

Воєнна академія імені Євгенія Березняка

Лисецький Ю.М., Зайцев О.В., Богун А.М.

**ОСНОВИ ВИКОРИСТАННЯ
КРИПТОВАЛЮТ
У ФАХОВІЙ ДІЯЛЬНОСТІ**

Навчальний посібник



Київ – 2023

УДК 004.056:339.72
ББК 32.97:65.58
Л63

*Затверджено до видання
начальником вищого військового навчального закладу*

Автори:

Лисецький Ю.М. – доктор технічних наук;
Зайцев О.В. – кандидат технічних наук, доцент;
Богун А.М.

Рецензенти:

Попов М.О. – доктор технічних наук, професор;
Присяжнюк М.М. – кандидат технічних наук, с.н.с.

Лисецький Ю.М., Зайцев О.В., Богун А.М

Основи використання криптовалют в фаховій діяльності:
навчальний посібник. – Київ : Видавець Бихун В.Ю., 2023. – 132 с.
ISBN 978-617-7699-45-2

У цьому навчальному посібнику предметом обговорення є використання криптовалют в фаховій діяльності. До навчального посібнику увійшли питання теорії та практики використання криптовалют в фаховій діяльності, застосування технологій забезпечення кіберзахисту та кібербезпеки, застосування прикладного програмного забезпечення обміну криптовалютами, забезпечення кіберзахисту автоматизованого робочого місця, застосування прикладного програмного забезпечення для кіберзахисту під час роботи в комп'ютерних мережах та Інтернет.

Навчальний посібник може використовуватися при вивченні дисциплін для підготовки слухачів академій та проведенні курсів підвищення кваліфікації, пов'язаних із забезпеченням інформаційної безпеки, кібербезпеки та кіберзахисту.

УДК 004.056:339.72
ББК 32.97:65.58

ISBN 978-617-7699-45-2 © Лисецький Ю.М., Зайцев О.В., Богун А.М., 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	5
ВСТУП.....	7
РОЗДІЛ 1. ОСНОВИ ВИКОРИСТАННЯ КРИПТОВАЛЮТ.....	8
1.1. Основні терміни та визначення.....	8
1.2. Види криптогаманців.....	19
1.3. Майнінг криптовалют.....	25
1.4. Регулювання ринку криптовалют в Україні.....	33
1.5. Регулювання ринку криптовалют в рф.....	38
1.6. Використання криптовалют з початком збройної агресії рф.....	41
Висновки до розділу 1.....	44
Питання для самоконтролю.....	45
РОЗДІЛ 2. ОСОБЛИВОСТІ ВИКОРИСТАННЯ КРИПТОВАЛЮТ В ФАХОВІЙ ДІЯЛЬНОСТІ.....	46
2.1. Особливості купівлі криптовалют.....	46
2.1.1. Поповнення криптогаманця кредитною картою.....	46
2.1.2. Поповнення криптогаманця через термінали самообслуговування.....	53
2.1.3. Поповнення криптогаманця в криптообміннику.....	55
2.1.4. Купівля криптовалюти іншими способами.....	56
2.2. Здійснення фінансових операцій з використанням криптовалют.....	58
2.2.1. Використання анонімних віртуальних кредитних карт.....	59
2.2.2. Використання криптоміксерів для підвищення анонімності платежів.....	60
2.2.3. Використання безпечних криптогаманців.....	65
2.3. Особливості виведення коштів з криптовалютної системи.....	69
2.3.1. Особливості роботи з криптоактивами в Україні.....	69
2.3.2. Особливості роботи з криптоактивами в рф.....	77
2.3.3. Виведення криптоактивів з території третіх країн.....	84
Висновки до розділу 2.....	90
Питання для самоконтролю.....	91
РОЗДІЛ 3. КІБЕРБЕЗПЕКА ПРИ ВИКОРИСТАННІ КРИПТОВАЛЮТ.....	92
3.1. Поняття псевдонімності криптовалют.....	92
3.2. Безпечні криптовалюты.....	92
3.3. Особливості забезпечення кібербезпеки та анонімності співробітника.....	95
3.4. Особливості використання анонімної ОС Live USB TAILS.....	102
3.5. Особливості використання анонімної віртуальної ОС Whonix.....	104

Висновки до розділу 3.....	108
Питання для самоконтролю.....	109
РОЗДІЛ 4. РОЗСЛІДУВАННЯ ЗЛОЧИНІВ В СФЕРІ	
КРИПТОВАЛЮТ.....	110
4.1. Основні типи злочинів з використанням криптовалют.....	110
4.2. Стан та перспективи розслідувань з використанням криптовалют....	113
4.3. Технології розслідування злочинів з використанням криптовалют....	120
Висновки до розділу 4.....	128
Питання для самоконтролю.....	129
ВИСНОВКИ.....	130
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	131

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AD	– ActiveDirectory
AML	– Anti-Money Laundering (Протидія відмиванню коштів)
API	– Application programming interface
ASIC	– Application-Specific Integrated Circuit
BTC	– абрр. криптовалюти Bitcoin
CLI	– Command Line Interface
CPFP	– Child pays for parent
CPU	– Central Processing Unit
DApps	– Decentralized Application
DeFi	– децентралізовані фінансові послуги
DEX	– децентралізована біржа
ETH	– абрр. криптовалюти Ethereum
FATF	– Financial Action Task Force on Money Laundering
GPG	– GNU Privacy Guard
GPU	– Graphics Processing Unit
ICO	– Initial Coin Offering
KYC	– Know Your Customer
LTC	– абрр. криптовалюти Litecoin
LUKS	– Linux Unified Key Setup
MISA	– Markets in cryptoassets
MFSA	– Malta Financial Services Authority
NFT	– Non-Fungible Token
OTC	– Over-the-Counter
P2P	– Peer-to-peer (англ. від особи до особи)
PoS	– Proof of Stake
PoW	– Proof of Work
RBF	– Replace by fee
SWIFT	– Society for Worldwide Interbank Financial Telecommunications
Tails	– The Amnesic Incognito Live System
TON	– The Open Network
Tor	– The Onion Router
VPN	– Virtual Private Network
БД	– бази даних
ЕПС	– електронні платіжні системи
ЄС	– Європейський Союз
ЗМІ	– засоби масової інформації
КНР	– Китайська Народна Республіка
МВД рф	– Міністерство внутрішніх справ російської федерації
Мінфін	– Міністерство фінансів
Мінцифри	– Міністерств цифрової трансформації України
МОУ	– Міністерство оборони України

НБУ	– Національний банк України
ОАЕ	– Об'єднані Арабські Емірати
ОС	– Операційна система
ПДВ	– податок на додану вартість
ПЗ	– програмне забезпечення
ПК	– персональний комп'ютер
ПФР	– підрозділ фінансової розвідки
РБК	– РосБизнесКонсалтинг
рф	– російська федерація
США	– Сполучені Штати Америки
ФНС	– Федеральна податкова служба
ФОП	– Фізична особа-підприємець
ФСБ рф	– Федеральна служба безпеки російської федерації
ФСКН	– Федеральна служба з контролю за обігом наркотиків
ЦБрф	– Центральний банк російської федерації

ВСТУП

Україна, як багато інших країн, зазнала впливу збройної агресії з боку російської федерації. Цей конфлікт не тільки призвів до геополітичних змін і гуманітарної кризи, але й мав значний вплив на економіку та фінансову систему України. У таких непевних умовах криптовалюти можуть стати важливим інструментом для збереження активів, переказу коштів та забезпечення анонімності.

Цей посібник призначений для тих, хто бажає ознайомитися з використанням криптовалют в Україні в умовах збройної агресії росії. Він надасть корисну інформацію про основні аспекти використання криптовалют, включаючи безпеку, анонімність та ризики.

Посібник охоплює наступні теми:

- вступ до криптовалют: дізнайтеся, що таке криптовалюта, як вона працює і які переваги вона може мати в умовах конфлікту;
- огляд криптовалютних гаманців: досліджуйте різні типи гаманців, які можуть бути використані для зберігання та керування криптовалютами;
- анонімність та приватність: дізнайтеся про технології, що дозволяють забезпечити анонімність та приватність при використанні криптовалют;
- безпека: ознайомтесь з основними принципами безпеки, які слід дотримувати при роботі з криптовалютами, включаючи захист від хакерських атак і крадіжки коштів;
- обмін та виведення коштів: дізнайтеся про різні способи обміну та виведення криптовалют, включаючи криптовалютні біржі та інші платформи.
- регулювання та правовий статус: ознайомтесь з правовим статусом криптовалют в Україні та РФ, питаннями регулювання цього сектора.
- ризики та заходи обережності: дізнайтеся про основні ризики, пов'язані з використанням криптовалют, та прийміть необхідні заходи обережності.

РОЗДІЛ 1

ОСНОВИ ВИКОРИСТАННЯ КРИПТОВАЛЮТ

В розділі наведено основні терміни та визначення щодо криптовалют, визначені основні види криптогаманців, розкрито поняття майнінгу криптовалют, питання щодо регулювання криптовалютного обігу в Україні та російській федерації (рф).

1.1. Основні терміни та визначення

Криптовалюта – засіб платежу, який існує тільки в інтернеті. У неї немає паперового вираження, і її цінність не залежить від держави [1, 2]. У 2009 році з'явилася перша цифрова монета – біткоїн, з тих пір кількість криптовалют зростає [3, 4].

Зазвичай, щоб переказати гроші від однієї людини іншій, потрібен посередник – банк. З криптовалютою по-іншому: в обміні банк не бере участі. Криптовалюта побудована на системі блокчейн – ланцюжку інформаційних блоків. Їх використовують для переведення цифрових грошей від людини до людини без посередника.

Блокчейн – це спосіб зберігання інформації з ланцюга.

Записи про транзакції учасників мережі кодуються, розподіляються між іншими учасниками і формують зв'язані між собою блоки (рис. 1.1).

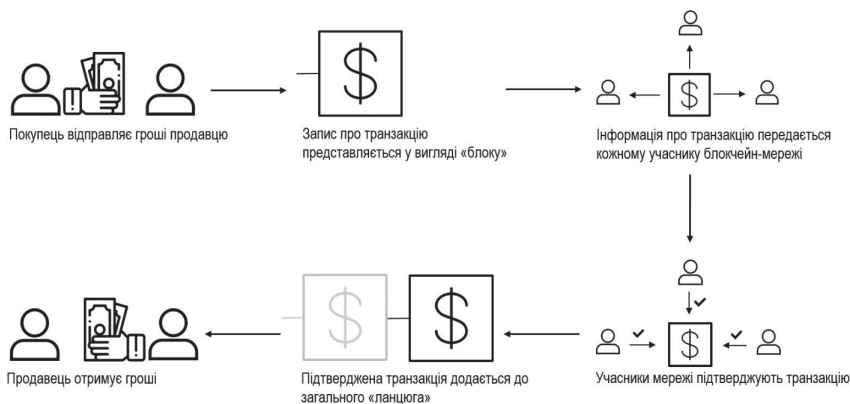


Рисунок – 1.1 Загальний процес криптовалютної транзакції

Якщо хтось спробує внести зміни, щоб отримати валюту нечесним способом, наприклад, переписати існуючу транзакцію або створити нову без згоди інших учасників, система порівняє цю інформацію з іншими

базами даних (БД) і заблокує операцію. Це ніби своя філія банку на вашому комп'ютері.

Щоб вийшло провести транзакції, потрібно підтримувати мережу в робочому стані – це роблять *майнери*. Вони віддають системі свої обчислювальні потужності, щоб виробляти нові блоки і монети, і отримують відсоток від операцій (рис. 1.2).



Рисунок – 1.2 Вигляд криптоферми для майнінгу

Автор блокчейна сам визначає, скільки ресурсів повинен надати майнер, щоб отримати нагороду. Усі учасники випуску криптовалюти наділені рівними правами та можливостями. Розробники закладають у систему обмеження на емісію криптовалюти – наприклад, біткоїн можна зробити лише 21 млн.

Майнінг. Створення нового блоку мережі, за який нараховується винагорода. Для цього треба надати системі свої обчислювальні потужності. Якщо на початку появи криптовалют майнути можна було зі звичайного персонального комп'ютера (ПК), то тепер рівень мережі ускладнився. З'явилися спеціальні пристрої – майнінгові ферми. Окремі користувачі об'єднують потужності своїх комп'ютерів і створюють об'єднання майнерів.

Стейкінг. Якщо дохід в майнінгу залежить від потужності техніки, то в стейкінгу – від кількості вже наявних монет криптовалюти. Це своєрідна інвестиція: власник відправляє коїни на обслуговування блокчейна і отримує за це винагороду.

Види криптовалют. Є три види криптовалют: децентралізовані, псевдодецентралізовані, стейблкоїни [5, 6].

Децентралізовані. Це криптовалюти, які видобуваються майнінгом, наприклад: Bitcoin, Ethereum, Zilliqa, Elastos, IOTA [7].

Псевдодецентралізовані. Випуск та обіг таких валют контролює замкнута група людей, вона ж може приймати рішення про блокування рахунків власників. При цьому видобути електронні гроші за допомогою майнінгу не можна – псевдодецентралізовану валюту купують. До таких криптовалют відносяться Bitcoin Cash, Ripple, TRON, EOS (рис. 1.3).

All

Currencies

Assets

USD

← Back to Top 100

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	 Bitcoin	BTC	\$73,079,806,875	\$4417.50	16,543,250	\$2,337,670,000	1.97%	-3.64%	2.85%
2	 Ethereum	ETH	\$29,601,821,904	\$313.51	94,421,867	\$1,175,620,000	1.07%	-9.34%	-8.36%
3	 Bitcoin Cash	BCH	\$9,315,818,255	\$562.56	16,559,600	\$391,960,000	1.06%	-2.87%	-7.22%
4	 Ripple	XRP	\$8,140,320,944	\$0.212298	38,343,841,883 *	\$187,679,000	0.36%	-5.91%	6.31%
5	 Litecoin	LTC	\$3,679,325,403	\$69.72	52,775,532	\$722,029,000	1.20%	-10.27%	12.55%
6	 NEM	XEM	\$2,600,712,000	\$0.288968	8,999,999,999 *	\$7,983,600	1.56%	-5.63%	2.85%
7	 Dash	DASH	\$2,511,268,909	\$333.19	7,537,002	\$32,148,000	1.01%	-6.11%	-6.98%
8	 IOTA	MIOTA	\$1,774,126,928	\$0.638283	2,779,530,283 *	\$22,900,400	-1.62%	-13.03%	-27.13%
9	 Monero	XMR	\$1,744,495,028	\$116.04	15,033,825	\$93,785,800	2.21%	-6.68%	-17.72%
10	 Ethereum Classic	ETC	\$1,621,112,372	\$17.03	95,185,418	\$228,043,000	1.14%	-10.33%	7.73%

Рисунок – 1.3 Найпопулярніші валюти світу

Нижче наведено характеристики декількох найпоширеніших криптовалют:

Bitcoin (BTC) – перша і найбільш відома криптовалюта, яка була запущена у 2009 році і працює на основі технології блокчейн. Bitcoin використовує механізм доказу роботи (Proof of Work) для підтвердження транзакцій. Він визначається як цифрове зберігання вартості і може використовуватися для проведення платежів.

Ethereum (ETH) – друга за розміром криптовалюта після Bitcoin, яка також працює на основі технології блокчейн, але має більш широкі можливості. Ethereum є платформою для розробки і виконання смарт-контрактів, що дозволяє створювати децентралізовані додатки (DApps) і виконувати комплексні операції.

Ripple (XRP) – криптовалюта та платіжна мережа, яка спрямована на забезпечення швидких та недорогих міжнародних грошових переказів. Відмінністю Ripple є його протокол консенсусу, який використовується для підтвердження транзакцій – XRP Ledger Consensus Protocol. Ripple також співпрацює з банками та фінансовими установами.

Litecoin (LTC) – криптовалюта, яка була створена як «легкі» варіант Bitcoin. Вона працює на тій самій основі, але має деякі технічні вдосконалення, такі як швидкіші часи блоків і інші покращення в екосистемі.

Bitcoin Cash (BCH) – виник як результат хардфорка Bitcoin. Він має більшу блокову ємність, що дозволяє проводити більше транзакцій за один блок. Bitcoin Cash зосереджений на поліпшенні масштабованості та зробленні Bitcoin більш придатним для повсякденних платежів.

Cardano (ADA) – блокчейн-платформа, яка ставить перед собою мету забезпечити безпеку, стійкість і масштабованість. Вона розвивається на основі наукових досліджень і використовує принципи доказу долі (Proof of Stake).

Polkadot (DOT) – блокчейн-платформа, яка має на меті забезпечити інтероперабельність між різними блокчейнами. Вона дозволяє різним блокчейнам обмінюватися даними та взаємодіяти між собою.

Binance Coin (BNB) – криптовалюта, що використовується в екосистемі Binance – одній з найбільших криптобірж у світі для зниження комісій на біржі, участі в ініціативах платформи та інших функцій.

Chainlink (LINK) – блокчейн-платформа, яка дозволяє підключати зовнішні дані (оракули) до блокчейнів і отримувати доступ до реальних даних з позачергових джерел розумним контрактам.

Stellar (XLM) – є відкритою блокчейн-платформою, спрямованою на швидкі та недорогі грошові перекази. Вона також підтримує емісію tokenів і створення власних цифрових активів.

EOS (EOS) – блокчейн-платформа, яка надає інфраструктуру для розробки децентралізованих додатків (DApps). Вона пропонує гнучкість та масштабованість для розгортання рішень на блокчейні.

Tezos (XTZ) – саморозвиваючийся блокчейн, який використовує механізм голосування, щоб приймати рішення щодо змін у протоколі. Вона також підтримує розумні контракти та може використовуватися для розробки DApps.

TRON (TRX) – блокчейн-платформа, яка спрямована на розвиток глобальної децентралізованої інтернет-екосистеми. Вона має на меті створити децентралізовану платформу для контенту, де користувачі можуть взаємодіяти без посередників.

