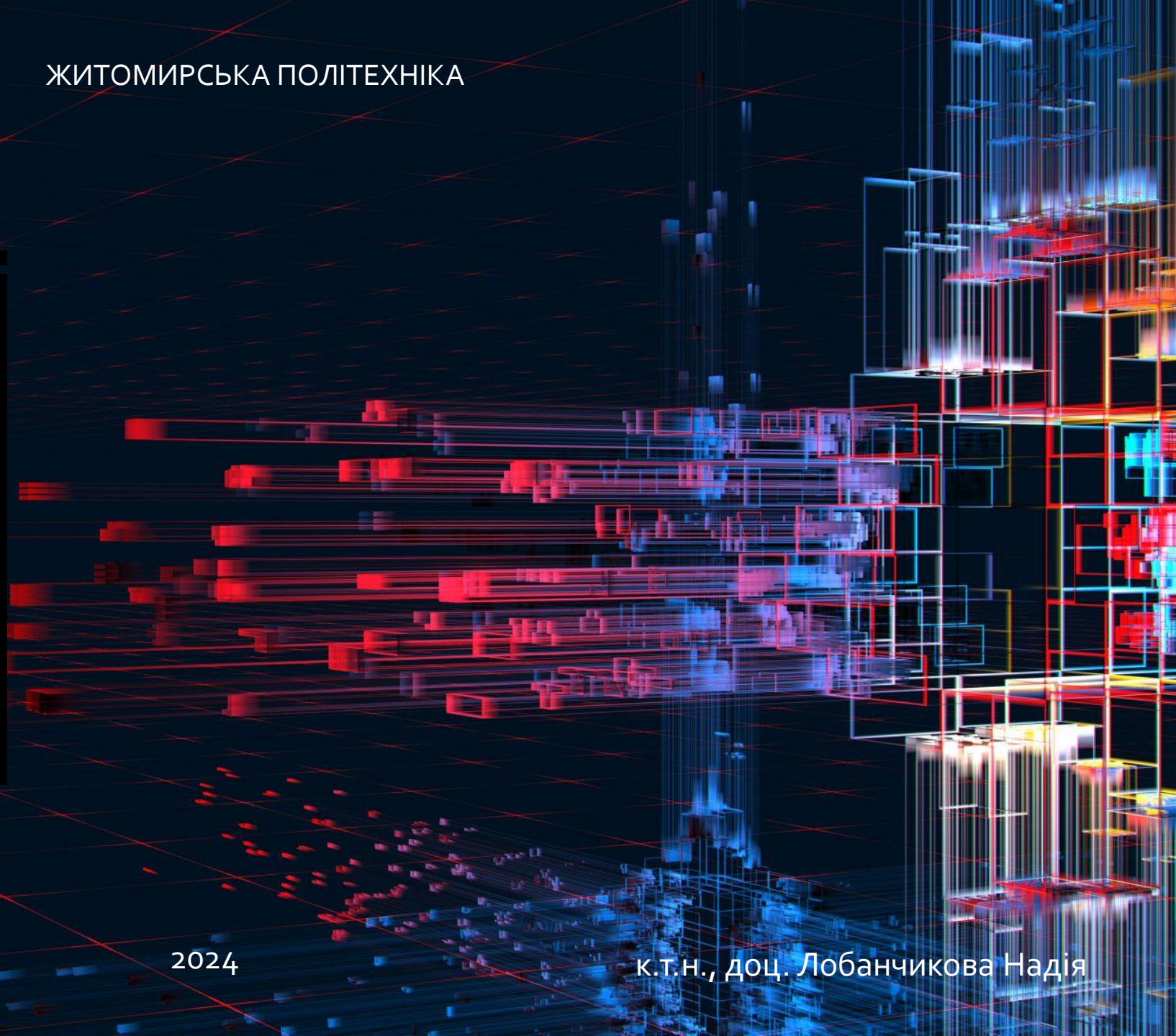
ЖИТОМИРСЬКА ПОЛІТЕХНІКА

ЛЕКЦІЯ 4

ЗБЕРІГАННЯ ТА ВИКОРИСТАННЯ КРИПТОВАЛЮТ



2024

к.т.н., доц. Лобанчикова Надія

ПЛАН

1. Одноосібне управління
2. Зберігання ключів.
3. Мультипідписи .
4. Сторонні послуги для використання криптовалют
5. Платежі.
6. Огляд гаманців.

1. ОДНООСІБНЕ УПРАВЛІННЯ.

ІДЕНТИФІКАТОРИ БЛОКЧЕЙН

- **Ідентифікатор – це адреса (аналог рахунку у банку).**

«Переведи мені біткойни на таку адресу».

Адреси в текстовому вигляді являють собою перетворені хеші відкритих ключів.

Використовується кодування base58 із 58 різних символів.

