paper wallet" is located below the input field. At the bottom, there's a blue button labeled "Swap Rate %" with a right-pointing arrow.

Lightning Withdrawals



- Auto decode invoices for users
- Buda charges no fee, but should in practice
- Custodial wallets
- Make faucets great again

Lightning Withdrawals

- Bitrefill's work on Lightning Withdrawals
- Currently there are issues with sending lightning payments: stuck HTLCs are annoying
- Better error codes needed for lightning sending api with Ind needed
- Better handling and documentation on lifecycle of lightning payments and knowing when a new payment can be attempted or when to refund balance for a user when payment stuck in transition or timed out
- Check payment status api coming for LND
- Currently can check for stuck HTLCs in listchannels
- Incoming in 2 weeks

Improvements to the Lightning User Experience

- Routing failures
 - Fallback addresses used as a backup when routing has failed when order over x amount
 - Uses our own infrastructure to check on chain payments
-
- Worked with BLW to support this
 - BLW will pay fallback address, and open channel in change output in some cases
 - Proposals to use push amount to pay and open channel as well

Lightning Refunds

Future UX

- Users may not have incoming capacity to receive a refund when sending their first payment due to the lightning reserve being held in channels
- Bitrefill can hold on to an Invoice and not settle immediately until the order is successful
- If the order fails we can fail the invoice and the user is automatically refunded once LND integrates this
- Doesn't apply for orders that seem successful on our end and end up needing to be refunded

Lightning Refunds

Future UX

- So many refund options
- For now we'll keep the on chain option
- In the future probably hold invoices and fail them
- Then maybe support paying invoices for refunds, or on chain if the invoice includes a fallback address