VeChain (VET) – блокчейн-платформа, спеціалізована на відстеженні походження та логістиці товарів. Вона забезпечує прозорість і довіру у постачальному ланцюзі шляхом використання технології блокчейн.

Цифрову валюту ділять на коїни та токени:

Коїн – грошова одиниця криптовалюти, яка працює у власному блокчейні. Її можна видобути за допомогою майнінгу – надання системі обчислювальних потужностей свого комп'ютера. Коїни можна переводити іншим користувачам системи блокчейн і продавати за звичайну валюту. Деякі компанії приймають їх як оплату товарів і послуг. Наприклад, Microsoft продає за біткоіни операційну систему Windows та ігрову приставку Xbox. Є коїни, які працюють на переписаному блокчейні біткоіну. Їх називають *альткоїнами* – альтернативними версіями біткоіну.

Це загальна інструкція, і конкретні кроки можуть варіюватися в залежності від криптовалюти та гаманця.

Ось загальна інструкція щодо використання криптовалюти:

1) Отримайте гаманець: Завантажте криптогаманець, який підтримує відповідний коїн. Це може бути офіційний гаманець від розробників коїна або сторонній гаманець, який підтримує цей коїн.

2) Створіть гаманець: Створіть новий гаманець у вашому криптогаманці. Це може включати створення нової адреси гаманця та отримання приватного ключа.

3) Отримайте коїни: Якщо ви купуєте коїни на криптобіржі, зареєструйтеся на біржі та придбайте коїни за допомогою криптовалюти, такої як Bitcoin або Ethereum. Якщо вам коїни відправляють іншою особою, надайте їй вашу адресу гаманця для отримання коїнів.

4) Зберігайте приватний ключ в безпеці: Приватний ключ є важливим для доступу до вашого гаманця та контролю над коїнами. Зберігайте його в безпечному місці, наприклад, на апаратному гаманці або за допомогою пароля.

5) Використовуйте коїни: Використовуйте ваші коїни для запланованих функцій або послуг, які вони надають. Це може включати оплату товарів або послуг, переказ коїнів іншим особам або участь в блокчейн-платформах.

6) Безпека: Забезпечуйте безпеку вашого гаманця і приватного ключа. Уникайте небезпечних посилань, небезпечного програмного забезпечення або нещасних випадків втрати ключа.

Токен – грошова одиниця криптовалюти створюється на основі вже існуючого блокчейна. Їх не можна видобути, але можна купити або отримати за активність. Токенами навіть у теорії не можна розплатитися, їх використовують, щоб дати користувачеві доступ до функцій платформи. Якщо коїн – це купюра, то токен – квиток. Але якщо вивести токен на біржу, його можна обміняти на звичайні гроші за поточним курсом. Токени можна використовувати як інструмент для інвестицій та свідоцтво права на бізнес, за допомогою яких можна брати участь у голосуваннях чи опитуваннях.

Для зберігання коїнів або токенів потрібен електронний гаманець. Наповнити гаманець криптовалютою можна кількома способами. Токени

можна купити на біржі, в онлайн-обміннику або безпосередньо в компанії, яка пропонує частину прибутку з компанії токена. Їх купують як за звичайні гроші, так і за криптовалюту. У токенів більше можливостей, але серед інвесторів більше цінуються коїни: їх важче створити.

Це загальна інструкція, і конкретні кроки можуть варіюватися в залежності від токена та його гаманця.

Ось стисла інструкція щодо використання токена криптовалюти:

1) Отримайте гаманець: Завантажте криптогаманець, який підтримує відповідний токен. Це може бути офіційний гаманець від розробників токена або сторонній гаманець, який підтримує цей токен.

2) Створіть гаманець: Створіть новий гаманець у вашому криптогаманці. Це може включати створення нової адреси гаманця та отримання приватного ключа.

3) Отримайте токен: Якщо ви купуєте токен на криптобіржі, зареєструйтеся на біржі та придбайте токен за допомогою криптовалюти, такої як Bitcoin або Ethereum. Якщо вам токен відправляють іншою особою, надайте їй вашу адресу гаманця для отримання токена.

4) Зберігайте приватний ключ в безпеці: Приватний ключ є важливим для доступу до вашого токена. Зберігайте його в безпечному місці, наприклад, на апаратному гаманці або за допомогою пароля.

5) Використовуйте токен: Використовуйте ваш токен для запланованих функцій або послуг, які він надає. Це може включати оплату товарів або послуг, участь в голосуванні або доступ до платформи, що підтримує токен.

6) Безпека: Забезпечуйте безпеку вашого гаманця і приватного ключа. Уникайте небезпечних посилань, небезпечного програмного забезпечення або нещасних випадків втрачати ключа.

Стейблкоїн – валюти вартість якої прив'язана до будь-якої цінності, рідше – до іншої криптовалюти, тому її ціна змінюється частіше, ніж у інших валют. Наприклад, Gemini Dollar дорівнює долару США, а DigixDAO – граму золота.

Стейблкоїни, випуск яких забезпечується національними грошима, повністю централізовані. Наприклад, компанія Tether Limited випустила криптовалюту Tether, яка на 20% забезпечується запасами доларів США з рахунків організації. А Gemini Dollar забезпечений повністю. Його контролює Департамент фінансових послуг штату Нью-Йорк. З цим пов'язані ризики використання криптовалюти.

Далі наведений список поширених стейблкоїнів:

Tether (USDT) – найбільш популярний стейблкоїн, прив'язаний до долара США в співвідношенні 1:1 і використовується для стабілізації ціни в криптовалютному просторі;

USD Coin (USDC) – інший популярний стейблкоїн, який також прив'язаний до долара США, ініційований криптовалютної компанії Circle і компанії Coinbase;

Binance USD (BUSD) – стейблкоїн, розроблений популярною криптобіржею Binance, також прив'язаний до долара США і має широке застосування на платформі Binance;

Dai (DAI) – стейблкоїн, який працює на базі блокчейну Ethereum, прив'язаний до долара США, але використовує децентралізовану систему управління стабільності, що робить його незалежним від централізованих установ;

TrueUSD (TUSD) – стейблкоїн, розроблений компанією TrustToken, прив'язаний до долара США і має сертифікований резерв для підтвердження його стабільності;

Paxos Standard (PAX) – стейблкоїн прив'язаний до долара США і використовує блокчейн Ethereum для забезпечення прозорості і швидкості транзакцій.

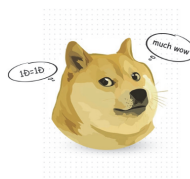
Купівля криптовалюти. Для придбання криптовалюти існують обмінники, де бажаючі продають і купують цифрові монети за іншу криптовалюту або за національну валюту. За обмін потрібно заплатити комісію. Альтернатива без комісії – p2p-обмінники, що дозволяють передати гроші від людини до людини, без посередників. Ще один спосіб, як можна купити криптовалюту – використовувати криптобіржі (рис. 1.4).



What is Dogecoin?

An open-source peer-to-peer digital currency, favoured by Shiba Inus worldwide.

At its heart, Dogecoin is the accidental crypto movement that makes people smile! It is also an open-source peer-to-peer cryptocurrency that utilizes blockchain technology, a highly secure decentralised system of storing information as a public ledger that is maintained by a network of computers called nodes. More than this though, is the ethos of Dogecoin, summarised in the *Dogecoin Manifesto*, and its amazing vibrant community made up of friendly folks just like you! [Learn more](#)



Getting started

01 choose your wallet

A wallet is necessary for people wanting to use, trade, or hold Dogecoin. You can pick a wallet.

[Learn more](#)

02 configure your wallet

After downloading, you can configure your wallet according to our

[guide](#)

03 get some dogecoin

There's lots of ways to get your hands on some Dogecoin.

[Learn more](#)

Рисунок – 1.4 Пропозиція розробників валюти Dogecoin способів заробітку криптовалюти: покупка, обмін, майнінг і надання потужності свого комп'ютера.

Трейдинг криптовалюти. Криптотрейдинг схожий зі звичайним трейдингом – він заснований на принципі «купити дешевше та продати

дорожче». Висока мінливість ціни криптовалют дозволяє укласти швидкі угоди. Трейдинг проводиться на торгових майданчиках.

Криптовалюту можна використовувати декількома способами.

Інвестиції в криптовалюту. Криптовалюта приваблює інвесторів високою прибутковістю вкладів. За підсумками першого кварталу 2023 року біткоїн став лідером серед інших інвестиційних інструментів – з 1 січня 2023 року його ціна зросла на 70% (рис. 1.5).

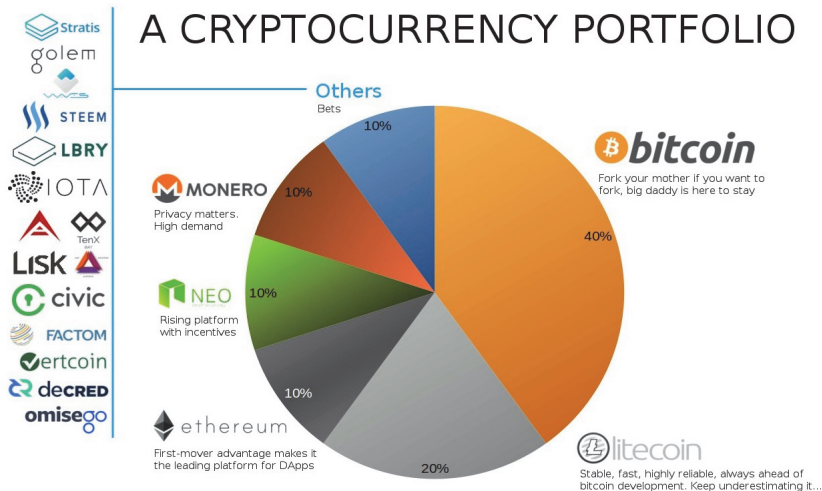


Рисунок – 1.5 Приклад криптовалютного портфелю інвестицій

Спекуляції криптовалютою. Ціни на криптовалютному ринку легкий предмет спекуляції. Мінливість вартості електронних грошей створює різницю в курсах валют. Цю різницю використовують трейдери та криптоброкери. Спекуляції кардинально впливають на ціну криптовалют. Так, після заяви Ілона Маска вночі 13 травня 2021 року біткоїн подешевшав приблизно до 46.000 \$, а вранці зріс до 50.000 \$ (рис. 1.6).

Обмін криптовалюти на товари та послуги. Обмін поширений не скрізь, але набирає обертів. Платежі криптовалютою приймають компанії Amazon, eBay, електронна система PayPal. З'являються банкомати для переведення в готівку коштів, розробляється єдина форма оплати криптовалютними дебетовими картами – BitPay (рис. 1.7).

NFT (Non-Fungible Token) – тип криптовалюти, яка представляє унікальні цифрові активи, що не є взаємозамінними. Відмінністю NFT від інших криптовалют, таких як Bitcoin або Ethereum, є те, що кожен NFT має унікальний ідентифікатор, який його відрізняє від інших токенів.

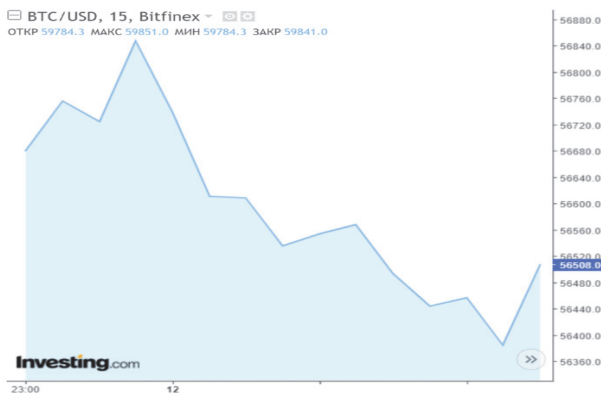


Рисунок – 1.6 Приклад коливань вартості біткоїну



Рисунок – 1.7 Платіжна картка BitPay

NFT забезпечують власність та автентичність цифрових активів, таких як мистецтво, музика, відео, графіка, віртуальні землі та багато іншого. Вони базуються на блокчейні, зазвичай Ethereum, і використовують смарт-контракти для запису власності та обміну активами.

Купуючи або володіючи NFT, ви отримуєте унікальний цифровий актив, який можна перевірити, що він оригінальний та належить вам. Ця технологія відкриває нові можливості для творців та колекціонерів, а також впливає на мистецтво, музику та інші галузі, дозволяючи здійснювати торгівлю та обмін унікальними цифровими активами.

Деякі приклади популярних NFT-проектів та колекцій, наведені нижче:

CryptoPunks – колекція 10.000 унікальних піксельних персонажів, які можна купувати, продавати та володіти;

Art Blocks – платформа, на якій художники створюють автоматично згенероване мистецтво, яке може бути продане у вигляді NFT;

NBA Top Shot – цифрова колекція моментів з найкращих моментів баскетбольних ігор, які можна збирати та торгувати;

Decentraland – віртуальна реальність на базі блокчейну, де користувачі можуть купувати, продавати та володіти віртуальною землею та нерухомістю.

Beeple's "Everydays: the First 5000 Days" – колекція 5.000 днів роботи художника Beeple, яку він продав за \$69,3 мільйона на аукціоні Christie's.

Далі наведена загальна інструкція по купівлі NFT:

1) Виберіть платформу: знайдіть платформу для купівлі NFT, таку як OpenSea, Rarible, SuperRare або інші. Реєстрація на платформі може бути необхідною для доступу до ринку.

2) Отримайте криптовалюту: більшість NFT платформ працюють на основі блокчейну Ethereum і приймають оплату у криптовалюті Ether (ETH). Отримайте достатню кількість ETH на свій криптогаманець.

3) Підключіть гаманець: підключіть свій криптогаманець до вибраної платформи, якщо це необхідно. Це може знадобитися для підпису транзакцій та передачі власності.

4) Перегляньте ринок: перегляньте доступні NFT на платформі, використовуючи фільтри, категорії або пошук. Виберіть той, який вас цікавить.

5) Перевірте деталі та ціну: клікніть на NFT, щоб переглянути деталі, опис, зображення та ціну. Впевніться, що ви розумієте, що ви купуєте, і зверніть увагу на вартість та комісії.

6) Зробіть ставку або придбайте: якщо NFT продається на аукціоні, ви можете зробити ставку, а якщо вона має фіксовану ціну, можете придбати її прямо. Слідуйте інструкціям на платформі для завершення покупки.

7) Підтвердіть транзакцію: перегляньте всі деталі та підтвердьте транзакцію. Зазвичай це включає підпис платіжного ордеру з використанням вашого криптогаманця.

8) Володійте своїм NFT: після успішної транзакції ви стаєте власником NFT. Він може бути збережений у вашому криптогаманці або в електронному кошельку на платформі.

9) Перевірте метадані: перевірте метадані вашого NFT, які можуть містити унікальні характеристики, права власності та іншу інформацію.

Важливо пам'ятати, що процес купівлі NFT може змінюватися залежно від платформи та конкретного NFT. Дотримуйтесь інструкцій та рекомендацій платформи, на якій ви здійснюєте покупку.

Безпека криптовалют. Дані, які потрапляють в Інтернет, можна присвоїти і змінити, але в блокчейні шахрайство з гаманцями або платежами практично неможливо. Високий рівень безпеки пов'язаний з тим, що інформація в кожному блоці зашифрована, а блоки пов'язані між собою по ланцюжку. Щоб зламати систему, потрібні занадто великі потужності, оскільки заради одного осередку інформації доведеться змінювати шифр у всіх інших.

Система має й інші особливості, які гарантують безпеку операцій:

- для переказу коштів використовують унікальні адреси: для кожної операції їх генерує сама система;
- транзакції відкриті і прозорі, але зв'язати дані з конкретною людиною і його місцезнаходженням неможливо;
- операції проводяться миттєво, їх не можна перехопити;
- справжність адрес перевіряється ключами шифрування.

В криптосистемі існують публічні та приватні ключі:

публічний ключ – це адреса електронного гаманця користувача, він знаходиться у відкритому доступі;

приватний ключ – це шифр, відомий лише власнику гаманця.

Ключі працюють наступним чином: один користувач хоче відправити криптовалюту іншому і шифрує її за допомогою публічного ключа, а одержувач використовує приватний ключ, щоб відкрити «лист» (рис. 1.8).

- Адреса Біткоїн гаманця: 1DcEeFRGc4mfRLXWIVZySprmmXk7SsVLfMG
- Коротка адреса: 1BSUkuwtmd7gkdy6W4Q954gNKWBgy4A19Q
- Публічний ключ (130 символів [0-9A-F]):
04D7AS1212E4EEFE40C72B201E74AA3557DEFD940ACESC3E1C76B75S77CD45FF9626065170497984F8
1C39 A0DA7FA296B3F6D
- Публічний ключ (короткий, 66 символів [0-9A-F]):
03D7A51212E4EEFE40C72B201E74AA3557DEFD940ACESC3E107687577CD45FF962

Рисунок – 1.8 Приклад публічного ключа криптогаманця

Від чого залежить ціна криптовалюти. На ціну криптовалюти впливають попит і пропозиція користувачів мережі. Вона не залежить від держави та національної валюти.

Чим популярніша криптовалюта, тим більше користувачів вона приваблює. Отже, збільшиться кількість операцій і зростає її цінність. Коли користувачів стає менше, ціна криптовалюти падає. Наприклад, у кінці 2020 року з бірж вивели багато біткоїнів, а попит залишився колишнім. Через це в січні 2021 року його ціна зросла в шість разів (рис. 1.9). Для майнерів ціна інша: вона складається з вартості обладнання і витрат на електроенергію.

Проблеми використання криптовалют. Використання криптовалют пов'язане з ризиками через те, що воно не регламентоване державою. Ось із якими проблемами можуть зіткнутися майнери і покупці криптовалют:

- нестабільність і різкі стрибки курсу;
- перспектива знецінення криптовалют з необмеженою емісією, наприклад Ethereum;
- можливість втратити всі коїни, якщо втратити ключ до гаманця.

