The Trezor Model T is the next generation of Trezor device, improving on the original Trezor Model One. The Model T is an advanced hardware wallet that allows its user to safely store sensitive data, such as cryptographic keys used in authentication. Created to protect owners of Bitcoin and other cryptocurrencies, Trezor devices make it easier to manage your portfolio while greatly reducing the risk of losing coins to many common attacks, including malware and phishing.

How does the Trezor Model T work?

The Trezor Model T is a touchscreen device that holds your cryptocurrency private keys, encrypted in its flash memory. The device has no onboard power source and draws its power via the USB-C port when it is connected to a computer or phone.

To access cryptocurrency stored at a certain address you own, connect your Trezor and use the Trezor Suite interface to enter the details of a transaction. Your Trezor makes you physically confirm details about the transaction directly on its touchscreen, protecting you from common threats like keyloggers, malware or other forms of spyware.

When you are ready to send a transaction, it will show you exactly what transaction you are confirming and let you see if someone has tried to manipulate the data in any way. The private key will only be used to sign a valid transaction that has been repeatedly verified by the user and will never be exposed to the internet, with the whole signing process taking place on the device's dedicated chip.

Security processes and benefits

All the core technologies that make up the Model T are open source, including its physical hardware. This allows for anyone to test and verify the code and components, allowing the Trezor to constantly react to new threats and upgrade its security.

The benefits of this process of constant community security audits is logged in detail on the Trezor security landing page, where you can browse the many bounties we have rewarded to pentesters and researchers who have responsibly disclosed security issues and helped propose a fix.

More about security and bounties

What does a hardware wallet do?

The essential function of a hardware wallet is that it keeps your private key isolated from the internet at all times, even when signing a transaction. The Trezor Model T does this transparently with open-source code and hardware, so everyone can verify that their keys are safe on the device. The Trezor Model T supports over 1600 coins and tokens.

To improve usability and privacy, the Model T has many other features. These include support for new authentication standards like FIDO2, a unique PIN entry keypad, and a Micro SD card slot which adds a second level of protection when accessing the device. The most notable feature is Shamir backup, a way of splitting your recovery seed into multiple shares, a new standard not yet available on any other wallet.

Protection from Online Attacks

Trezor hardware wallets are designed to accept only a limited number of external commands. This means that it is only capable of performing a number of functions, and always requires the user's input to do so. When sending a transaction, for example, the device will be given the destination address, transfer value, and any associated fees. It will only show the correct information used for the transaction to the user, so it is plain to see if the destination address appearing on their computer has been switched or in any way manipulated.

Protection from Physical attacks

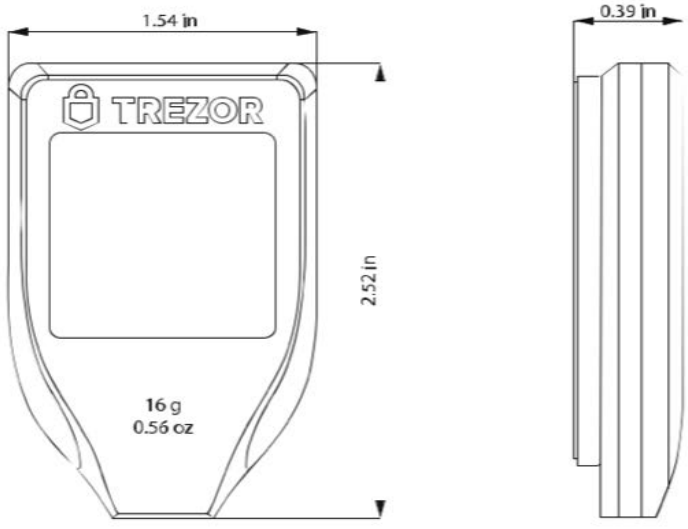
Should an attacker get their hands on your device, two protective mechanisms are in place to prevent access to your funds. Both these features can be disabled but are highly recommended.

Firstly, using a PIN to unlock the device is recommended, which stops anyone from using the device. Trezor's unique, randomized PIN entry layouts make it more difficult for anyone to observe you enter it.

Secondly, the device is protected from more advanced attacks directed at the chip itself, by a passphrase which encrypts the private seed data. Unlike the PIN, your Passphrase is not stored anywhere on the device and not vulnerable to extraction. As an extra benefit, entering the wrong passphrase will simply create an empty account, which could be used as a decoy when needed.

What features does the Trezor Model T have that the Model One doesn't?

Feature	Model One	Model T
Bitcoin-only firmware	Yes	Yes
Shamir backup	No	Yes
Password Manager	Yes	Yes
U2F authentication	Yes	Yes
FIDO2 authentication	No	Yes
Encryption via GPG	No	Yes
SSH	Yes	Yes
Data & file encryption	No	Comming soon
microSD card	No	Yes



Shamir backup

The most common way to recover a Bitcoin wallet is to use the BIP-39 mnemonic recovery seed standard, developed by SatoshiLabs founders Marek “Slush” Palatinus and Pavol “Stick” Rusnak with the help of the Bitcoin community. This is a list of words that can be deciphered to produce the very long random number that represents your Bitcoin keys. This standard for recovery seeds is easy and practical but leaves a single point of failure. Shamir backup, or SLIP-39, is an improvemen to the recovery seed that derives multiple lists of words, which can be combined to provide the seed. This means that exposing one list, known as a share, would not result in your keys being found and your funds stolen. You can also lose a share and still have access to your funds. This makes Shamir safer and more reliable than a standard physical backup of your recovery seed.

USB-C

This simple upgrade keeps your Trezor Model T forward-compatible. The device has no onboard power source, rather drawing power directly over USB from the computer it is plugged in to. Its high-quality connector ensures firm contact that prevents the deice from unplugging when in use.

Touchscreen

The Trezor Model T features a full-color touchscreen that makes it easier and more secure to use the device. It enables a number of features that let you manage all sensitive operations directly on the device, meaning you are kept safe from keyloggers, screen recorders, and other malware that can target your peripheral inputs or clipboard items.

U2F, 2FA and FIDO2 authentication

The Trezor Model T is also easy to use as a security token, for holding and authenticating FIDO U2F and 2FA keys, taking users through a clear step-by-step process that ensures no accidental transactions occur. As the only touchscreen device that works with FIDO2, users are shown exactly what account credentials are being requested and used on any FIDO2-supporting platforms.

More about features

Where are Trezor hardware wallets sold?

The Model T is available directly from the Trezor shop, as well as Amazon and through X trusted resellers.

Are there accessories for the Model T?

Yes, Trezor sells a range of accessories for the Model T. Premium silicone cases that offer protection from scratches and impact are available in a range of colors. Trezor lanyards, which can be fixed to the silicone cases to keep your Trezor on you wherever you need it, are also for sale, as are a range of charging cables, and third-party accessories to backup your recovery seed, such as Cryptosteel capsules.