- Адреса у текстовому вигляді – перетворення хешів відкритих ключів, використовуючи кодування base58 (123456789ABCDEFGHJKLMNPQRSTUVWXYZ abcdefghijkmnopqrstuvwxyz)- в ній немає схожих символів I (великої) та l(прописна L), O та 0 залишені 1 (одиниця) та o

https://www.dcode.fr/base-58-cipher
(мову можна вибрати)

Таблиця відповідності для **Base58** є

Індекс	База58	Індекс	База58	Індекс	База58	Індекс	База58
0	1	**1**	2	**2**	3	**3**	4
4	5	**5**	6	**6**	7	**7**	8
8	9	**9**	A	**10**	Б	**11**	C
12	Д	**13**	E	**14**	Ф	**15**	Г
16	X	**17**	Дж	**18**	K	**19**	Л
20	M	**21**	H	**22**	П	**23**	Q
24	P	**25**	C	**26**	T	**27**	U
28	B	**29**	B	**30**	X	**31**	Ю
32	З	**33**	a	**34**	b	**35**	в
36	d	**37**	д	**38**	f	**39**	g
40	ч	**41**	i	**42**	j	**43**	k
44	м	**45**	п	**46**	o	**47**	стор
48	q	**49**	r	**50**	c	**51**	t
52	u	**53**	v	**54**	w	**55**	x
56	p	**57**	з				

Приклади адрес:

- ✓ Звичайні (P2PKH), починаються з 1:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

Приклади адрес:

- ✓ Мультипідписи (P2SH), починаються з 3:

32enhmyGVXg2H98qgKwYRQxPFR2apEYLtb

Для зручності оплати використовується QR-код.

Для використання криптовалюти, потрібно знати наступні речі:

- Кількість монет і яких у вас є на рахунку (ця інформація з публічного блокчейну - доступна всім;
- Закриті ключі (для проведення транзакцій) – знаємо тільки ми.

Таким чином питання зберігання і використання зводиться до зберігання та управління закритими ключами, які дозволяють проводити операції з криптовалютами.

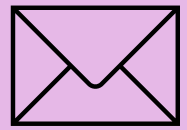
Мета:

- *Доступність: можливість «тратити» свої монети;*
- *Захищеність: ніхто інший не може їх потратити;*
- *Зручність використання.*

1	Bitcoin BTC Buy	$58,217.43	-3.30%	-3.20%	$1,101,910,353,408	$32,894,457,714 563,809 BTC	18,886,675 BTC
2	Ethereum ETH Buy	$4,433.97	-4.42%	-8.44%	$528,346,854,481	$19,383,000,433 4,348,844 ETH	118,541,922 ETH
3	Binance Coin BNB Buy	$622.93	-3.15%	-11.10%	$104,096,589,789	$2,482,944,984 3,978,594 BNB	166,801,148 BNB
4	Tether USDT Buy	$1.00	-0.03%	-0.01%	$73,179,778,582	$74,384,359,482 74,324,861,084 USDT	73,121,243,702 USDT
5	Solana SOL	$206.77	-4.70%	-4.38%	$62,819,593,182	$2,190,304,627 10,605,820 SOL	304,182,948 SOL
6	Cardano ADA	$1.61	-3.15%	-9.22%	$53,904,548,724	$1,905,391,861 1,177,540,505 ADA	33,313,246,915 ADA
7	XRP XRP	$1.00	-4.92%	-3.60%	$47,224,902,863	$2,946,403,977 2,942,290,673 XRP	47,158,974,920 XRP
8	USD Coin USDC	$1.00	-0.06%	-0.00%	$38,565,474,783	$4,529,879,576 4,526,757,649 USDC	38,538,896,021 USDC
9	Polkadot DOT	$36.96	-5.00%	-6.48%	$36,899,687,063	$1,272,184,157 34,048,602 DOT	987,579,315 DOT
10	Dogecoin DOGE	$0.2162	-6.02%	-1.76%	$28,735,015,431	$1,876,184,817 8,639,381,805 DOGE	132,317,865,089 DOGE

2. ЗБЕРІГАННЯ КЛЮЧІВ

Зберігати ключі можна у файлі на комп’ютері чи смартфоні



- Зручність;
- Доступність монет рівна доступності девайсу. Проблема: якщо девайс втрачено→ ключі втрачено → монети пропали
- Надійність зберігання рівна надійності зберігання девайсу. Проблема: девайс скомпрометовано (втрата, вірус) → ключі пропали.

•

Як ми використовуємо звичайні гроші?

У гаманці якась певна сума, інші – у більш надійному місці (сейфі)

Криптовалюта: невелику суму можна «довірити» комп'ютеру або смартфону (додаток «гаманець»), а інші накопичення – в «сейфі»

ГАМАНЦІ

Криптовалютні гаманці — це програми чи засоби, що зберігають публічні та приватні ключі, за допомогою яких можна керувати своїми активами у цифровій валюті та взаємодіяти з блокчейн-мережами.

https://academy.binance.com/uk/articles/custodial-vs-non-custodial-wallets-what-s-the-difference

Криптогаманець насправді не містить криптовалюту, а містить привілейовані облікові дані, необхідні у формі приватних ключів для доступу до блокчейну певної криптовалюти.

