Peer-to-peer Lightning Exchange
(NAME TBD)

Concept draft v0.0.1
Author: Reckless_Satoshi
27/12/2021

Summary: Simple privacy focused p2p swap of Sats ↔ fiat over lightning using hodl invoices.

Focus: - Privacy first. (leave no room for users to do silly privacy mistakes)
- Trust minimized. (Peers need no trust on each other)
- Open source. (TBD: MIT or AGPL3.0).
- Easy, Snappy and Beautiful.

Inspiration / original idea: p2plnbot project by @negrunch https://github.com/grunch/p2plnbot

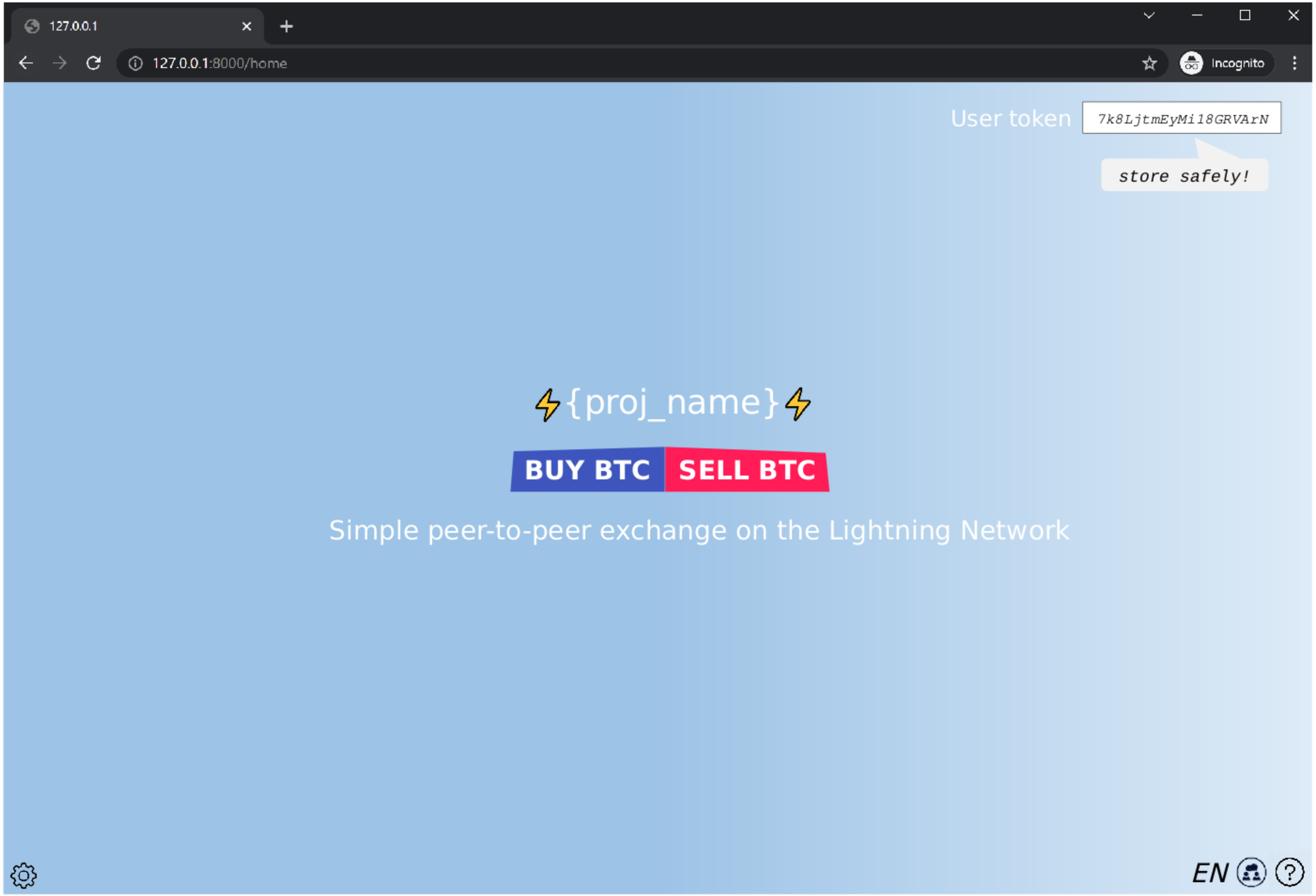
Table of content

1) Vision Front-End walk-troughs (forgive the ugliness)

    - Walk-trough as buyer and maker. Slide 3
    - Walk-trough as seller and taker. Slide 15

2) Preview of */preliminary_tests/.* Slide 23

3) Rough concept for Back-End REST API. Slide 26



User token 7k8LjtmEyMi18GRVArN

store safely!

⚡{proj_name}⚡

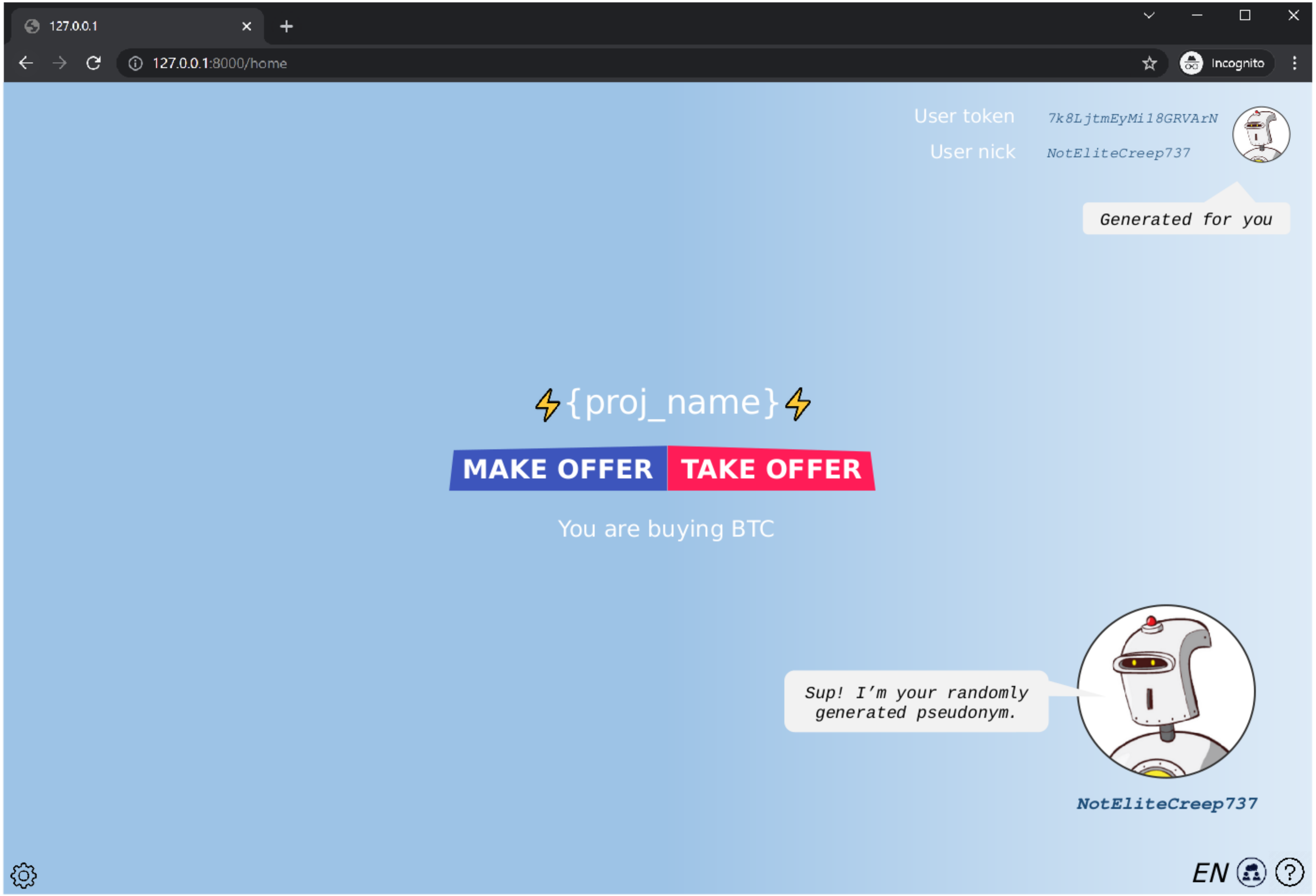
Simple peer-to-peer exchange on the Lightning Network

{proj_name} : TBD (p2psats.bot, hodlnow, justsats, p2psats.space (...))
User token: Base58 random string of (28-44) characters (160-256 bits entropy) generated locally (or input from user). Only its SHA256 hash is sent to server to generate a new ID / API authentication token.

Clicked

BUY BTC

- Gets user nick
- Moves into peer-kind selection



127.0.0.1:8000/home

User token 7k8LjtmEyMi18GRVArN

User nick NotEliteCreep737

Generated for you

{proj_name}

You are buying BTC

Sup! I’m your randomly generated pseudonym.

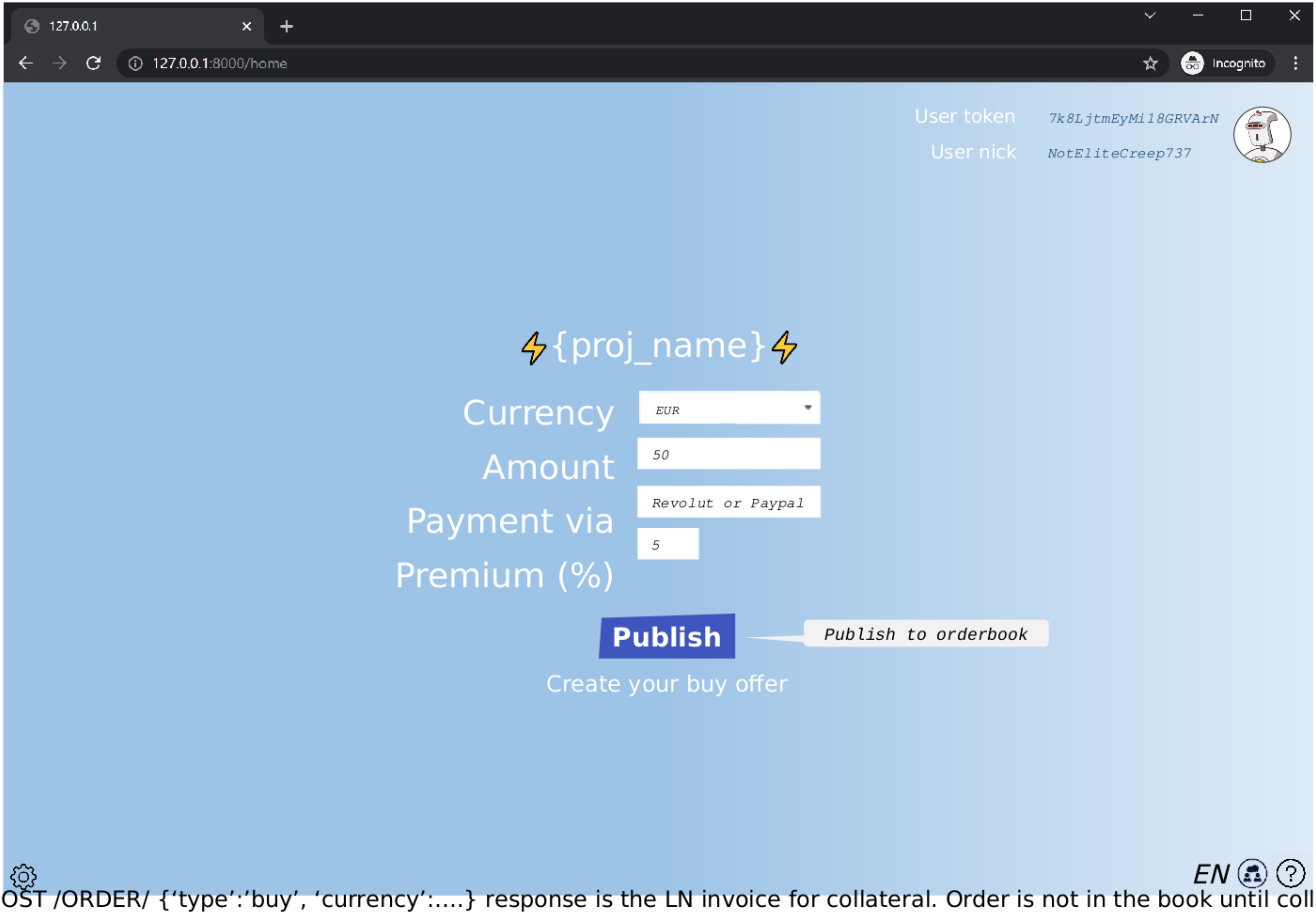
NotEliteCreep737

User nick and avatar generated deterministically from token hash (use robohash and nick_generation).

