Understanding Bitcoin's Underlying Security Inbox x

Team Bitcoin.com <team@bitcoin.com> Aug 29 (4 days ago)
to me

Bitcoin.com

Hey Ben,

Want to keep hackers off your Bitcoins?
Just learn how cryptography works, and you'll know how to secure your coins.

Both the private and public keys of your Bitcoin wallet come from cryptography. **Asymmetric, or public key, cryptography uses public and private keys** to encrypt and decrypt data.

Both keys are basically large numbers, which were paired together. Their asymmetric nature is due to the two keys not being identical.

While the public key is shared with everyone, the private key is always kept secret.

In Bitcoin's case, this means that **the public key is your wallet address**, which is shared with everyone so they can send you coins. On the other hand, **the private key is used for accessing your account.** If it falls into the wrong hands, your cryptos could be easily stolen.

Bitcoin is built on cryptography. We are not trusting anyone - not even your neighbor or your best friend - with securing transactions in the network, but math.

Bitcoin's cryptography is so secure that there is a higher probability that lightning strikes you on a sunny day than that a Bitcoin address gets hacked by someone who is not in control of your private keys.

How does it work?

Let's take a simple example.

You want to send an email to your colleague Bob. **The content of the email is sensitive, so you use cryptography to encrypt it.**

After writing the email, **you use Bob's public key to encrypt the email.** When sending the message, you sign it with your private key so Bob can verify (by decrypting your signature with his public key) that you were the actual sender.

As the public key is paired with a private key, **Bob can use the latter to decrypt and read your email.**

As you used (only) Bob's public key to encrypt your email, **you shouldn't worry about anyone eavesdropping your conversation as only he can decrypt the content inside.**

Even if someone acquires your email, they can't decode it.

Using cryptography in real life

It isn't just Bitcoin that uses cryptography. As the private and public keys are used to encrypt and decrypt data, asymmetric cryptography is very useful for other things as well.

Let's see some examples where cryptography is used:

- **Messages and emails.** Pretty Good Privacy (PGP) is a popular method for safe messaging. You encrypt your message using the public key of your recipient, while your recipient uses his private key to decrypt and read your message. **The Bitcoin.com Team uses PGP** to ensure that our company emails won't fall in the wrong hands.
- RSA (Rivest-Shamir-Adleman) is one of the most widely-used asymmetric algorithms in the world. **We bet you have seen a website using SSL protocol. It's one good example of the RSA asymmetric cryptography,** which is used to secure communications over a computer network.
- **You can even encrypt your hard drive with cryptography.** PGP is a popular method for that; you encrypt your data with your private key and a password, and you use the same keys for decryption too.

Where to store your private and public keys

As your public key is used to send transactions to your address, it is not important to store that in a safe place.

On the other hand, **if anyone has access to your private keys, he has access to your Bitcoins too,** as well as everything that's secured by those keys, such as your work emails.

That's why it is essential to **use a wallet that stores your private keys offline.**

Avoid exchanges whenever you can as they don't even give you access to your private keys. That means **you are not in full control of your funds!**

Physical wallets are the best option, as they store your private keys offline.

While paper wallets let you generate, print, and store both your public and private keys offline on a piece of paper, hardware wallets **come with a device that has to be connected to your computer to access your funds.** While the device is not connected via USB, your wallet stays offline giving additional security for your cryptos.

If you care about your security, check out our paper wallet generator and/or The Store at Bitcoin.com's hardware wallets.

You can also try our software wallet, which balances security and convenience. Unlike exchange wallets, you have access to your private keys.

Best,
Team Bitcoin.com