Source : www.thehindu.com Date : 2021-07-13

BITCOIN HARDWARE WALLET EXPLAINED

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Hardware wallets store details of the user's private keys in secure format. | Photo Credit: Trezor

Last week, Twitter CEO Jack Dorsey announced his payments firm Square would soon build a hardware wallet to store bitcoin. The wallet will be a type of plug-in device, much like a USB pendrive that stores, manages and secures a user’s crypto assets.

(Subscribe to our Today's Cache newsletter for a quick snapshot of top 5 tech stories. Click here to subscribe for free.)

Each digital asset is linked to a cryptographic password called a ‘private key’ to allow users to access it. This key safeguards cryptocurrencies from theft and unauthorised access.

The asset owner, with the help of a secure hardware wallet, can access the private key to buy and sell crypto assets from anywhere. Most hardware wallets allows users to manage multiple accounts; some even allow users to connect to their Google or Facebook accounts. Popular hardware wallets include Trezor, Ledger, KeepKey and Prokey.

Cryptocurrency keys can be stored in two kinds of wallets - software and hardware.

Also Read | Cryptocurrency holders targeted with ‘intrusive’ new access tool

Software wallets are like smartphone apps that digitally store private keys. Most software wallets don’t charge users to store private keys, but may collect commission for trading via the app. These wallets can be vulnerable to malware.

Hardware wallets and physical devices act like cold storage for confidential keys. The passwords are protected by a PIN, making it difficult for hackers to extract private keys as the information is not exposed to the Internet.

Hardware wallets are said to be convenient as they can be connected to trading exchanges to complete transactions.

Also Read | In a world first, El Salvador makes bitcoin legal tender

Hardware wallets are often stored in a protected microcontroller and cannot be transferred out of the device, making them secure. Their isolation from the Internet also mitigates the risk of the assets being compromised. Moreover, it does not rely on any third-party app.

Since the wallet is in physical form, the device could be stolen or destroyed. A 2016 study by the University of Michigan also noted prominent hardware backdoors that could be used by malicious actors to steal confidential data.

The device can also be expensive as compared to software wallets. Some hardware wallets can also have complex features, making it difficult for first-timers to understand.

Our code of editorial values

At the heart of the dispute between Twitter and the Union government is who gets to decide what goes on the platform, and both parties are claiming to be defenders of free speech.

Will they become law? How will the move impact India?

END