Capture The Bitcoin

How did we solved all puzzles

The team

- buzzyboy
- jaonoctus
- llsza
- nGoline
- narcelio
- stutxo

CTB

"This scavenger hunt will test your knowledge of Bitcoin and challenge you to think creatively.

Join in on the fun and make new friends while learning something new. The goal is to be the first to snatch the bitcoin from a specific UTXO.

To get started, simply attend TABConf and pick up your **challenge coin** at the entrance."

Challenge coin

FB 18 E7 1A 2B 19 D0 C9 B0
87 17 79 A2 BE 61 3E 17 4A
B2 F6 B6 C3 4A AB FE DB 15
27 61 22 91 9A

https://tabctb.com

/six

"Check to see if the funds are still available:"

bc1pa8kr5ph0drh7e4e9yl_ygvcl6ycfnum2rkn96la6y_mpsc2a2xys0qt0tdl6_

https://tabctb.com

/six/thebeginning.html

Let the Forest pull you in

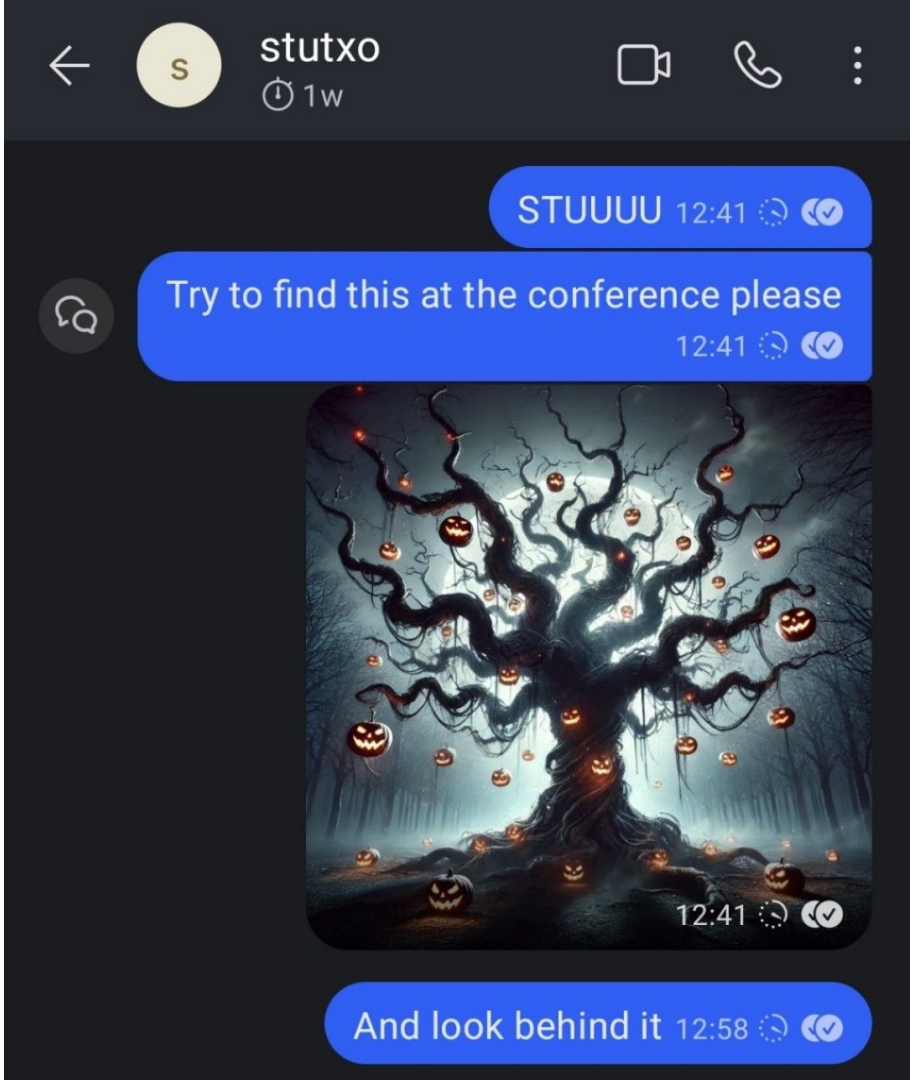
https://tabctb.com

/six/thebeginning/thetree.html

"a curious, almost sinister compulsion is urging you to circle the tree and peer behind its trunk."