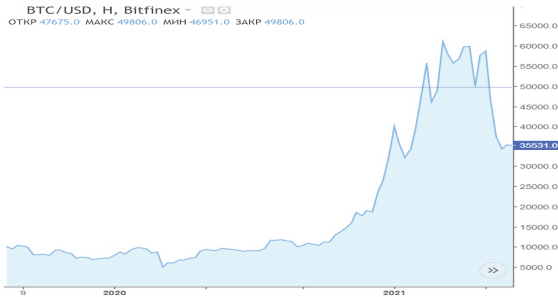


Рисунок – 1.9 Приклад зростання цін на біткоїни, як результат зв'язку попиту та пропозиції

Звернутися до банку чи поліції не вийде. У більшості країн криптовалюту не можна офіційно обмінювати на товари та послуги. Це пов'язано з тим, що її видобуток і передача анонімна, а значить, учасники процесу можуть ухилятися від сплати податків.

Її приймають деякі онлайн-магазини, а ще їй можна торгувати, але ціна безпосередньо залежить від попиту. Якщо попит впаде, валюта знеціниться і власник може втратити всі вкладені в неї гроші.

Важливо пам'ятати, що криптовалюта – це віртуальні гроші, які зазвичай не підкріплені фізичними активами. Їх використовують тільки в інтернеті. Криптовалюта не керується державою і не захищена від інфляції. Криптовалюту добувають за допомогою майнінгу. Її використовують для інвестицій, трейдингу, купівлі та продажу товарів.

1.2. Види криптогаманців

Існує кілька видів криптогаманців, зокрема: «холодний», «гарячий», мобільний ті інші:

1) *«Холодний» криптогаманець* – це фізичний пристрій, який зберігає ваші криптовалюти офлайн. Такий тип гаманця вважається найбезпечнішим, оскільки його неможливо взломати з Інтернету. Холодні криптогаманці можуть бути у вигляді USB-накопичувачів, паперових гаманців, апаратних гаманців тощо.

1.1) *USB-накопичувач* – це невеликий пристрій, який можна підключити до комп'ютера або мобільного пристрою з USB-портом. Цей тип гаманця забезпечує зручність та легку переносимість, оскільки його можна легко зберігати в кишені чи на ключовому кільці.

Однак, USB-гаманці мають свої недоліки. Вони можуть бути підвержені ризику втрати чи крадіжки, якщо ви не зберігаєте їх у безпечному місці. Крім того, віруси чи шкідливі програми на комп'ютері можуть вплинути на безпеку USB-гаманця (рис. 1.10).

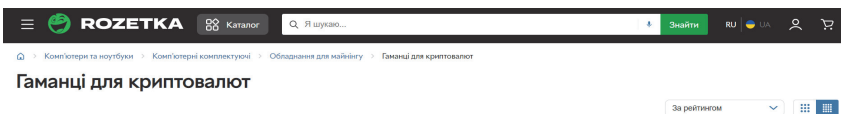


Рисунок – 1.10 Пропозиції купівлі криптогаманців в інтернет-магазині

1.2) *Паперовий гаманець* – це простий аркуш паперу, на якому зберігається приватний ключ для доступу до вашої криптовалюти. Цей тип гаманця вважається найбільш безпечним, оскільки приватний ключ не зберігається в Інтернеті та не піддається ризику взлому. Проте, паперовий гаманець також може бути підвержений ризику втрати або пошкодження, якщо ви не зберігаєте його у безпечному місці (рис. 1.11).



Рисунок – 1.11 Зразок паперового криптогаманця

На ринку існує достатньо багато виробників холодних криптогаманців, і кожен з них має свої особливості. Ось декілька з найпопулярніших виробників: Ledger, Trezor, KeepKey, BitBox.

Ledger – французька компанія, що спеціалізується на розробці холодних гаманців. Найпопулярніші продукти цієї компанії – це Ledger Nano S та Ledger Nano X. Обидва пристрої підтримують більшість популярних криптовалют та мають різні функції, такі як підтримка декількох гаманців

у одному пристрої та можливість використання у поєднанні з мобільними додатками (рис. 1.12).

Trezor – чеська компанія, що виробляє холодні гаманці. Найбільш популярні пристрої цієї компанії – це Trezor One та Trezor Model T. Вони також підтримують більшість популярних криптовалют та мають різні функції, такі як можливість створення бекапів гаманців та підтримка двофакторної аутентифікації.

KeepKey – американська компанія, що спеціалізується на виробництві холодних гаманців. KeepKey підтримує більшість популярних криптовалют та має гарний дизайн та додаткові функції, такі як можливість використовувати у поєднанні з різними програмними гаманцями.

BitBox – швейцарська компанія, що виробляє холодні гаманці. BitBox підтримує більшість популярних криптовалют та має високий рівень безпеки та захисту від зламів.



Рисунок – 1.12 Зразок «холодного» криптогаманця Ledger Nano X Onyx Black

2) «Гарячий» криптогаманець (*Hot Wallet*) – це електронний гаманець, що зберігається на підключеному до Інтернету пристрої, такому як комп'ютер, смартфон або планшет. Цей тип гаманця є найбільш доступним та зручним для користування, оскільки він дозволяє виконувати транзакції швидко та без зайвих труднощів (1.13).

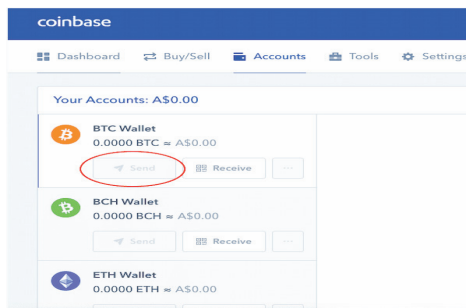


Рисунок – 1.13 Зразок гарячого криптогаманця *CoinBase*

Проте, гарячі криптогаманці мають певні ризики, пов'язані з можливими кібератаками на пристрій, який зберігає приватні ключі. Якщо пристрій із гарячим гаманцем стане жертвою зламу, то зловмисники можуть отримати доступ до приватного ключа і використовувати його для викрадення криптовалюти з гаманця.

Отже, користувачі повинні приділяти особливу увагу захисту свого гарячого гаманця. Найбільш розповсюдженими методами захисту є використання пароля, двофакторної аутентифікації, резервних копій та підтримки різних рівнів доступу для різних користувачів.

Існують різні види гарячих гаманців, такі як програмні гаманці, веб-гаманці, гаманці для мобільних пристроїв та гаманці на обмінних платформах. Кожен з них має свої особливості, але вони всі мають загальний принцип роботи – зберігати приватні ключі на підключеному до Інтернету пристрої.

Серед найпопулярніших «гарячих» криптогаманців можна виділити наступні:

Coinbase – одна з найбільших обмінних платформ та гарячих гаманців у світі, яка підтримує більшість популярних криптовалют та забезпечує високий рівень безпеки;

Binance – ще одна з найбільших обмінних платформ, яка також пропонує гарячий гаманець для зберігання криптовалют, яка підтримує широкий вибір криптовалют та надає користувачам безкоштовну двофакторну аутентифікацію;

Atomic Wallet – програмний гарячий гаманець з підтримкою більшості популярних криптовалют, який має простий та інтуїтивно зрозумілий інтерфейс користувача і підтримує резервні копії для забезпечення безпеки;

Exodus – інший програмний гарячий гаманець з підтримкою більшості популярних криптовалют, який має простий та зрозумілий інтерфейс, а також підтримує обмін криптовалют між різними гаманцями;

MyEtherWallet – веб-гарячий гаманець для зберігання Ethereum та ERC-20 токенів, який має простий та зручний інтерфейс, а також підтримує резервні копії для забезпечення безпеки.

3) *Гібридний криптогаманець* – це комбінація холодного та гарячого криптогаманців. Цей тип гаманця забезпечує баланс між зручністю та безпекою, оскільки частину вашої криптовалюти зберігають офлайн, а іншу частину – онлайн.

4) *Мобільний криптогаманець* – це додаток для мобільних пристроїв, який забезпечує зберігання криптовалют. Мобільні гаманці можуть бути зручними для тих, хто постійно перебуває в дорозі або хоче мати швидкий доступ до своїх криптовалют, але їхній рівень безпеки залежить від безпеки вашого мобільного пристрою. Цей тип гаманців забезпечує доступ до криптовалют та дозволяє здійснювати транзакції на мобільному пристрої. Існують версії мобільних гаманців для різних операційних систем, таких як Android та iOS.

Мобільні криптогаманці мають кілька переваг, серед яких:

- *зручність та доступність* – користувачі можуть легко отримати доступ до своїх криптовалют на мобільному пристрої з будь-якого місця з доступом до Інтернету;
- *простота використання* – більшість мобільних криптогаманців мають інтуїтивно зрозумілий інтерфейс та можуть бути легко налаштовані та використані навіть користувачами, які не мають досвіду в роботі з криптовалютами;
- *мобільна автентифікація* – більшість мобільних криптогаманців підтримують використання Touch ID або Face ID для більш зручної та безпечної автентифікації;
- *безпека* – деякі мобільні криптогаманці забезпечують високий рівень безпеки, наприклад, за допомогою двофакторної аутентифікації та шифрування даних.

Деякі з найбільш популярних мобільних криптогаманців на сьогоднішній день:

Coinbase Wallet – мобільний гаманець від популярної криптобіржі Coinbase, який підтримує більшість популярних криптовалют та має вбудовану можливість купівлі та продажу криптовалют;

Trust Wallet – мобільний гаманець з відкритим вихідним кодом для зберігання криптовалют на мобільному пристрої, який підтримує більшість популярних криптовалют та дозволяє здійснювати обмін між ними;

Exodus – мобільний гаманець, який підтримує більшість популярних криптовалют, має привабливий інтерфейс і забезпечує високий рівень безпеки за допомогою шифрування даних та можливості використання Touch ID або Face ID для автентифікації (рис. 1. 14);

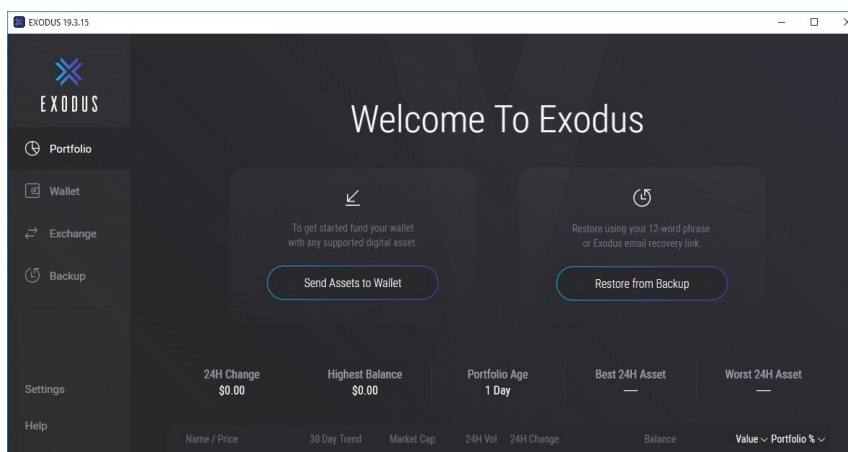


Рисунок – 1.14 Зовнішній вигляд криптогаманця Exodus

Mycelium – мобільний гаманець для Bitcoin, який має простий інтерфейс та підтримує бездротові платежі, забезпечує високий рівень безпеки за допомогою шифрування даних та можливості використання PIN-коду для автентифікації;

Jaxx Liberty – мобільний гаманець, який підтримує більшість популярних криптовалют, має вбудований обмінник і забезпечує високий рівень безпеки за допомогою шифрування даних та можливості використання PIN-коду для автентифікації.

5) *Веб-криптогаманець* – це онлайн-сервіс, який забезпечує зберігання криптовалют у віртуальному просторі. Цей тип гаманця дозволяє користувачам отримувати доступ до своїх активів з будь-якого місця, де є Інтернет-підключення. Однак, веб-криптогаманці не є найбезпечнішими способами зберігання криптовалют, оскільки вони піддаються ризику кібератак та злому.

До популярних веб-криптогаманців можна віднести: *MyEtherWallet*, *MetaMask*, *Coinbase Wallet* та *Blockchain.info* (рис. 1.15). Більшість веб-криптогаманців забезпечують безкоштовне створення гаманців, проте можуть стягувати комісії за транзакції та обслуговування рахунку.

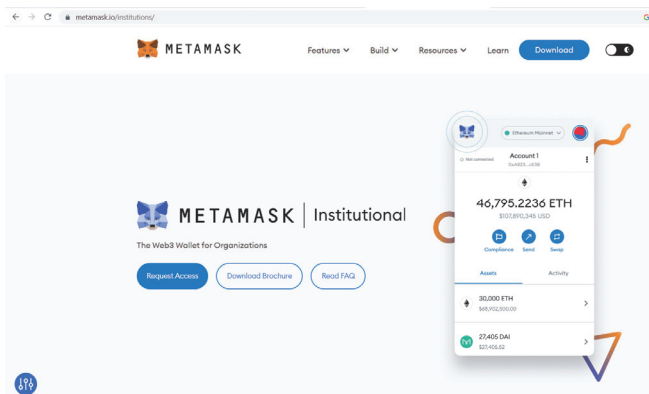


Рисунок – 1.15 Сайт криптогаманця MetaMask

Однією з головних переваг веб-криптогаманців є їх зручність та доступність. Користувачі можуть легко створити новий гаманець, призначити пароль та почати зберігати свої криптовалюти. Більшість веб-криптогаманців дозволяють користувачам отримувати доступ до своїх активів через веб-інтерфейс, мобільну програму або розширення для браузера.

Однак, веб-криптогаманці також мають свої недоліки та ризики. Наприклад, якщо ваш акаунт був підданий кібератаці, ваші криптовалюти можуть бути викрадені. Також, якщо веб-криптогаманець зупинить свою роботу або буде зламаний, ваші криптовалюти можуть бути втрачені.

1.3. Майнінг криптовалют

Майнінг – це процес створення нових блоків та підтвердження транзакцій в криптовалютній мережі. Основна ідея майнінгу полягає в тому, що спеціальні програми на комп'ютері або спеціалізовані майнінгові пристрої (ASIC – Application-Specific Integrated Circuit) виконують математичні розрахунки, які підтверджують нові транзакції в мережі та додають їх до блокчейну – це розподілена БД, яка зберігає всі транзакції в мережі (рис. 1.16).

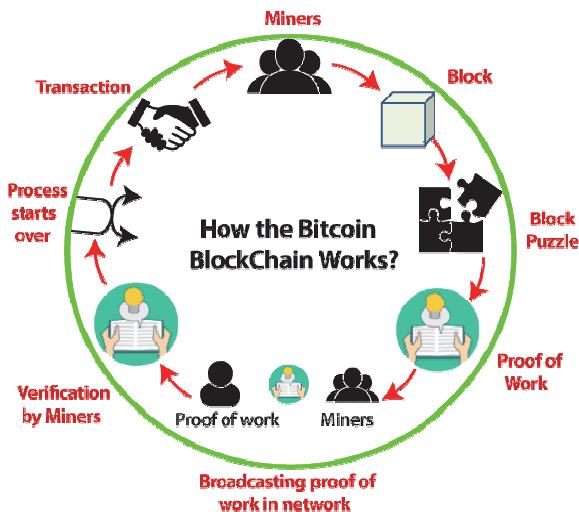


Рисунок – 1.16 Загальний процес майнінгу криптовалюти

У процесі майнінгу використовується складний алгоритм, який вимагає великої обчислювальної потужності та спеціалізованого обладнання. Майнери отримують винагороду за кожен блок, який вони знаходять та підтверджують в мережі. Винагорода складається з новостворених криптовалютних монет, які додаються до системи, та комісійних винагород за обробку транзакцій.

Майнінг є ключовим елементом функціонування криптовалют та забезпечує безпеку та стійкість мережі. Однак, з часом вимоги до майнінгу стають все вищими, а винагороди зменшуються, що робить його менш вигідним та доступним для широкої аудиторії. Крім того, майнінг вимагає значного електричного споживання, що може впливати на довкілля та призводити до значного енерговитратного підходу до видобутку криптовалют.

Існують різні види майнінгу в залежності від типу криптовалюти та способу видобутку (рис. 1.17).

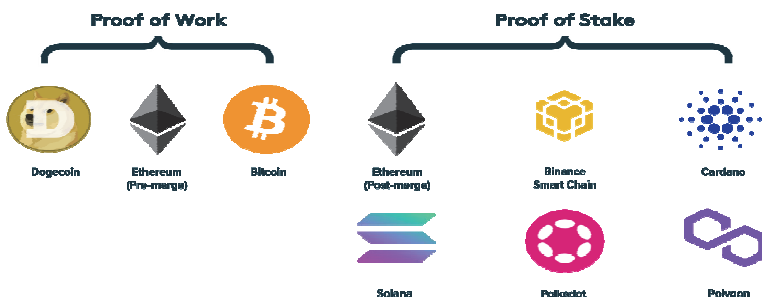


Рисунок – 1.17 Різновиди майнінгу

Нижче описані декілька різновидів майнінгу:

Proof of Work (PoW) – це найбільш поширений спосіб майнінгу, який використовується в більшості популярних криптовалют, таких як *Bitcoin* та *Ethereum*. У цьому виді майнінгу майнери використовують обчислювальну потужність свого обладнання для розв'язування складних математичних задач, які підтверджують нові транзакції та створюють нові блоки в мережі (рис. 1.18).

