

Forum:[Hack Forums](#)

Thread: [Every Bitcoin Private Key](#)

Omniscient - January 6, 2023, 10:13 am

<https://keys.lol/>

That's a funny site. Basically every key for ETH and BTC on it. You can do random pages and look for a TXN. If there is one, you've potentially hit a jackpot for a private key. I've done about 20 pages, nothing. You could spend an eternity on this page and probably never get one but hey, you never know.

Omniscient - January 6, 2023, 10:20 am

(Jan 6, 2023 11:18 AM)Focus Broken Wrote: [\[CITE\]](#) That's pretty cool. Here's an even more smug way to do it ?

I saw that tweet. It's true. I wonder if anyone spends their time just running systems to look for privkey combos with balances?

SUI-3183372 - January 6, 2023, 10:24 am

(Jan 6, 2023 11:20 AM)Admin Wrote: [\[CITE\]](#) I wonder if anyone spends their time just running systems to look for privkey combos with balances?

Our old friend Kill Joy probably spent more time than he'd like to admit doing this.

Truth - January 6, 2023, 10:24 am

anyone's better off spending their time looking outside for empty cans to redeem and buy lottery tickets, higher odds to actually win something

if it truly is random, you can theoretically just use one of the private keys on there, deposit some bitcoin, and not even need to worry about someone stealing it

shreder - January 6, 2023, 10:39 am

Once a day look at the page, the universe might align perfectly for you.

SUI-3183372 - January 6, 2023, 10:47 am

(Jan 6, 2023 11:24 AM)Truth Wrote: [\[CITE\]](#) if it truly is random, you can theoretically just use one of the private keys on there, deposit some bitcoin, and not even need to worry about someone stealing it

That's technically what we're all doing anyways, the choice just gets made for us when we create the wallet.

Funny how uneasy you feel selecting a key from that page, somehow having the data in front of you on a publicly facing website just makes everything feel so insecure. Yet you feel perfectly fine when you're not looking that data in the face and the choice is made for you by your wallet software (which increases your threat landscape and may introduce additional security risks, such as the Solana wallet storing keys on a webserver).

SecureOp - January 6, 2023, 11:22 am

I know I should trust the system, but damn. Technically, it is possible for someone to just snatch and run? ?

shreder - January 6, 2023, 11:25 am

(Jan 6, 2023 12:22 PM)Fvck Wrote: [\[CITE\]](#) I know I should trust the system, but damn. Technically, it is possible for someone to just snatch and run? ?

I mean if someone had a 1 in

904625697166532776746648320380374280100293470930272690489102837043110636675
chance and hit it on my address. They fucking deserve it.

SUI-3183372 - January 6, 2023, 11:33 am

(Jan 6, 2023 12:25 PM)shreder Wrote: [\[CITE\]](#) I mean if someone had a 1 in

904625697166532776746648320380374280100293470930272690489102837043110636675
chance and hit it on my address. They fucking deserve it.

Let's say a well resourced attacker can check 1 quadrillion (1,000,000,000,000,000) addresses a day.

That still only makes their chances of finding a valid wallet 1 in

904,625,697,166,532,776,746,648,320,380,374,280,100,293,470,930,272,690,489,102 (per day).
That's just for ANY wallet, could be zero balance with no transactions, doesn't mean there will be funds in it.

In comparison, your chances of winning the Powerball jackpot are 1 in 293,000,000

904625697166532776746648320380374280100293470930272690489102837043110636675
vs
293000000

shreder - January 6, 2023, 11:36 am

(Jan 6, 2023 12:33 PM)BV1 Wrote: [\[CITE\]](#) Let's say a well resourced attacker can check 1 quadrillion (1,000,000,000,000,000) addresses a day.

That still only makes their chances of finding a valid wallet 1 in

904,625,697,166,532,776,746,648,320,380,374,280,100,293,470,930,272,690,489,102 (per day).
That's just for ANY wallet, could be zero balance with no transactions, doesn't mean there will be funds in it.