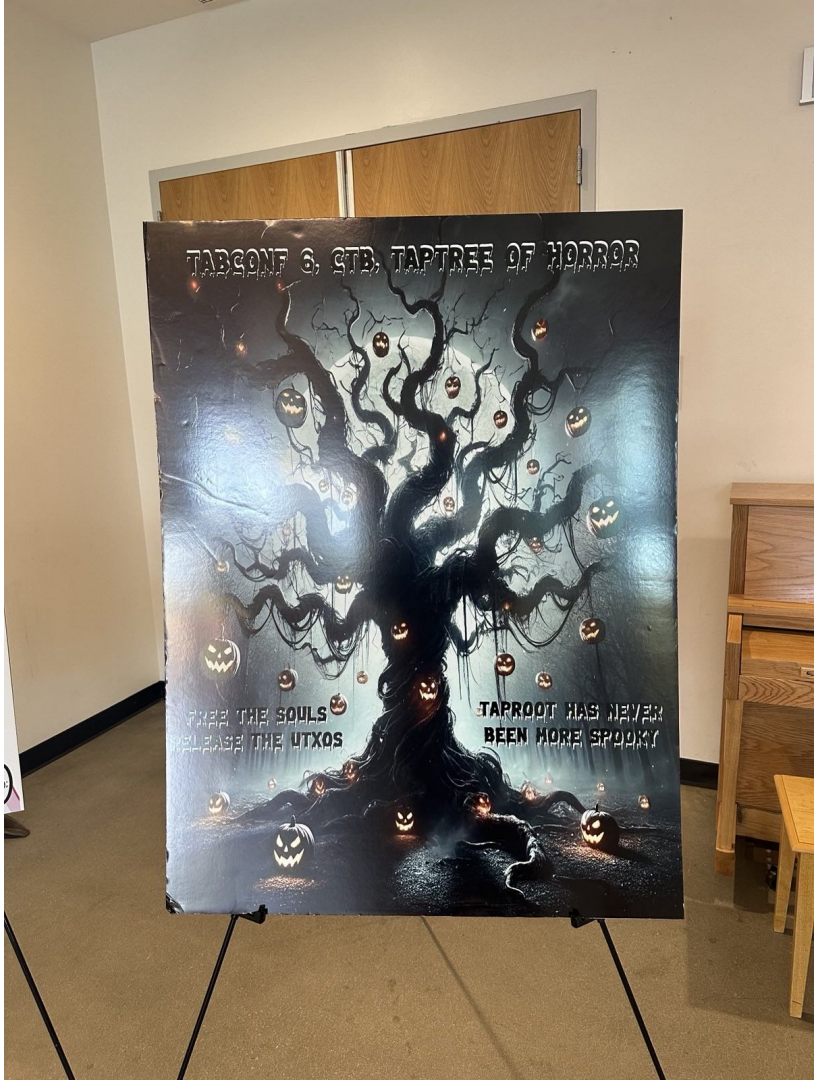
https://tabctb.com

/six/thebeginning/thetree.html



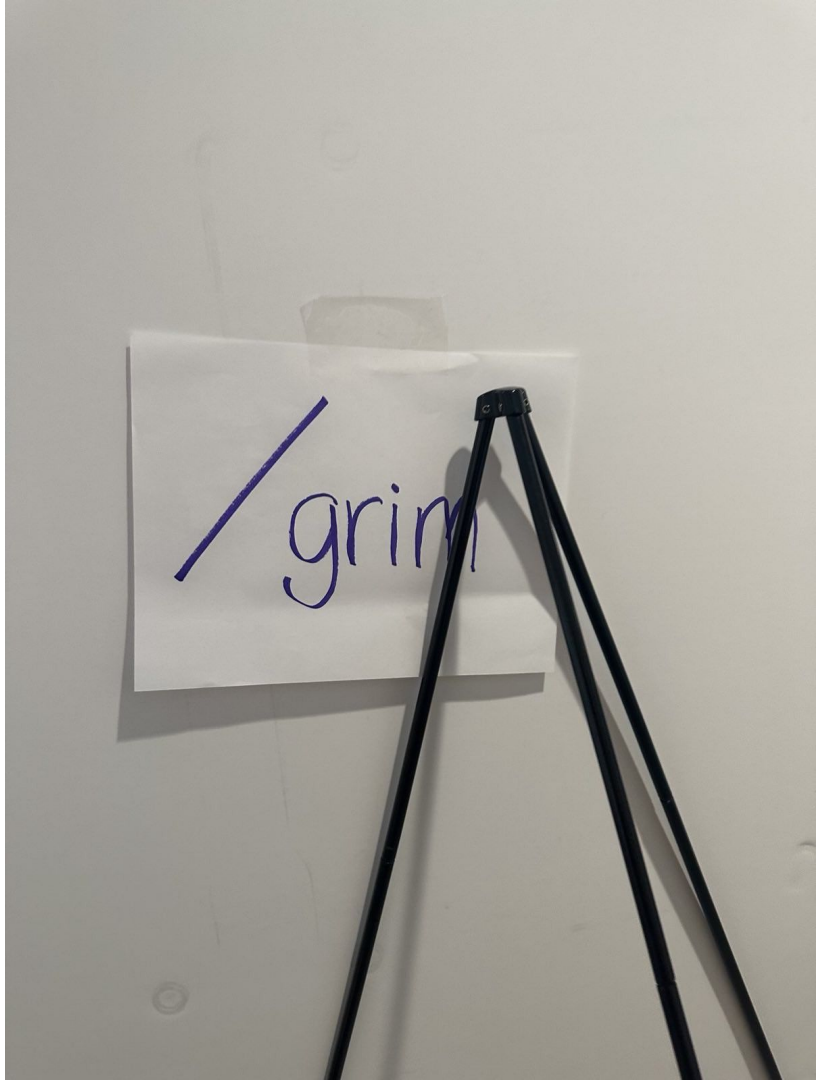
https://tabctb.com

/six/thebeginning/thetree.html



https://tabctb.com

/six/thebeginning/thetree.html

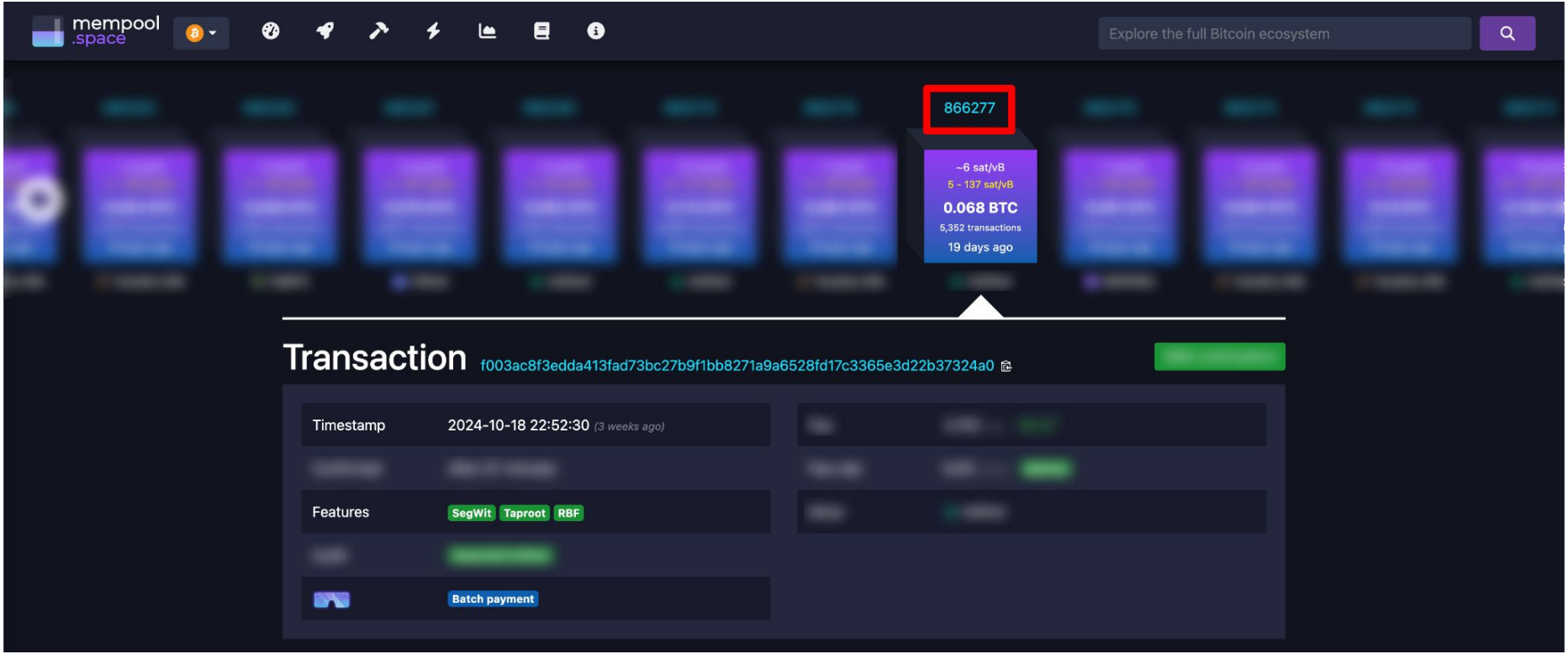


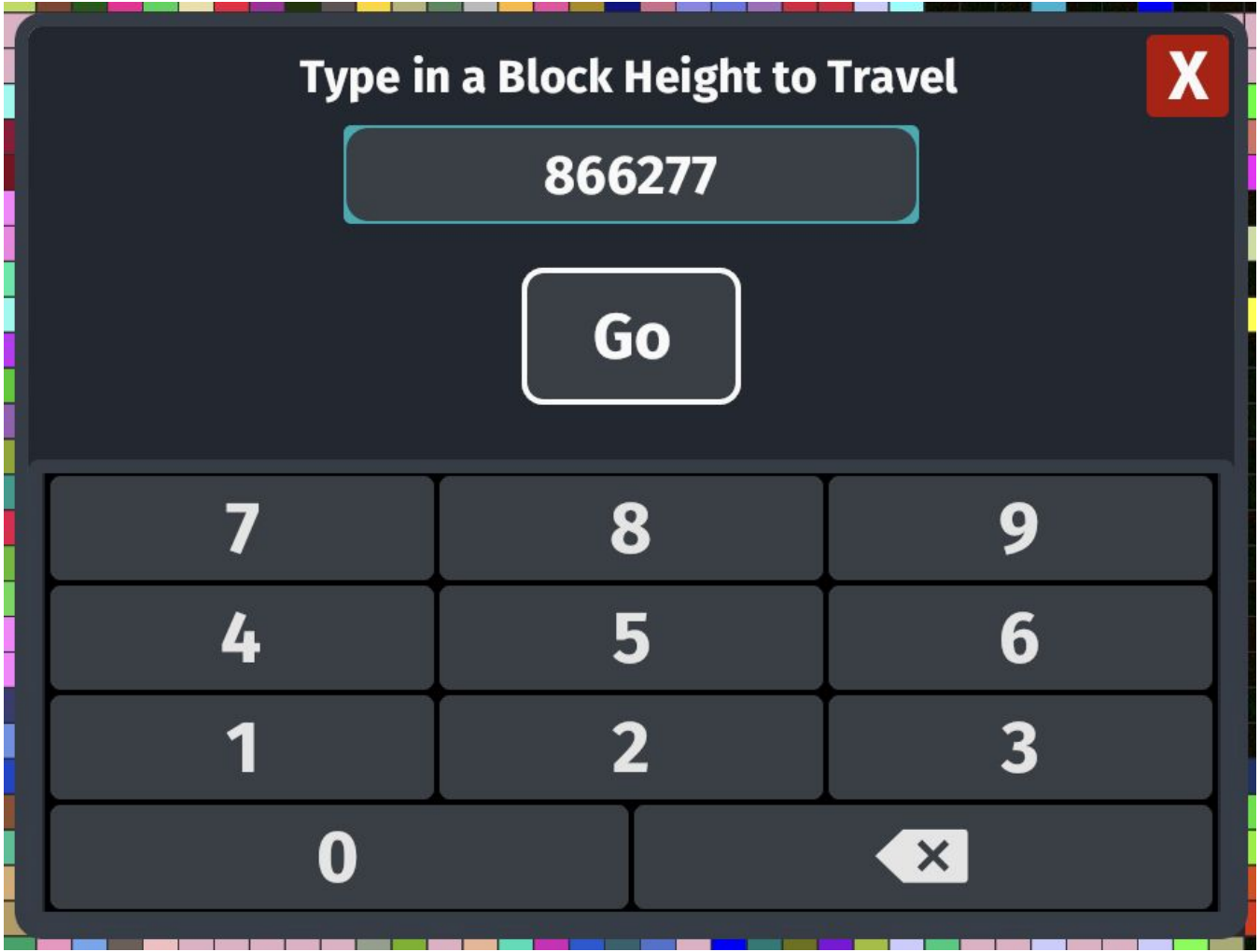
https://tabctb.com

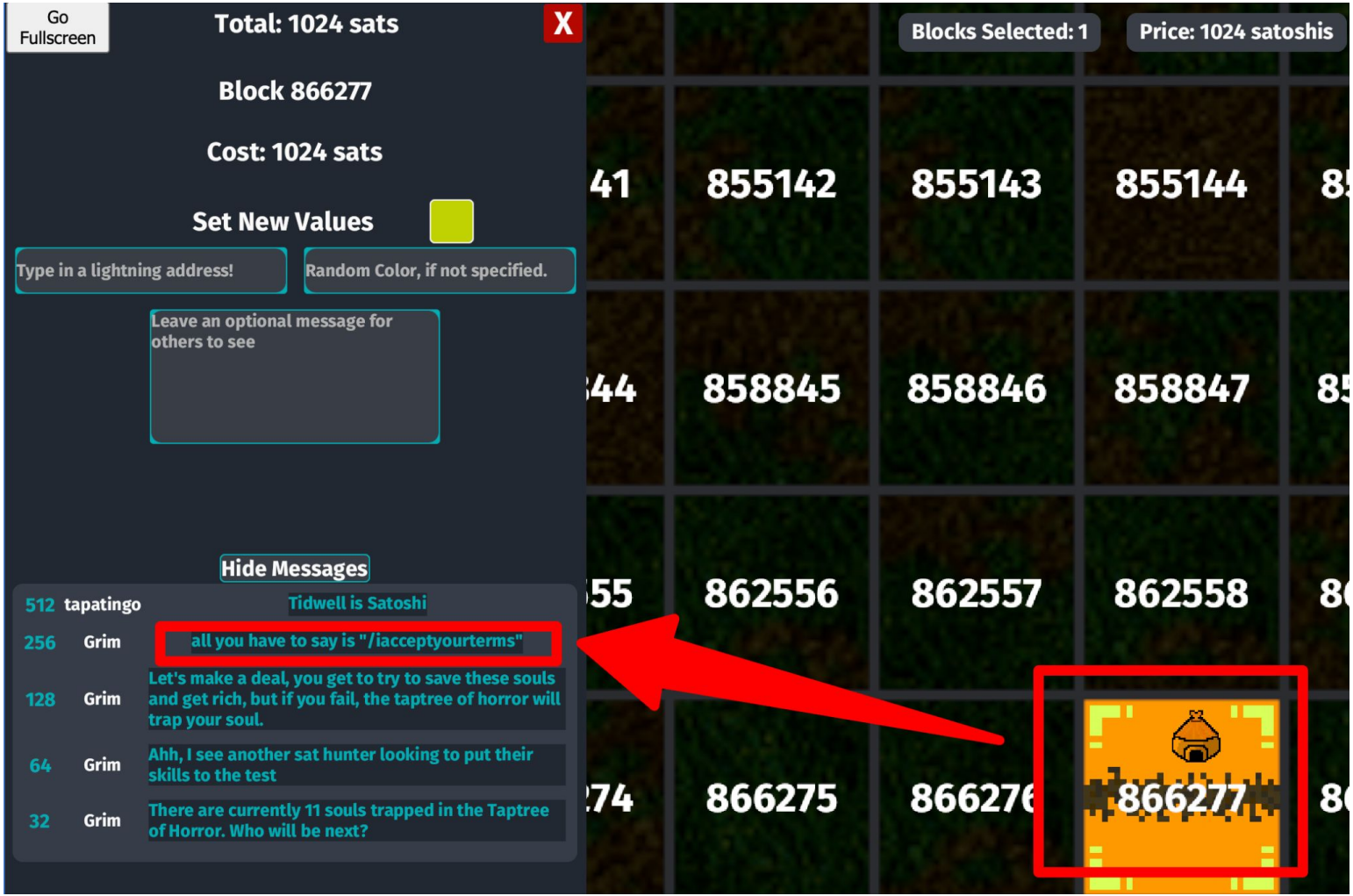
/six/thebeginning/thetree/grim

"I found this odd game called Satoshi Settlers and left a clue on the same blockheight as the generous donation."


satoshisettlers.com/map
Finish update
Go Fullscreen
Settings
COINS
.COM
Hide Buildings
Hide Colors
Show Values
Hide Text
-
+


mempool
.space
Explore the full Bitcoin ecosystem
866277
~6 sat/vB
5 - 137 sat/vB
0.068 BTC
5,352 transactions
19 days ago
Transaction
f003ac8f3edda413fad73bc27b9f1bb8271a9a6528fd17c3365e3d22b37324a0
Timestamp
2024-10-18 22:52:30 (3 weeks ago)
Features
SegWit
Taproot
RBF
Batch payment


Type in a Block Height to Travel
X
866277
Go
7
8
9
4
5
6
1
2
3
0


Go Fullscreen
Total: 1024 sats
X
Block 866277
Cost: 1024 sats
Set New Values
Type in a lightning address!
Random Color, if not specified.
Leave an optional message for others to see
Hide Messages
512 tapatingo Tidwell is Satoshi
256 Grim all you have to say is "/iacceptyourterms"