Криптогаманці зберігають приватні ключі користувачів та інформацію про те, де в блокчейні розташовані відкриті ключі. Завдяки поєднанню відкритих і закритих ключів криптогаманець може забезпечити захищену операцію для перевірки балансу та надсилання чи отримання транзакцій у криптовалюті.

Криптогаманці

Trezor

Ledger

Холодні гаманці

Використовують фізичний носій для зберігання ключів офлайн

Кастодіальні гаманці

Приватні ключі зберігаються третьою стороною

Некастодіальні гаманці

Тільки власник володіє і контролює приватні ключі

Гарячі гаманці

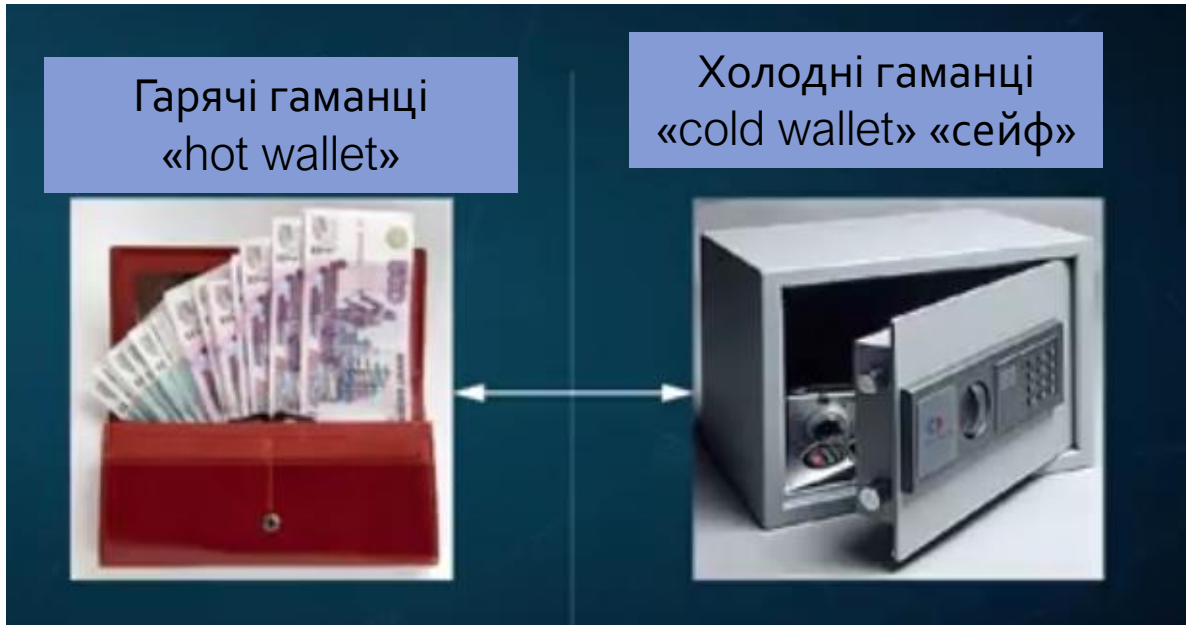
Будь-який гаманець, котрий підключений до інтернету