Clicked

MAKE OFFER

- Moves into form



User token 7k8LjtmEyMi18GRVArN

User nick NotEliteCreep737

⚡{proj_name}⚡

Currency: EUR

Amount: 50

Payment via: Revolut or Paypal

Premium (%): 5

Publish — Publish to orderbook

Create your buy offer

PUBLISH calls POST /ORDER/ {‘type’:’buy’, ‘currency’:….} response is the LN invoice for collateral. Order is not in the book until collateral is posted.

Currency: string from dropdown menu. Amount: int. Payment method: string. Premium: float.

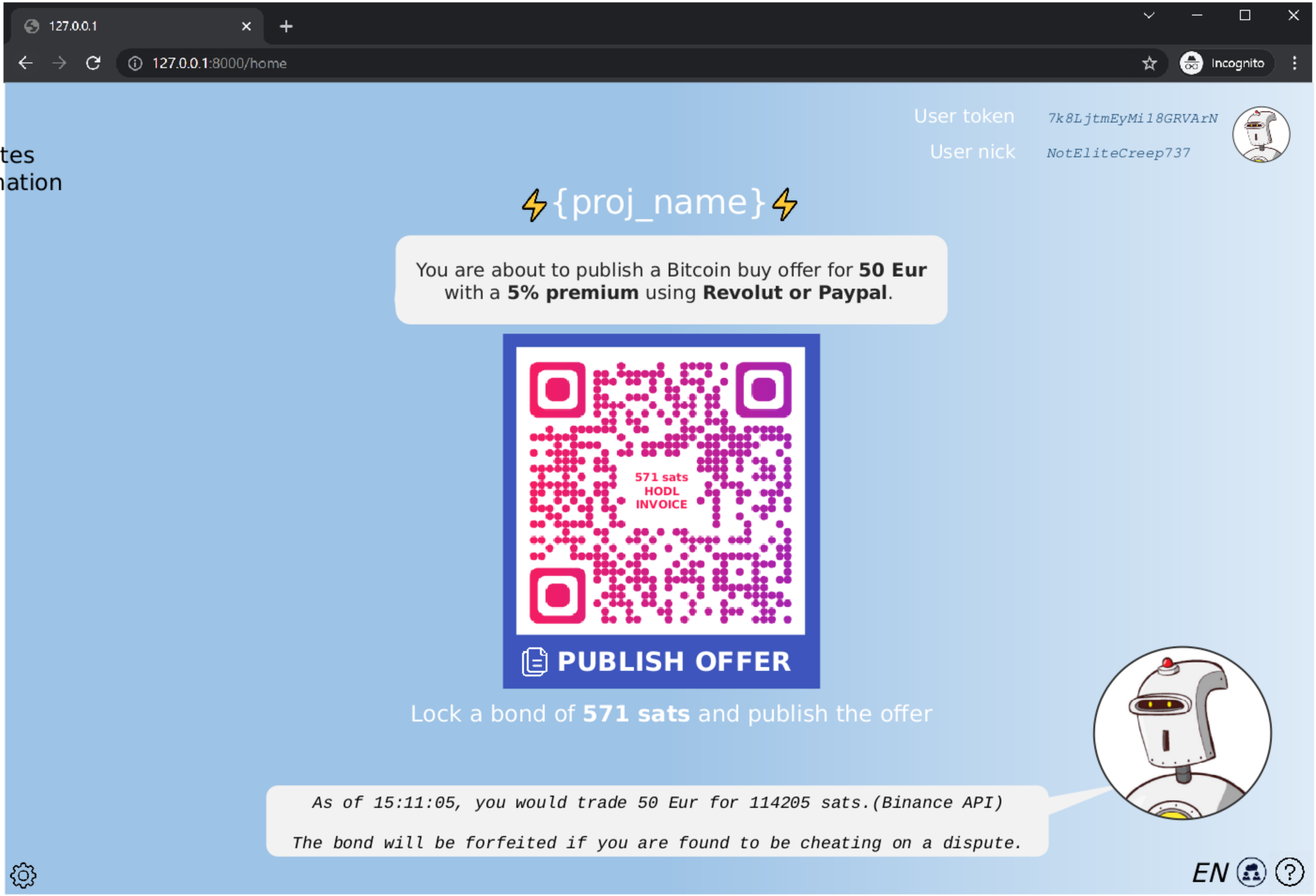
Extra feature: Option to add Amount of sats instead of premium; effectively creating a new price for {proj_name}
last trade price of {proj_name} could be offered via the publicAPI. Meant to reflect Non-KYC Bitcoin exchange rate.

Clicked **Publish**

- Creates summary

Computes current rates

Asks user for confirmation



User token 7k8LjtmEyMi18GRVArN

User nick NotEliteCreep737

⚡{proj_name}⚡

You are about to publish a Bitcoin buy offer for **50 Eur** with a **5% premium** using **Revolut or Paypal**.

PUBLISH OFFER

Lock a bond of **571 sats** and publish the offer

As of 15:11:05, you would trade 50 Eur for 114205 sats.(Binance API)

The bond will be forfeited if you are found to be cheating on a dispute.

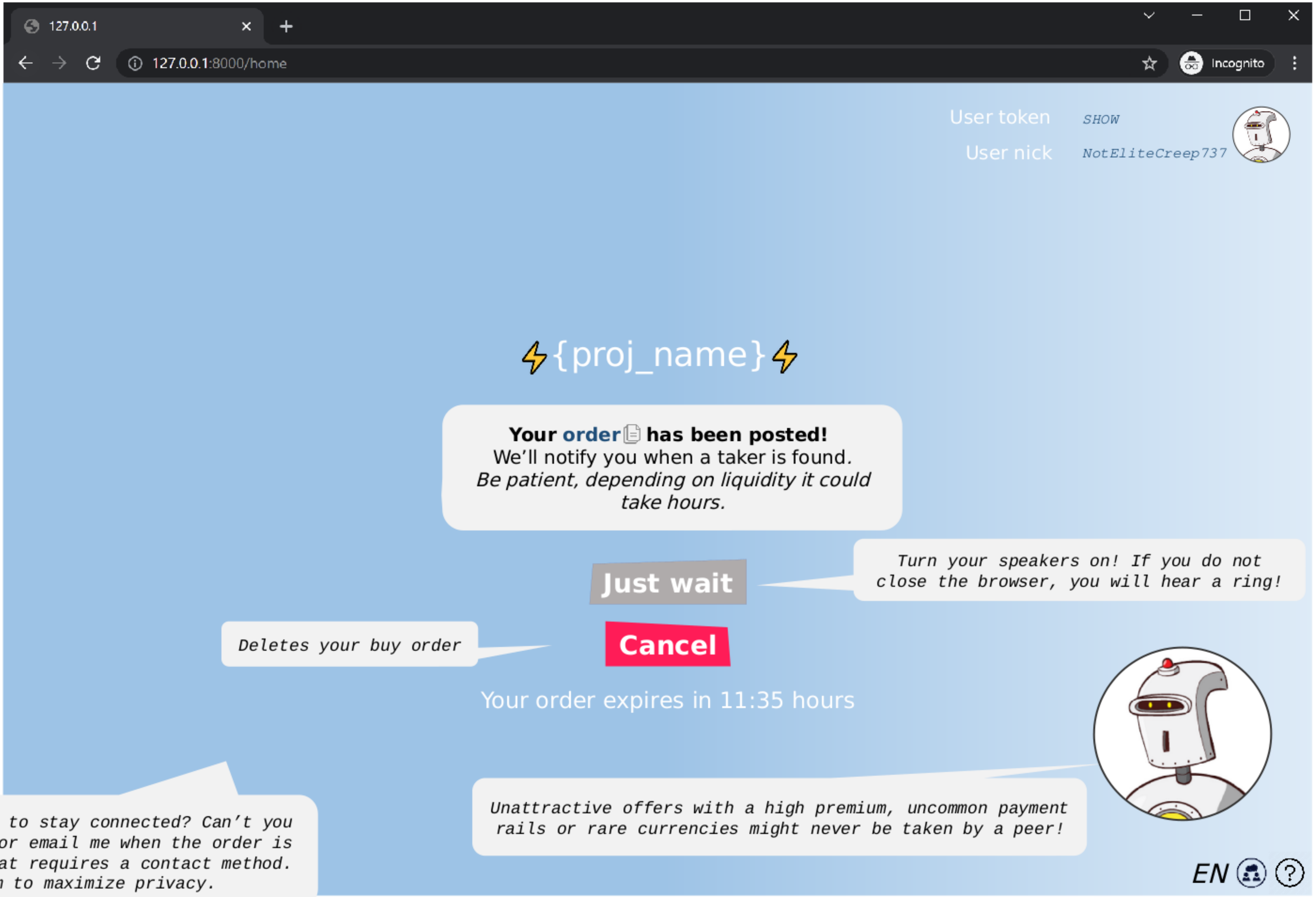
Why a bond? Reduce order spamming, reduce cheating incentives.

The backend notices via LND gRPC that the invoice was paid and publishes the offer (next slide). It should take a couple seconds between QR scanning and letting user proceed.

Wait

Sure!

- Adds transaction To order book



⚡{proj_name}⚡

Your order has been posted!
We'll notify you when a taker is found.
Be patient, depending on liquidity it could take hours.

Your order expires in 11:35 hours

Turn your speakers on! If you do not close the browser, you will hear a ring!

Deletes your buy order

Unattractive offers with a high premium, uncommon payment rails or rare currencies might never be taken by a peer!

