Hardware wallets: paper or plastic? A starter guide - Crypto News Review

6/14/18, 11:57 AM

CryptoNews Review

HOME   NEWS   BLOCKCHAIN   ICOS   CRYPTO   MARKETS   LEGAL & REGULATION

RESEARCH

LATEST: Businesses shouldn't just integrate blockchain for the sake o

Search

LIVE: 87 %)   ₿ BCH: $ 874.27 (5.37 %)   ◆ ETH: $ 509.02 (8.89 %)   ✕ XRP: $ 0.5494

CryptoCompare

USD	EUR	CNY	GBP

$ 6,542.44 (3.94%) ▲

₿ **BTC**	
◆ **ETH**	**$ 512.21** (9.54%) ▲
Ⓜ **XMR**	**$ 129.75** (10.00%) ▲
Ⓛ **LTC**	**$ 98.75** (7.97%) ▲
Ⓓ **DASH**	**$ 263.48** (8.13%) ▲

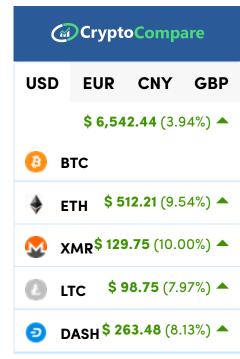** Price & chart conversion through BTC*

Hardware wallets: paper or plastic? A starter guide

Gareth Halfacree | Crypto, Feature on May 22nd, 2018

More and more people are using hardware wallets for their cryptocurrency. But what are they, and what do you need to know?

Hardware wallets: paper or plastic? A starter guide - Crypto News Review

6/14/18, 11:57 AM

While having some cryptocurrency in a hot-wallet on your phone or computer is certainly handy from the perspective of spending it, it's not the most secure way to store your assets. Malware, theft, or even a simple hardware failure can be enough to put your coins out of reach – which is why many are turning to hardware wallets to secure their crypto.
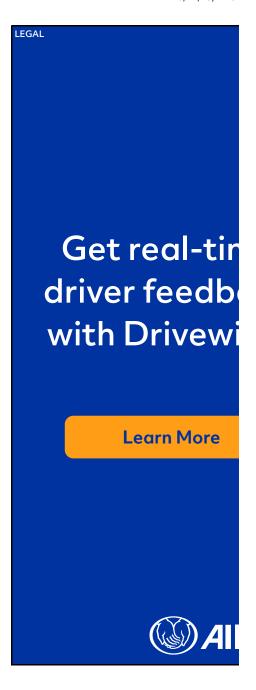
Paper

The simplest, and oldest, form of hardware wallet is a paper wallet. As the name implies, a paper wallet is made entirely out of paper – and, if you think you can jot down long hexadecimal strings without error, can even be 'printed' by hand.

A paper wallet is nothing more than the private key associated with a cryptocurrency address printed or written onto paper or, for improved durability, etched or stamped into metal. A more advanced variant includes the public address, allowing the user to add funds to the wallet over time and check its current balance – these transactions occurring on the currency's blockchain without the need for the private key.

A paper wallet, if generated correctly, printed on a known-safe system whose print buffer is cleared afterwards, and stored in a safe location, is absolutely secure, but it's also an awkward beast to use. There's no way to spend money from a paper wallet without exposing the private key; when you want to actually use your stored funds, you need to move the entire contents in one transaction – a process known as "sweeping". Once its contents are swept, the paper wallet should be destroyed.

Plastic

The awkward nature of paper cold wallets and the relative insecurity of computer-based hot wallets has given rise to so-called "warm wallets": hardware-based wallets which are capable of live transactions, like a hot wallet, but which guard the private key from theft, like a cold wallet.

Popular Posts:

John McAfee vows to include "as much of the cryptocurrency world as I can" in his US Presidential bid

by
Simon Brew

SEC allows buying of stocks with crypto for first time

Hardware wallets: paper or plastic? A starter guide - Crypto News Review

6/14/18, 11:57 AM

As interest in cryptocurrencies grow, the number of hardware wallets – both single-purpose wallets for a particular cryptocurrency and multi-purpose wallets which support multiple currencies – grows also. The two most popular manufacturers, Ledger and Trezor, approach the issue in much the same way: protecting the private key by storing it in the "secure enclave" of a chip encased in a standalone device. This key is generated on the device and never leaves it: when transactions are made the device is connected to a host computer, proper ownership verified by the entering of a personal identification number, and the transaction signed by the device itself – meaning the host computer never, if all has gone well, sees the private key.

It's an approach that works well, and many of these wallets include additional security features such as an on-board screen on which the transaction is confirmed – a means of beating crypto-jacking malware which may be installed on the host system and which changes addresses as they are copied and pasted.

Proof of Security

It's still relatively early days for dedicated hardware wallets, however, and the companies producing them don't necessarily have the proven track record of long-established companies working outside the cryptocurrency sector. In the past year both Trezor and Ledger have had to issue security updates for their respective hardware wallets, following the discovery of design flaws or implementation issues which allow attackers to access the supposedly locked-away private keys or fool the companion software into accepting a fake device as genuine.

Even with these issues, however, a hardware wallet is considerably more secure than a software-based hot wallet – and as the companies developing them improve both the software and hardware, this security advantage is only going to get larger.

Features:

Exclusive: Lawyer behind first crypto stock buy predicts global economic shift

The only remaining issue, then: price. Simpler and cheaper hardware wallets, like the Ledger HW.1, have largely been phased out in favour of more complicated and secure devices with on-board displays, buttons, and in some cases even wireless connectivity. Buyers can expect to pay anything up to £100 for a current-generation Trezor or Ledger hardware wallet, which given its status as a single-purpose device seems steep – but for anyone with more than a fraction of a Bitcoin to protect, the peace of mind it affords could be worth many times the asking price.

Main image: BigStock

14th June 2018
Litecoin suffers from Coinrail hack, but the bulls bite back

12th June 2018
Investigating the problems with ICO tracking websites

25th May 2018
'Inevitable' mainstream exchanges will follow LMAX Digital to offer crypto trading

24th May 2018
Hardware wallets: paper or plastic? A starter guide

22nd May 2018

Sign up to our newsletter

Email address [Go]

About
Team
Advertise
Contact

Home
News
Blockchain
ICOs
Crypto
Markets
Legal & Regulation
Research