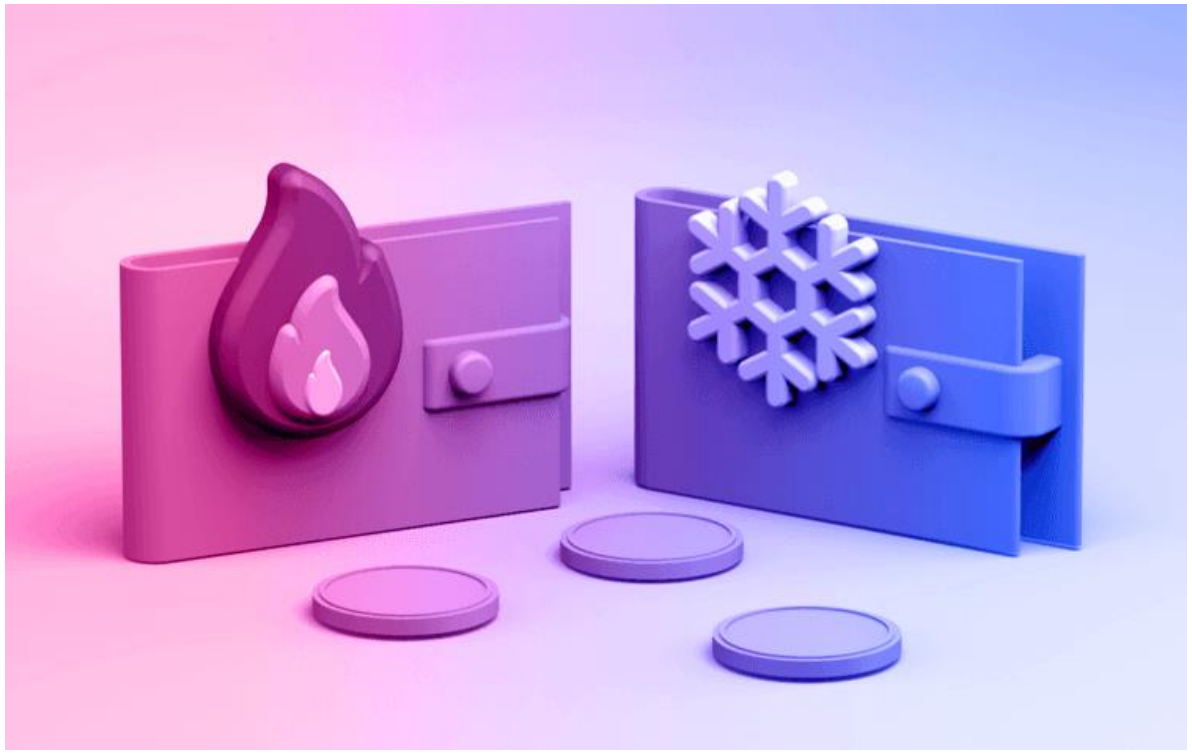
Binance

MetaMask

Гарячі гаманці

Будь-який гаманець, котрий підключений до інтернету





Зручно, але ризиковано

Не зручно, але безпечно

ГАРЯЧІ ТА ХОЛОДНІ СХОВИЩА

- Генеруємо окремо ключі для гарячого та холодного сховищ
- Якщо у гарячому сховищі забагато коштів – переводимо в холодне сховище
- Якщо не вистачає коштів у гарячому гаманці – переводимо один із закритих ключів холодного зберігання в гаманець

https://kosht.media/kryptovaliutni-hamantsi-kliuchova-informatsiia-dlia-pochatkivtsiv/

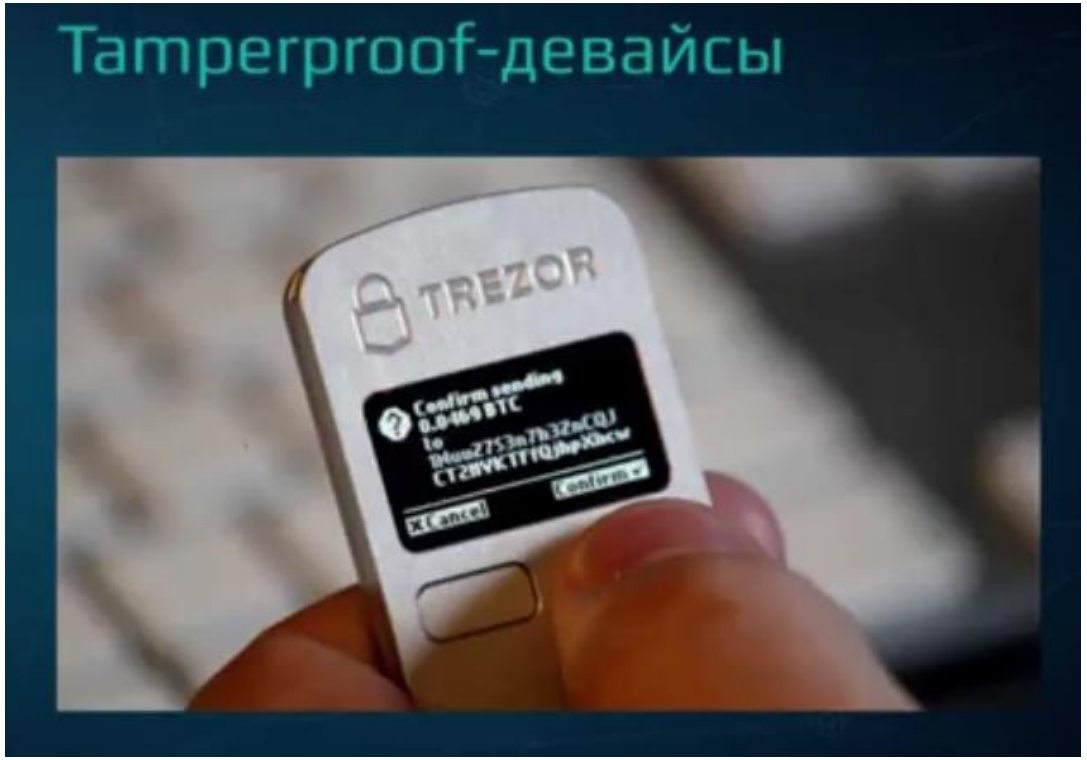
ГАРЯЧІ ТА ХОЛОДНІ СХОВИЩА

- Для генерації ключів не потрібен ні блокчейн ні Інтернет
- Можливо генерувати множину ключів, використовуючи кожного разу випадкове чи (seed), але зберіати потрібно всі ключі.
- Можна згенерувати один раз (seed), і з його допомогою отримати необмежений масив ключів: зберігати достатньо тільки (seed), , у будь-який момент можна дізнатися закритий ключ **Deterministic wallet.**