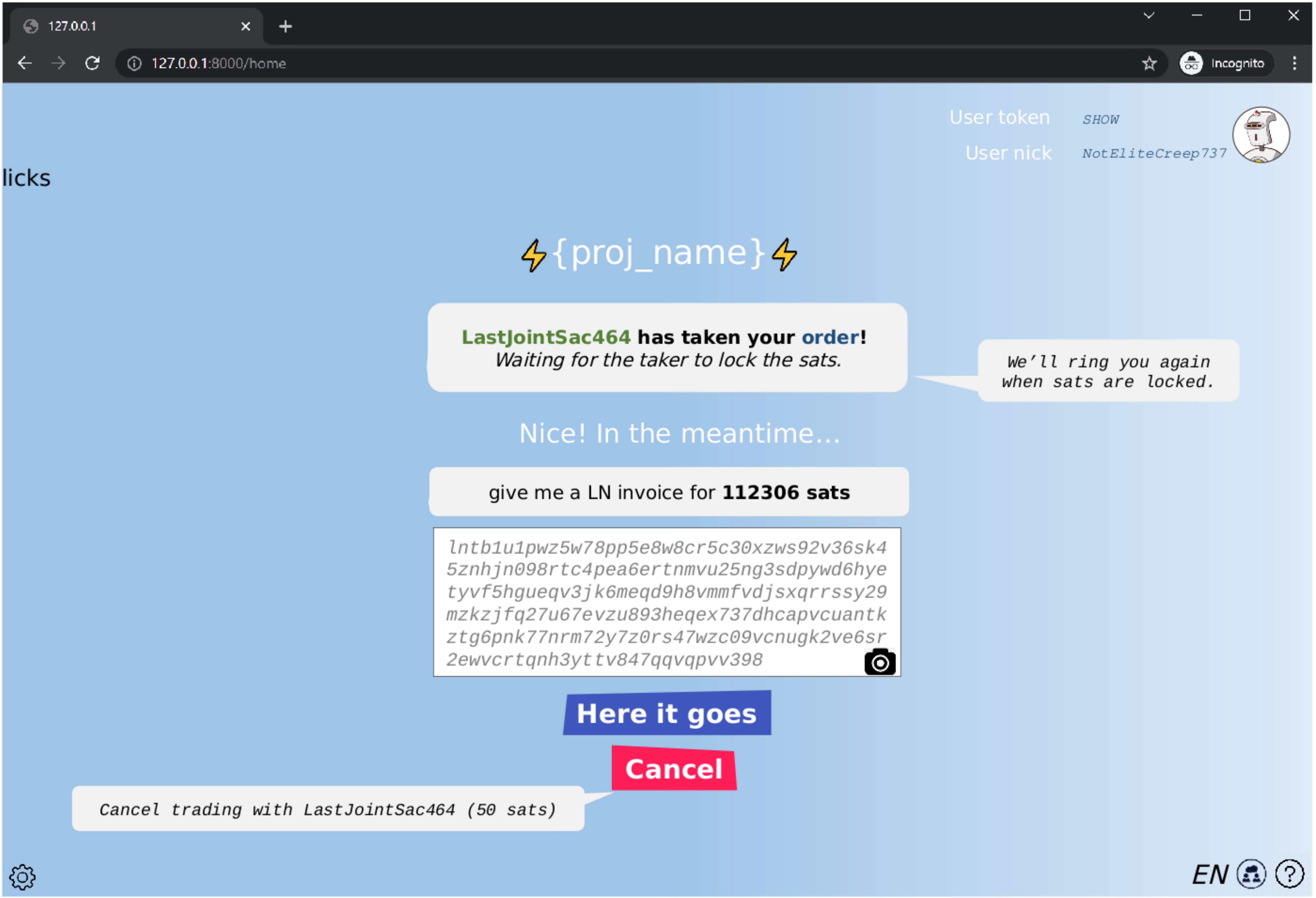
*Why do I have to stay connected? Can't you just text me or email me when the order is taken? **NO:** that requires a contact method. We aim to maximize privacy.*

Event

Order taken

- Ring
- Exchange price

Is fixed when taker clicks



User token *SHOW*

User nick *NotEliteCreep737*

⚡{proj_name}⚡

LastJointSac464 has taken your order!
Waiting for the taker to lock the sats.

We'll ring you again when sats are locked.

Nice! In the meantime...

give me a LN invoice for **112306 sats**

```
lntb1u1pwz5w78pp5e8w8cr5c30xzws92v36sk4
5znhjn098rtc4pea6ertnmvu25ng3sdpywd6hye
tyvf5hgueqv3jk6meqd9h8vmmfvdjsxqrrssy29
mzkzjfq27u67evzu893heqex737dhcapvcuantk
ztg6pnk77nrm72y7z0rs47wzc09vcnugk2ve6sr
2ewvcrtqnh3yttv847qqvqpvv398
```

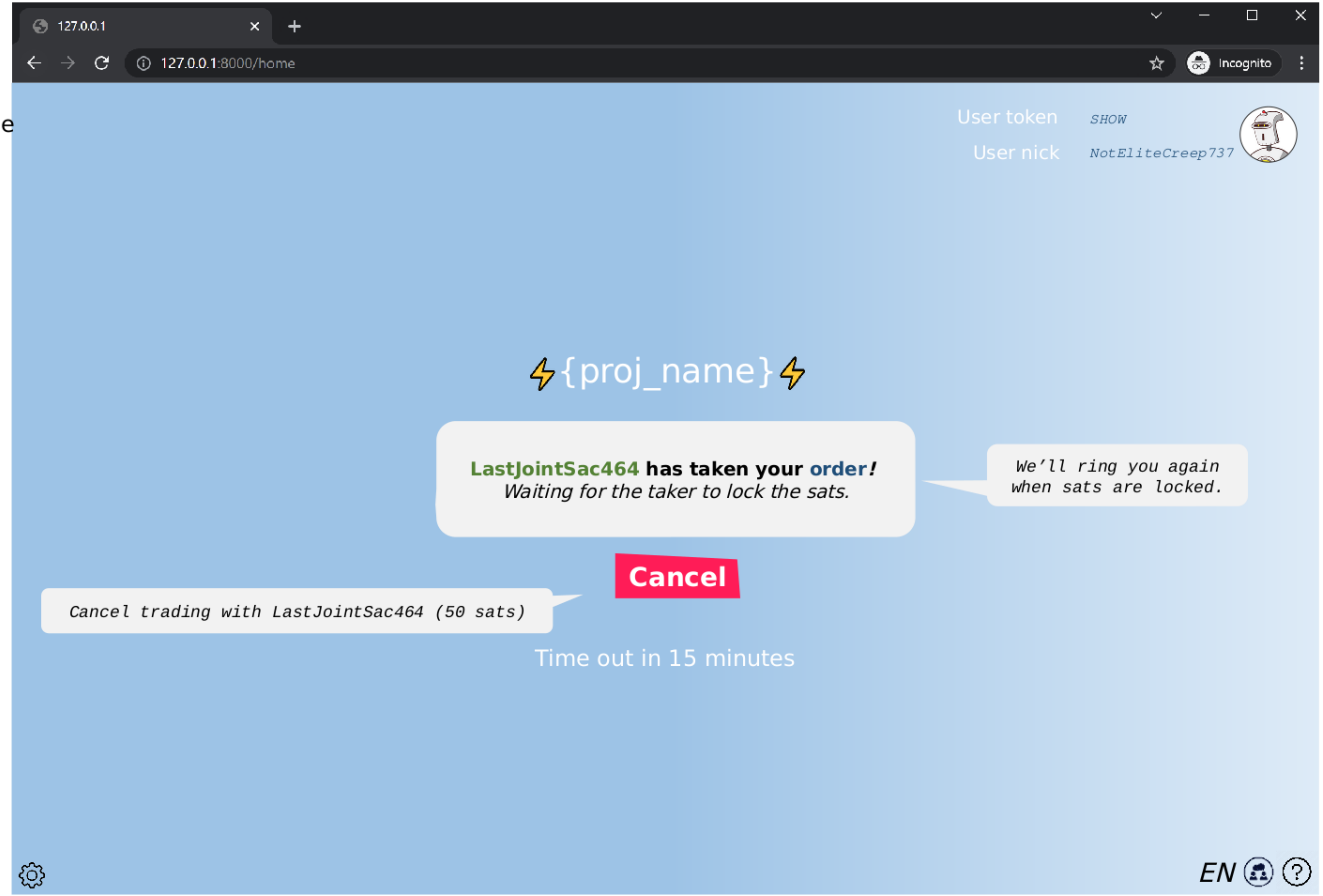
Cancel trading with LastJointSac464 (50 sats)

Click on order: calls GET /ORDER/ {'order_id'...} to get a summary of the order

Click

Here it goes

- Submit LN invoice



LastJointSac464 has taken your order!
Waiting for the taker to lock the sats.

We'll ring you again when sats are locked.

Cancel trading with LastJointSac464 (50 sats)

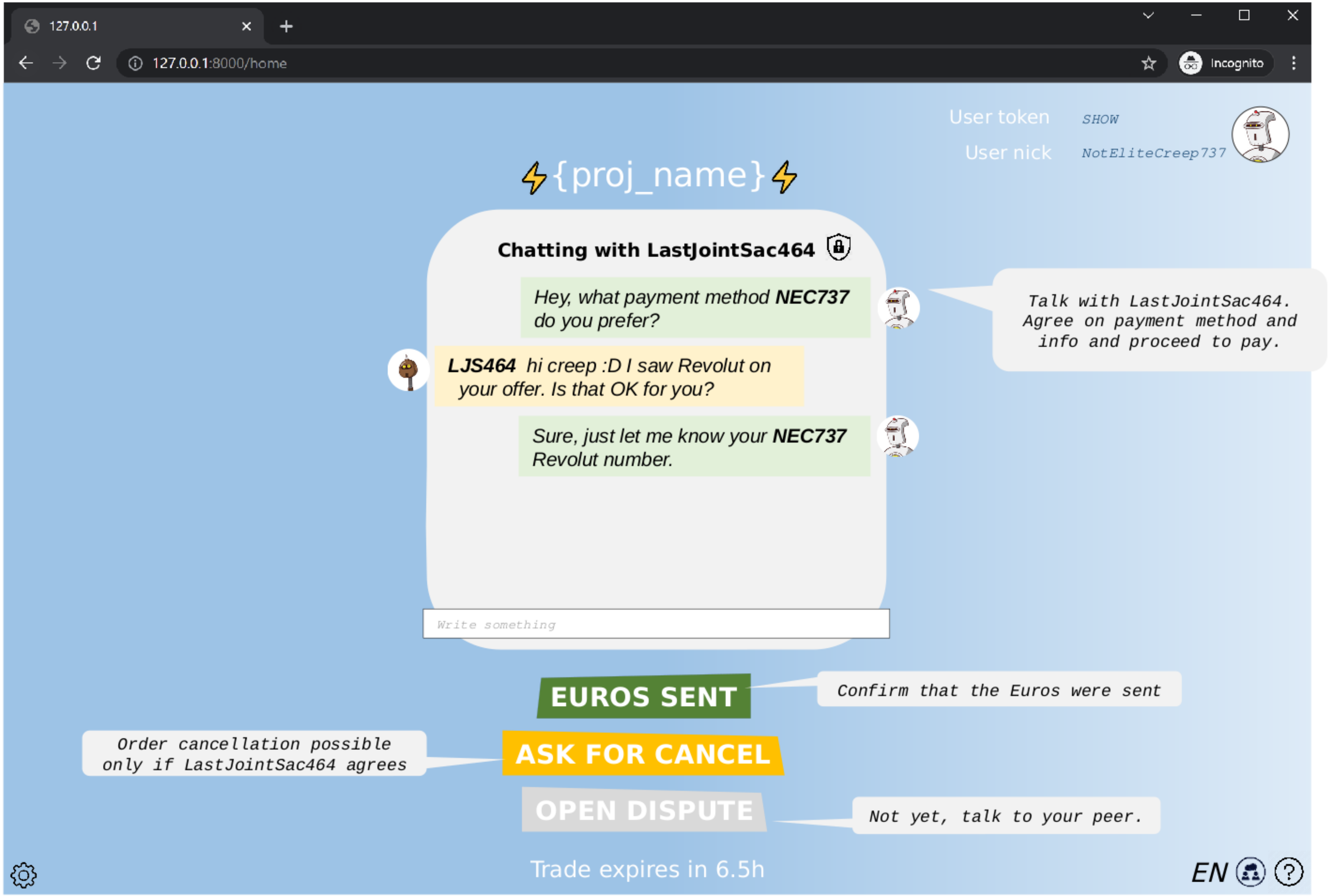
Time out in 15 minutes

Cancelling taken orders could be a way to DDOS the order book (and it's awful user experience). Must have a small fee.