In comparison, your chances of winning the Powerball jackpot are 1 in 293,000,000

904625697166532776746648320380374280100293470930272690489102837043110636675
vs
293000000

That's what I'm saying lol if they get it, they deserve to keep it.

Omniscient - January 6, 2023, 11:39 am

(Jan 6, 2023 12:33 PM)BV1 Wrote: [\[CITE\]](#) Let's say a well resourced attacker can check 1 quadrillion (1,000,000,000,000,000) addresses a day.

That still only makes their chances of finding a valid wallet 1 in

904,625,697,166,532,776,746,648,320,380,374,280,100,293,470,930,272,690,489,102 (per day).
That's just for ANY wallet, could be zero balance with no transactions, doesn't mean there will be funds in it.

904625697166532776746648320380374280100293470930272690489102837043110636675
vs
293000000
So what you're really saying is, I got a chance? ?

(Jan 6, 2023 12:39 PM)Admin Wrote: [CITE](#) So what you're really saying is, I got a chance? ? If LBC's trophy page is to be believed, then they've pulled it off two or three times:
<https://lbc.cryptoguru.org/trophies>
(Ignore the puzzle transactions, those are intentionally weak keys)

(Jan 6, 2023 12:43 PM)BV1 Wrote: [\[CITE\]](#) If LBC's trophy page is to be believed, then they've pulled it off two or three times:
<https://lbc.cryptoguru.org/trophies>
(Ignore the puzzle transactions, those are intentionally weak keys)

I have probably spent a few hours in total looking at that site. The amount of pages is insane and I realized that I have a better chance buying a lottery ticket so I stopped looking into it.

I wonder if people have set up bots to look through the pages until it finds an adress with funds in it.

Number of possible unique Bitcoin addresses
vs
Number of atoms in the observable universe

web0m - January 6, 2023, 12:50 pm

I actually found 10 cents worth of BTC.

For a moment I thought I was about to get rich - >

<https://keys.lol/ethereum/904625697166532776746648320380374280100293470930272690489102837043110636675>

Apparently, they are all empty.

SUI-3183372 - January 6, 2023, 1:14 pm

(Jan 6, 2023 01:50 PM)t0xi Wrote: [\[CITE\]](#) I actually found 10 cents worth of BTC.

For a moment I thought I was about to get rich - >

<https://keys.lol/ethereum/904625697166532776746648320380374280100293470930272690489102837043110636675>

Apparently, they are all empty.

The one address there that has 10.33 ETH is an interesting one.

The correlated private key is: ffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141

It's interesting because if you use the private key '0000000000000000000000000000000000000000000000000000000000000000', you also derive the same wallet address with the same 10.33 Ethereum balance.

I'm pretty sure this is because the 000 address is the "first" and the ffff address exceeds what should be possible for the "last" private key on the curve, leading to some sort of overlap/collision.

Neither key is valid for use, sending to that address is essentially burning funds.

Vibe - January 6, 2023, 1:24 pm

I definitely spent more time I'd like to admit on those private key sites back in the day lmao, personally I think they probably have it coded so if there was one with TX someone finally found it wouldn't get displayed and would send notifications to owner of website.

Get other people to do the searching for you lol

web0m - January 6, 2023, 1:56 pm

(Jan 6, 2023 11:47 AM)BV1 Wrote: [\[CITE\]](#) That's technically what we're all doing anyways, the choice just gets made for us when we create the wallet.

Funny how uneasy you feel selecting a key from that page, somehow having the data in front of you on a publicly facing website just makes everything feel so insecure. Yet you feel perfectly fine when you're not looking that data in the face and the choice is made for you by your wallet software (which increases your threat landscape and may introduce additional security risks, such as the Solana wallet storing keys on a webserver).

Huh, wait, what?

Is Solana wallet actually storing their keys on a webserver?