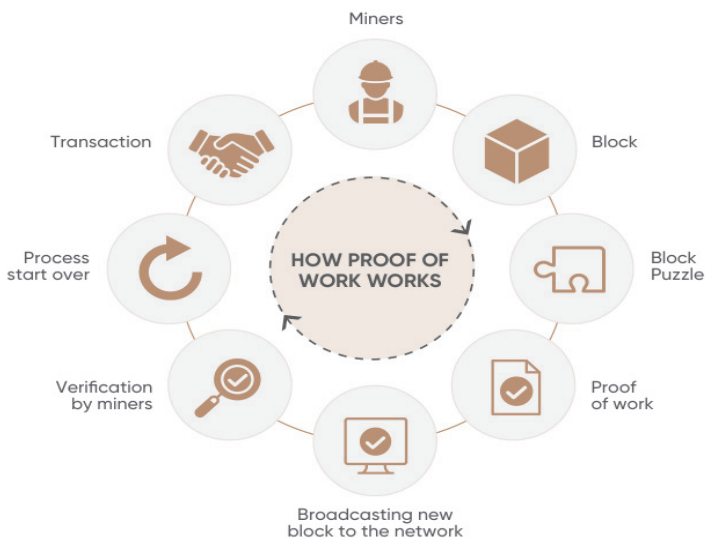
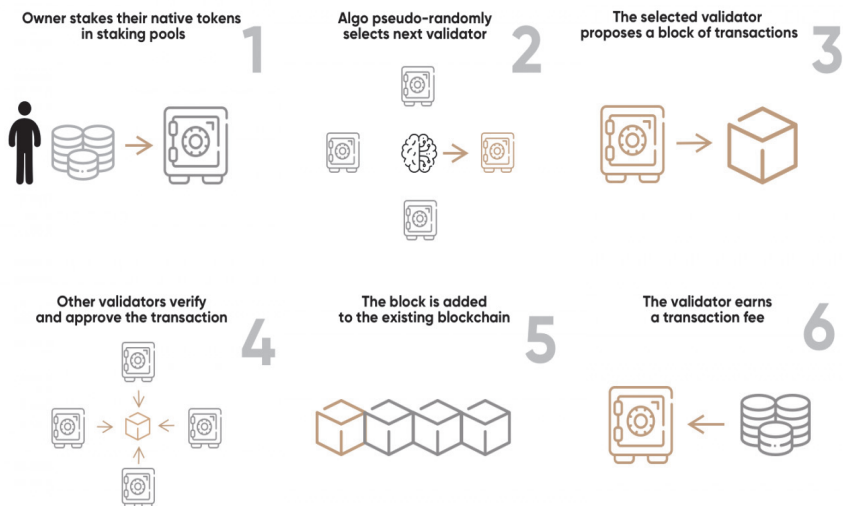


Рисунок – 1.18 Загальний алгоритм транзакцій типу *Proof of Work*

Proof of Stake (PoS) – цей спосіб майнінгу використовується в деяких криптовалютах, таких як *Cardano* та *Ethereum 2.0*. У цьому випадку майнери не виконують складних обчислень, а замість цього блоки

створюються на основі власних фінансових вкладень у криптовалюту. Майнери, які мають більшу кількість монет, мають більші шанси на створення нових блоків (рис. 1.19).



Source: SEBA Research

Рисунок – 1.19 Загальний алгоритм транзакцій типу *Proof of Stake*

CPU майнінг – це майнінг на процесорі комп'ютера. Цей метод майнінгу є найпростішим, але найменш ефективним. Він використовується для майнінгу криптовалют, які мають низький рівень складності.

Для CPU майнінгу зазвичай використовують звичайні процесори, що мають вбудований графічний процесор (рис. 1.20).

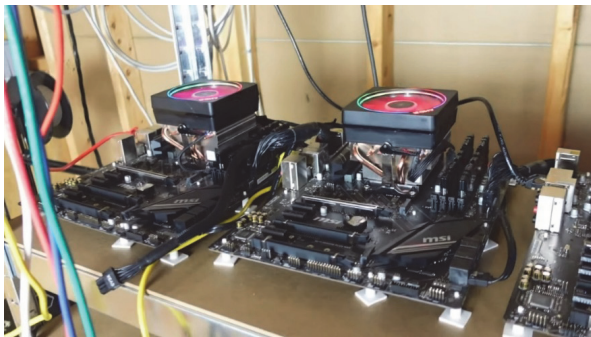


Рисунок – 1.20 Система майнінгу на процесорах AMD Ryzen 9

Оскільки CPU не спеціалізований для майнінгу криптовалют, його швидкість зазвичай нижча порівняно з іншими методами майнінгу, такими як GPU майнінг або ASIC майнінг. Однак, для деяких криптовалют, таких як Monero, CPU майнінг є ефективнішим, оскільки алгоритм майнінгу Cryptonight, який використовує цю криптовалюту, більш оптимізований для CPU.

Для CPU майнінгу можна використовувати будь-який комп'ютер, який має достатньо потужного процесора. Однак, для підвищення продуктивності можна використовувати комп'ютери з більш потужними процесорами або встановлювати додаткові процесори у наявні системи.

GPU майнінг – це майнінг на графічному процесорі. Цей метод майнінгу є більш ефективним, ніж CPU майнінг, оскільки графічні процесори можуть виконувати більше обчислювальних операцій за один раз. GPU майнінг використовується для майнінгу більш складних криптовалют, таких як Ethereum.

Для GPU майнінгу використовуються спеціальні пристрої, які складаються з графічних процесорів та систем охолодження (рис. 1.21, 1.22).

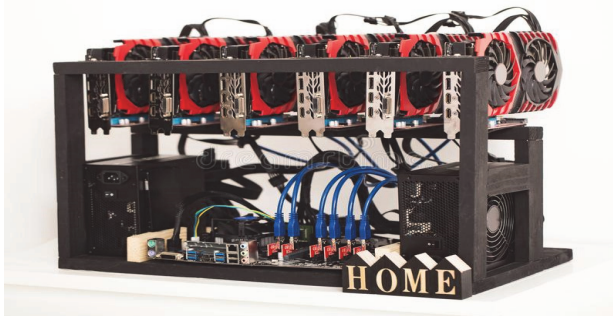


Рисунок – 1.21 Зовнішній вигляд майнінг ферми на відеокартах

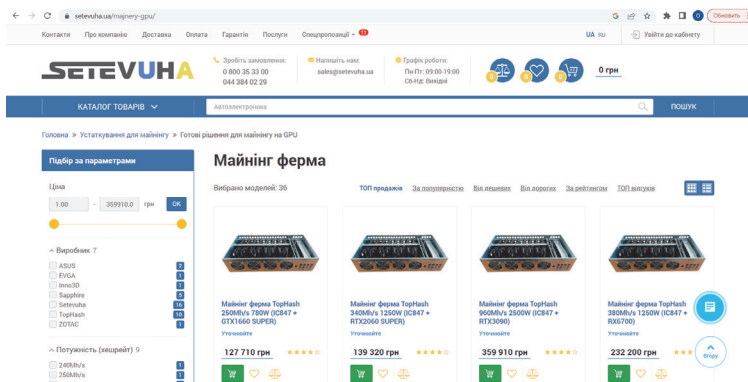


Рисунок – 1.22 Пропозиції продажу готової GPU майнінг ферми

Такі пристрої називаються графічними картами або відеокартами. Відеокарти є одним з найпоширеніших засобів для майнінгу криптовалют, зокрема Ethereum, Litecoin, Zcash та інших (рис. 1.23).

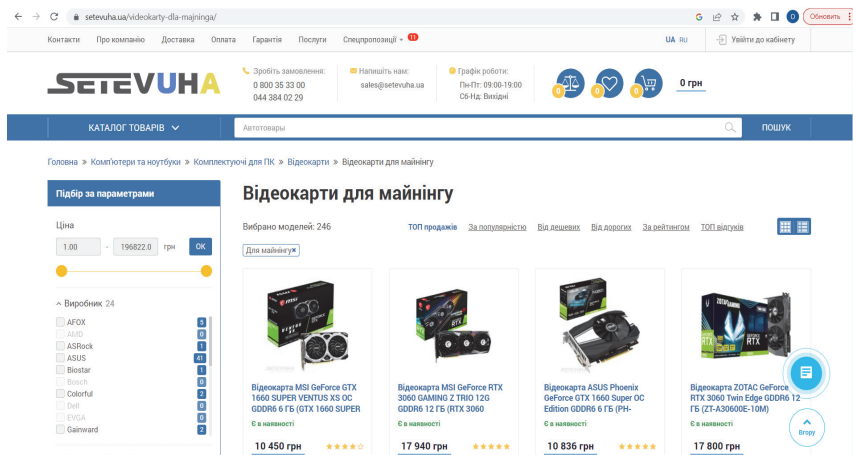


Рисунок – 1.23 Пропозиції інтернет-магазину щодо купівлі відеокарт

Для ефективного майнінгу на відеокартах потрібно мати потужний комп'ютер з великою кількістю відеокарт. Також необхідно додаткове обладнання для забезпечення стабільності роботи відеокарт та їх охолодження.

Основні виробники відеокарт для майнінгу – AMD та Nvidia. Компанії випускають спеціальні версії відеокарт з підвищеною продуктивністю та ефективністю споживання електроенергії для майнінгу.

ASIC майнінг – це майнінг на спеціалізованому обладнанні *Application-Specific Integrated Circuit*. Цей пристрій, спеціально розроблений для виконання конкретних операцій, який дозволяє досягнути високої продуктивності та ефективності енергоспоживання за рахунок виключення непотрібних функцій, та максимального використання можливостей для розв'язання конкретної задачі (рис. 1.24, 1.25).

ASIC майнінг використовується для майнінгу криптовалют, які використовують складні алгоритми, такі як Bitcoin.

Основною перевагою ASIC майнінгу є висока швидкість та продуктивність при майнінгу криптовалют, таких як Bitcoin, Litecoin, Dash та інші. Відмінність ASIC майнінгу від GPU майнінгу полягає в тому, що обладнання розроблене спеціально для однієї конкретної криптовалюти та не може бути використане для інших криптовалют або завдань.

ASIC майнінг працює на основі спеціальних чіпів, які розробляються і виробляються під конкретний алгоритм майнінгу. Ці чіпи розміщуються

на платі, яка може містити до сотень чіпів, і з'єднується з блоком живлення та іншими компонентами для стабільної роботи.



Рисунок – 1.24 Майнінг на пристроях ASIC

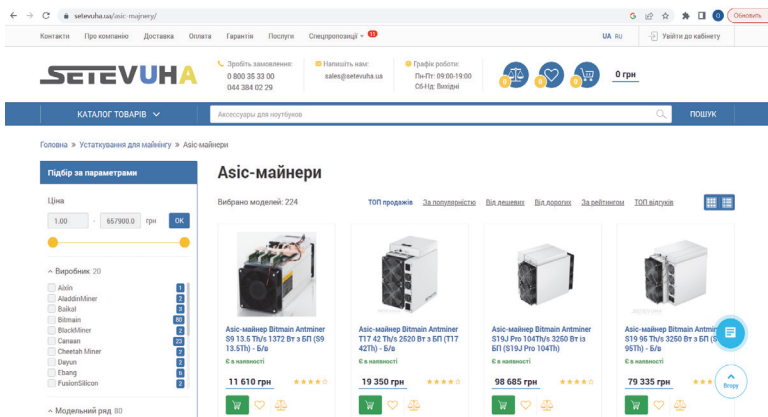


Рисунок – 1.25 Пропозиції інтернет-магазину ASIC майнерів

Важливо зазначити, що вартість та складність виготовлення ASIC майнерів є значною, тому вони найбільш популярні серед професійних майнерів, які мають значний бюджет та мету отримання великих прибутків від майнінгу. Виробниками ASIC майнерів є Bitmain, Canaan, Ebang та інші.

Cloud майнінг – це майнінг у хмарному сервісі. Цей метод майнінгу забезпечує можливість здійснювати майнінг без необхідності володіти спеціалізованим обладнанням (рис. 1.26). Користувачі можуть купувати хмарні майнінгові контракти від компаній, які надають ці послуги (рис. 1.27).



Рисунок – 1.26 Вигляд ферми для майнінгу у хмарному сервісі

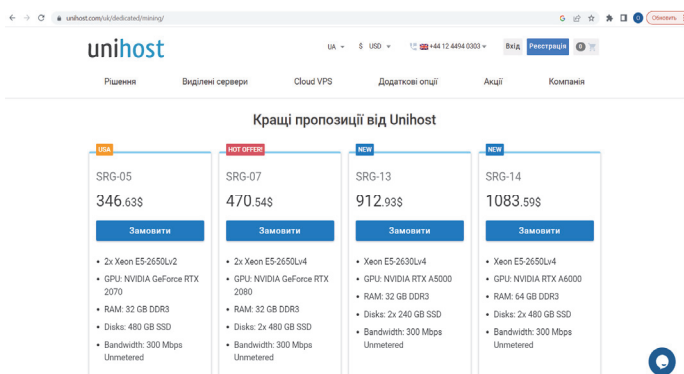


Рисунок – 1.27 Типова пропозиція майнінгу в хмарному сервісі

Майнінг на жорстких дисках (Hard Drive Mining або HDD Mining) – є одним із способів добування криптовалют, таких як Chia (XCH) або Burstcoin (BURST). У майнінгу на жорстких дисках використовується потужність і місце на жорсткому диску для здійснення обчислень (рис. 1.28).

Основна ідея майнінгу на жорстких дисках полягає у використанні простору для зберігання на жорсткому диску для створення псевдовипадкових чисел. Ці числа використовуються для згортання (plotting) або генерації графів, які слугують основою для майнінгу. Графи зберігаються на жорсткому диску і використовуються для розрахунку доказів простору (proofs of space), що підтверджують роботу майнера.

Для майнінгу на жорстких дисках потрібен великий обсяг вільного простору на жорсткому диску. Перед початком майнінгу необхідно

створити графі на основі потужності і простору на жорсткому диску. Цей процес може зайняти певний час, але після його завершення майнер може почати розраховувати докази простору.

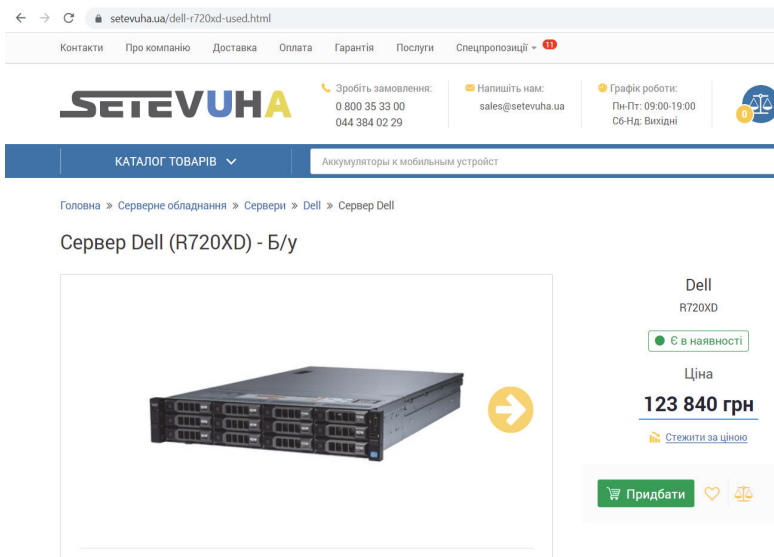


Рисунок – 1.28 Пропозиції інтернет магазину – сервер для майнінгу на жорстких дисках

Майнінг на жорстких дисках відмінний від традиційного майнінгу на базі обчислювальної потужності, такого як майнінг на графічних процесорах (GPU) або майнінг на спеціалізованих пристроях (ASIC). Він використовує менше електроенергії, оскільки обчислення здійснюються на жорсткому диску, а не на високопотужних пристроях. Однак, майнінг на жорстких дисках може вимагати великої кількості місця для зберігання і тривати довше у порівнянні з іншими методами майнінгу.

Важливо відзначити, що вибір криптовалюти і методу майнінгу залежить від вашого обладнання, вільного простору на жорсткому диску, вартості електроенергії та інших факторів. Перед початком майнінгу на жорсткому диску слід провести детальну аналізу і дослідження для зрозуміння потенційних вигод та обмежень цього методу. Рейтинг країн за поширеністю майнінгу. Майнінг криптовалют є глобальним явищем і може здійснюватись в будь-якій країні світу, де є доступ до Інтернету та необхідних ресурсів. Однак, існують країни, де майнінг є особливо поширеним і розвиненим завдяки доступності дешевої електроенергії та відносно низьким витратам на життя та обладнання.

За даними з серпня 2021 року, топ-5 країн з найбільшою кількістю майнерів були такими:

Китай – більшість майнерів були розміщені у провінціях Сінцзян, Внутрішня Монголія та Сичуань, завдяки дешевій гідроенергії та вітровій енергії.

США – багато майнерів розташовані у штатах Техас, Каліфорнія, Нью-Йорк, зокрема через дешеву електроенергію та великі простори.

росія – багато майнерів зосереджено в Сибіру та Уралі, завдяки доступності дешевої енергії та низьким витратам на обладнання.

Канада – багато майнерів розташовані в провінції Квебек, завдяки дешевій електроенергії та добре розвиненій інфраструктурі.

Казахстан – багато майнерів знаходяться в столиці Алмати, завдяки доступності дешевої електроенергії та великим територіям для розміщення обладнання.

Проте, слід зазначити, що ці дані можуть змінюватись залежно від багатьох факторів, таких як рівень складності майнінгу, ціна криптовалют, рівень доступності електроенергії тощо.

Майнінг криптовалют в Україні досить поширений, хоча й не є основним видом діяльності українців. Україна має досить низьку вартість електроенергії порівняно з багатьма іншими країнами світу, що робить її привабливим місцем для майнерів.

Однак, уряд України не регулює цю сферу виробництва криптовалют, що може призвести до зловживань та ухиляння від оподаткування. Також в Україні не існує спеціального законодавства щодо криптовалют, хоча деякі законодавчі ініціативи у цьому напрямку все ж таки з'являються.