Event

Peer locked funds

- Adds transaction To order book



Chatting with LastJointSac464

*Hey, what payment method **NEC737** do you prefer?*

LJS464 *hi creep :D I saw Revolut on your offer. Is that OK for you?*

*Sure, just let me know your **NEC737** Revolut number.*

Talk with LastJointSac464. Agree on payment method and info and proceed to pay.

Confirm that the Euros were sent

Order cancellation possible only if LastJointSac464 agrees

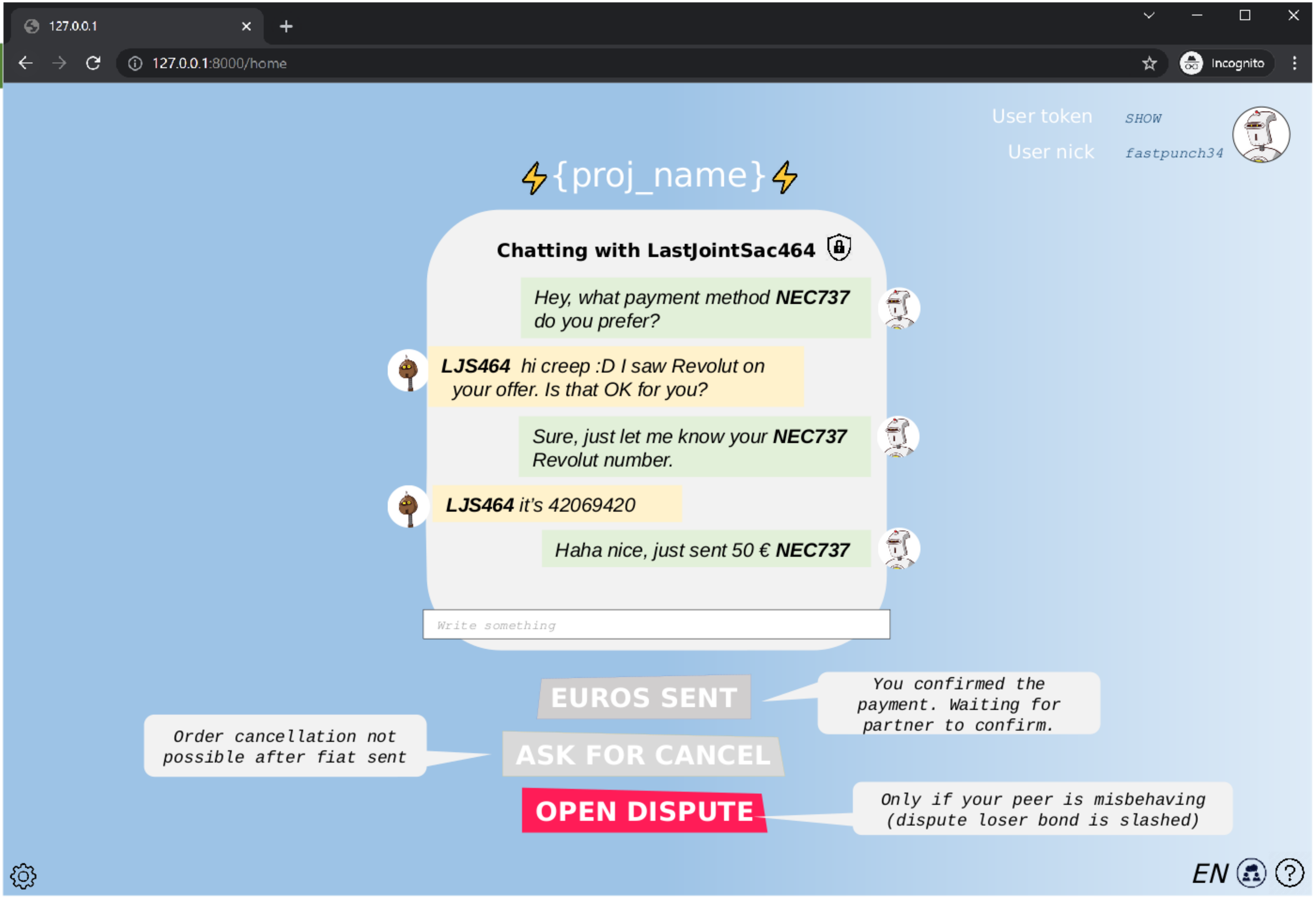
Not yet, talk to your peer.

Open dispute only available after expiration of trade or EUROS SENT has been clicked.
The trade expires when HODL invoice expires and fiat sent is not clicked 8 hour.

Clicked

EUROS SENT

- Adds transaction To order book



Chatting with LastJointSac464

Hey, what payment method ***NEC737*** *do you prefer?*

LJS464 *hi creep :D I saw Revolut on your offer. Is that OK for you?*

Sure, just let me know your ***NEC737*** *Revolut number.*

LJS464 *it's 42069420*

Haha nice, just sent 50 € ***NEC737***

You confirmed the payment. Waiting for partner to confirm.

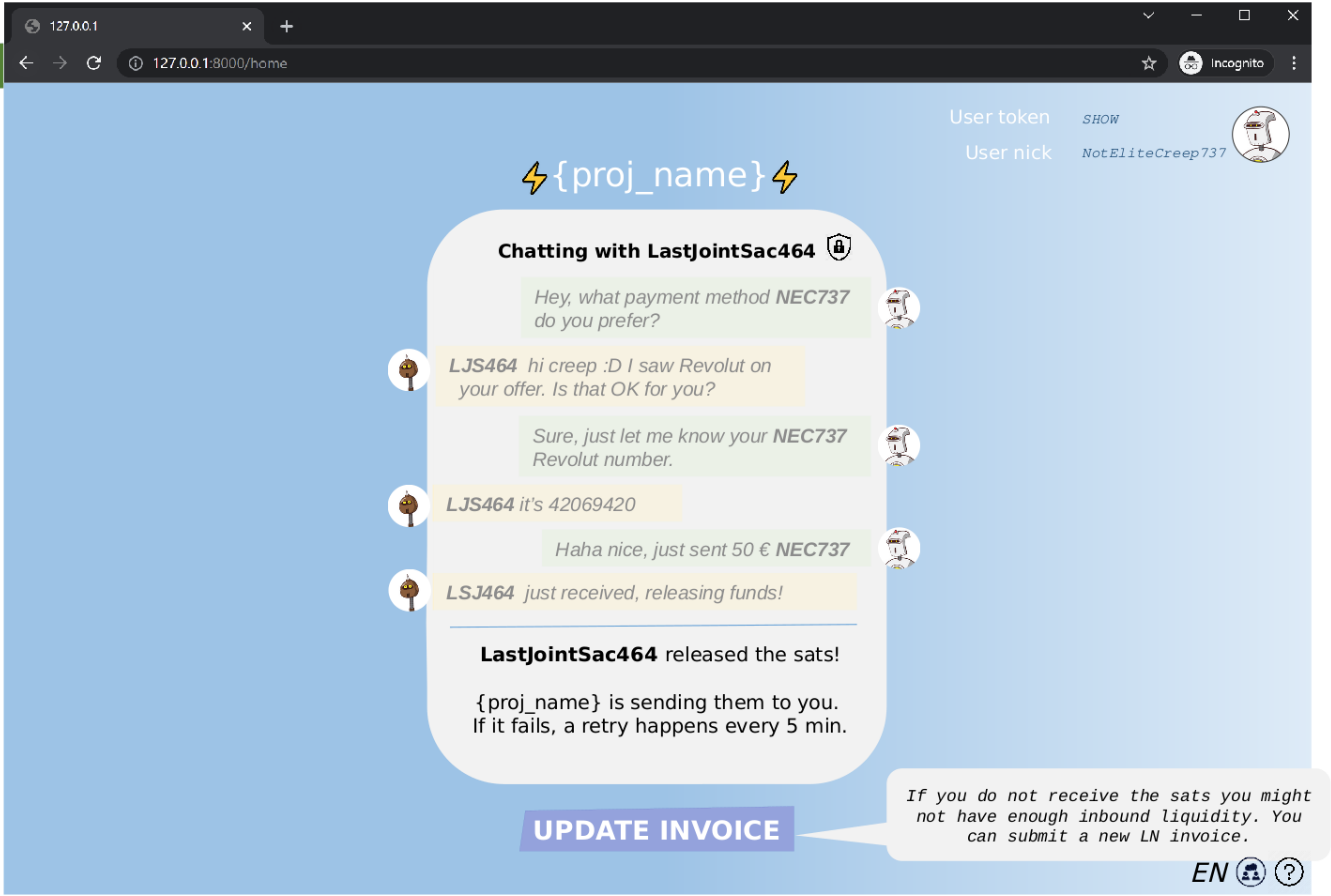
Order cancellation not possible after fiat sent

Only if your peer is misbehaving (dispute loser bond is slashed)

Clicked

EUROS SENT

- Adds transaction To order book



Chatting with LastJointSac464

Hey, what payment method **NEC737** do you prefer?

LJS464 hi creep :D I saw Revolut on your offer. Is that OK for you?

Sure, just let me know your **NEC737** Revolut number.

LJS464 it's 42069420

Haha nice, just sent 50 € **NEC737**

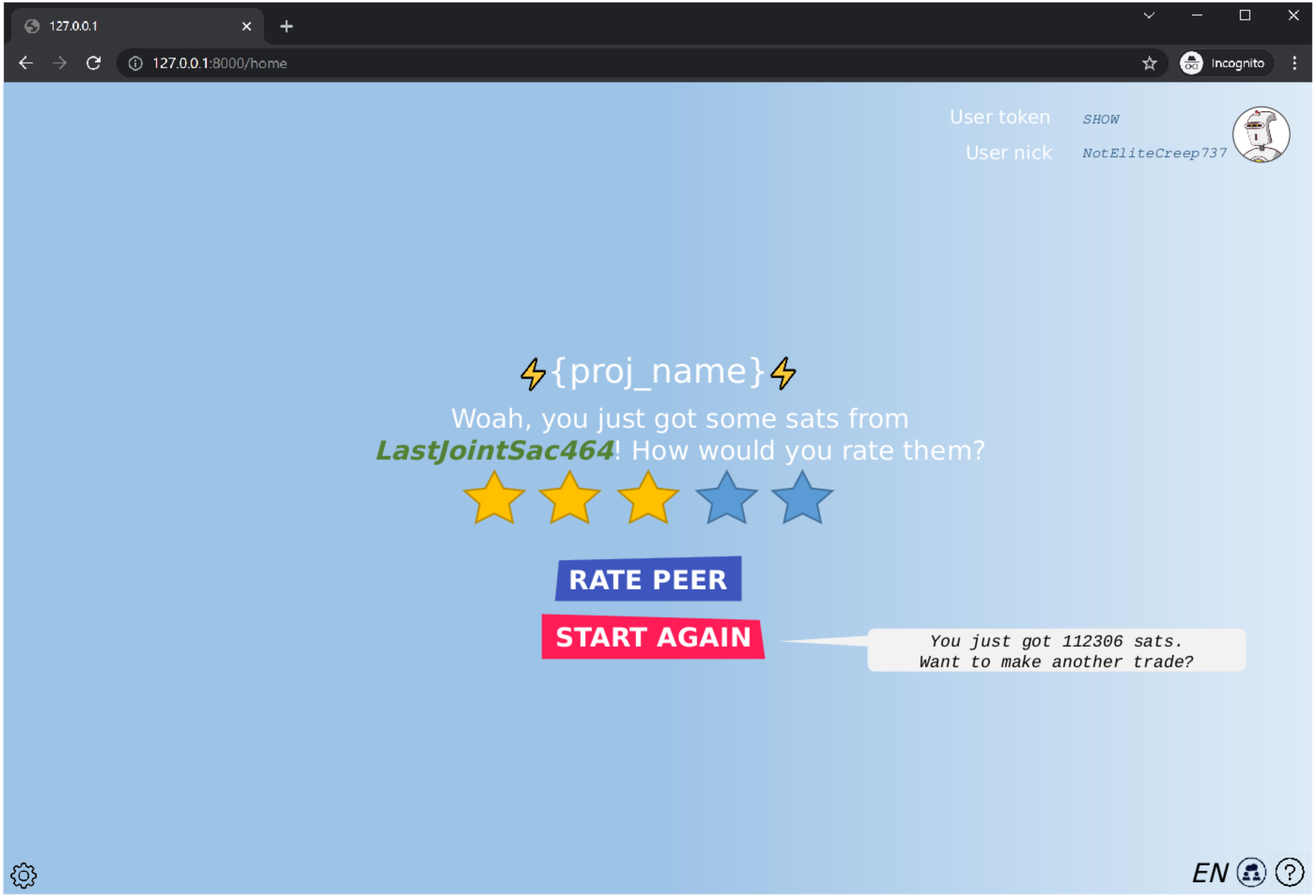
LSJ464 just received, releasing funds!