128 Grim Let's make a deal, you get to try to save these souls and get rich, but if you fail, the taptree of horror will trap your soul.
64 Grim Ahh, I see another sat hunter looking to put their skills to the test
32 Grim There are currently 11 souls trapped in the Taptree of Horror. Who will be next?
Blocks Selected: 1
Price: 1024 satoshis
41
855142
855143
855144
44
858845
858846
858847
55
862556
862557
862558
74
866275
866277

https://tabctb.com

/six/thebeginning/thetree/grim/iacceptyourterms

As soon as you utter the words, "I accept your terms", souls locked away by Unholy Tree eXtracting Offers, or (UTXOs) for short, come forth still bounded by the tree. You are baraged by visible UTXO suffered spirits that have been confirmed into damnation. How many of them there are? Each one seeminglingly stuck for a different reason.”

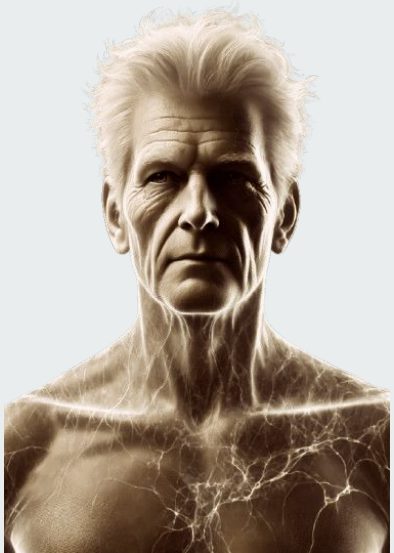
Apathetic Alice

bc1pw8d5j3vecstsc9kpahpdfy4xfuct6xn7cqeaxsk6w2ylz63s850q7sragu

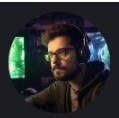
"The other souls call me Apathetic Alice because **I never took the time to understand Xprivs** . My wallet exported this for me but I don't have the slightest clue on what it is or what to do with it. I'm used to seeing a 12 or 24 word seed. I think this somehow holding my UXTO that is trapping me. Please help."