За даними CryptoDiffer, Україна знаходиться на 28 місці в світовому рейтингу країн за кількістю майнерів. Українські майнери активно використовують різні типи обладнання, включаючи ASIC-майнери та GPU-майнери. Також в Україні є кілька крупних ферм для майнінгу, які займаються виробництвом криптовалют на комерційній основі.

Загалом, майнінг криптовалют в Україні є достатньо розвинутою галуззю, хоча й не отримав повної легальної регуляції та підтримки з боку влади.

1.4. Регулювання ринку криптовалют в Україні

На даний момент, в Україні ринок криптовалют не має повноцінного законодавчого регулювання, але існує ряд законопроектів, які планують врегулювати цю галузь.

Нормативно-правова база України в сфері використання криптовалют включає такі законодавчі акти:

- Закон України «Про валюту та валютні операції» – регулює валютні операції, включаючи операції з криптовалютами [8].
- Закон України «Про фінансові послуги та державне регулювання ринків фінансових послуг» – встановлює правила та вимоги до проведення фінансових операцій, включаючи операції з криптовалютами [9].

- Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» – встановлює правила та процедури контролю за фінансовими операціями, зокрема з криптовалютами, з метою запобігання легалізації доходів та фінансуванню тероризму [10].

- Роз'яснення Національного банку України щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» – визначає порядок регулювання криптовалютних операцій та встановлює вимоги до суб'єктів, які займаються обміном та зберіганням криптовалют [11].

- Спільна заява фінансових регуляторів щодо статусу криптовалют в Україні – встановлює правила та умови для суб'єктів, які займаються діяльністю з криптовалютами на фондовому ринку [12].

Наразі, криптовалюти не є законним засобом платежу в Україні, але їх можна купувати, продавати та використовувати в інвестиційних операціях. Також, біржі криптовалют повинні реєструватися в органах державної влади та виконувати вимоги щодо боротьби зі відмиванням грошей та фінансуванням тероризму.

Проте, 1 липня 2021 року вступив у дію закон «Про валюту та валютні операції», який визначає криптовалюту як «цифрове зображення (цифровий запис) створене за допомогою математичних обчислень та засноване на децентралізованій системі реєстрації операцій (блокчейн), що може використовуватися як засіб обміну та (або) зберігання цінності».

Цей закон передбачає, що українці можуть здійснювати операції з криптовалютами за допомогою електронних гаманців, торгових платформ та інших засобів, які не суперечать законодавству України. Також, біржі криптовалют повинні зареєструватися в Національному банку України (НБУ) та дотримуватися встановлених норм безпеки та захисту інформації.

За збігом обставин епоха розвитку та популяризації блокчейн-технологій припала на період повномасштабної війни в Україні, зумовленої російським вторгненням. Українці разом зі світовою спільнотою використовують усі можливі інструменти для боротьби з агресором, у тому числі й криптовалюту. Її значення у цій війні досягло такого рівня, що «The Washington Post» охрестило події довкола України «Першою світовою криптовійною».

Відповідно до рейтингу Глобального індексу впровадження криптовалют за 2022 рік, за звітом «Chainalysis», і Україна, і росія входять до першої десятки лідерів за минулий рік (третє та дев'яте місце відповідно).

Безумовний вплив на перебіг воєнних дій має економічна спроможність держав-учасниць. Допоки функціонує економіка, доти будуть сили та ресурси продовжувати бойові дії. При цьому роль криптовалют не однозначна, оскільки її активно використовує не лише українська сторона, а й російська. Спробуємо зважити всі «за» та «проти» і

визначити справжнє місце віртуальних активів під час повномасштабної війни в Україні.

Головна перевага, яку надає криптовалюта – це можливість вільного, швидкого та анонімного руху коштів. Шанс уникнути зайвих бюрократичних процедур та обмежень банківської системи сприяє благодійності, особливо коли йдеться про міждержавні перекази. Саме це дало змогу вже з перших місяців війни збирати величезні суми пожертв на підтримку української армії по всьому світу. Звісно, це далеко не єдиний, але досить вагомий інструмент для збору коштів.

За даними Міністерства цифрової трансформації України (Мінцифри), цьому сприяло створення на урядовому рівні офіційних криптогаманців для перерахування коштів. Ще в лютому 2022 року було створено Криптовалютний фонд благодійних організацій України на основі біржі «Купа» разом із Мінцифрою та Міністерством оборони України (МОУ).

На перший погляд, можуть виникнути складнощі з подальшим використанням таких донатів при закупівлі обладнання для військових чи в гуманітарних цілях, оскільки не всі учасники ринку мають опцію розрахунку криптовалютою.

Загалом є два напрями подальших дій: перший – проводити розрахунки безпосередньо криптовалютою (наприклад, саме так відбувається на Kupa, де переважна більшість витрат – у криптовалюті), або ж конвертувати криптовалюту у звичайну фіатну. Наразі одними з найпопулярніших є Bitcoin та Ethereum, які до того ж є більш ліквідними, ніж решта, та простіше конвертуються. За допомогою використання спеціальних криптобірж відбувається переведення кriptи у гривню чи долар, які вже потім направляються на рахунки Мінцифри чи НБУ.

Ще однією перевагою є те, що криптовалюта більш захищена від зламів і крадіжок, ніж звичайні фіатні рахунки. Однак все-таки трапляються випадки шахрайства під виглядом збору благодійної допомоги. Саме тому слід уважно перевіряти інформацію та реквізити. Не менш важливо згадати, що на початку російського вторгнення саме віртуальні активи стали для багатьох єдиним надійним сховищем власних коштів. Невпевненість в стійкості банківської системи та інфляція зумовили підвищення активності на ринку криптовалюти, яка є своєрідною безпечною альтернативою.

Отже, у цій війні криптовалюта виконує три основні завдання:

- 1) швидкий, анонімний і транскордонний інструмент для збору благодійної допомоги;
- 2) спосіб збереження активів громадян в умовах інфляції та підвищених ризиків стабільності фінансової системи держави;
- 3) репутаційні стимули: налагодження механізмів для збору коштів, створення фондів (у тому числі й державних) для використання криптопожертв характеризують Україну позитивно, як передову цифрову державу.

Однак законодавче врегулювання обігу криптовалюти досі викликає багато запитань.

Законодавство у сфері віртуальних активів. В українському правовому полі фігурують три основні поняття:

- *електронні гроші* – як одиниці вартості, що зберігаються в електронному вигляді, випущені емітентом електронних грошей для виконання платіжних операцій, які приймаються як засіб платежу іншими особами та є грошовим зобов'язанням такого емітента електронних грошей, відповідно до п. 14 ч. 1 ст. 1 Закону України «Про платіжні послуги» [13];

- *цифрові гроші* – електронна форма грошової одиниці України, емітентом якої є НБУ, відповідно до п. 96 ч. 1 ст. 1 Закону України «Про платіжні послуги» [13];

- *віртуальні активи* як нематеріальні блага, що є об'єктом цивільних прав, мають вартість та виражені сукупністю даних в електронній формі, відповідно до п. 1 ч. 1 ст. 1 Закону України «Про віртуальні активи» [14].

Проблематика щодо відмежування понять залишається, але більшість правників підтримують думку, що криптовалюта, цифрові токени та NFT відносяться швидше до віртуальних активів та не є електронними грошима. Окремі спроби врегулювання цього питання були здійснені ще в березні 2022 року і завершилися прийняттям Закону України «Про віртуальні активи», який досі не набрав чинності.

Процес реформування ринку електронних грошей (і криптовалюти в тому числі) триває. Наразі в Європейському Союзі (ЄС) активно ведеться робота над розробкою стандартів врегулювання криптоактивів, щоб протидіяти незаконному відмиванню коштів. Втіленням цих положень має стати Закон MiCA (Markets in cryptoassets), метою прийняття якого є створення єдиної правової бази для криптоактивів у межах ЄС.

Передбачається, що згідно з новими правилами буде введено положення про нагляд, захист прав споживачів та криптосередовища. В той час як споживачі матимуть право на ширший доступ до інформації про можливі ризики та витрати, сама торгівля криптовалютою передбачатиме належну авторизацію, прозорість та розкриття необхідної інформації. Узгоджений текст Закону передбачатиме заходи протидії маніпулюванню ринком, відмиванню грошей, фінансуванню тероризму та іншій злочинній діяльності.

На жаль, криптовалютний фронт має і зворотний бік. Всі переваги, які дають змогу швидко, анонімно та в обхід банківської системи робити пожертви на підтримку України, можуть ідентично працювати і на користь агресора. Численні санкції завдають відчутного удару по російській економіці, хоча їх все ще недостатньо для повної економічної блокади агресора. Крім цього, ворог стає винахідливішим та пристосовується до сучасних реалій, в тому числі використовуючи віртуальні активи.

Звісно, неможливо повністю перевести економіку цілої країни на криптовалюту, однак обходити деякі санкційні обмеження цілком реально.

Відповідно до статистичних даних зі Звіту про географію криптовалюти за 2022 рік від Chainalysis, спостерігається цікава статистика використання криптовалюти у Східній Європі (рис. 1.29).

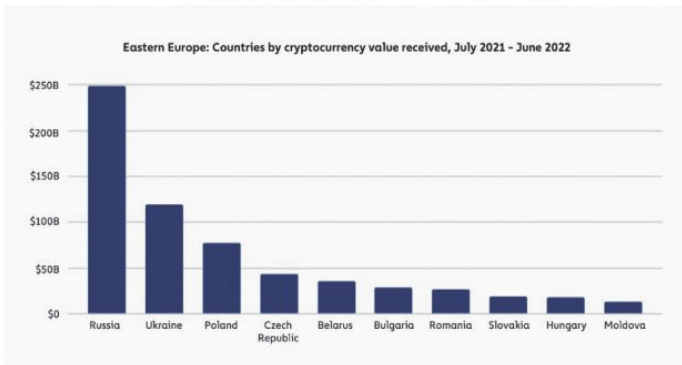


Рисунок – 1.29 Статистика використання криптовалюти у Східній Європі

Як бачимо, за вартістю отриманих активів у криптовалюти за липень 2021 – червень 2022 року зі значним відривом лідирує саме рф, Україна ж знаходиться на другому місці (рис. 1.30). Це свідчить про активний обіг криптовалюти в цей період. Звісно, існує практика як законного, так і незаконного використання криптовалюти в росії. Однак експерти дотримуються позиції, що ринки криптовалют недостатньо ліквідні, щоб повністю нівелювати економічний вплив санкцій.

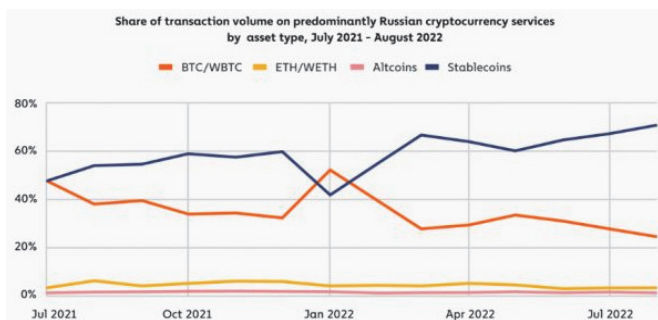


Рисунок – 1.30 Вебтрафік відвідування з окремих країн російських криптовалютних сервісів, липень 2021 – червень 2022

Після впровадження санкційних обмежень для багатьох росіян постала нагальна проблема виведення коштів із росії. На основі проксі-метрик із відвідування російськими користувачами вебресурсів різних

криптовалютних сервісів можна зазначити, що після початку війни в лютому 2022 року відбулось різне зростання активності в Об'єднаних Арабських Еміратах (ОАЕ), Казахстані, Грузії та Туреччині. Проте вже є окремі прецеденти, пов'язані із блокуванням російських криптогаманців.

Крім функції виведення та збереження активів, криптовалюта може зіграти вагомий роль у фінансуванні зовнішньої торгівлі після виведення рф зі SWIFT. Це зумовлено рішенням Центрального банку російської федерації (ЦБрф) щодо легалізації використання криптовалюти для транскордонних платежів і міжнародної торгівлі. Як наслідок, росія зможе продовжити співпрацю із такими потенційними партнерами, як Іран та Китай.

1.5. Регулювання ринку криптовалют в рф

Криптовалюта в рф заборонена для оплати товарів і послуг. За законом її можна використовувати тільки для інвестування. Однак із 2020 року ЦБрф розробляє ще один вид валюти – цифровий рубль. Він частково схожий на криптовалюту. Крипторубль буде цифровим кодом, який зберігається на електронних гаманцях в ЦБрф.

Банки забезпечать громадянам доступ до операцій з цифровим рублем, ставши посередниками між ЦБрф і споживачами. Наприклад, у 2020 році влада Китаю ввела тестування національної цифрової валюти *DCEP* у чотирьох містах.

Станом на вересень 2021 року, ринок криптовалют у рф був регульований рядом законодавчих актів та офіційними заявами з боку російських органів влади.

Ось перелік деяких законодавчих актів рф, що стосуються регулювання криптовалют:

- Федеральний закон «Про центральний банк російської федерації (Банк росії)» від 10.07.2002 № 86-ФЗ – про діяльність ЦБрф, який також містить положення про валютне регулювання [15];
- Федеральний закон «Про валютний регулювання та валютний контроль» від 10.12.2003 №173-ФЗ, що регулює валютні операції, включаючи операції з криптовалютами [16];
- Указ президента російської федерації «Про затвердження Основ стратегічного розвитку цифрової економіки російської федерації до 2030 року» від 09.03.2018 №204, який визначає стратегічні напрями розвитку цифрової економіки, включаючи регулювання криптовалют [17];
- Указ президента російської федерації «Про додаткові заходи щодо розвитку децентралізованих криптографічних платіжних систем» від 12.05.2021 №269, що регулює розвиток децентралізованих криптографічних платіжних систем [17];
- Постанова Правління Центрального банку російської федерації «Про визнання окремих видів цифрових фінансових активів еквівалентами іноземної валюти або іноземних валютних цінностей» від 28.07.2017

№335-П, яка регулює питання визнання деяких видів цифрових фінансових активів [15].

У липні 2020 року був прийнятий Федеральний закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты российской федерации» від 31.07.2020 №259-ФЗ, який встановлює правовий статус криптовалют в росії [18]. Згідно з цим законом, криптовалюти визнаються окремою категорією активів, регульованих російським законодавством.

Органом, відповідальним за регулювання цифрових фінансових активів, є росфінмоніторинг, федеральна служба з контролю фінансових ринків. Він встановлює правила та вимоги до суб'єктів, що здійснюють операції з криптовалютами, включаючи обмінники та криптовалютні біржі.

Також варто зазначити, що російські власті висловлювали суперечливі погляди на криптовалюти та їхню регуляцію. Уряд росії виражав обурення щодо використання криптовалют для незаконних операцій та фінансування тероризму, але також висловлювались позитивні погляди на потенціал блокчейн-технологій та криптовалют у розвитку економіки країни.

2022 почався для учасників криптоспільства рф з потрясіння. 20 січня ЦБрф запропонував запровадити повну заборону на обіг криптовалют. Ініціатива зустріла опір. Наприклад, банк криптовалют у рф розкритикували у Міністерстві фінансів (Мінфіне). Пізніше, 27 січня, за легалізацію цифрових активів виступив президент росії, після чого в країні почали з подвоєною силою формувати правову базу нового фінансового інструменту.

Регулятори рф ведуть розробку правових норм для криптовалют з 2017 року. З 1 січня 2021 року в країні набув чинності федеральний закон №259 «Про цифрові фінансові активи, цифрову валюту та про внесення змін до окремих законодавчих актів рф» [18]. У документі подали базові правила обороту цифрових активів рф. При цьому в законі багато прогалин: наприклад, він не регламентує роботу майнерів.

У 2022 році на тлі тиску санкцій на фінансовому ринку рф зіткнулася з необхідністю пошуку альтернативних інструментів. Для багатьох росіян вирішенням проблеми стали криптовалюти. До грудня 2022 року, за даними Bloomberg, росія увійшла до топ-10 країн, населення яких активніше за інших у світі використовує розрахунки в цифрових активах.

На тлі зростання популярності крипторерахунків у рф влада країни зайнялася формуванням правового поля для нового фінансового інструменту. Найбільше обговорення викликав законопроект про легалізацію майнінгу, який внесли на розгляд до Держдуми 17 листопада 2022 року. Автори документа запропонували дозволити майнерам продаж видобутої криптовалюти на вітчизняних платформах. У цьому законотворці хочуть заборонити рекламу цифрових активів.

«Олії у вогонь» підлили різні трактування документа. Так, голова комітету Держдуми з фінансового ринку Анатолій Аксаков, який стоїть на

чолі розробки законопроекту, зазначив, що документ має на увазі повну заборону криптовалют у РФ у майбутньому. Депутат Державної думи федеральних зборів РФ Антон Горелкін представив альтернативну трактування. За його словами, у документі про жодну заборону криптовалют не йдеться.

На тлі критики законопроекту з боку криптоспільства Держдума перенесла слухання про майнінг криптовалют на 2023 рік. Аксаков при цьому не виключив появу нової редакції документа.

1.6. Використання криптовалют з початком збройної агресії РФ

Відтоді як росія розпочала повномасштабне вторгнення в Україну в лютому, групи, які підтримують російську армію в Україні, зібрали криптовалюту на щонайменше 4 мільйони доларів. Відповідно до аналізу компаній Chainalysis, Elliptic і TRM Labs, які займаються відстеженням криптовалют, а також дослідників Binance, найбільшої у світі біржі криптовалют, одержувачі включають воєнізовані групи, що пропонують боєприпаси та обладнання, військових підрядників і виробників зброї. Цей потік коштів, часто до офіційно санкційних груп, не має жодних ознак зменшення та може навіть прискорюватися: лише за останні два місяці Chainalysis відстежила фінансування російських військових угруповань у розмірі приблизно 1,8 мільйона доларів США, що майже дорівнює 2,2 мільйона доларів, які було виявлено групами, отримані за п'ять попередніх місяців.