Vibe - January 6, 2023, 2:15 pm

(Jan 6, 2023 02:56 PM)t0xi Wrote: [\[CITE\]](#) Huh, wait, what?

Is Solana wallet actually storing their keys on a webserver?

When you make a wallet, it just generates a random private key for you, this website just took every combination and put them in order. If you hit the random button it's pretty much the same as generating a "new" wallet and key

web0m - January 6, 2023, 2:17 pm

(Jan 6, 2023 03:15 PM)Vibe Wrote: [\[CITE\]](#) When you make a wallet, it just generates a random private key for you, this website just took every combination and put them in order. If you hit the random button it's pretty much the same as generating a "new" wallet and key
Yes. I am aware of that. :D

But BV1 said something about Solana is storing their private keys for wallets on a webserver.
Which is kind of scary to think about.
Edit: Never mind, I realize I misunderstood something.

shreder - January 6, 2023, 2:26 pm

(Jan 6, 2023 01:50 PM)t0xi Wrote: [\[CITE\]](#) I actually found 10 cents worth of BTC.

For a moment I thought I was about to get rich - >
<https://keys.lol/ethereum/904625697166532776746648320380374280100293470930272690489102837043110636675>

Apparently, they are all empty.
You randomly stumbled on this?

web0m - January 6, 2023, 2:27 pm

(Jan 6, 2023 03:26 PM)shreder Wrote: [\[CITE\]](#) You randomly stumbled on this?
Yessir, stumbled on like 5 wallets now with \$0.1 and 2 wallets with 0.3\$

SUI-3183372 - January 6, 2023, 2:27 pm

(Jan 6, 2023 03:17 PM)t0xi Wrote: [\[CITE\]](#) Yes. I am aware of that. :D

But BV1 said something about Solana is storing their private keys for wallets on a webserver.
Which is kind of scary to think about.
Edit: Never mind, I realize I misunderstood something.
It was a specific Solana wallet, I'm not that familiar with their ecosystem so the name isn't coming to mind right now.

Edit: Slope Wallet

web0m - January 6, 2023, 2:29 pm

(Jan 6, 2023 03:27 PM)BV1 Wrote: [\[CITE\]](#) It was a specific Solana wallet, I'm not that familiar with their ecosystem so the name isn't coming to mind right now.

Edit: Slope Wallet
Question, what if you were looking for less saturated coins?
Wouldn't that up your chances?

Might be a stupid question, I don't know a lot about this specific topic

th3c0rrupt3d0n3 - January 6, 2023, 2:29 pm

I remember when directory.io was posted on bitcointalk and I went nuts scanning for funds. Then I made a bot to scan a copy of the site i hosted locally. IIRC it was scanning a billion keys a minute. At some point I began reading about the math and turned it off. Obviously, I never found shit but it was a fun learning experience.

Not gonna lie, I like to open a random page here and there; hoping it would contain my 1000 BTC wallet someday :)

SUI-3183372 - January 6, 2023, 2:32 pm

(Jan 6, 2023 03:29 PM)t0xi Wrote: [\[CITE\]](#) Question, what if you were looking for less saturated coins?

Wouldn't that up your chances?

Might be a stupid question, I don't know a lot about this specific topic

All depends on the chain and how many possible addresses there are. Not all chains use the same algorithm.

I imagine more saturated = better because you'll have more wallets with balance that you can potentially hit on. Would lead to more competition too though (I don't imagine too many people are doing this).

shreder - January 6, 2023, 2:32 pm

(Jan 6, 2023 03:27 PM)t0xi Wrote: [\[CITE\]](#) Yessir, stumbled on like 5 wallets now with \$0.1 and 2 wallets with 0.3\$

Oh lmao this is the last page some idiot probably used the keys from this site that's how.

web0m - January 6, 2023, 2:37 pm

(Jan 6, 2023 03:32 PM)BV1 Wrote: [\[CITE\]](#) All depends on the chain and how many possible addresses there are. Not all chains use the same algorithm.