LastJointSac464 released the sats!

{proj_name} is sending them to you.
If it fails, a retry happens every 5 min.

If you do not receive the sats you might not have enough inbound liquidity. You can submit a new LN invoice.

Event
Sats sent



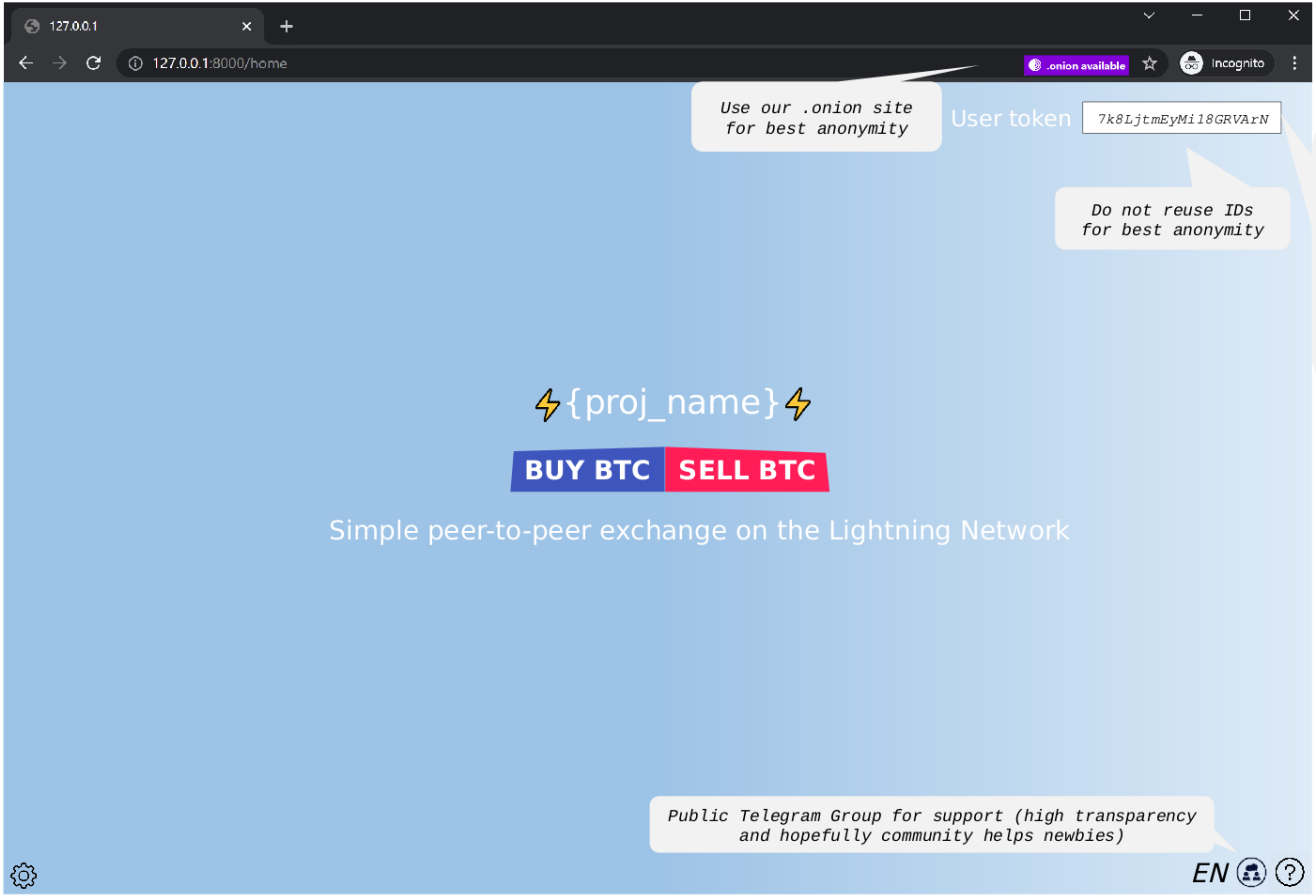
User token SHOW

User nick NotEliteCreep737

⚡{proj_name}⚡

Woah, you just got some sats from **LastJointSac464**! How would you rate them?

You just got 112306 sats.
Want to make another trade?



User token: 7k8LjtmEyMi18GRVArN

Simple peer-to-peer exchange on the Lightning Network

Use our .onion site for best anonymity

Do not reuse IDs for best anonymity

For **PROs**: If you do not trust the rng you can generate your own entropy using your own tools.

The string must BASE58 and [28-48] characters long (~160-260 bits of entropy)

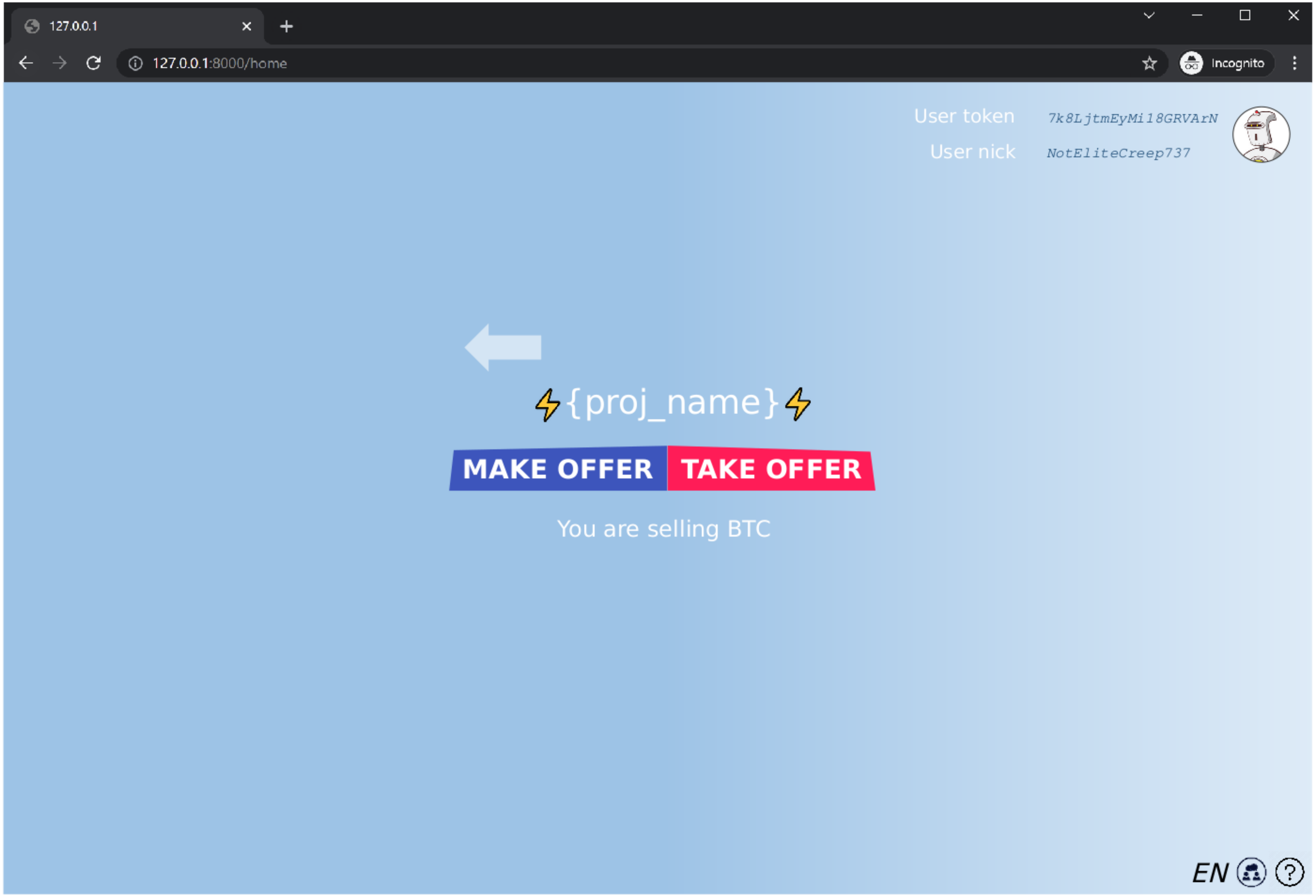
Public Telegram Group for support (high transparency and hopefully community helps newbies)

Onion hidden service so no user IP is logged
No re-use of ID is best for anonymity for casual takers. But for makers, buiding reputation might be a priority