«Наша мета – ідентифікувати всі крипто-гаманці, які використовують російські військові групи, і людей, які їм допомагають; знайти, вилучити та заблокувати всю цю діяльність, яка допомагає купувати кулі, боєприпаси цієї окупації», – каже Сергій Кропива, який донедавна був заступником кіберполіції України та радником генпрокурора країни. «Завдяки тісній співпраці таких компаній, як Chainalysis і Binance, ми можемо побачити всі гаманці, залучені в цю злочинну діяльність, ці грошові потоки мільйонів доларів. Але ми, на жаль, бачимо, що передача триває весь час».

В окремих звітах компанії з відстеження криптовалют та дослідницька група Binance відстежували пожертви на військові дії Росії, які дуже часто починалися з публічних публікацій у додатку для обміну повідомленнями Telegram із закликом до краудфандингу. Наприклад, Chainalysis знайшов дописи в Telegram від таких організацій, як проросійські медіа-сайти «Рибар» і «Південний фронт», а також воєнізоване угруповання «Русич», яке має зв'язки з сумнозвісною групою найманців Вагнера – усі адреси розміщення пожертв у криптовалюті в Telegram. Ці дописи повідомляли підписникам, що зібрані там гроші будуть використані на все: від збройових безпілотників до радіостанцій, аксесуарів для гвинтівок і бронежилетів. В іншому випадку Chainalysis вказує на збір коштів групою під назвою Project Terricon, яка намагалася продати на аукціоні NFT для підтримки проросійських ополченців у

Східній Україні, хоча NFT були видалені з ринку, на якому вони розміщувалися, до того, як було зроблено будь-які ставки.

Команда розслідувачів Binance у своєму власному звіті виявила, що з лютого російським військовим групам було направлено криптовалюту на загальну суму 4,2 мільйона доларів. Групи, названі в дослідженні, не повністю збігаються з групами, названими у звіті Chainalysis, що свідчить про те, що загальне фінансування може бути набагато більшим, ніж загальне фінансування Binance або Chainalysis. Binance, наприклад, вказує на проросійську групу «культурної спадщини», відому як MOO Veche, яка проводила збори коштів на військову техніку, подібну до тієї, яку фінансують групи, позначені Chainalysis. У той час як Binance, TRM Labs і Elliptic називають MOO Veche одним із головних джерел збору коштів, Elliptic відстежила 1,7 мільйона доларів криптопожертвувань для групи, що набагато більше, ніж інші дослідники.

Інші організації, які Binance помітили, збираючи гроші за допомогою криптовалютного краудфандингу в Telegram, включають проросійські націоналістичні групи Save Donbas і REAR, а також російський виробник зброї Lobaev, який безпосередньо збирав пожертви на платформі. Ще одна група, відома як Romanov Light, збір коштів якої помітили TRM Labs і Elliptic, стверджувала, що збирає криптовалюту для російського спецназу. Згідно з даними Elliptic, Romanov Light зібрав пожертвувань на суму \$330.000, які вони повідомили донорам, що витратили на військове обладнання, як-от аксесуари до зброї, ліхтарики та бронеplastини.

Незважаючи на відносну ясність усього цього фінансового відстеження, перешкодити криптовалюті продовжувати підтримувати неспровоковане вторгнення росії в Україну було непросто. Біржі можуть блокувати або заморожувати кошти в пунктах їх обміну на традиційну валюту. Але згідно з даними Chainalysis, більшість криптокоштів, зібраних групами, були переведені в готівку через те, що компанія називає «високоризиковими» російськими біржами, майже без запобіжних заходів проти злочинного відмивання грошей. У попередніх звітах Chainalysis називав Chatex, Suex і Garantex прикладами тих російських шахрайських бірж – усі вони вже потрапили під санкції Заходу через їх широке використання злочинцями. Chatex і Garantex не відповіли на запит WIRED про коментарі. Suex більше не має загальнодоступного веб-сайту.

Однак не кожна біржа, яка служила банкоматом для російського військового краудфандингу, розміщена в росії. Аналітики блокчейну, які спілкувалися з WIRED, вказали на сім інших обмінних сервісів, деякі з яких розміщені в Індії та Китаї, які отримували кошти від проросійських груп, яких вони відслідковували, хоча вони відмовилися офіційно назвати їх, частково тому, що суми цих коштів в більшості випадків становили однозначні тисячі або менше.

Проте в одному показовому прикладі того, наскільки важко запобігти цим виведенням готівки, аналітики побачили, як MOO Veche відправляє біткойни на суму понад \$150.000 на біржу, розміщену в

інфраструктурі китайської біржі криптовалют Huobi – «вкладеної» біржі, яка, по суті, використовує Huobi як свою торгову платформу. Але будь-яка відповідальність, яку Huobi могла нести за блокування або заморожування цих коштів, була ускладнена іншою невідомою посередницькою службою, через яку аналітики бачили, як переміщуються гроші перед входом у службу, розміщену на Huobi. Коли WIRED звернувся до Huobi за коментарем, він написав у своїй заяві, що в нього є процес «знай свого клієнта», «який максимально гарантує, що джерело коштів наших клієнтів є надважливим».

Binance, зі свого боку, каже, що його біржові рахунки також використовувалися чотирма групами, які вона відстежувала, і отримали криптовалюту на суму понад \$208.000. Він повідомляє WIRED, що заморозив усі чотири облікові записи, які виявив. «Ми гарантуємо, що цивільні особи не зазнають жодної шкоди в результаті збору коштів, який відбувається в цих екстремістських просторах» – каже Дженніфер Хікс, яка керує групою розвідки та розслідувань Binance. «Коли криптовалютні біржі знають, що відбувається щось незаконне, що призведе до подібних кінетичних ефектів у реальному світі, біржа зобов'язана зупинити це якомога швидше».

Навіть коли біржі відстежують криптовалюту, надіслану від санкційних груп, таких як ці проросійські фандрайзери, ці брудні гроші не завжди буде легко виявити, попереджає Тібо Мадлін, який проводить дослідження в Elliptic. Він каже, що все частіше бачить, як російські джерела незаконних коштів використовують «мости» або «обмін монет» – послуги, які дозволяють легко обмінювати одну криптовалюту на іншу, часто не пропонуючи жодної ідентифікаційної інформації, як методи відмивання грошей.

Він спостерігав за зростанням популярності цих інструментів серед чорних ринків DarkNet та користувачів кіберзлочинців, і очікує, що те саме станеться з тими, хто прагне відмити незаконне фінансування зброї. «Трохи рано говорити остаточно. Але те, що ми бачимо, полягає в тому, що це, ймовірно, стане більшою проблемою» – каже Медлін. «Вони, ймовірно, віддзеркалюють методологію, яку бачать користувачі сервісів DarkNet, уможливлючи масштабне відмивання грошей і потенційно ухилення від санкцій».

Мільйони доларів криптовалютного фінансування російських військ можуть бути найменшою проблемою України у війні, де росія кинула мільярди на свої сили вторгнення. Варто зазначити, що Україна також значно випередила росію за криптовалютою: за підрахунками Elliptic, український уряд зібрав понад 77 мільйонів доларів у вигляді пожертвуваних криптовалют з початку війни. Але цього слід було очікувати, враховуючи широку підтримку Заходом України після неспровокованої агресії росії та глобальних санкцій, накладених на росію. І навіть менша сума криптовалют, яку зібрали російські сили, демонструє постійний потенціал

криптовалюти для обходу цих санкцій і надання ще одного фінансового порятунку для російської військової машини.

«Це не те, що росія купує нові танки на ці гроші. Вони платять за тепловізори та БПЛА», – каже Ендрю Фірман, дослідник Chainalysis, який займається санкціями. Але будь-яка сума грошей, яку вони отримують на посилення свого спорядження, матиме вплив». І незважаючи на все світло, яке можуть пролити криптовалютні трейсери на це фінансування – і на всі зусилля Заходу зупинити це – криптовалютний потік у військову скриню росії продовжується.

ВИСНОВКИ ДО РОЗДІЛУ 1

Таким чином, роль криптовалюти в цій війні дійсно важлива, але неоднозначна. З одного боку, величезні суми пожертв допомагають українській армії та постраждалим, а з іншого – відсутність належного контролю дає змогу ворогу зловживати віртуальними активами та знаходити можливості для відмивання коштів і обходу санкцій.

Однак є перспективи впровадження механізмів запобігання незаконним угодам із використанням віртуальних активів, які мають бути втілені у Законі МіСА. У зв'язку із цим важливо віднайти баланс регулювання, що не суперечитиме самій природі блокчейну, але водночас створити запобіжники для таких ситуацій, яку наразі маємо із росією.

Криптовалюти, такі як Bitcoin, Ethereum, та інші, мають потенціал стати майбутнім фінансовим інструментом, забезпечуючи швидкі, безпечні та незалежні транзакції.

Безпека є ключовим аспектом використання криптовалют. Технології, такі як шифрування та блокчейн, забезпечують високий рівень безпеки та захисту фінансових активів.

Анонімність є важливим фактором для багатьох користувачів криптовалют. Деякі криптовалюти, наприклад Monero або Zcash, надають розширені функції приватності, дозволяючи здійснювати анонімні транзакції.

Криптовалюти можуть використовуватися для переказу коштів між країнами без необхідності проміжних фінансових посередників. Це сприяє зручності та зниженню комісійних витрат.

Розумний контракт, що базується на блокчейні, може відкривати нові можливості для автоматизації та безпечності угод, а також для створення децентралізованих додатків та платформ.

Регулювання криптовалют є актуальною темою, і багато країн виробляють свої правила та політику в цьому напрямку. Розумний підхід до регулювання може сприяти розвитку криптовалютного сектору та забезпечити захист інвесторів.

Використання криптовалют може мати вплив на традиційну фінансову систему, банківську сферу та глобальну економіку. Це викликає як можливості, так і ризики, і вимагає обережного вивчення та аналізу.

Враховуючи ці тези, використання криптовалют має потенціал змінити спосіб функціонування фінансової системи, забезпечуючи широкі можливості для інновацій та фінансової свободи. Однак, важливо пам'ятати про ризики, пов'язані з криптовалютами, і дотримуватися найкращих практик безпеки та обережності.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Розкрийте поняття – криптовалюта.
2. Розкрийте поняття – блокчейн.
3. Розкрийте поняття – майнер.
4. Розкрийте поняття – криптобіржа.
5. Розкрийте поняття – токен.
6. Розкрийте поняття – NFT.
7. Розкрийте поняття скорочення – BTC.
8. Які бувають види криптогаманців?
9. Розкрийте особливості використання «холодних» криптогаманців.
10. Розкрийте особливості використання «гарячих» криптогаманців.
11. Розкрийте особливості використання «мобільних» криптогаманців.
12. Розкрийте зазальну схему майнінгу криптовалют.
13. Які основні закони регламентують ринок криптовалют в Україні?
14. Які основні закони регламентують ринок криптовалют в рф?
15. Які є особливості використання криптовалют з початком збройної агресії рф 2022 року?

РОЗДІЛ 2

ОСОБЛИВОСТІ ВИКОРИСТАННЯ КРИПТОВАЛЮТ В ФАХОВІЙ ДІЯЛЬНОСТІ

В розділі розглядаються питання введення валюти в криптосистему, використання різноманітним криптогеманців та криптоміксерів, питання виводу грошей з криптосистеми. Особлива увага приділена питанням забезпечення кібербезпеки.

2.1. Особливості купівлі криптовалют

Є кілька способів купити криптовалюту, ці способи розглянуті нижче.

Біржі криптовалют. Ви можете зареєструватися на біржах криптовалют, таких як Binance, Bitfinex, Coinbase і т.д., і купити криптовалюту через банківський переказ або кредитну картку.

Криптовалютні банкомати. В Україні є кілька криптовалютних банкоматів, де ви можете купити криптовалюту за готівку. Деякі з них знаходяться у торгових центрах та магазинах.

Обмінні пункти. Крім бірж криптовалют, є також обмінні пункти, які пропонують криптовалюту за готівку або банківський переказ. Деякі з них можуть також пропонувати послуги продажу криптовалют та зворотного обміну криптовалют на фіатні гроші.

Приватні продавці. Ще один спосіб купити криптовалюту – це звернутися до приватних продавців, які продають криптовалюту через соціальні мережі та інші платформи. Однак, при покупці у приватних продавців слід бути обережним та використовувати лише надійні та перевірені джерела.

Перед покупкою криптовалюти рекомендується ознайомитися з правилами та вимогами кожного з перерахованих способів, а також з обмеженнями, якщо такі є. Також варто переконатися, що ви розумієте ризики, пов'язані з криптовалютою, і маєте достатню інформацію про те, як зберігати та використовувати криптовалюту.

2.1.1. Поповнення криптогеманця кредитною картою

Сервіс обміну криптовалют Binance. Створено 2017 року, у січні 2018 року сервіс став найбільшим в світі за обсягами торгів (рис. 2.1). Компанію засновано у Китайській Народній Республіці (КНР), але згодом вона перенесла свої сервери та штаб-квартиру до Японії після заборони урядом КНР торгівлі криптовалютами у вересні 2017 року.

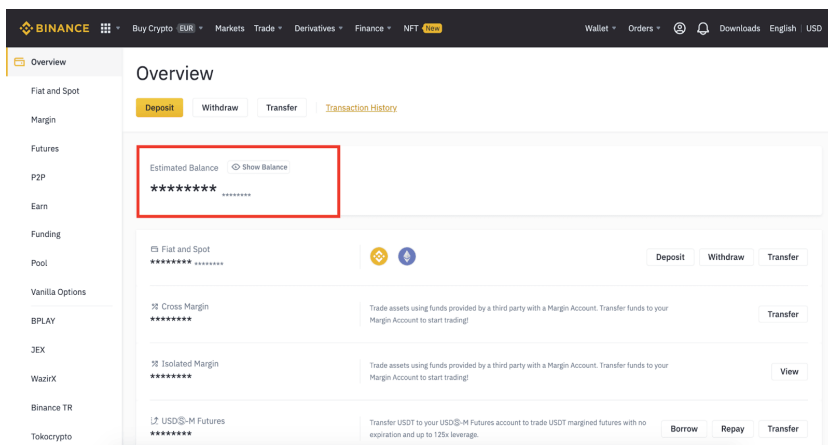


Рисунок – 2.1 Зовнішній вигляд інтерфейсу додатку Binance

До березня 2018 року компанія створила офіси в Тайвані. У березні 2018 року після введення більш жорстких норм в Японії та Китаї Binance заявили про наміри відкрити офіс на Мальті.

У квітні 2018 року Binance підписали меморандум про взаєморозуміння з урядом Бермудських островів. За кілька місяців аналогічний меморандум було підписано з Мальтовою фондовою біржею для розробки платформи електронної торгівлі.

У 2019 році компанія оголосила про створення Binance Jersey, незалежної від своєї материнської Binance.com, з метою розширити свій європейський вплив. Технічна база нового сервісу розташована в Джерсі і пропонує пари «фіат-криптовалюта», включаючи євро та британський фунт.

У січні 2019 року Binance оголосили, що співпрацює з платіжним сервісом Ізраїлю Simplex, що дозволяє придбання криптовалюти дебетовими та кредитними картками, включаючи Visa та Mastercard.

7 травня 2019 року у Binance виявили, що стали жертвою «масштабного порушення безпеки», в ході якого хакери вкрали 7.000 біткоїнів на суму близько 40 мільйонів доларів США. Сайт зобов'язався відшкодувати клієнтам втрати через захищений фонд активів.

У 2021 році торговельний майданчик зіткнувся з наполегливістю світових фінансових регуляторів, які вимагали обов'язкової верифікації акаунтів користувачів для кращого захисту їхніх активів та боротьби з фінансовими злочинами. 4 листопада 2021 року на Binance почав роботу продукт Auto-Invest, автоматичне інвестування у криптовалюту.

У квітні 2022 року підрозділ російської фінансової розвідки зустрівся в московії з регіональним главою Binance Глібом Костаревим. росіяни хотіли, щоб компанія передала дані клієнтів (імена та адреси), щоб

допомогти росіянам «боротися зі злочинністю». Агенція росфін намагалася відстежити перекази на мільйони доларів у біткойнах, зібраних Олексієм Навальним. Навальний, якого росфінмоніторинг додав до списку терористичних організацій, заявив, що пожертви було використано для розслідування корупції в уряді путіна. Костарєв заявив, що він «не мав великого вибору» в цьому питанні.

У березні 2023 року Binance в рамках десятого пакета санкцій ЄС проти росії заборонила росіянам купувати й продавати долари та євро через свій p2p-сервіс.

Binance діє як сукупність національних компаній, кожна з яких діє лише на обмеженій території і несе відокремлену відповідальність. Для окремих компаній у різних країнах діють різні юридичні норми, отримуються різні ліцензії. У більшості випадків вони передбачають надання послуг зі зберігання, торгівлі та обміну цифровими активами. При цьому станом на грудень 2022 року у жодній з країн Binance не має ліцензії на біржову діяльність.

21 лютого 2020 року MFSA (Malta Financial Services Authority) опублікувало публічну заяву, у якій спростувало повідомлення ЗМІ, нібито Binance є «криптовалютна компанія, що базується на Мальті». У заяві вказувалось, що Binance не має дозволу від MFSA працювати у сфері криптовалют.

6 листопада 2019 року віце-прем'єр-міністр України, міністр цифрової трансформації України Михайло Федоров повідомив, що на основі меморандуму до кінця року Binance мала запрацювати в Україні. Також про перемовини з Binance повідомив секретар Національної інвестиційної ради України, голова фракції «Слуга народу» Давид Арахамія.

7 листопада 2019 у Binance оголосили про відкриття гривневого шлюзу через Advcash.