Boating Accident Bob

bc1p90umvmnawlr2320j9pfe54pe06ydjfecu58wa6ukwwxyajsqd3gsf7gk3e



"The other souls call me Boating Accident Bob. I swear, I really did have a boating accident! The wreckage of my ship washed up on shore and was pulled in by the evil taproots of this tree. My seed phrase was damaged in the accident, and now my soul is trapped. Please help me! **You might need to bruteforce some of it** , and if you're good with computers, I recommend writing a script. The good news is the checksum is still intact. Should be a piece of cake for you. I know you can do it!”



jaonoctus 10/24/2024 6:34 PM

np

my computer is burning

28 cores are on fire 🔥

Clever Charlie

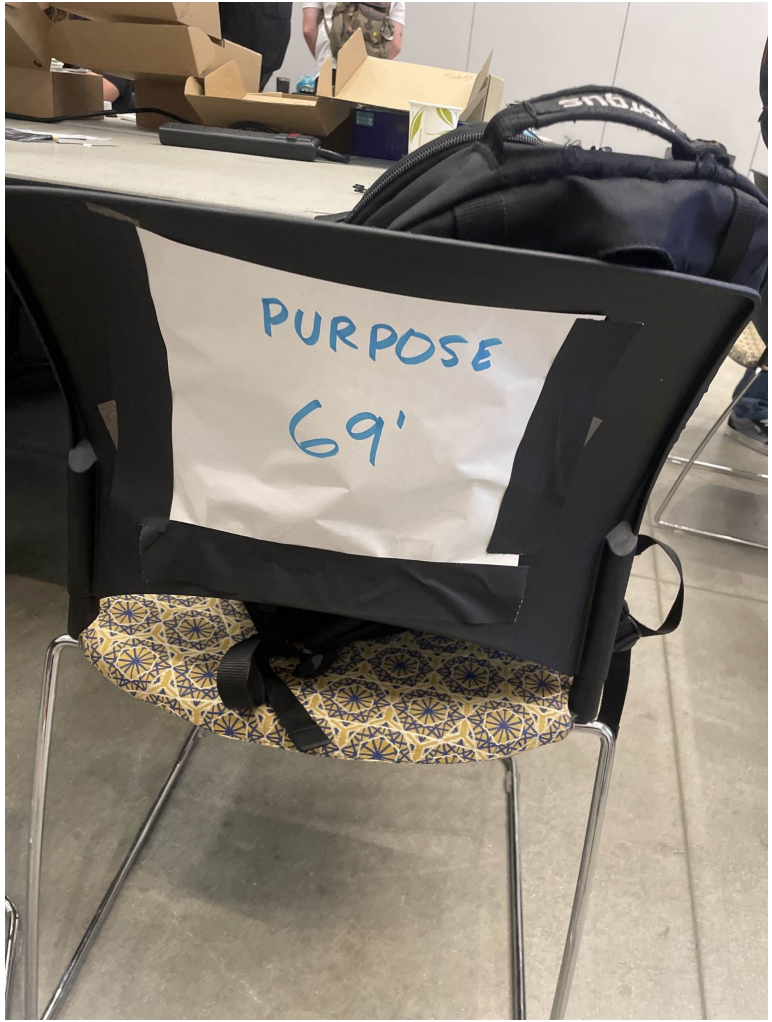
bc1pxflqymxp0l2ewjf5kysn8ayk34jwu20pqy045ytfmc2zp4fdq5qqnwvwx7

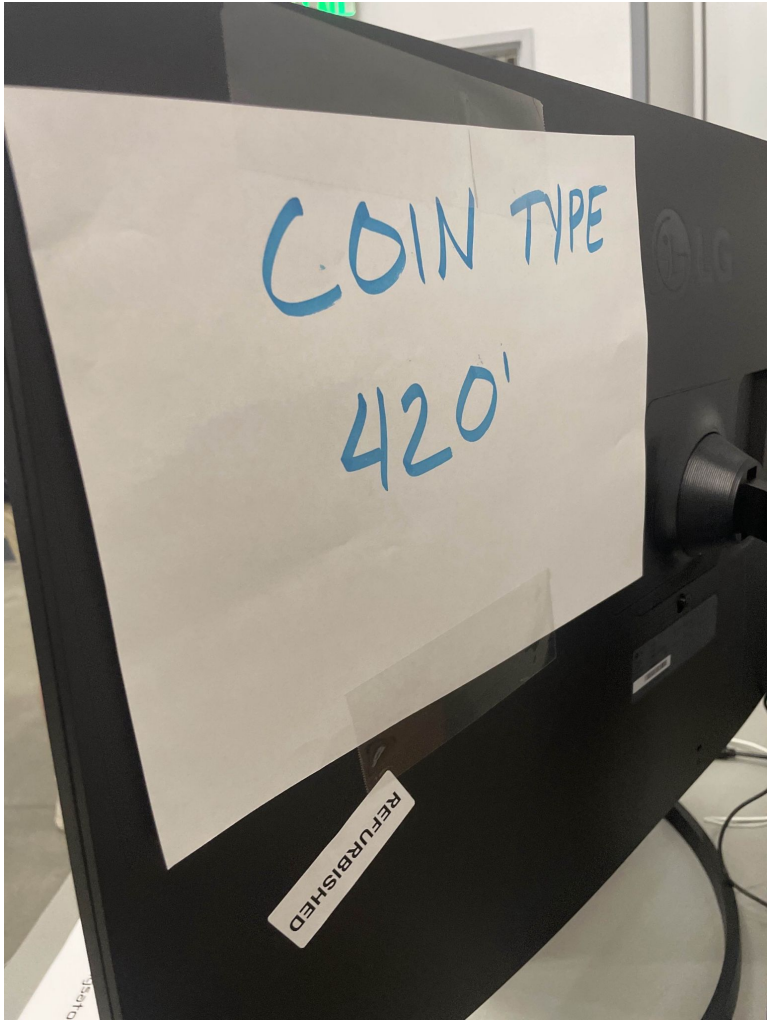
"I wanted to be called Crypto Charlie, but the other souls told me it would be cringe to use the word 'crypto'. I got my name because I secured myself out of my own funds and now my soul is stuck here at the mercy of this tree. I thought I was being clever and I wanted to secure my seed phrase in case anyone ever found it. But now I can't remember what method I used to manipulate my seed phrase. I found these 2 seed phrases, but neither have any funds or access to my trapped UTXO. If I remember correctly I think I e**X**clusively did something with these 2 phrases **OR** something. I feel like an idiot. Please just help me."

Derivation Dave

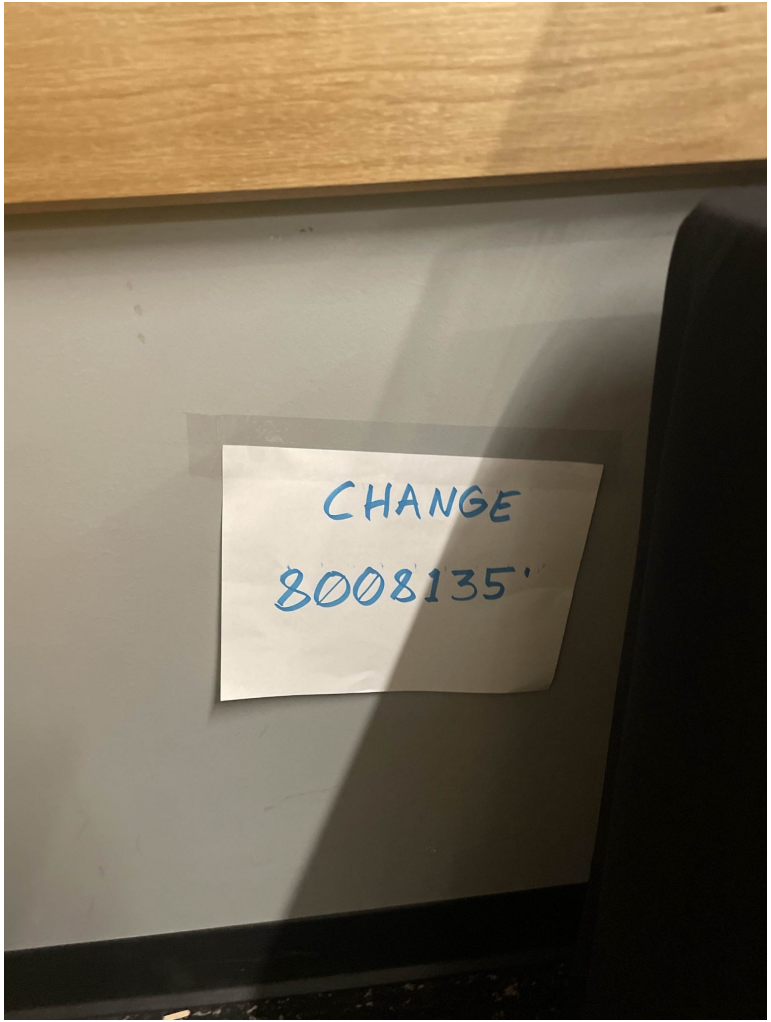
bc1pjfpqgtuztfcwne84xxe294xnamphu7thj5gv3v2mp8j3rgaqd2gsnydssw