КЛЮЧІ У ХОЛОДНОМУ СХОВИЩІ

1. Ключі зберігаються на якомусь девайсі.
2. «Brainewallet» – ключі із seed, які пам’ятає користувач (звичайно набір слів).
3. «Paperwallet» – ключі, що розруковані на папері.
4. Tamperproof-девайси – ключі генерує і зберігає девайс, але не розкриває його, тільки підписує ним повідомлення.


Paper wallet
bitcoin
bitcoin PAPER WALLET


Tamperproof-девайсы
TREZOR
Confirm sending
0.0464 BTC
Cancel
Confirm

МУЛЬТИПІДПИСИ

Скриптова мова Біткойна дозволяє створювати такі повідомлення:
«Потратити ці X біткоїнів може той, хто наддасть як мінімум m валідних підписів, що відповідають наступним n відкритим ключам: «ВК1, …ВКn»

Приклад: «Потрати може той, хто наддасть хоча б 2 із 3 підписів до $ВК_{Alice}$, $ВК_{Bob}$, $ВК_{Nick}$»

Можливість розподіленої відповідальності: щоб потратити криптовалюту, що належить компанії, потрібні підписи відразу декількох співробітників (вони не повинні зберігати ключі в одному і тому ж місці

Можливість багатофакторності для одного користувача: один ключ зберігається за допомогою Brain wallet, інший за допомогою Trezor і т.п.

Сторонні сервіси для використання криптовалют

Веб-гаманці

Є хмарними аналогами локальних гаманців, які працюють у бразузері або у додатку:

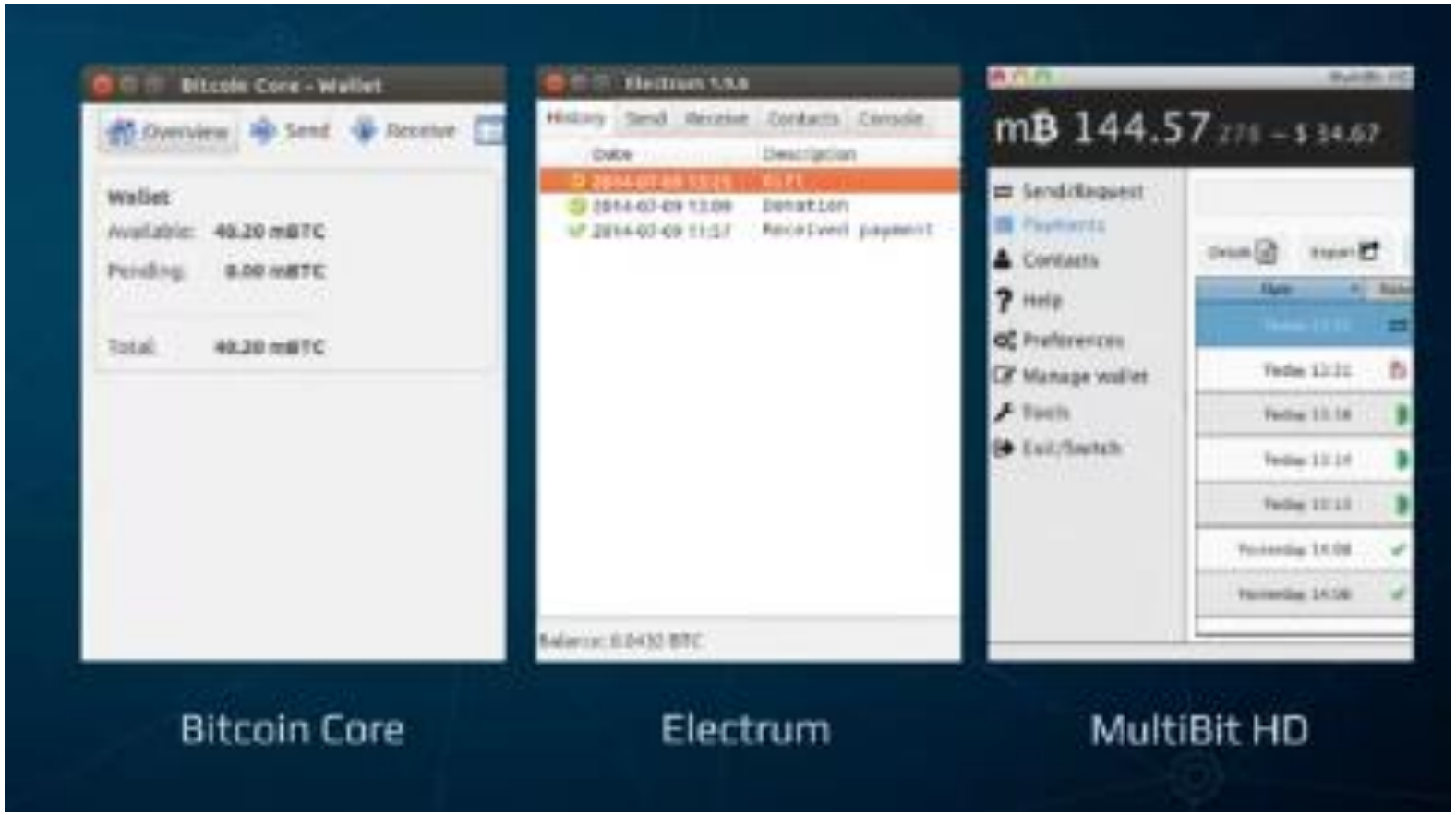
Сервіс зберігає всі ключі у себе (у зашифрованому вигляді