Clicked

SELL BTC

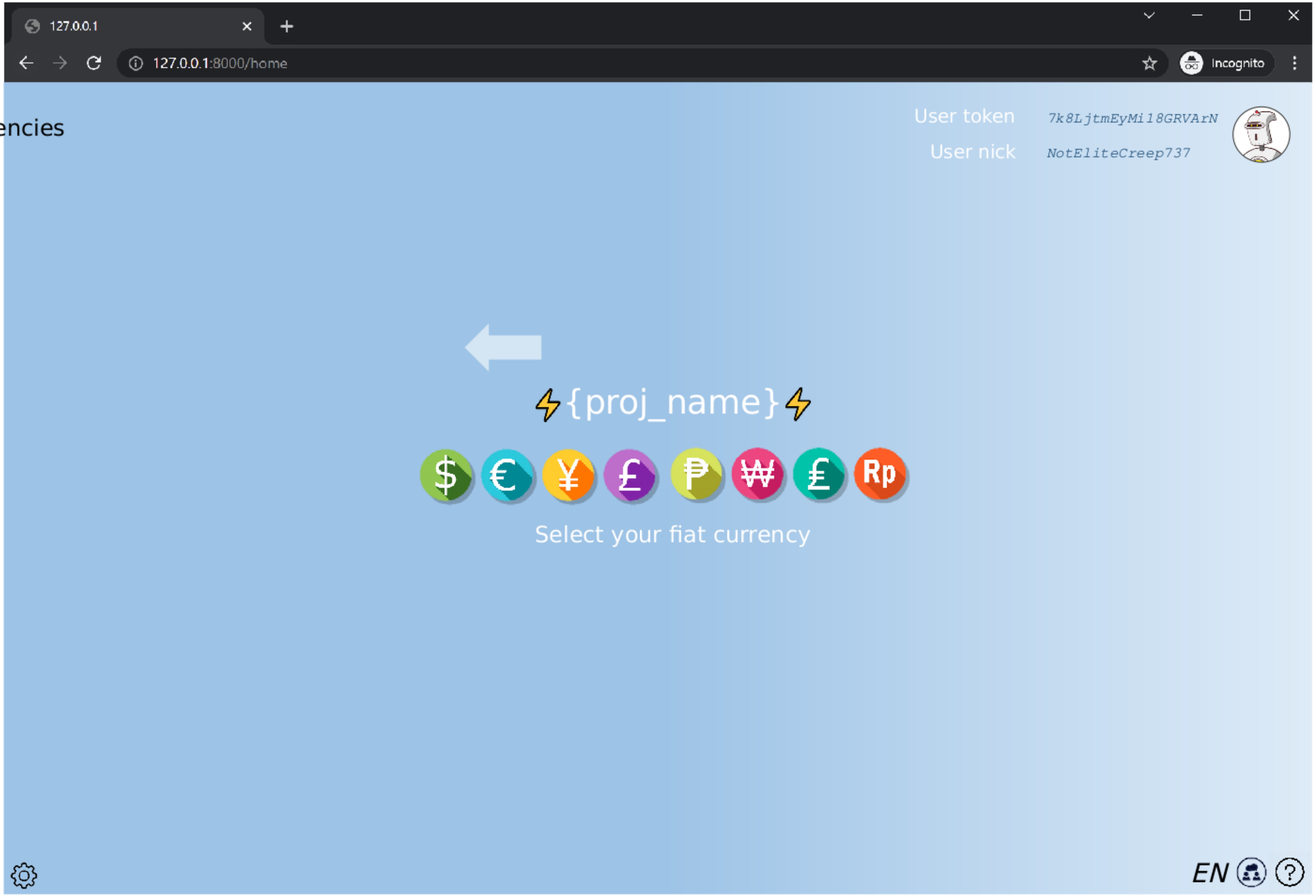
- Gets user nick
- Moves into peer-kind selection



Clicked

TAKE OFFER

- Gets available currencies



User token 7k8LjtmEyMi18GRVArN

User nick NotEliteCreep737

⚡{proj_name}⚡

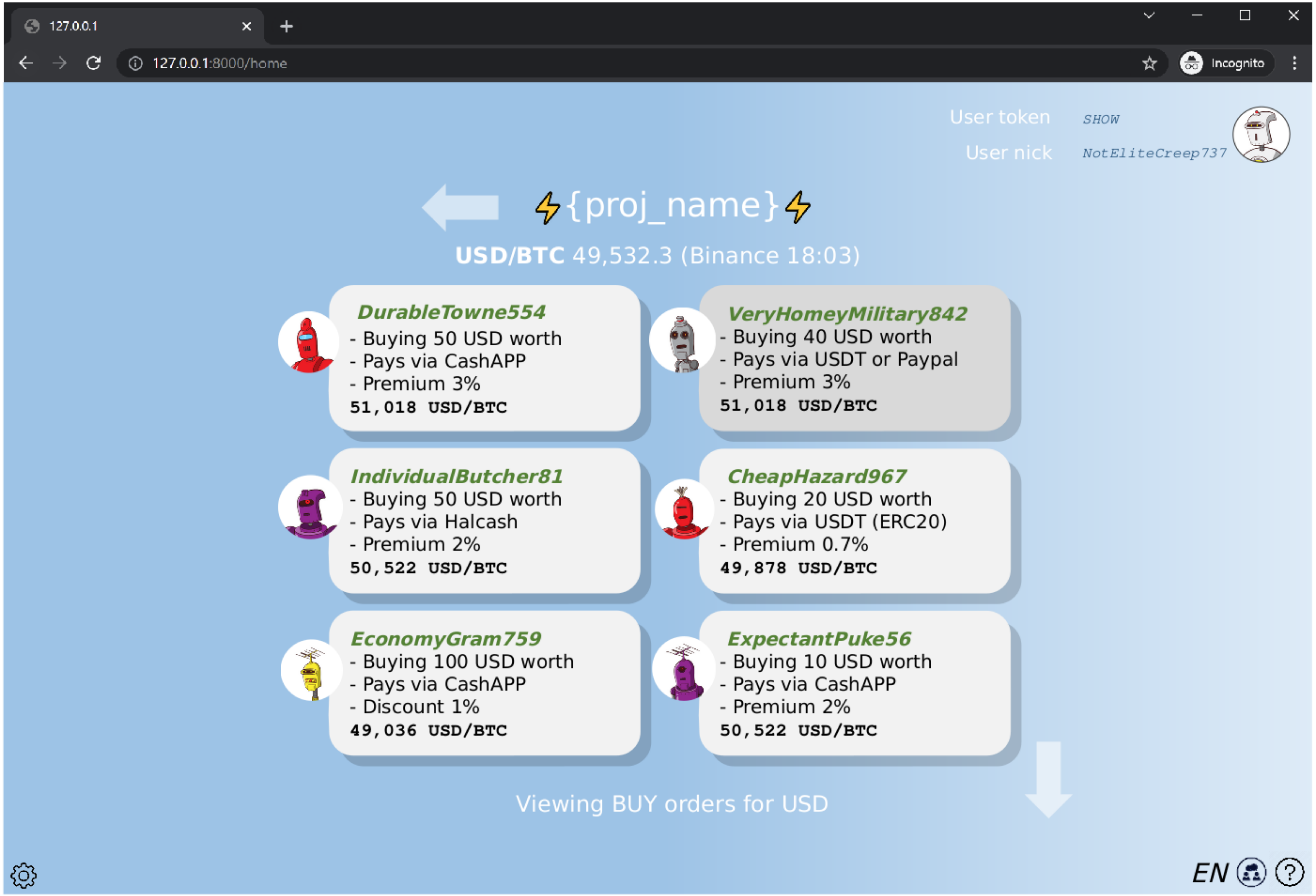
$ € ¥ £ ₱ ₩ £ Rp

Select your fiat currency

Clicked

$

- Gets order book



User token *SHOW*

User nick *NotEliteCreep737*

⚡{proj_name}⚡

USD/BTC 49,532.3 (Binance 18:03)

DurableTowne554
- Buying 50 USD worth
- Pays via CashAPP
- Premium 3%

51,018 USD/BTC

VeryHomeyMilitary842
- Buying 40 USD worth
- Pays via USDT or Paypal
- Premium 3%

51,018 USD/BTC

IndividualButcher81
- Buying 50 USD worth
- Pays via Halcash
- Premium 2%

50,522 USD/BTC

CheapHazard967
- Buying 20 USD worth
- Pays via USDT (ERC20)
- Premium 0.7%

49,878 USD/BTC

EconomyGram759
- Buying 100 USD worth
- Pays via CashAPP
- Discount 1%

49,036 USD/BTC

ExpectantPuke56
- Buying 10 USD worth
- Pays via CashAPP
- Premium 2%

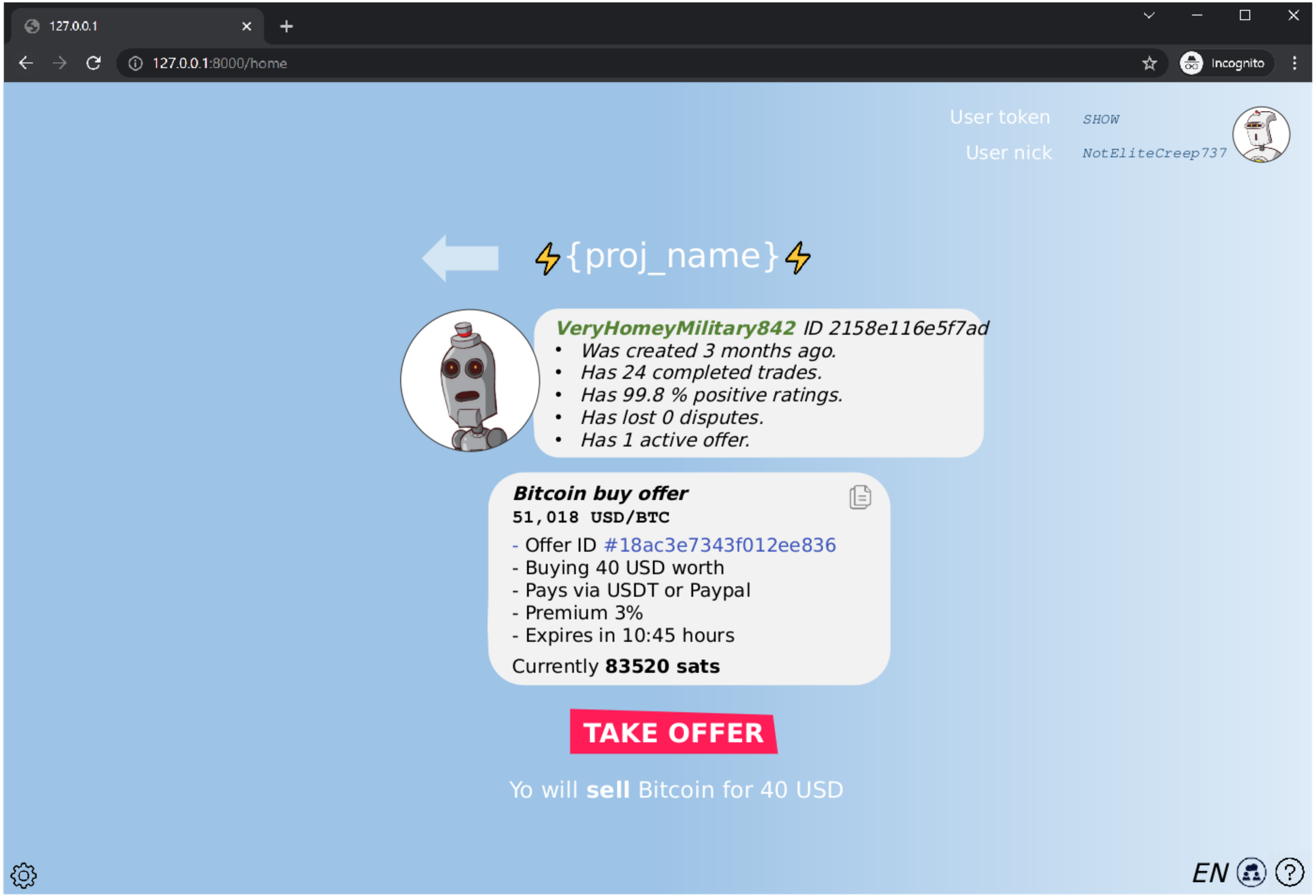
50,522 USD/BTC

Viewing BUY orders for USD

Tapping on user nicks or bot pics shows calls GET /USER ({Num trades, total amount traded, ratings, ...)
Tapping on OFFERS shows complete order and user overview (GET /ORDER

Clicked

- Gets order book



User token *SHOW*

User nick *NotEliteCreep737*

⚡{proj_name}⚡

VeryHomeyMilitary842 *ID 2158e116e5f7ad*

- *Was created 3 months ago.*
- *Has 24 completed trades.*
- *Has 99.8 % positive ratings.*
- *Has lost 0 disputes.*
- *Has 1 active offer.*

Bitcoin buy offer

51,018 USD/BTC

- Offer ID #18ac3e7343f012ee836
- Buying 40 USD worth
- Pays via USDT or Paypal
- Premium 3%
- Expires in 10:45 hours