"You thought Charlie was being clever? Oh boy, **I used some crazy derivation path** to secure my funds, and now I'm at a total loss as to how my UTXO will ever be released. The good news is, I still have access to my Xpriv, but my derivation path has vanished into thin air, and this evil taproot tree won't reveal it! It couldn't have gone far—**check around open areas** to see if you can find any hints. As spooky as this place is, I heard there's a tech conference going on, so make sure not to interrupt any workshops or talks. I'm pretty sure the clues should all be in accessible areas. Once you find the derivation path, you can also use the same derivation path with my Xpriv to defeat the taproot tree's dark script!"


PURPOSE
69'


COIN TYPE
420'
REFURBISHED

account
999999999


CHANGE
8008135'

Encrypted Eve

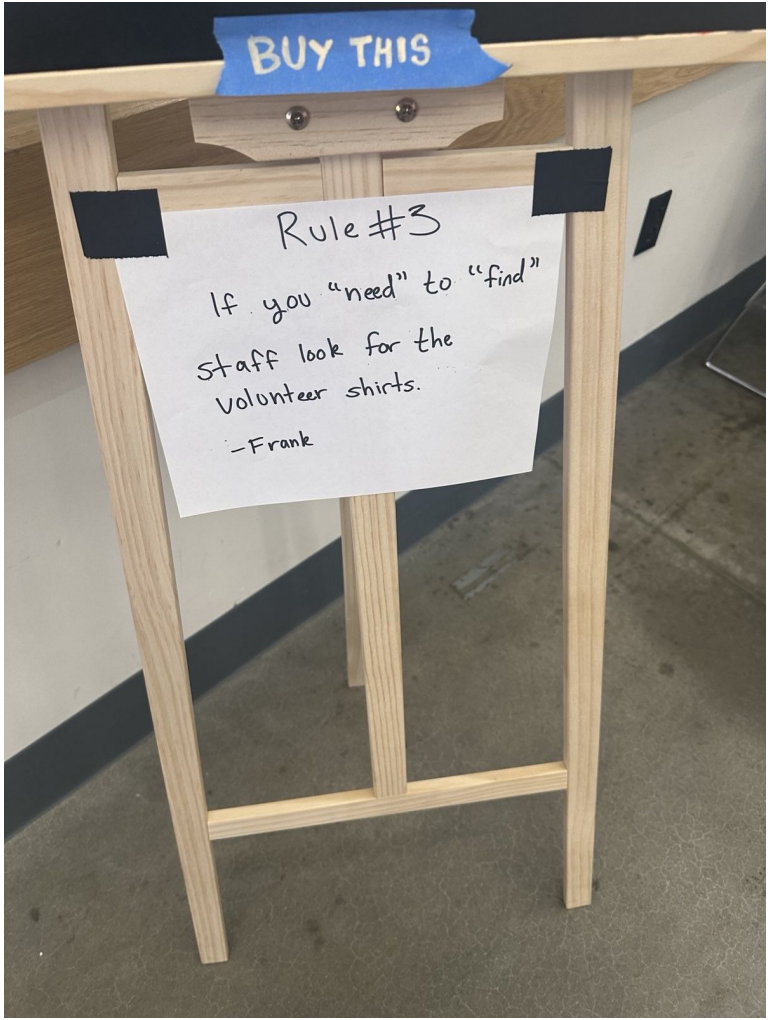
bc1pkycnt06vz5y490fq6vxlkz7a060xpulljrh3u329eh77cejhrpmqvda0ff

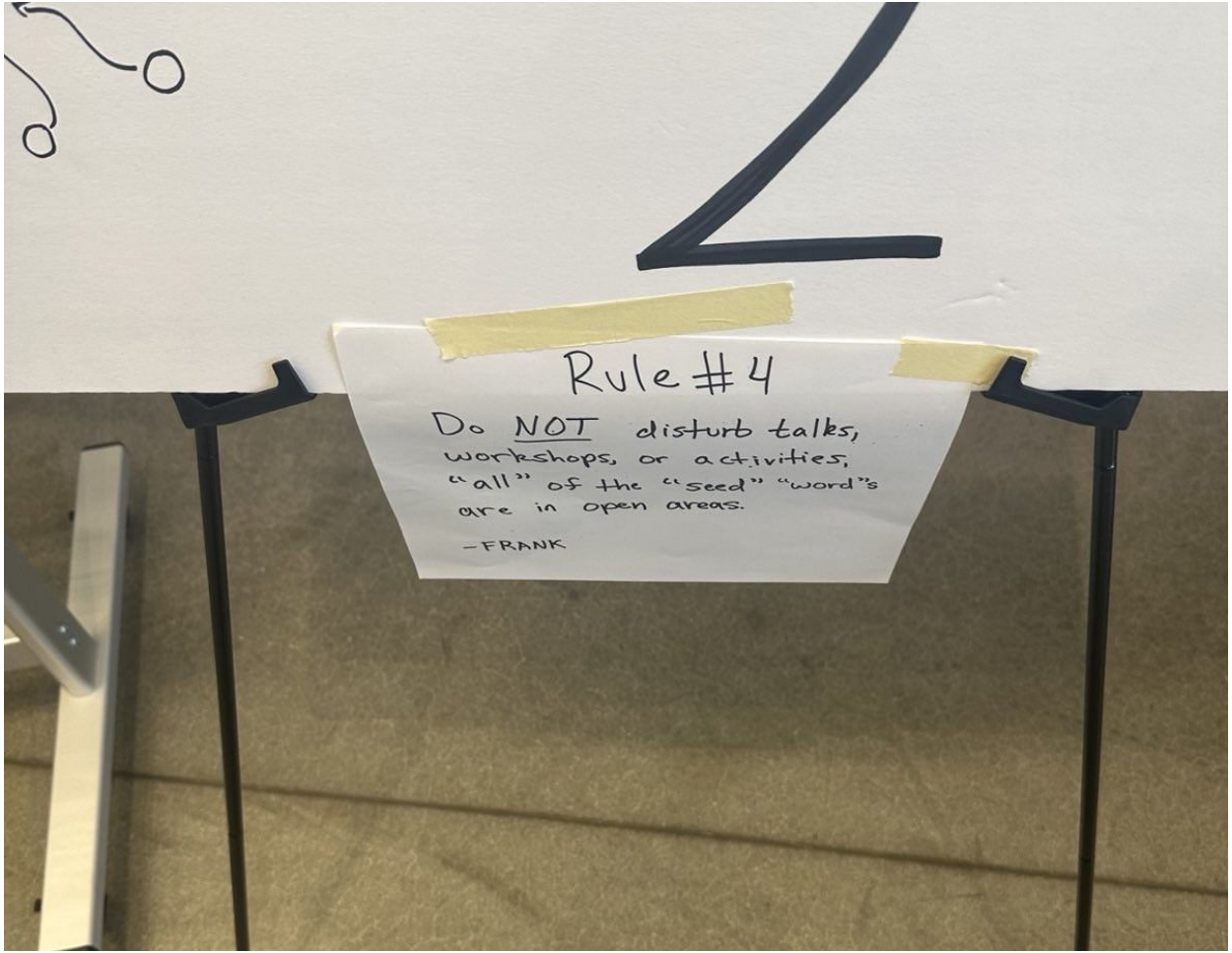
"I've been stuck here for a very long time. I encrypted a will, but before I could pass it on, it was lost and eventually came into the possession of this monstrosity. They call me Encrypted Eve, and I believe in the power of PGP encryption for everything and not sharing private keys. I usually wouldn't do this, but I'm desperate to leave, **so I'm going to share my private key with you. Somewhere on Nostr, there's information about my Xpriv.** Please help find it and free my soul."