Користувачі отримують доступ до гаманця за допомогою логіна та паролю (ключі зашифровані або основним, або додатковим платіжним паролем)

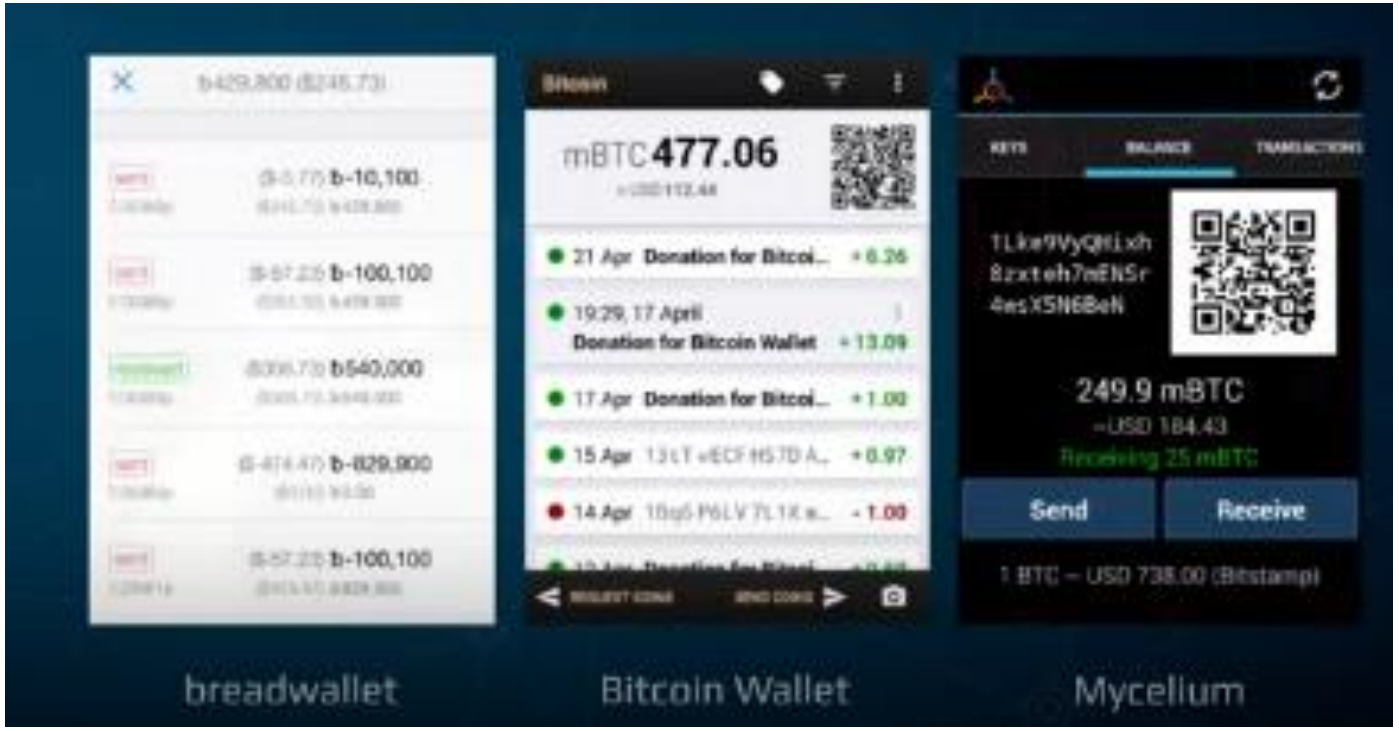
Переваги та недоліки:

- ✓ Зручність: не потрібно нічого встановлювати, працює на багатьох девайсах;
- ✓ Сервісу необхідно частково довіряти (централізація);
- ✓ Проблеми з безпекою (сервіс можуть зламати)

Популярні гаманці - десктоп



Популярні гаманці - смартфони



Популярні гаманці - фізичні

Популярні веб-гаманці

ЯК СТВОРИТИ ГАМАНЕЦЬ?

https://bitcoin.org/ru/

https://vc.ru/crypto/245686-kak-zavesti-bitkoin-koshelek-posobie-dlya-chaynikov-2021

https://play.google.com/store/apps/details?id=de.schildbach.wallet&hl=ru&gl=US

ЩО ТАКЕ КАСТОДІАЛЬНИЙ КРИПТОВАЛЮТНИЙ ГАМАНЕЦЬ?

