СЪХРАНЕНИЕ НА БИТКОЙН. ВИДОВЕ ПОРТФЕЙЛИ. ОСНОВНИ ПОЗНАНИЯ

Съхранението на Биткойн изисква разбиране на няколко важни концепции, които гарантират, че активите ще бъдат в безопасност. Важно е да разберете как работят Биткойн портфейлите и как да ги използвате правилно, за да защитите средствата си. Тук ще разгледаме подробно тези елементи.

1. Какво е Биткойн портфейл?

Биткойн портфейлът не съхранява действителните биткойни, а частния ключ ("паролата"), който дава достъп до тях. Биткойн активите съществуват в блокчейна — децентрализирана публична книга, която записва всички транзакции. Биткойн портфейлът управлява частния и публичния ключ, което позволява да се извършват транзакции и да се следи баланса.

1.1. Частен ключ

Частният ключ е много важен, тъй като дава пълен контрол върху Вашите биткойни. Той е нещо като парола – само този, който притежава частния ключ, може да подпише транзакция и да изпрати биткойни на друг адрес. Ако някой друг получи достъп до частния Ви ключ, той може да прехвърли всичките ви средства.

1.2. Публичен ключ и Биткойн адрес

От частния ключ се генерира публичен ключ, а от него се създава Биткойн адрес. Биткойн адресът е този, който споделяте с други хора, за да получавате биткойни. Можете да мислите за него като за банков IBAN.

2. Горещи и студени портфейли

Има два основни типа портфейли:

- **Горещи портфейли**: Те са свързани с интернет и са удобни за ежедневни транзакции, но са по-малко сигурни.

- **Студени портфейли**: Те не са свързани с интернет, което ги прави изключително сигурни за дългосрочно съхранение. Хардуерните портфейли са най-добрият пример за студени портфейли.

3. Хардуерни портфейли: сигурно съхранение

Хардуерните портфейли като **Ledger**, **BitBox02**, **Jade**, **ColdCard** и **Trezor** (като съществуват и много други), са малки физически устройства, които съхраняват Вашия частен ключ офлайн. Те са защитени срещу хакери, защото никога не свързват частния ключ с интернет.

Примери за популярни хардуерни портфейли:

1. Ledger

Плюсове:

- **Висока сигурност:** Частният ключ никога не напуска устройството.
- **Мобилна съвместимост:** Nano X и по-високите модели поддържат Bluetooth за лесна работа с мобилни устройства.
- **Лесен за използване интерфейс:** Подходящ за начинаещи потребители.
- **Защитен чип (*Secure element):** Притежава защитен чип, което придава допълнителна сигурност.
- **Разнообразие от модели:** Предлагат няколко модела на различни цени.

Минуси:

- **Bluetooth свързаността** (при някои от моделите) може да създаде притеснения относно сигурността за по-параноични потребители.
- **Затворен код** за някои компоненти, което може да бъде проблем за някои потребители, защото трябва доверие на сляпо.

---

2. BitBox02

Плюсове:

- **Отворен код:** Всички компоненти са с отворен код, което дава повече доверие в сигурността.
- **Много лесен за употреба:** Има интуитивен интерфейс и лесна настройка, особено за начинаещи.
- **Швейцарска сигурност:** Частният ключ никога не напуска устройството.
- **Защитен чип (*Secure element):** Притежава защитен чип, което придава допълнителна сигурност.

Минуси:

- **По-висока цена:** Малко по-висока цена от някои конкуренти.
- **Без дистанционна свързаност:** Няма Bluetooth свързаност за по-лесна работа, но някои потребители го намират за плюс от гледна точка на сигурност.

---

3. Jade

Плюсове:

- **Отворен код:** Създаден от Blockstream, което гарантира доверие и прозрачност.
- **Батерия:** Има вградена батерия и може да се използва без физическа връзка.
- **Много видове свързаност:** Поддържа работа с мобилни устройства чрез QR кодове (air-gapped), Bluetooth, Type-C.
- **Виртуален защитен чип (Virtual *Secure element):** Притежава виртуален защитен чип, което придава допълнителна сигурност.
- **По-ниска цена:** Малко по-ниска цена от някои конкуренти.

---

4. ColdCard

Плюсове:

- **Изключително висока сигурност:** Ориентиран изцяло към Биткойн потребителите с много защитни функции.
- **Възможност за работа напълно офлайн:** Може да подписва транзакции офлайн чрез microSD карта.
- **Отворен код:** Прозрачен код, който може да бъде проверен от потребители.
- **Защитен чип (*Secure element):** Притежава защитен чип, което придава допълнителна сигурност.