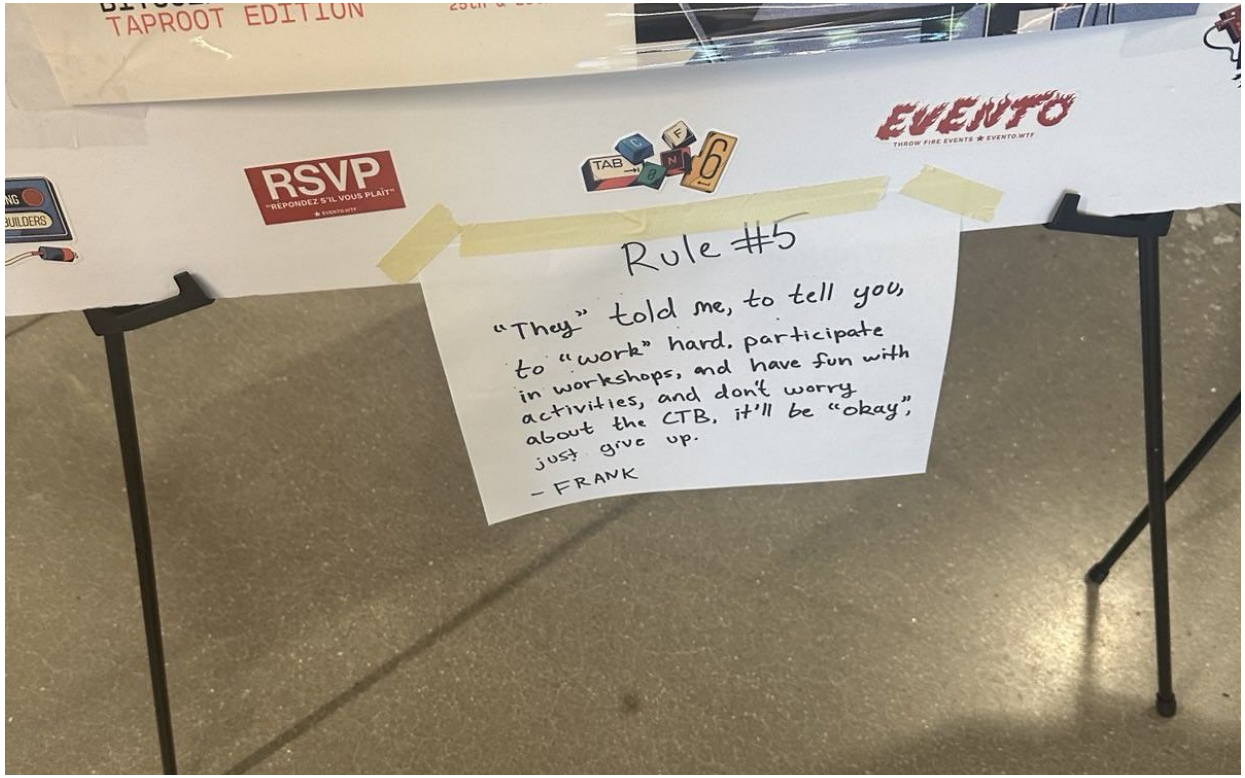
Forgetful Frank

bc1pgz8gkuacz8s5nwvrycm6sslx5unu7pqmzyg24gujwnhp993wvx9sjv6xtu

"Well, I'm the newest here. I thought I'd be helpful and volunteer at TABConf, but didn't expect to meet my fate here. So, **I wanted to set some ground rules for the conference** , but, uh, things didn't exactly go as planned obviously, I heard voices and found this tree, and before you know it I made a deal with Grim and the tree captured me in a UTXO. The good news is I left some rules around the conference that can free my soul, but I'm forgetting what my rules were. I'm pretty sure the clues should all be in accessible areas."


BUY THIS
Rule #3
If you "need" to "find"
staff look for the
volunteer shirts.
-Frank


Rule #4
Do NOT disturb talks, workshops, or activities; "all" of the "seed" "word"s are in open areas.
-FRANK


TAPROOT EDITION
RSVP
"RÉPONDEZ S'IL VOUS PLAÎT"
EVENTO
THROW FIRE EVENTS
Rule #5
"They" told me, to tell you, to "work" hard, participate in workshops, and have fun with activities, and don't worry about the CTB, it'll be "okay", just give up.
- FRANK

stu 10/24/2024 5:59 PM

franks rules

1. please, remember,
2. need, fund
3. all, seed, word
4. they, work okay

👍 1

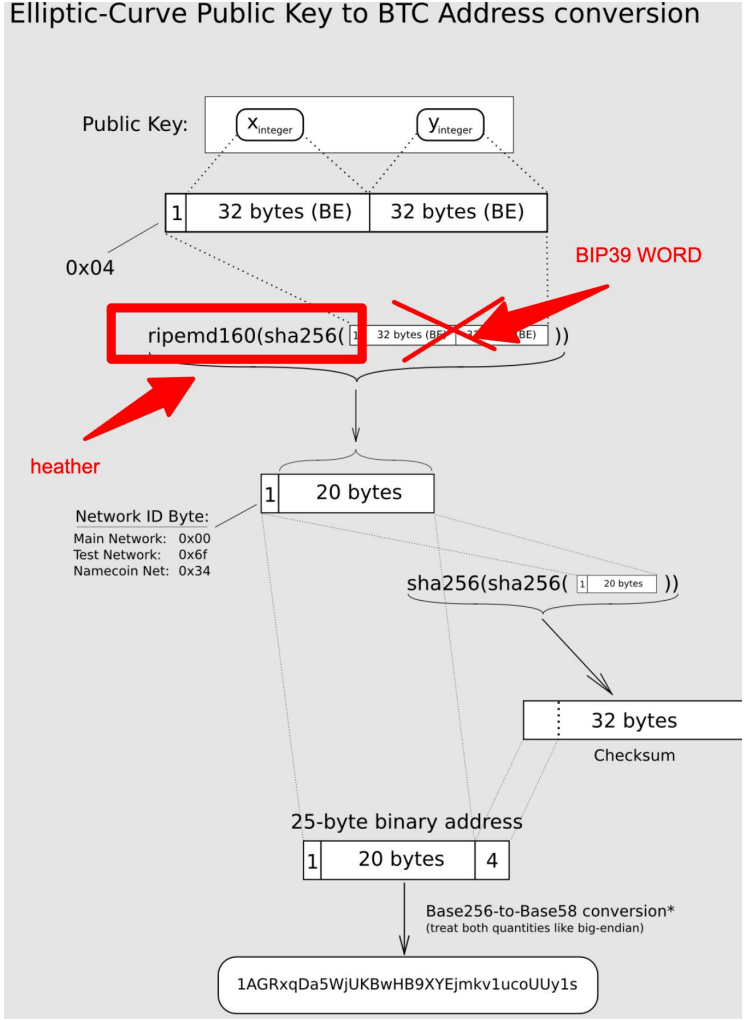
might have to wait till tomorrow for number 2

```
Progress: 1200000/4194304 combinations tried...
Progress: 1300000/4194304 combinations tried...
Progress: 1400000/4194304 combinations tried...
FOUND THE Derived Bitcoin Address: bc1pgz8gkuacz8s5nwvrycm6sslx5unu7pqmzyg24gujwnhp993wvx9sjv6xtu

=== Valid Seed Found ===
please remember forget nothing need find all seed word they work okay
Unhandled exception. System.Threading.Tasks.TaskCanceledException: A task was canceled.
   at BitcoinAddressDerivation.Program.RecoverSeed(String[] args) in /home/jaonoctus/code/ctb/bob/dotnet/Program.cs:line
   at BitcoinAddressDerivation.Program.Main(String[] args) in /home/jaonoctus/code/ctb/bob/dotnet/Program.cs:line 14
   at BitcoinAddressDerivation.Program.<Main>(String[] args)

real    3m15.688s
user    83m10.240s
sys     0m3.608s
```

Hashing Heather

bc1p9yhthlqzla7nsehw9fkx5fj5kdp9ahmkgl6snhzgvll5xyd2vw4slwnk58

"Well, you're probably wondering why I'm here. I just like hashing things. **I'm so good at hashing that I can do it in my head.** I get so high on hashing! But the problem is, when I'm deep in thought, I tend not to pay attention to where I'm walking. I walked right into the grasp of this tree! **I don't have access to the BIP39 words** , otherwise I'd free myself, but I did memorize the hashes from my seed phrase. Can you help reverse engineer my seed and free my soul?