Currently **83520 sats**

TAKE OFFER

Yo will **sell** Bitcoin for 40 USD

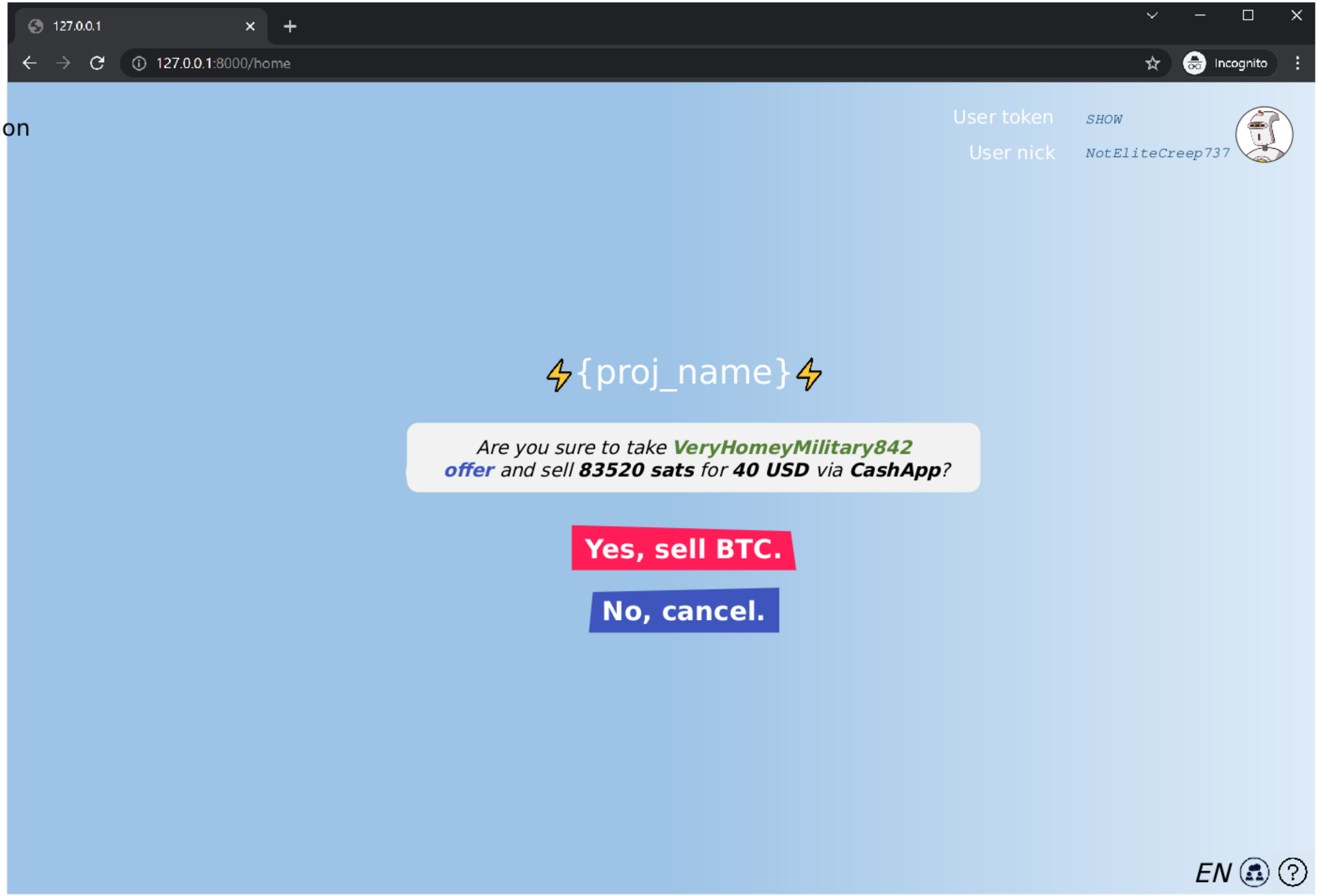
pping on user pics or nicks shows user profiles (Num trades, total amount traded, ratings, ...)

pping on orders shows complete order overview

Clicked

SELL BTC

- Asks for confirmation



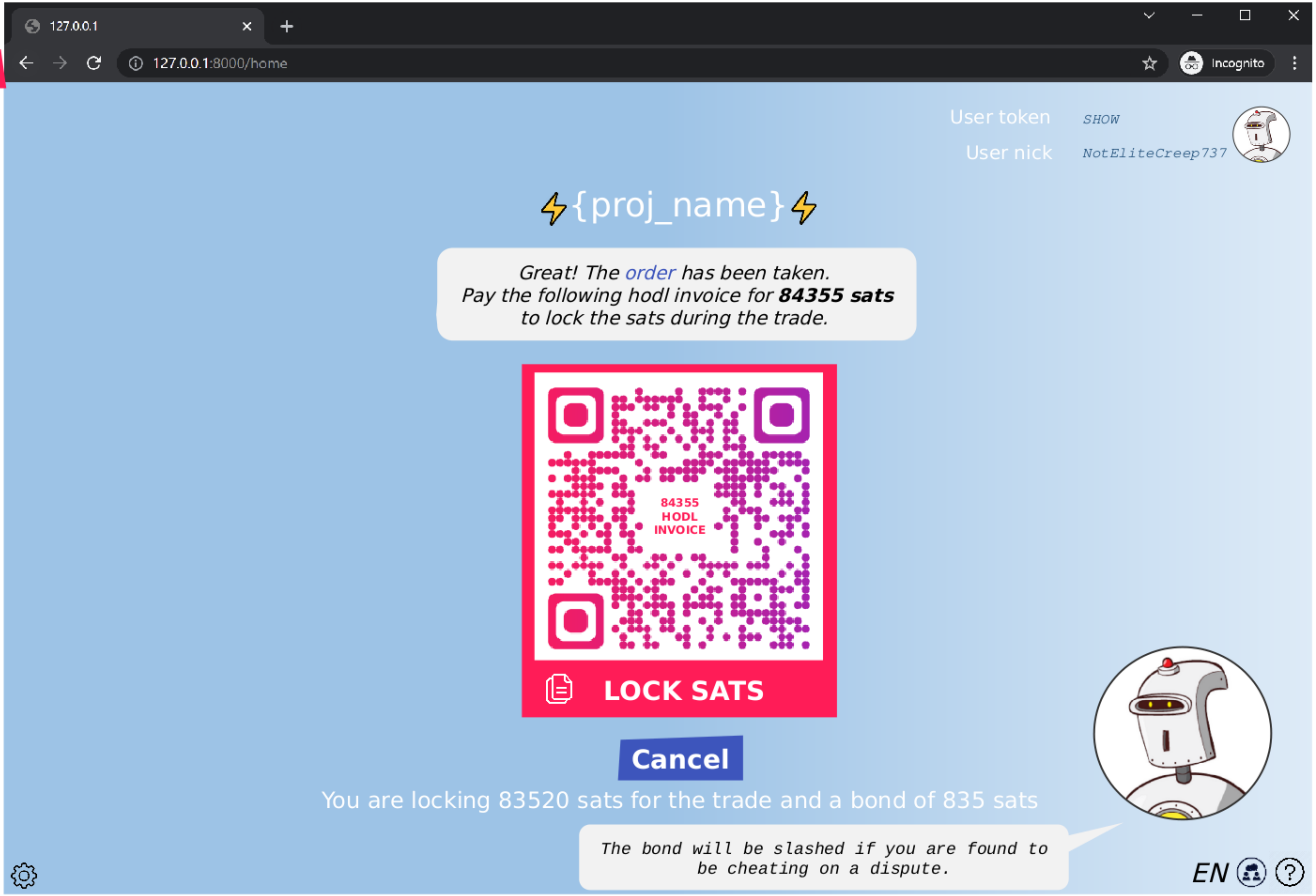
Are you sure to take ***VeryHomeyMilitary842 offer*** *and sell* ***83520 sats*** *for* ***40 USD*** *via* ***CashApp****?*

Sats update every second from Binance API

Clicked

Yes, sell BTC.

- Asks for LN



User token *SHOW*

User nick *NotEliteCreep737*

⚡{proj_name}⚡

Great! The order has been taken.
Pay the following hodl invoice for ***84355 sats***
to lock the sats during the trade.

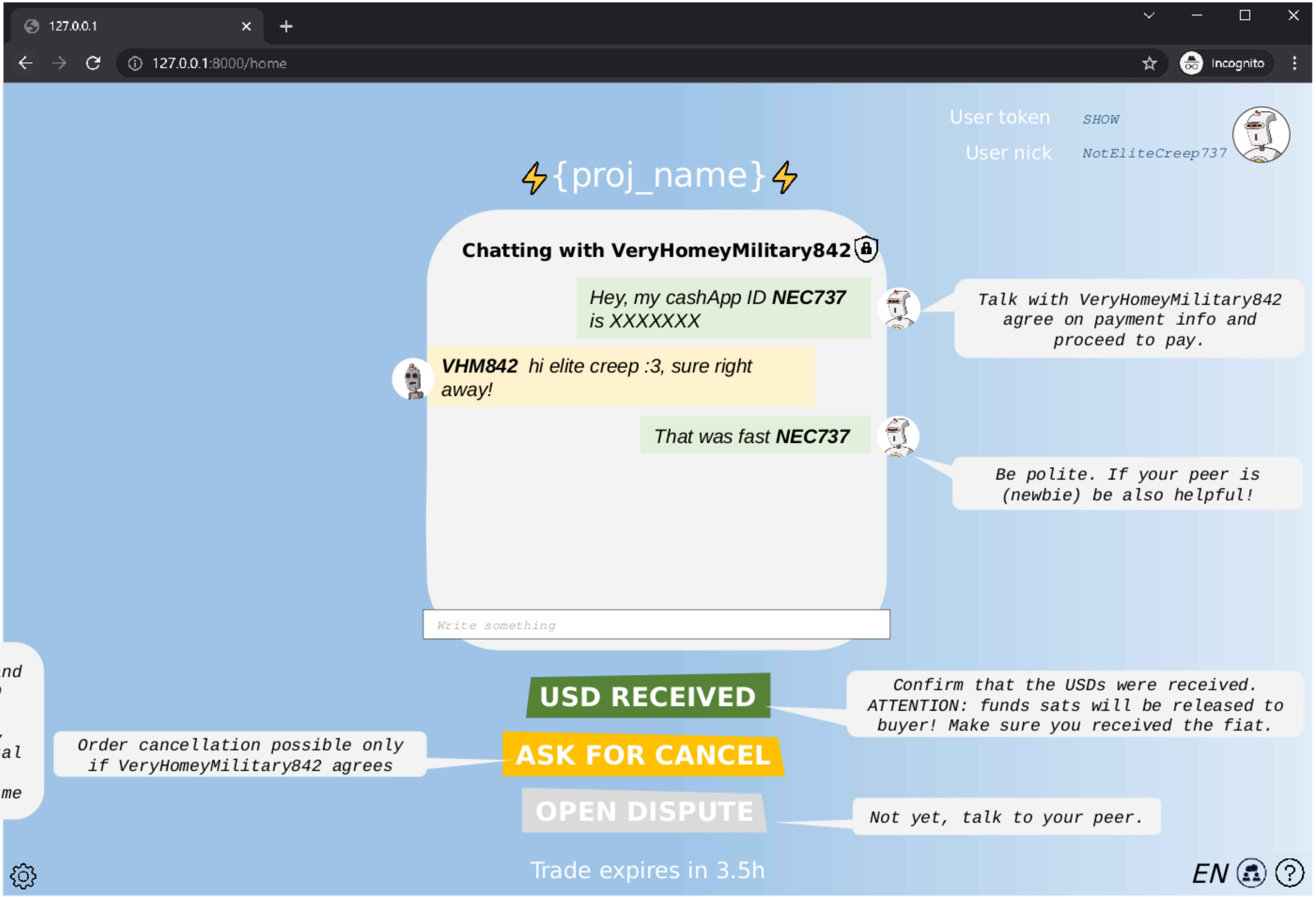
You are locking 83520 sats for the trade and a bond of 835 sats

The bond will be slashed if you are found to be cheating on a dispute.