- Кастодіальний криптовалютний гаманець – це гаманець, в якому приватні ключі зберігаються третьою стороною. Це означає, що третя сторона буде зберігати та керувати вашими приватними ключами від вашого імені. Іншими словами, у вас не буде ні повного контролю над своїми коштами, ні можливості підписувати транзакції.

Ось чому важливо вибрати надійну біржу чи постачальника послуг.

ЩО ТАКЕ НЕКАСТОДІАЛЬНИЙ КРИПТОВАЛЮТНИЙ ГАМАНЕЦЬ?

- Некастодіальний гаманець – це гаманець, в якому тільки власник володіє і контролює приватні ключі. Цей варіант найкраще підходить для користувачів, яким важливо мати повний контроль над своїми коштами. Оскільки посередників немає, ви можете торгувати криптовалютою прямо зі своїх гаманців. Це хороший варіант для досвідчених трейдерів та інвесторів, які знають, як керувати та захищати свої приватні ключі і seed фрази.

Вам знадобиться некастодіальний гаманець для взаємодії з децентралізованою біржею (DEX) або децентралізованим додатком (DApp). Uniswap, SushiSwap, PancakeSwap та QuickSwap – популярні приклади децентралізованих бірж, для яких потрібен некастодіальний гаманець.
Trust Wallet та MetaMask – чудові приклади постачальників некастодіальних гаманців. Але пам'ятайте, що з цими гаманцями ви несете повну відповідальність за збереження вашої seed фрази та приватних ключів.

Кастодіальні гаманці проти некастодіальних гаманців

	Кастодільні сервіси	Некастодільні сервіси
Приватний ключ	Доступний третім особам	Доступний тільки власнику гаманця
Доступність	Зареєстрованим акаунтам	Доступний будь-кому
Вартість транзакцій	Зазвичай висока	Зазвичай низька
Безпека	Зазвичай низька	Зазвичай висока
Підтримка	Зазвичай висока	Зазвичай низька
Вимоги KYC	Так	Ні

Існують різні блокчейн-мережі, які використовують різні типи криптовалют. Ми можемо класифікувати ці типи за їхніми стандартами токенів, але майте на увазі, що у нас можуть бути одні й ті ж токени, що працюють на декількох блокчейнах за різними стандартами. Наприклад, ви можете знайти BNB як токен BEP-20 на BNB Smart Chain, а також як токен BEP-2 на BNB Beacon Chain.

Найбільш поширені стандарти токенів:

- BNB Smart Chain: BEP-20, BEP-721, BEP-1155
- BNB Beacon Chain: BEP-2
- Ethereum: ERC-20, ERC-721, ERC-1155
- Solana: SPL

ОГЛЯД ГАМАНЦІВ: ОГЛЯД ПРОГРАМНИХ ГАМАНЦІВ

Blockchain Wallet

Trust Wallet

Coinbase Wallet

Guarda

Binance

Coinbase PRO

Currency.com

Huobi

ОГЛЯД БІРЖОВИХ ГАМАНЦІВ

ОГЛЯД АПАРАТНИХ ГАМАНЦІВ

Апаратний гаманець — це найбезпечніше місце для зберігання криптовалют, що робить його популярним вибором для тих, хто має більшу кількість криптовалют або для довготривалого зберігання. Якщо ви хочете купити свій перший апаратний гаманець і не знаєте, який вибрати, ця стаття допоможе вам знайти пристрій, що підходить саме вам.

1. CoolWallet – найкращий в цілому
2. Trezor – найкращий рівень безпеки
3. Ledger – підтримує найбільше токенів
4. KeepKey – бюджетний варіант
5. BitBox – найпростіший у використанні

COOLWALLET

CoolWallet займає перше місце серед апаратних гаманців завдяки своїй широкій функціональності. Окрім збереження вашої криптовалюти, гаманець надає торгові функції та можливість під'єднуватися до DeFi та dApps через WalletConnect.
Версія Pro також пропонує стейкінгу та підтримку NFT в додатку, що робить її ідеальним вибором для всіх користувачів криптовалют. Просто завантажте додаток CoolBitX і з’єднайте його зі своїм гаманцем через зашифрований Bluetooth, щоб відстежувати та торгувати криптовалютою, де б ви не були.