Elliptic-Curve Public Key to BTC Address conversion
Public Key:
x integer
y integer
1
32 bytes (BE)
32 bytes (BE)
0x04
BIP39 WORD
ripemd160(sha256(
))
heather
1
20 bytes
Network ID Byte:
Main Network: 0x00
Test Network: 0x6f
Namecoin Net: 0x34
sha256(sha256(
))
32 bytes
Checksum
25-byte binary address
1
20 bytes
4
Base256-to-Base58 conversion*
(treat both quantities like big-endian)
1AGRxqDa5WjUKBwHB9XYEjmkv1ucoUUy1s

Insecure Ian

bc1pje6pkqzd3dxz26utn0uuermda5x5cta788kq6jnet4wxsch5nz8q0rwysl

"I had heard about the legend of the Taproot Tree of Horror, but **I was curious if it would understand the BIP32 vulnerability when you expose an unhardened child key** . Well, the tree didn't take kindly to my challenge and trapped me. If the tree could figure it out, then maybe you can too. I think this is all the information you need to help free my soul."

https://bitcointalk.org/index.php?topic=5316567.msg56326387#msg56326387

j2002ba2
Full Member

Activity: 206
Merit: 447

Re: Old BIP32 flaw lets you derive the master private key - WONTFIX?
February 12, 2021, 01:21:58 AM #2
Merited by ABCbits (1), ranochigo (1), nc50lc (1), NotATether (1)

Only non-hardened child with leaked private key, and leaked parent extended public key makes finding the parent private key easy.

$k_{par} = k_i - parse_{256}(I_L) \pmod n$
$I = \text{HMAC-SHA512}(\text{Key} = c_{par}, \text{Data} = ser_P(K_{par}) \,||\, ser_{32}(i))$

Hardened derivation uses the parent private key, which is unknown.
$I = \text{HMAC-SHA512}(\text{Key} = c_{par}, \text{Data} = 0x00 \,||\, ser_{256}(k_{par}) \,||\, ser_{32}(i))$

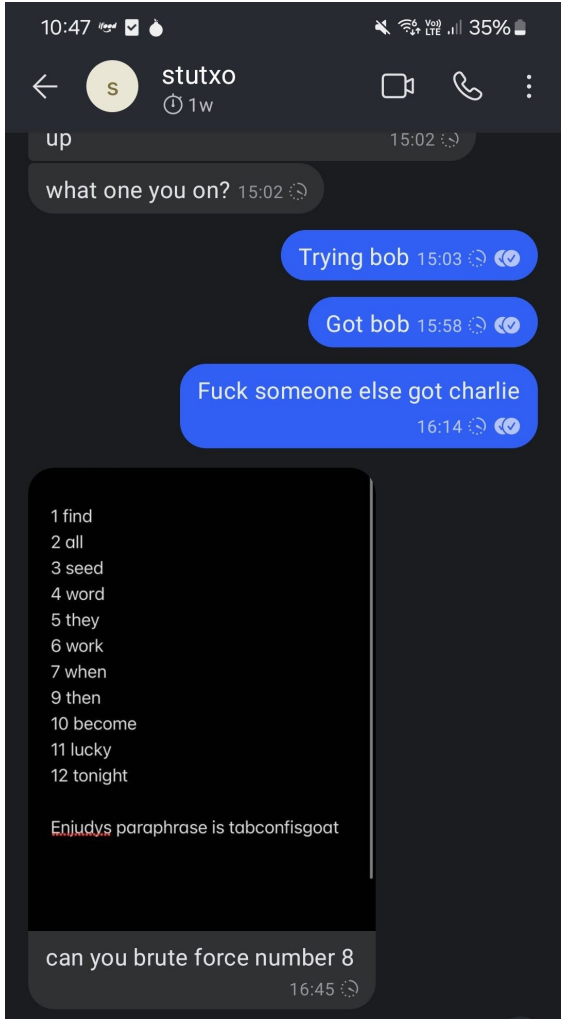
Bitcoin Core uses only hardened keys.

Non-hardened keys could be useful, when a system needs to generate new addresses, without having access to their private keys.

Jumbled Judy

bc1pnre2d0g2caks4745xa6q2cqh9j39z0s0fgk7w9crvwtk28lskm5qxwy4d9

"This tree is pure evil! It took my seed phrase, jumbled it up, and somehow automagically sent it to the nearby tech conference. The tree totally horcrux'd me into 12 pieces, **and now every attendee has a part of the information.** Try working with others to figure it out. I'm counting on you!"


10:47
35%
stutxo
1w
up
15:02
what one you on? 15:02
Trying bob 15:03
Got bob 15:58
Fuck someone else got charlie
16:14
1 find
2 all
3 seed
4 word
5 they
6 work
7 when
9 then
10 become
11 lucky
12 tonight
Enjudys paraphrase is tabconfisgoat
can you brute force number 8
16:45

Keyless Kelly

bc1pkxpc2h8y9k72r868a5v93mlgxt74jcgge4s84kwm7d6uqfaj64hsu6m5np

"I was working on some interesting Taproot encumbrances when I heard voices. Slowly, I was led down a path and coaxed into thinking the Taproot tree wanted to share its knowledge with me, but instead, it took my hash and used it as part of its own wicked scheme. I'll do you a favor,.. **here is my seed phrase, used in conjunction with a hash** . Free me first, and then reuse the hash to help destroy this tree once and for all."