Минуси:

- **Сложен интерфейс:** Не е подходящ за начинаещи потребители; може да изисква напреднали технически познания.
- **По-висока цена:** Малко по-висока цена от някои конкуренти.

---

5. Trezor

Плюсове:

- **Отворен код:** Trezor има напълно прозрачен код, което дава високо ниво на доверие.
- **Цветен екран (Model T):** Позволява по-лесно въвеждане на PIN и работа с устройства.
- **Разнообразие от модели:** Предлагат няколко модела на различни цени.
- **Защитен чип (*Secure element) на новите модели:** Новите модели, като Safe3 и Safe 5 притежава защитен чип, което придава допълнителна сигурност.
- **Разнообразие от модели:** Предлагат няколко модела на различни цени.

Минуси:

- **Без защитен чип (*Secure element) на старите модели:** По-старите модули, като Model T и Model One, нямат защитен чип (*Secure element), което намаля сигурността.

***** Secure Element е специализиран хардуерен чип, който съхранява частните ключове изолирано и ги предпазва от хакерски атаки. Той осигурява допълнителен слой на защита, като не позволява на зловреден софтуер или физически атаки да компрометират ключовете.

4. Seed фраза и passphrase (25-та дума)

При създаването на хардуерен портфейл ще Ви бъде генерирана **seed фраза**, която обикновено се състои от 12 или 24 думи. Това са реални думи на английски език, целия списък може да видите тук. Тази фраза представлява резервно копие на Вашия частен ключ. Ако загубите устройството си, можете да възстановите достъпа до Вашите средства **само** чрез seed фразата на друго устройство. Затова е изключително важно да съхранявате тази фраза на сигурно място и **никога** да не я споделяте с никого.

Какво е passphrase?

Passphrase (или 25-та дума) е допълнителен слой на защита, който може да добавите към Вашата seed фраза. Дори ако някой получи достъп до Вашите 24 думи, без passphrase той няма да може да достъпи средствата Ви. Passphrase е уникална дума или фраза, която Вие създавате (може да включва всичко) и само Вие знаете. Препоръчва се за хора, които искат максимална сигурност.

5. Къде всъщност са биткойните Ви?

Важно е да разберете, че **биткойните Ви не се съхраняват физически в портфейла или на устройството**. Те винаги се намират на блокчейна. Това, което съхранявате в портфейла си е

частния ключ, който Ви дава достъп до биткойните Ви на блокчейна. По този начин можете да прехвърляте тези средства. Вашето устройство само съхранява достъпа до тези активи. Това означава, че ако изгубите/изхвърлите устройството или решите да използвате друго, просто трябва да въведете своята seed фраза.

6. Резервни копия и защита

След като получите своята seed фраза, трябва да я съхранявате офлайн. **Никога не я записвайте в дигитален формат**, като например на компютъра си или в облачни услуги. **Никога не я снимайте!** Най-добре е да запишете фразата на хартия и/или метал, и да я съхранявате на поне 2 или повече сигурни места/локации.

Допълнителни съвети за сигурност:

- **Използвайте метален защитен носител** за вашата seed фраза, за да я предпазите от пожар или други физически щети.
- **Активирайте 2-факторно удостоверяване** (2FA) за всичките си акаунти, свързани с криптовалути като борси и горещи портфейли.
- **Регулярно актуализирайте софтуера** на своя хардуерен портфейл.
- **Seed фразата се въвежда само и единствено на хардуерния портфейл,** за да отключи средствата. Никога на телефон или компютър. **Никой никога няма причина да Ви иска 24-те думи.** Ако получите имейл от фирмата производител на Вашия или който и да било хардуерен портфейл/борса, в който се казва, че средствата Ви са под заплаха и единственият начин да ги спасите е да пратите seed фразата, то това е **ИЗМАМА! НЕ ГО ПРАВЕТЕ!**
- **Отнасяйте се сериозно към съхранението**, защото объркате ли, тук няма съпорт, на който да се обадите, както в банка. За да притежавате наистина своя Биткойн, трябва да сте образовани и внимателни.

7. Как да изпращате и получавате Биткойн?

- **За да получите Биткойн**, трябва да споделите своя Биткойн адрес с изпращача. Той ще изпрати средствата към този адрес.

- **За да изпратите Биткойн**, трябва да използвате своя частен ключ, за да подпишете транзакцията. Хардуерните портфейли ще Ви помогнат да направите това сигурно, като защитят частния Ви ключ.

Заключение

За да съхранявате Биткойн сигурно, е важно да използвате хардуерни портфейли и да пазите частните си ключове безопасно **офлайн**. Seed фразата е Вашето резервно копие, а passphrase добавя още един слой защита. Вашите биткойни са на блокчейна, а портфейлът Ви е ключът към тях.