На початку 2020 року Binance відкрили рахунок в українському банку. 20 липня 2020 року Binance оповістили, що додали шлюз для української гривні.

Верифікація на Binance обов'язкова, без її проходження функції депозиту та виводу активів недоступні. Система працює в 2х режимах: стандарт та профі.

Стандарт – заповнення стандартної форми достовірними особистими даними, прикріплення сканів документів і селфі користувача. Крім того, для завершення реєстрації потрібно завантажити додаток Binance і виконати ряд простих рухів на камеру (поворот голови, відкрити рот і т.д). Дозволяє виводити до 100 біткойнів на добу.

Профі – потрібно пройти співбесіду із співробітником Binance. Дозволяє необмежений вивід.

Сервіс обміну криптовалютою MetaMask. Metamask є одним з найпопулярніших сервісів криптогаманця та обміну криптовалют на основі блокчейну Ethereum. Він є розширенням для веб-переглядачів, таких як

Google Chrome та Mozilla Firefox, та дозволяє користувачам взаємодіяти з децентралізованими додатками (DApps – Decentralized Application) та здійснювати транзакції на основі Ethereum (рис. 2.2).

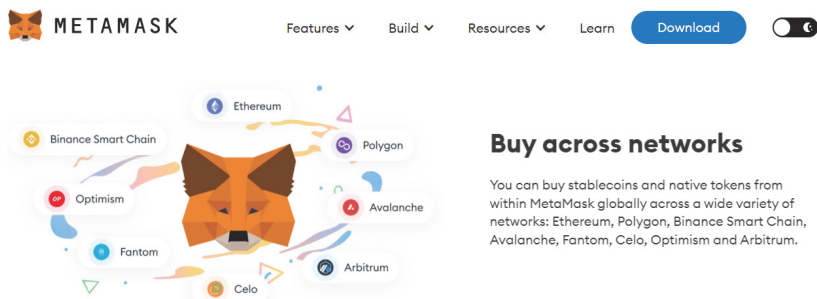


Рисунок – 2.2 Сайт криптогаманця MetaMask.

Основні функції та можливості Metamask включають наступне:

Гаманець Ethereum: Metamask дозволяє створювати та керувати Ethereum-гаманцями, де ви можете зберігати свої криптовалюти (наприклад, Ether-ETH) та ERC-20 токени (стандартні токени, що базуються на блокчейні Ethereum).

Обмін криптовалютою: Metamask інтегрований з різноманітними обмінними сервісами, які дозволяють користувачам обмінювати свої криптовалюти безпосередньо з гаманцем. Це дозволяє швидко та зручно обмінювати криптовалюти прямо зі свого Metamask-гаманця.

Взаємодія з DApps: Metamask дозволяє вам взаємодіяти з різноманітними децентралізованими додатками, які побудовані на блокчейні Ethereum. Ви можете використовувати Metamask для доступу до DApps (Decentralized Application) виконання розумних контрактів, участі у ICO (Initial Coin Offering – ініціальні монетні пропозиції) та багато іншого.

Безпека та приватність: Metamask захищає ваші приватні ключі та особисту інформацію шляхом збереження їх безпосередньо на вашому пристрої, а не на серверах. Ви отримуєте повний контроль над своїми криптовалютами і маєте можливість налаштовувати рівень безпеки за допомогою пароллю та інших заходів захисту.

Керування різними мережами: Metamask дозволяє вам переключатися між різними мережами Ethereum, такими як основна мережа (Mainnet), тестові мережі (наприклад, Ropsten, Rinkeby) та приватні мережі. Це дає можливість розробникам та користувачам тестувати свої додатки або використовувати альтернативні блокчейн-мережі.

Загалом, Metamask надає зручний інтерфейс для взаємодії з екосистемою Ethereum. Він дозволяє користувачам зберігати, обмінювати та використовувати криптовалюти та брати участь у децентралізованому фінансовому середовищі.

Сервіс обміну криптовалютою Huobi. Huobi є однією з провідних криптовалютних бірж у світі, яка заснована в 2013 році, Huobi надає послуги обміну, торгівлі та зберігання криптовалют для користувачів з усього світу (рис. 2.3). Ось деякі ключові аспекти та функціональні можливості Huobi:

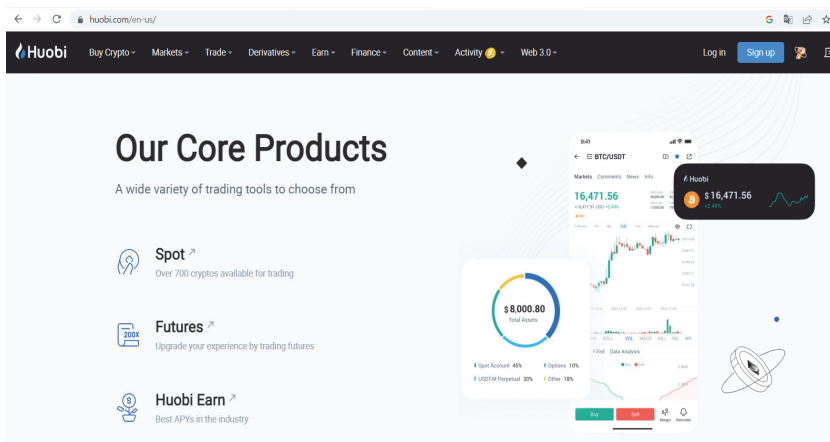


Рисунок – 2.3 Сайт сервісу для обміну криптовалют Huobi

Торгівля криптовалютами: Huobi пропонує широкий спектр торгових пар, включаючи криптовалюти як Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Litecoin (LTC) та багато інших. Користувачі можуть використовувати Huobi для купівлі та продажу криптовалют за ринковими цінами.

Маржева торгівля: Huobi надає можливість маржевої торгівлі, що дозволяє користувачам використовувати позики для збільшення своїх торгових можливостей. Користувачі можуть використовувати позики для відкриття позицій на купівлю або продаж криптовалют з підвищеним фінансовим плечем.

Ф'ючерси та опіони: Huobi також надає ф'ючерси та опіони на криптовалюти. Це дає можливість користувачам здійснювати угоди на майбутні ціни криптовалют і захищати свої позиції від ризиків коливання цін.

Сховище активів: Huobi забезпечує послуги зберігання криптовалют, які допомагають користувачам зберігати свої активи в безпечному середовищі. Вони використовують різні заходи безпеки, включаючи холодні гаманці та двофакторну автентифікацію, для захисту активів користувачів.

Додатки та інтеграції: Huobi має мобільні додатки для iOS та Android, що дозволяють користувачам здійснювати торгівлю та отримувати доступ до своїх активів у режимі реального часу. Крім того,

Huobi також надає API (Application programming interface) для інтеграції з іншими сервісами та програмним забезпеченням.

Міжнародні операції: Huobi має представництва та обслуговує клієнтів у багатьох країнах світу. Вони надають підтримку різних мов і валют, що робить їх доступними для глобальної аудиторії.

Варто зазначити, що криптовалютні біржі, включаючи Huobi, підлягають законодавству та регуляції у країнах, де вони надають свої послуги. Переконайтеся, що добре розумієте правила та обмеження, пов'язані з використанням біржі, перш ніж використовувати її для обміну та торгівлі криптовалютами.

Huobi, як біржа, зазвичай вимагає від користувачів проходження процесу верифікації та надання особистої інформації для дотримання вимог з протидії відмиванню грошей (AML – Anti-Money Laundering) та забезпечення безпеки користувачів.

Проте, для збереження анонімності під час використання Huobi, можна вжити деякі заходи:

Використання псевдоніму: При реєстрації на Huobi ви можете використовувати псевдонім або нікнейм, щоб не розголошувати свої особисті дані. Зробіть вибір унікального псевдоніма, який не пов'язаний з вашою особистістю.

Використання анонімних електронних адрес: Використовуйте анонімні електронні адреси, наприклад, тимчасові електронні адреси або адреси, які не містять особистої інформації, при реєстрації на Huobi. Це може допомогти уникнути пов'язаності між вашим аккаунтом на біржі та особистою інформацією.

Використання VPN (Virtual Private Network): Використання віртуальної приватної мережі може допомогти зберегти вашу приватність та анонімність. VPN дозволяє шифрувати ваше з'єднання та приховувати вашу реальну IP-адресу, що робить важчим відстеження вашої активності в Інтернеті.

Використання децентралізованих бірж: Замість централізованих бірж, таких як Huobi, ви можете розглянути використання децентралізованих бірж (DEX), де не потрібна верифікація користувачів і не вимагається надання особистої інформації. DEX дозволяють вам зберігати контроль над вашими приватними ключами і торгувати напряму з вашого гаманця.

Децентралізована біржа (DEX) – це платформа для обміну криптовалютою, яка працює на основі технології блокчейн та не вимагає посередництва централізованих посередників, таких як традиційні банки або фінансові інституції. DEX дозволяє користувачам обмінюватися криптовалютами без потреби довіряти свої кошти третім особам, оскільки управління активами здійснюється безпосередньо з їх криптогаманцями (рис. 2.4).

Основні риси та переваги децентралізованих бірж:

Контроль над приватністю: Децентралізовані біржі не зберігають особисті дані користувачів, такі як ім'я, адреса або ідентифікаційні

документи. Це забезпечує більшу приватність та анонімність під час проведення торгів.

Контроль над активами: Користувачі мають повний контроль над своїми криптовалютними активами, оскільки вони зберігаються у їх власних гаманцях, а не на біржі. Це зменшує ризик втрати коштів через вторгнення або крадіжку.

Відсутність посередників: У децентралізованих біржах відсутні посередники, що забезпечує прямий обмін між користувачами без необхідності передавати кошти третім особам. Це зменшує комісійні витрати та час, пов'язаний з виконанням операцій.

Відкритість та прозорість: Більшість децентралізованих бірж працюють на блокчейн-платформах, які забезпечують відкритість та прозорість операцій. Історія торгів, ордери та інші дані доступні для перевірки в блокчейні, що забезпечує довіру до системи.

Відсутність цензури: Децентралізовані біржі не контролюють та не фільтрують торгові пари або операції. Вони надають волю користувачам вибирати, які активи обмінювати та з ким проводити операції.

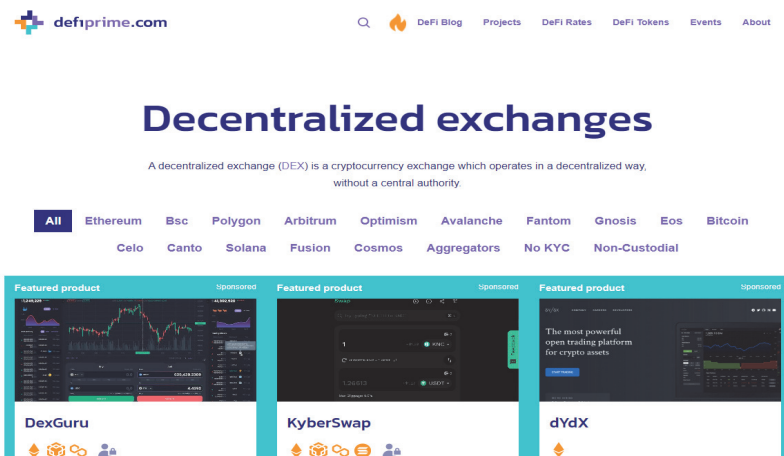


Рисунок 2.4 – Сайт децентралізованої біржі defiprime.com

Деякі приклади децентралізованих бірж включають Uniswap, SushiSwap, PancakeSwap, Kyber Network, 1inch та інші. Кожна з них має свої особливості та функціонал, але загальний принцип роботи полягає в безпосередньому обміні активів між користувачами на основі умовних контрактів та ліквідності, що надають учасники мережі.

Важливо пам'ятати, що деякі заходи анонімності можуть мати обмежену функціональність або здатність досягти повної безпеки. Перед

використанням будь-яких анонімних методів варто ретельно оцінити ризики та вимоги безпеки.

Варто використовувати анонімні крипто-гаманці.

Використання анонімних крипто-гаманців. Це такі онлайн гаманці від платіжних систем, у яких під час реєстрації та використання гаманця не потрібно вказувати будь-які особисті дані та надавати документи для підтвердження особи, тобто не потрібна верифікація особистості.

KYC (Know Your Customer) – у перекладі з англійської означає «Знай свого клієнта», процедура верифікації особистості користувачів у різних онлайн сервісах (працюючих з грошима або криптовалютою), при якій кожен користувач повинен надати інформацію про себе та документи, що підтверджують цю інформацію (паспорт, права водія, дані про прописку, виписки з банку).

Топ анонімних гаманців без верифікації: *Guarda Wallet, Metamask, Ledger, Trezor, Payeer, Jaxx, AdvCash, MyEtherWallet*. В прикладі наведений гаманець *Guarda Wallet*, оскільки він має розширення для Chrome, робочий стіл для Mac OS, Windows, Linux, додатки для Android та iOS (рис. 2.5). Також він мультивалютний, тобто підтримує різні криптовалюти такі як: Binance Coin BNB, Біткоїн BTC, Bitcoin Cash BCH, Bitcoin Gold BTG, Біткоїн SV BSV та інші.

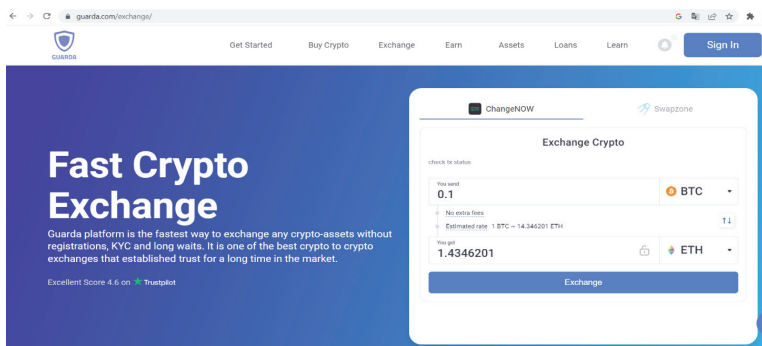


Рисунок – 2.5 Сайт анонімного криптогаманця *Guarda Wallet*

Для створення достатньо перейти по посиланню на сайті та створити пароль, після створення пароллю отримуємо готовий криптогаманець.

2.1.2. Поповнення криптогаманця через термінали самообслуговування

Для пошуку терміналів самообслуговування, призначених для купівлі та продажу біткоїнів, можна використовувати спеціалізовані сайти та додатки, наприклад:

Coin ATM Radar – на цьому сайті можна знайти найближчі біткоїн-термінали, у тому числі в Києві. Для цього потрібно ввести адресу або поставити мітку на карті.

MyCelium – це мобільний додаток, який дозволяє знайти найближчі біткоїн-термінали на карті. Програма доступна для пристроїв на Android та iOS.

Bitcoin ATM Map – це ще один сайт, на якому можна знайти найближчі біткоїн-термінали у Києві та інших містах. Для цього потрібно вибрати країну та місто (рис. 2.6).

Конкретна адреса терміналу самообслуговування для обміну біткоїну в конкретному місті може змінюватися з часом, тому краще використовувати спеціалізовані ресурси для пошуку біткоїн-терміналів.

Криптомат Bitcoin ATM – Shitcoins.club. Знаходиться за адресою: вул. Антоновича, 176, Київ, 03150 (Ocean Plaza) на 0 поверсі поблизу ліфту (рис. 2.7). Отримання грошових засобів в даному банкоматі тимчасово призупинено.

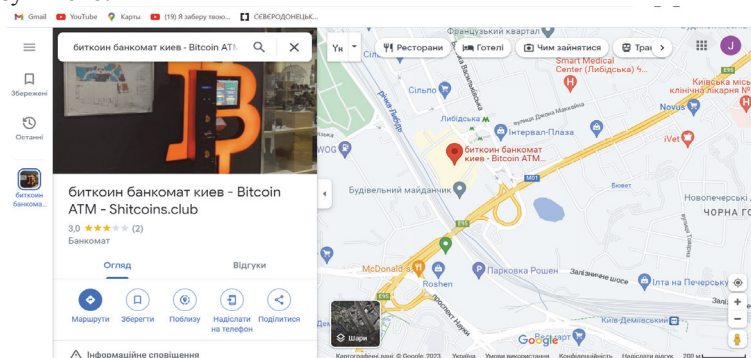


Рисунок – 2.6 Процес пошуку криптомату в м. Києві на карті Гугл

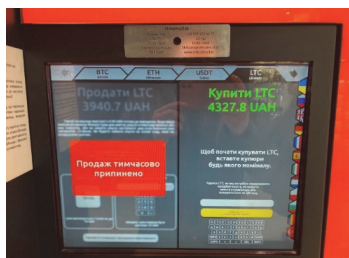
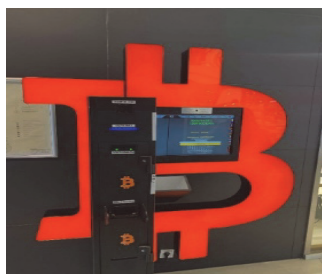


Рисунок – 2.7 Криптомат Shitcoins.club в м. Києві

2.1.3. Поповнення криптогаманця в криптообміннику

Криптообмінник – cashout. Представлений у вигляді орендованого приміщення в м. Києві в невеликому бізнес-центрі в Подільському районі з невеликим штатом співробітників (3–5 осіб), що проводять операції з обміну, використовуючи ПК та мережу інтернет. Вхід до приміщення тільки за попереднім записом, не більше 2-х осіб, кошти для обміну – не менше 3.000 доларів США. Даний офіс представляє собою один з філіалів єдиної системи (компанії), що проводить такі операції, мають власний телеграм канал, сайт (<https://cashout.biz>), де описано всі деталі, деякі з них [19–23]:

Покупка криптовалют. Обслуговуємо в офісі суми від 3.000 \$, суми вище 3.000 USD: – 0,4%.