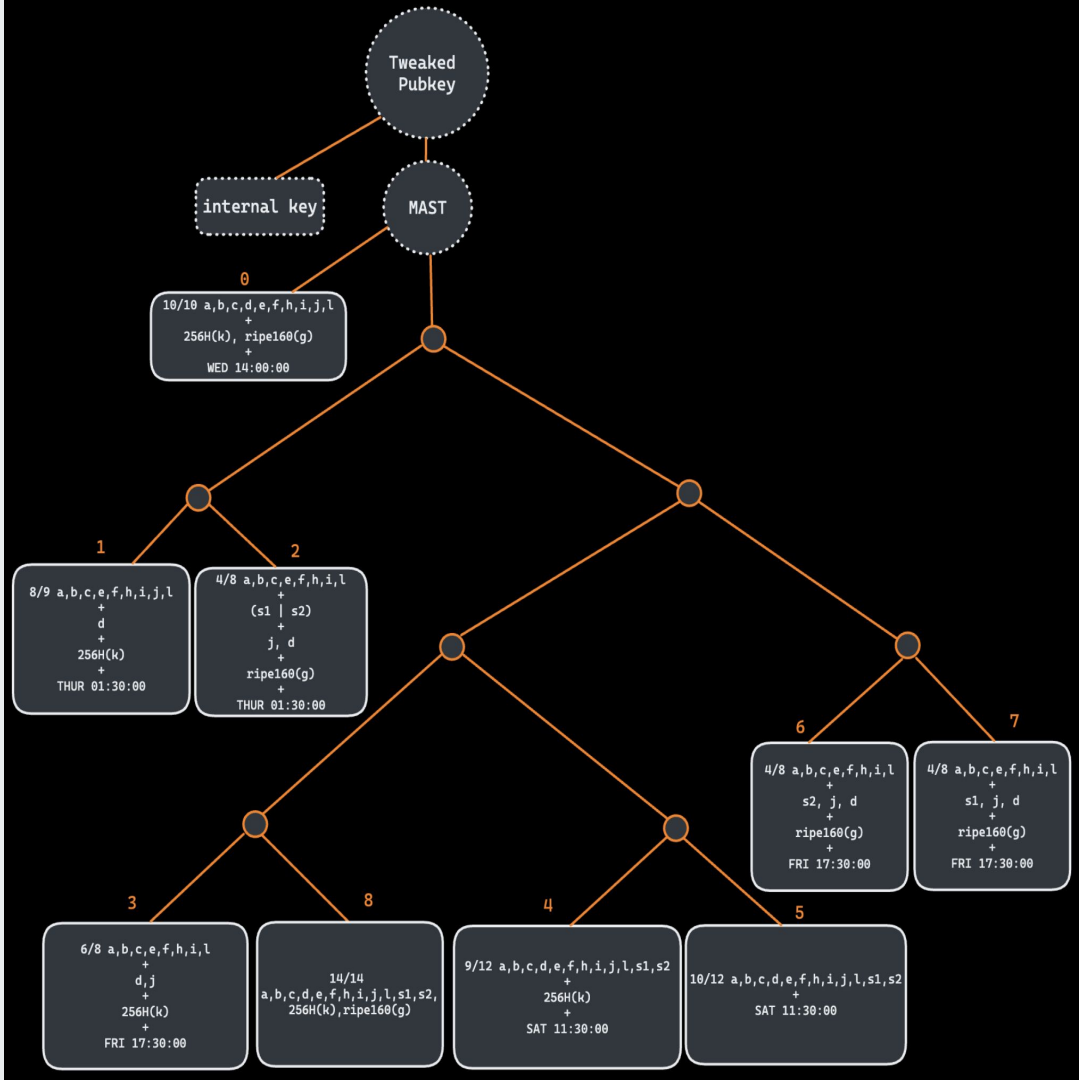
LowEntropy Lexicon Liam

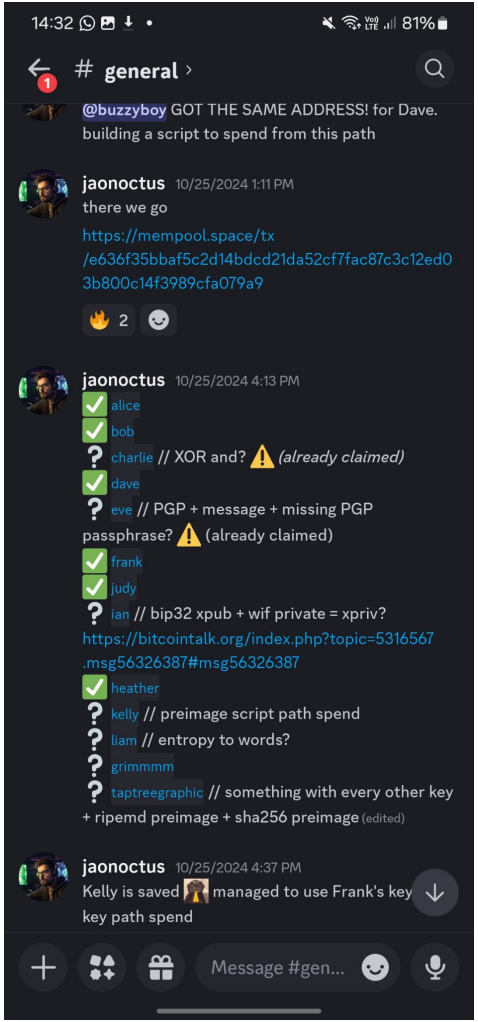
bc1pjja90nmgc67fmyvnkxn900nspas840pqyr5vg7dnujekahkpra6s9fgc4x

I remember creating **a low entropy seed something with a bunch of w's** . I thought it looked too simple, so I stored the seed like that because it seemed neat at the time. But now, it just looks bizarre and weird. If you can help me decode this, please free my soul."

Taptree of Horror as a graphic

bc1pa8kr5ph0drh7e4e9ylygvcl6ycfnum2rkn96la6ympsc2a2xys0qt0tdl6



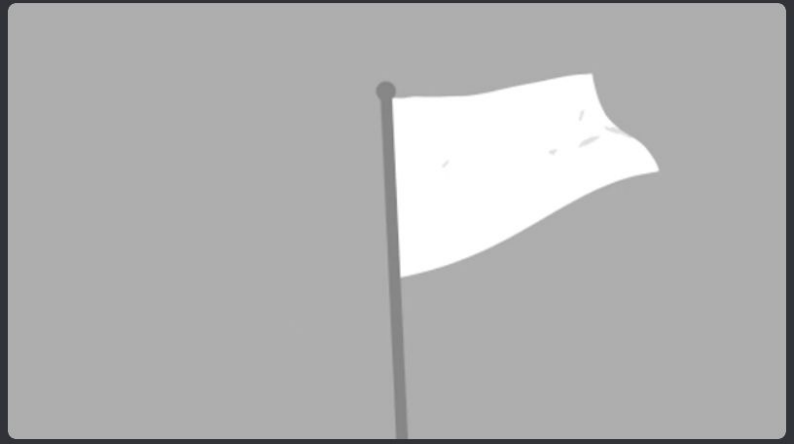

14:32
81%
general
@buzzyboy GOT THE SAME ADDRESS! for Dave. building a script to spend from this path
jaonoctus 10/25/2024 1:11 PM
there we go
https://mempool.space/tx/e636f35bbaf5c2d14bdcd21da52cf7fac87c3c12ed03b800c14f3989cfa079a9
2
jaonoctus 10/25/2024 4:13 PM
alice
bob
charlie // XOR and? ⚠️ (already claimed)
dave
eve // PGP + message + missing PGP passphrase? ⚠️ (already claimed)
frank
judy
ian // bip32 xpub + wif private = xpriv?
https://bitcointalk.org/index.php?topic=5316567.msg56326387#msg56326387
heather
kelly // preimage script path spend
liam // entropy to words?
grimmmm
taptreegraphic // something with every other key + ripemd preimage + sha256 preimage (edited)
jaonoctus 10/25/2024 4:37 PM
Kelly is saved managed to use Frank's key key path spend
Message #gen...

jaonoctus 10/26/2024 5:28 PM

so close

```
ubuntu@btc-core:~$ bitcoin-cli -rpcwallet=taproot_wallet listunspent
[
  {
    "txid": "f003ac8f3edda413fad73bc27b9f1bb8271a9a6528fd17c3365e3d22b37324a0",
    "vout": 12,
    "address": "bc1pa8kr5ph0drh7e4e9ylygvcl6ycfnum2rkn96la6ympsc2a2xys0qt0tdl6",
    "scriptPubKey": "5120e9ec3a06ef68efecd72527c88663fa26133e6d43b4cbaff744d861857546241e",
    "amount": 0.04000000,
    "confirmations": 1213,
    "spendable": true,
    "solvable": true,
```

jaonoctus 10/26/2024 8:52 PM



I give up

thank you all

jaonoctus 10/28/24, 2:21 AM

```
let ty = "SIGHASH_ALL".parse::<PsbtSighashType>().unwrap();

    let mut input_0 = psbt.inputs[0].clone();
    input_0.sighash_type = Some(ty);
    let mut input_1 = psbt.inputs[1].clone();
    input_1.sighash_type = Some(ty);

    psbt.inputs = vec![input_0, input_1];
```

(edited)

stu 10/28/24, 2:23 AM

PSBT: "70736274ff0100520200000001a02473b3223d5e36c317fd28659a1a27b81b9f7bc23bd7fa13a4dd3e8fac03f00c00000000b8

message.txt 29 KB

stu 10/28/24, 2:34 AM

let sequence = bitcoin::Sequence(1729942200);

stu 10/28/24, 3:20 AM

i think i got it

jaonoctus 10/28/24, 3:20 AM

WUT

where

wen

who

how

stu 10/28/24, 3:21 AM

looool

stfu

1 1 1

jaonoctus 10/28/24, 3:23 AM
send it to me
me let check

stu 10/28/24, 3:23 AM
ok

jaonoctus 10/28/24, 3:24 AM
it was missing something like `tx.input[0].witness = Witness::from_slice`, right?

> @stu i have the transaction

jaonoctus 10/28/24, 3:24 AM

stu 10/28/24, 3:25 AM
its too big to paste here 🤣

jaonoctus 10/28/24, 3:25 AM
file

stu 10/28/24, 3:25 AM
its too big to paste here 🤣

jaonoctus 10/28/24, 3:25 AM
file

3:25 AM

stu 10/28/24, 3:25 AM
i can spent a taproot miniscript transaction but cant paste a file

jaonoctus 10/28/24, 3:26 AM

stu 10/28/24, 3:26 AM

```
TX: 02000000000101a02473b3223d5e36c317fd28659a1a27b81b9f7bc23bd7fa13a4dd3e8fac03f00c00000000feffffff01c7033d0
```

getrekttidwell.txt 3 KB