I imagine more saturated = better because you'll have more wallets with balance that you can potentially hit on. Would lead to more competition too though (I don't imagine too many people are doing this).

Makes sense, thanks!

I imagine a lot of people is doing it to be honest, with automated tools.

trashy - January 6, 2023, 2:41 pm

This is fun. It's impressive how even knowing the maths and being almost impossible to find your key stills have some fear about it haha.

Also great that the probability to find some wallet with funds is also ?0 but we still click that random button for a time, I love it hahah will try once every day

web0m - January 6, 2023, 2:43 pm

(Jan 6, 2023 03:29 PM)th3c0rrupt3d0n3 Wrote: [\[CITE\]](#) I remember when directory.io was posted on bitcointalk and I went nuts scanning for funds. Then I made a bot to scan a copy of the site i hosted locally. IIRC it was scanning a billion keys a minute. At some point I began reading about the math and turned it off. Obviously, I never found shit but it was a fun learning experience.

Not gonna lie, I like to open a random page here and there; hoping it would contain my 1000 BTC wallet someday :)

Just read this online " There is one caveat though. If you own quantum computer with 2330 qubits and 126 billion Toffoli gates, teoretically you could get private key from public key. "

Any thoughts on this?

grady - January 6, 2023, 2:55 pm

(Jan 6, 2023 03:43 PM)t0xi Wrote: [\[CITE\]](#) Just read this online " There is one caveat though. If you own quantum computer with 2330 qubits and 126 billion Toffoli gates, teoretically you could get private key from public key. "

Any thoughts on this?

If you own a quantum computer that exceeds current bleeding edge research by about 200x, knew how to operate it, and how to break modern encryption schemes (trivial in comparison to the first two), you'd be able to crack it in non-exponential time. It would still take a LONG fucking time, but that's the baseline for getting one within your lifetime IIRC.

SIM-1169085 - January 6, 2023, 2:55 pm

In short, you'd have an easier time guessing Omnis password and 2FAC Authentication before you generate someone's private key.

web0m - January 6, 2023, 2:58 pm

(Jan 6, 2023 03:41 PM)trashy Wrote: [\[CITE\]](#) This is fun. It's impressive how even knowing the maths and being almost impossible to find your key stills have some fear about it haha.

Also great that the probability to find some wallet with funds is also 2^{-256} but we still click that random button for a time, I love it hahah will try once every day
Don't do it, it's gonna become an addiction haha

Vitaly - January 6, 2023, 3:35 pm

its a thrilling feeling knowing that if you think about it, literally anyone can access your money

of course in reality the chances are basically 0, but still an interesting thought

Blazin - January 6, 2023, 5:40 pm

Pretty sure people have setup bots on the internet to do this, check if wallet has balance and if it does empty it.

Marvelous - January 18, 2023, 7:19 pm

It would be interesting to use Check4Change on this. Imagine getting a Satoshi wallet? You could get a bunch of money and sell the wallet to Craig Wright for a bunch more money.

SUI-3183372 - January 18, 2023, 7:40 pm

(Jan 18, 2023 08:19 PM)Marvelous Wrote: [\[CITE\]](#) sell the wallet to Craig Wright for a bunch more money.

Weird way to say 'get sued by Craig, win in court, and then never get paid damages while Craig and Calvin twist the verdict to act as if it means nothing in the grand scheme of things.'

Flyrect - January 18, 2023, 11:04 pm

Imagine getting access to Elon musk's wallet, half of the existing bitcoin will be gone to some random guy :P

SMMFlare - January 19, 2023, 7:41 am

596208136659018344293845810633440973768619683634253065962549756119482719440 of 904625697166532776746648320380374280100293470930272690489102837043110636675

Holy shit!

_daniel - January 19, 2023, 3:45 pm

This reminds me of the video explaining just how secure SHA256 is (today):

[Video: https://www.youtube.com/watch?v=S9JGmA5_unY]

^ Will show you your chances of getting a private key from a site like this

