

Forum:[Hack Forums](#)

Thread: [bitcoin seed generator from addresses](#)

drfeelgood7161 - April 9, 2025, 6:24 am

I have a giant btc addresses list with millions of dollars in them.

I need a program that generates the seeds for them, is there such a program available?

badbart - April 9, 2025, 9:39 am

Those giant btc addresses are supposedly public. If there's a program that could generate seeds for each btc addresses, it would probably worth millions of dollars too, if there is any, it would defy the purpose and sacrosanct of its privacy with cryptography. Not an expert, but as I am writing this, I don't think it exists. Still I might be wrong.

DramaKing - April 9, 2025, 12:54 pm

(Apr 9, 2025 06:24 AM)drfeelgood7161 Wrote: [\[CITE\]](#) I have a giant btc addresses list with millions of dollars in them.

I need a program that generates the seeds for them, is there such a program available?

Would you like a money making machine, too?

Forgive the sarcasm. Yes, you can generate seeds for BTC addresses. However, the cryptography is designed to be one-way; that is, you cannot simply enter a BTC address and calculate the seed phrases (or the private key, see Public Key Infrastructure). That would be ludicrous.

Let me ask you a statistics question. There are 12 words in a seed phrase. There are 2000 possible words that can be used. How long would it take to randomly generate and verify a seed phrase for one of these addresses?

Also, think about what you actually need.

drfeelgood7161 - April 10, 2025, 2:58 am

Let me ask you a statistics question. There are 12 words in a seed phrase. There are 2000 possible words that can be used. How long would it take to randomly generate and verify a seed phrase for one of these addresses?

I did not consider the math, yes thank you :)

It is clear that you would need quantum computer power to find the seed

Thank you for the info!