Event

Peer locked funds

- Adds transaction To order book



User token *SHOW*

User nick *NotEliteCreep737*

⚡{proj_name}⚡

Chatting with VeryHomeyMilitary842 🔒

*Hey, my cashApp ID **NEC737** is XXXXXXX*

VHM842 *hi elite creep :3, sure right away!*

*That was fast **NEC737***

Write something

Talk with VeryHomeyMilitary842 agree on payment info and proceed to pay.

Be polite. If your peer is (newbie) be also helpful!

USD RECEIVED

Confirm that the USDs were received. ATTENTION: funds sats will be released to buyer! Make sure you received the fiat.

ASK FOR CANCEL

Order cancellation possible only if VeryHomeyMilitary842 agrees

OPEN DISPUTE

Not yet, talk to your peer.

Trade expires in 3.5h

EN

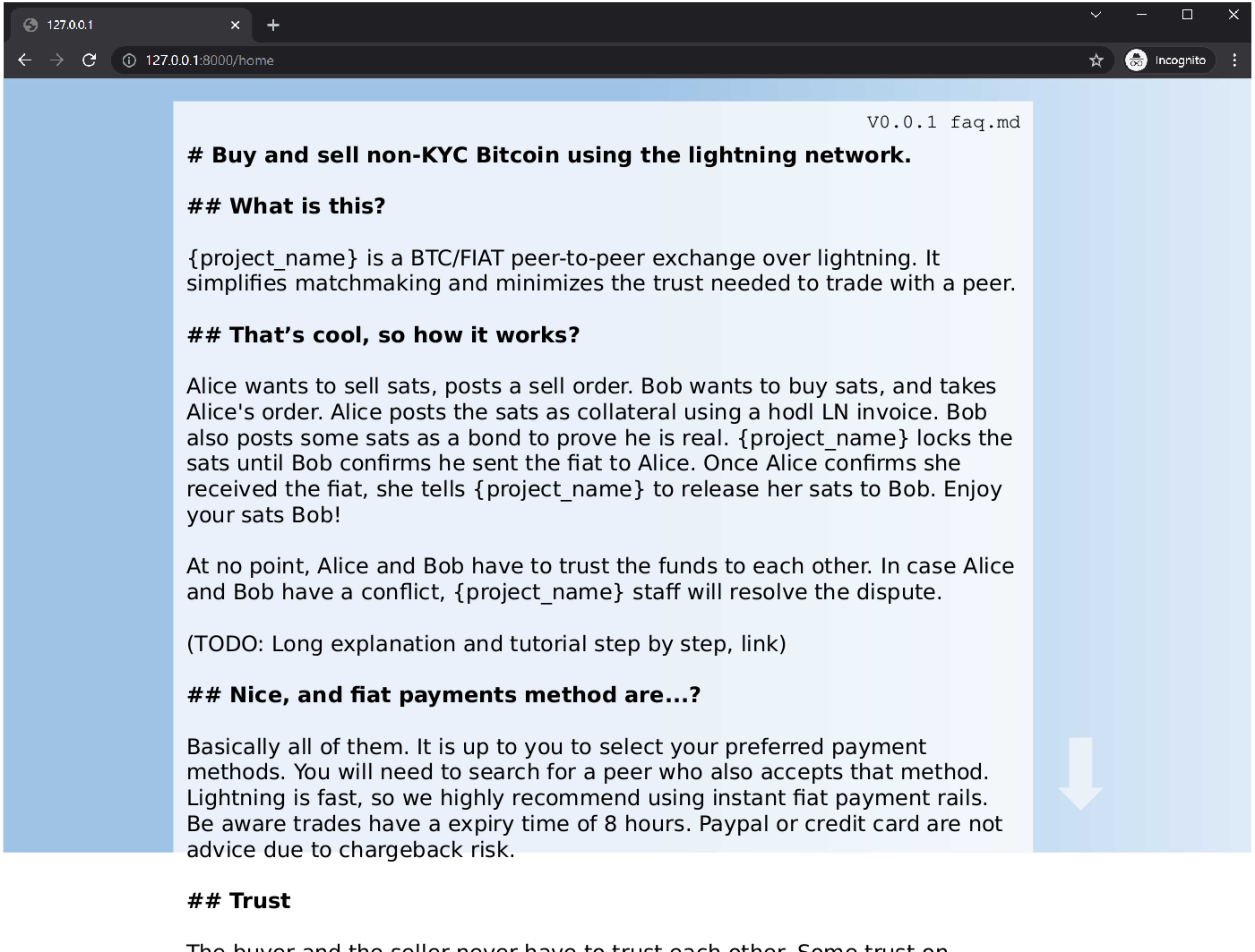
Stats-for-nerds: {proj_name} front_end and back_end verions, LND 0.14.2, Node_ID: 0291afc1102ff82813(…), daily sats settled, total sats in order book, lifetime trades, lifetime volume, etc

Open dispute only available after expiration of trade or EUROS SENT has been clicked. The trade expires when HODL invoice expires and fiat sent is not clicked 8 hour.

Clicked

?

Show markdown Pop FAQ with scroll



# Buy and sell non-KYC Bitcoin using the lightning network.

## What is this?

{project_name} is a BTC/FIAT peer-to-peer exchange over lightning. It simplifies matchmaking and minimizes the trust needed to trade with a peer.

## That’s cool, so how it works?

Alice wants to sell sats, posts a sell order. Bob wants to buy sats, and takes Alice's order. Alice posts the sats as collateral using a hodl LN invoice. Bob also posts some sats as a bond to prove he is real. {project_name} locks the sats until Bob confirms he sent the fiat to Alice. Once Alice confirms she received the fiat, she tells {project_name} to release her sats to Bob. Enjoy your sats Bob!

At no point, Alice and Bob have to trust the funds to each other. In case Alice and Bob have a conflict, {project_name} staff will resolve the dispute.

(TODO: Long explanation and tutorial step by step, link)

## Nice, and fiat payments method are...?

Basically all of them. It is up to you to select your preferred payment methods. You will need to search for a peer who also accepts that method. Lightning is fast, so we highly recommend using instant fiat payment rails. Be aware trades have a expiry time of 8 hours. Paypal or credit card are not advice due to chargeback risk.

## Trust

The buyer and the seller never have to trust each other. Some trust on

Preliminary_test preview

Summary: Just a fork of private_chat_2 for Django and some test of serving nickname_generator and Robohash for user creation.

Django Private Chat2 example
127.0.0.1:8000/api/home
Incognito (2)

Tip: Use particle.js or something else that resembles the Lightning Network and is alive

Hello! 🙋

Your nick and avatar generated from the date and salt:

⚡FictionalOxen273⚡

token/pwd: 📋vrTKgcF3nzC4k5g6RgiL5u5H1pBc

Dec. 28, 2021, 11:05 a.m. Generated in 165 milliseconds.

-Demo “preliminary_tests” Django project “/api/home/”. Simple view function that renders a site with a new token, nick and avatar and adds it to user database.

Django Private Chat2 example
127.0.0.1:8000/api/home
127.0.0.1:8000
Incognito (2)
Search...

FictionalOxen273 1 minute ago
Awesome, what's you CashApp ID?

admin 14 hours ago
You: Thanks for the help

FictionalOxen273

FictionalOxen273
Hey StuckVictory :D how are you? 1 minute ago

StuckupVictory641
Doing good, wbu? 1 minute ago

FictionalOxen273
Not bad :') How do you prefer the receive the fiat? 45 seconds ago

StuckupVictory641
CashApp would be best 35 seconds ago

FictionalOxen273
Awesome, what's you CashApp ID? 22 seconds ago

Connection state: Connected

-Demo “preliminary_tests” Django project main “/”. Just an instance of “Django Private Chat2”. Out-of-the-box example.

Rough v0.0.1 concept of Back-End endpoints.

(note: I have never designed an API, I have not studied/read how to do it best. I have absolutely no idea what I am doing)

Auth, did not research what is best suited.

GET /**BOOK** (request {‘type’: ‘buy’, ‘currency’: ‘USD’, ...}, response with view of the filtered order book
[{‘order_id’:’8fa5…’, ‘maker_id’ ‘expiry’:122651…,’amount’:50, etc}, {‘order_id’:’68fae41’, …}…]

GET /**ORDER** (request {‘order_id’: ‘8fa51ec8’,(…)}, response with full order details {‘currency’:
USD,’amount’:50,’maker_id:16qcd6…’,

POST /**ORDER** ({‘type’: ‘buy’, ‘currency’:’EUR’, ‘amount’:’20’,’premium’:3,’sats’: …}, response {order_ID, bond_hodl_invoice,
expiry_time, etc}) # Creates a new order that won’t show up in the order book until bond_hodl_invoice is paid

GET /**ORDERSTATUS** (request {“order_id: 8fa51ec8(…)}, response {status_code:’’, message:’waiting for buyer to lock bond’}

GET /**USER/** (request “user_id: 16qcd6(…), response with details {‘nick’: ‘VeryEloquent152’,
’avatar’:’static/assets/1889aeg.png’, ’num_trades’:16…’,’rating’:’99.8%’}

POST /**TAKEBUY** (request {“order_id: 8fa51ec8(…), ‘type’:’buy’}, response
{‘trade_hodl_invoice’:’lncb...’,trade_hodl_invoice_qr’:’BASE64 image’,}

POST /**TAKESELL** (request {“order_id: 8fa51ec8(…), }, response {‘bond_hodl_invoice’:’lncb...’,bond_hodl_invoice_qr’:’BASE64
image’,}

PUT /**INVOICE** (request {“order_id: 8fa51ec8(…), ‘buyer_ln_invoice’:’lncb1…’}, response {‘message’:’OK / Error: invalid LN
invoice, must start with lnbc…’} #Allows buyer to put or updates invoice for an existing taken order

DEL /**CANCELLALL** # Deletes offer from orderbook or cancels ongoing trade (fails if collaborative cancel is needed and peer
does not cancel too)

POST /**DISPUTE** (request {‘order_id’: ‘8fa51ec8(…)’, ‘chat_viewkey’:’key’,…}, response {‘message’:’dispute started’, }

POST /**RATING** {‘order_id’:8fa51ec8, ‘user_id’: ‘16qcd6’, ‘stars’:’5’, ...}

Miscellaneous

GET **/APP/NODE** {‘lnd_version’:’0.14.1’,’Bitcoin Network’:’testnet’,’blockheight’:712121,’{proj_name}_version’:’0.0.7a’,’commit_height’:’26b90fc69e’,‘total_trades’, 10, etc}

GET **/APP/ANNOUNCEMENTS** [{‘title’:‘Good news’, ‘text’:‘Your avatar bot is 25% on its way to be selfconscious’, ‘ts’:1621129462129}{‘title’:‘Bad news’,’text’:’Your avatar bot has 75% to go to be selfconscious’…}]

Get /**APP/SETTINGS** {‘max_trade_amount’: 500000,‘min_trade_amount’: 10000, ‘trade_fee’: 0.002, ‘dispute_fee’: 0.01}