Плюси
- 150+ офіційно підтримуваних токенів плюс кастомні токени
- Легкий і портативний
- Зашифроване Bluetooth з’єднання з мобільним додатком
- Функції торгівлі та DeFi
- Підтримка стейкінгу та NFT
- Багатофакторна автентифікація
- Сертифікований EAL 5+ елемент безпеки
- Гарантія на 1 рік

Мінуси
- Немає підтримки через телефон
- Немає підключення USB

Trezor

Trezor надає одні з найбезпечніших автономних сховищ для управління та торгівлі криптовалютою. Він поставляється з апаратною ультразвуковою печаткою, перевіркою мікропрограми та автентифікацією PIN-коду для будь-яких операцій, пов’язаних із ключами. Технологія також перевірена дослідниками безпеки та має надійний процес резервного копіювання та відновлення.

Інтуїтивно зрозумілий інтерфейс призначений для початківців, а досвідчені користувачі можуть використовувати розширені функції, сумісні з багатьма програмами. Існує також експертна служба підтримки клієнтів, до якої можна звернутися по допомогу.

Плюси

•Сумісний з понад 1000 монетами та токенами
•Простий у використанні інтерфейс
•Керуйте монетами, ключами та паролями в одному місці
•Доступ до розширених функцій і програм
•Прозорість безпеки
•Пройшов аудит
•Надійне резервне копіювання та відновлення
•Експертна підтримка клієнтів

Мінуси

•Може бути досить дорогим
•Немає мобільного додатка

Ledger Blue

підтримує найбільше токенів

Плюси
•Підтримка понад 5500 цифрових активів
•Підтримка NFT
•Встановіть до 100 програм
•Купуйте, обмінюйте та ставте активи у стейкінг за допомогою платформи Ledger Live
•Простий у використанні чималий екран
•Коштує менше за багатьох конкурентів
•Сертифікований безпечний чіп
•Є Bluetooth (Nano X)
•Є академія, подкаст і посібники для початківців

Мінуси
•Немає підтримки через телефон
•Батарея не замінна

Якщо у вас є якісь невідомі токени, то Ledger — ідеальне рішення для зберігання. За допомогою платформи Ledger Live ви можете купувати, зберігати та обмінюватися понад 5500 цифрових активів, а також ставити активи у стейкінг та встановлювати до 100 програм.
Простий у навігації гаманець також може зберігати NFT і дозволяє керувати ними, а його сертифікований безпечний чіп захистить від хакерів. Ledger надає комплексні ресурси та вибір пристроїв за дуже прийнятними цінами, тобто щось певно підійде користувачам з будь-яким бюджетом або рівнем досвіду.

Ledger Nano S

KEEPKEY

найкраще підійде на невеликі бюджети

KeepKey є одним з найдешевших апаратних гаманців на ринку для зберігання провідних світових криптовалют. Але низька ціна не означає відсутність безпеки — ви можете створювати та керувати своїми приватними ключами в автономному режимі, а також використовувати PIN-код і додатковий захист пароль-фрази.

Процес резервного копіювання та відновлення простий, як і обмін криптовалют безпосередньо з вашого гаманця. Платформа ShapeShift захищена сервісом KeepKey і забезпечує доступ до всіх необхідних інструментів через дохідливий інтерфейс.

Плюси

- Підтримка 40+ найпопулярніших криптовалют
- Вебінтерфейс для обміну активами
- Великий, чіткий дисплей
- Необмежена кількість адрес гаманців
- Швидкість транзакцій можна налаштувати
- PIN-код і додатковий захист паролем
- Просте резервне копіювання та відновлення
- Доступна ціна

Мінуси

- Підтримує менше криптовалют, ніж конкуренти
- Обмежена місткість для встановлення додатків

BITBOX – НАЙПРОСТІШИЙ ДЛЯ ВИКОРИСТАННЯ

Плюси

- Підтримка 1500+ монет
- Швидке налаштування
- Інтуїтивно зрозумілий інтерфейс
- Чіп безпеки
- Додаток для купівлі та управління криптовалютою
- Відкритий код
- Безпечний мультипідпис
- Легке резервне копіювання та відновлення

Мінуси

- Мобільний додаток доступний лише для Android пристроїв
- Екран трохи маленький

Багато рецензентів високо оцінили дизайн і зручність BitBox, а також його привітність до початківців. Налаштування гаманця займає лише кілька хвилин, а його інтуїтивно зрозумілий інтерфейс та інструкція в додатку полегшують навігацію та забезпечують захист ваших активів.

Приватні ключі зберігаються в автономному режимі для більшої безпеки, а процес резервного копіювання та відновлення простий. Ви можете безпечно купувати свої монети та керувати ними через додаток BitBox, а чіп безпеки захистить ваш пристрій від фізичного втручання.

Дякую за увагу!!!