Продажа криптовалют. Обслуговуємо в офісі суми від 3.000 \$, суми вище 3.000 USD: +1,7%, суми вище 20.000 USD: +1,4%.

Працюють з картками: Приват24, Монобанк, ПУМБ, Райффайзен, Ощадбанк, будь-яка карта Visa/Mastercard.

Криптообмінник – BUY. Знаходиться за адресою: м. Київ, вул. Антоновича, 45, Київ, 02000 (рис. 2.8, 2.9).

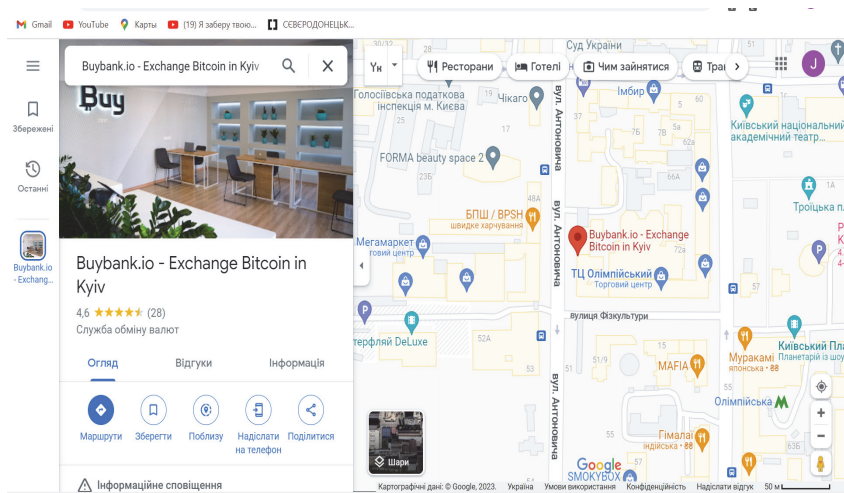


Рисунок – 2.8 Пошук на карті Гугл: криптообмінник – BUY в м. Києві.



Рисунок – 2.9 Криптообмінник – BUU в м. Києві

2.1.4. Купівля криптовалюти іншими способами

Україна має розвинений ринок криптовалют, і є кілька способів, якими фізичні особи можуть купити криптовалюту в Україні. Ось деякі з них:

Криптовалютні біржі: Ви можете зареєструватися на криптовалютній біржі, яка працює в Україні і підтримує обмін національної валюти (гривні) на криптовалюту. Деякі популярні криптовалютні біржі в Україні включають Kuna, BTC Trade UA та Exmo. Вам потрібно буде пройти процес реєстрації та верифікації на біржі, а потім поповнити свій рахунок валютою і купити криптовалюту за поточними ринковими цінами [24–28].

OTC (Over-the-Counter) угоди: OTC-угоди дозволяють вам купувати та продавати криптовалюту безпосередньо з іншими особами, обходячи публічні біржі. Це може бути вигідним випадком, якщо ви шукаєте більш гнучкі умови, обсяги або анонімнішу торгівлю. В Україні є OTC-платформи, які забезпечують такі угоди між фізичними особами (рис. 2.10, 2.11).

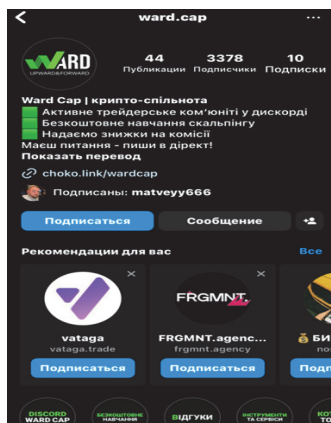
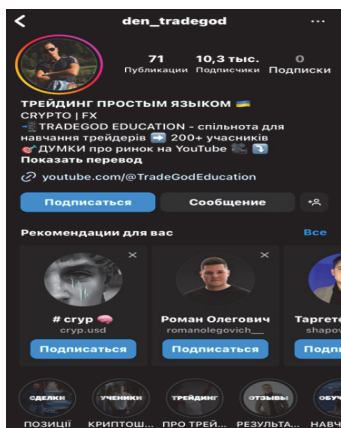


Рисунок 2.10 Приклад Телеграм-каналу приватного валютного трейдера

Персональні угоди: Ви також можете укласти угоди безпосередньо з іншими фізичними особами, які мають криптовалюту, наприклад, через різноманітні форуми, соціальні мережі або спеціалізовані платформи. У цьому випадку важливо бути обережним і використовувати безпечні методи оплати та забезпечення угоди.

Bitcoin-телеринки: Україна також має ряд Bitcoin-телеринків, які дозволяють вам придбати криптовалюту на місцевих фізичних точках обміну. Ви можете знайти ці телеринки за допомогою онлайн-ресурсів або додатків, які надають інформацію про місця обміну.

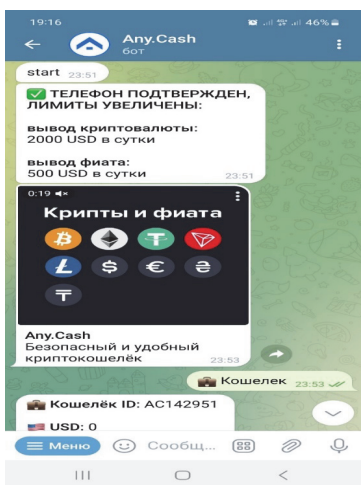


Рисунок – 2.11 Приклад чат-бот каналу Телеграм – купівля криптовалюти

Перш ніж купувати криптовалюту від фізичних осіб, завжди перевіряйте їх репутацію, безпекові заходи та будь-які умови угоди. Додатково, пам'ятайте про необхідність зберігання своїх криптовалютних активів у безпечному гаманці.

2.2. Здійснення фінансових операцій з використанням криптовалют

З використанням криптовалют можна здійснювати різноманітні операції. Ось кілька основних операцій, які можна здійснювати з використанням криптовалют:

Перекази: Криптовалюти дозволяють здійснювати швидкі та безпечні перекази коштів між особами по всьому світу без прив'язки до традиційних фінансових інституцій. Ви можете відправляти криптовалюту до будь-якої адреси гаманця в мережі, і операція буде проведена відразу або за декілька хвилин.

Оплата за товари і послуги: за допомогою криптовалют Ви можете оплачувати товари та послуги в Інтернеті або в реальному житті. Деякі підприємства та онлайн-магазини приймають криптовалюту як засіб платежу. Ви можете сканувати QR-код або ввести адресу гаманця, щоб здійснити платіж.

Торгівля на криптовалютних біржах: криптовалютні біржі дозволяють вам купувати, продавати та торгувати криптовалютами. Ви можете використовувати криптовалюту для торгівлі з іншими криптовалютами або навіть звичайними валютами, такими як долари або євро.

Інвестування: криптовалюти також можна використовувати як інвестиційний актив. Ви можете придбати криптовалюту з метою довгострокового інвестування в очікуванні зростання її вартості.

Децентралізовані фінансові послуги (DeFi): криптовалюти стали основою для розвитку DeFi-протоколів, які надають доступ до різних фінансових послуг, таких як позики, ставки, обмін токенів і т.д., без необхідності залучення посередників.

Додаткові послуги: крім вищезгаданих операцій, існує також широкий спектр інших послуг, які можна здійснювати з використанням криптовалют, таких як створення смарт-контрактів, участь у криптовалютних ICO (Initial Coin Offering), створення власних токенів та багато інших.

Варто пам'ятати, що криптовалюти можуть мати високу волатильність і ризики, пов'язані з безпекою. Перед здійсненням операцій з криптовалютами важливо ретельно досліджувати та розуміти ризики, а також забезпечити безпечне зберігання своїх криптовалютних активів.

2.2.1. Використання анонімних віртуальних кредитних карт

Віртуальна кредитна карта – це електронна версія звичайної пластикової кредитної карти, яку можна використовувати для здійснення онлайн-платежів. Вона не має фізичного носія та номера, який звичайно наноситься на пластикову карту. Замість цього, дані віртуальної кредитної карти, такі як номер карти, термін дії та CVV-код, надсилаються електронним шляхом.

Основна мета віртуальних кредитних карт – забезпечити безпеку під час онлайн-транзакцій. Оскільки вони не мають фізичної форми і не пов'язані з основними рахунками або кредитними лініями, вони можуть бути використані для одноразових або обмежених платежів без ризику витоку основних фінансових даних.

Деякі віртуальні кредитні карти дозволяють користувачам задавати обмеження на суму або час дії карти, що надає додатковий контроль і безпеку під час онлайн-покупок. Вони також можуть бути пов'язані з платіжними системами, такими як Visa або Mastercard, і приймаються в онлайн-магазинах та сервісах, які підтримують ці системи платежів.

Віртуальні кредитні карти зручні для користувачів, які хочуть зберегти свої основні фінансові дані конфіденційними під час онлайн-покупок, або для тих, хто має обмежений доступ до традиційних кредитних карт. Вони дозволяють здійснювати безпечні та контрольовані платежі в Інтернеті.

Анонімна віртуальна кредитна карта PaywithMoon – це фінтех-стартап, який надає сервіс оплати криптовалютами за покупки в Інтернеті. За допомогою PaywithMoon користувачі можуть здійснювати оплату за товари та послуги в режимі онлайн, використовуючи свої криптовалютні гаманці та без необхідності вводити банківські картки або інші особисті дані. Сервіс пропонує свої послуги в більш ніж 160 країнах та має партнерські угоди з понад 250.000 онлайн-магазинів (рис. 2.12).

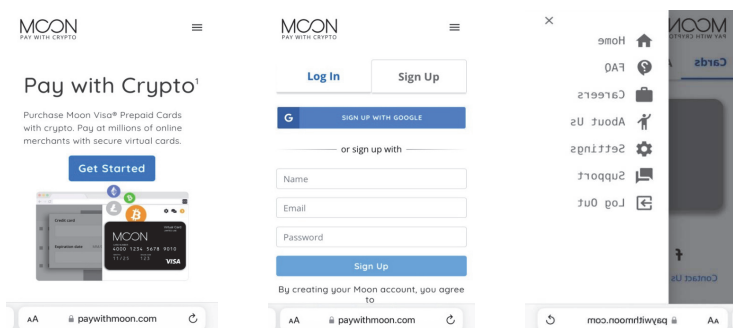


Рисунок – 2.12 Інтерфейс мобільного додатку PayWithMoon

2.2.2. Використання криптоміксерів для підвищення анонімності платежів

Криптоміксери, також відомі як криптовалютні міксери або туманізатори, є сервісами, що надають приватність і анонімність при здійсненні транзакцій з криптовалютами. Вони використовуються для змішування або перемішування криптовалютних транзакцій з метою унеможливлення прослідковування шляху коштів.

Основна ідея криптоміксерів полягає в тому, що вони приймають вхідні криптовалютні транзакції від користувачів і змішують їх з іншими транзакціями, розподіляючи кошти між різними адресами. Це ускладнює відстеження переказів і робить їхнє походження та призначення менш очевидними.

Криптоміксери використовують різні алгоритми і протоколи для забезпечення анонімності. Деякі з них використовують систему мультипідпису, де багато користувачів підписують транзакцію, що робить неможливим визначення окремого походження коштів. Інші використовують розподілені мережі або алгоритми змішування, що роблять аналіз транзакцій складним завданням.

Головна перевага використання криптоміксерів полягає в тому, що вони допомагають зберегти приватність та конфіденційність у сфері криптовалютних транзакцій. Вони можуть бути корисними для тих, хто бажає захистити свою фінансову приватність, уникнути прослідковування або запобігти аналізу своїх фінансових даних.

Варто зазначити, що використання криптоміксерів може мати легітимні та нелегітимні застосування. В деяких юрисдикціях вони можуть бути обмежені або незаконними, оскільки їх використання може сприяти легалізації злочинних коштів. Перед використанням криптоміксера варто ознайомитися з правовими аспектами та дотримуватися законодавства своєї країни.

Біткоїн-міксер (Bitcoin mixer) – це сервіс, призначений для анонімізації, за допомогою якого можна заборонити відстеження своїх транзакцій у біткоїн-мережі. Є додатком або сайтом, що приймають монети користувача і змішує їх з чужими. Відбувається це так: монети дробляться на безліч дрібних частин, потім ці частки довільно перемішуються з частками, що прийшли від інших користувачів (mix – змішувати (англ.)).

Сутність роботи біткоїн-міксерів. Процес мікшування відбувається відповідно до заданого алгоритму. В результаті до адресата приходять саме стільки грошей, скільки потрібно, але складатиметься ця сума з безлічі шматочків, які раніше належали невідомим учасникам (рис. 2.13).

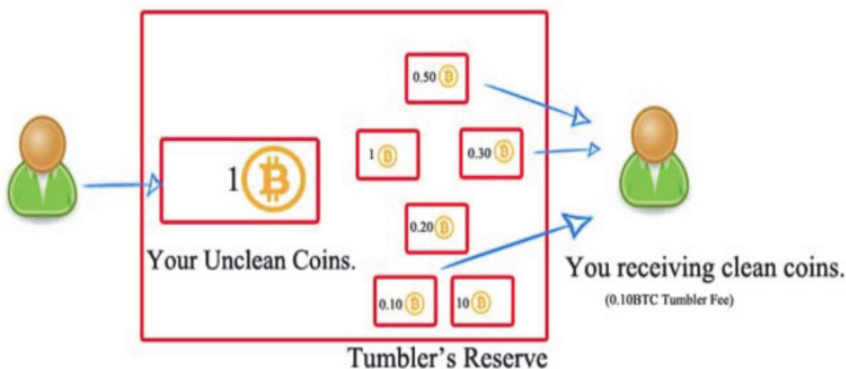


Рисунок – 2.13 Схема роботи криптоміксера

Протягом кількох років біткоїн-міксери використовувалися активно та повсюдно, щоб замітити сліди (наприклад, при виконанні незаконних операцій). Але зараз із ними організована боротьба – доведено, що таким чином дуже легко відмивати гроші. Однак далеко не завжди програми потрібні для нелегальних цілей: часто ними користуються ті, хто хоче убезпечити себе або приховати факт володіння криптовалютою від зловмисників.

Зрозуміло, що всі сервіси беруть комісію за свої послуги. Її розмір залежить як від суми, що відправляється, так і від числа вироблених змішувань (що більше, тим надійніше). В ідеалі жодна частка суми монет, що вийшла, не пов'язана з початковим користувачем.

Bitcoin-міксери поділяються на такі типи:

Централізовані ресурси. До таких належить перше покоління міксерів, зараз вони дещо вийшли з вжитку, хоча кілька сервісів досі залишилося. Принцип полягає в тому, що клієнт відправляє біткоїни, платить комісію, і на вказану адресу надходять монети від іншого користувача на аналогічну суму. Чим більше в системі користувачів та грошей, тим вищий рівень анонімності. Зниження популярності подібних ресурсів частково пов'язане з тим, що при доступі до логів анонімність сильно падає.

Пірингові майданчики. Дозволяють обмінюватися біткоїнами без посередників, безпосередньо контактуючи з іншими користувачами. Імовірність шахрайства при цьому дуже мала. Існує ряд протоколів (CoinSwap, SharedCoin, CoinJoin), які дають можливість кільком клієнтам об'єднатися та створити одну загальну транзакцію, яка здійснюється поетапно, в міру набору необхідної кількості учасників. Ніхто з користувачів не зберігає адреси одержувачів або відправників, цим займається сервер, що перемішує. Ускладнення операції здійснюється шляхом збільшення кількості перемішування поспіль.

Міксери на смарт-контрактах. Як і попередні, є некастодіальними. Проте працюють не так, як попередні – не отримують та не відправляють кошти користувачів за одну транзакцію. Натомість, як тільки користувач надсилає кошти на мікшер, він отримує криптографічний запис, що доводить, що саме він вніс депозит. Потім з нової адреси клієнт може відправити транзакцію мікшеру, яка використовує цей запис для виведення коштів на нову адресу. Клієнт може почекати скільки завгодно перед тим, як виводити гроші.

Останній варіант міксерів також працює спільно з ретрансляторами, які можуть надавати криптовалюту для оплати комісій за транзакцію виведення, гарантуючи, що користувач зможе здійснити виведення без історії транзакцій або підключень до сторонніх сервісів.

Далі наведені зразки популярних криптоміксерів (рис. 2.14).

Міксер	Сайт	TOR	Криптовалюта	Мінімальна сума	Комісія
Coinomize	Coinomize.biz	TOR Link	Bitcoin	від 0,003 BTC	від 1% до 5%
Unjoin	Unjoin.io	TOR Link	Bitcoin	варіюється	від 1 до 3%
CryptoMixer	CryptoMixer.io	TOR Link	Bitcoin	від 0,001 BTC	0.5% + 0.0005BTC
ChipMixer	ChipMixer.com	TOR Link	Bitcoin	від 0,001 BTC	На розсуд користувача
Blindmixer	Blindmixer	-	Bitcoin	від 100 sat	100 sat для сум менше ніж 0,01 BTC. Інші безкоштовно
MixTum	MixTum.io	TOR Link	Bitcoin	от 0,005 BTC	від 4 до 5% + 0,0007 BTC
Anonymixer	Anonymixer.com	TOR Link	Bitcoin	1 sat	від 1% до 2%
Mixer.money	Mixer.money	TOR Link	Bitcoin	від 0,003 BTC	до 4-5% + 0,0007 BTC
Mixtura	Mixtura.money	TOR Link	Bitcoin	від 0,003 BTC	до 5% + 0,0007 BTC

Рисунок 2.14 Порівняльна таблиця відомих криптоміксерів

Криптоміксер Coinomize. Криптоміксер, який не зберігає логи, IP-адреси, інші дані та забезпечує користувачам повну анонімність. Дозволяє відправити змішані монети на кілька адрес (до п'яти) (рис. 2.15).

Особливості: Один із найдешевших сервісів серед аналогів: комісія від 1% до 5% + 0,0003 BTC. Мінімальна сума змішування 0,003 BTC. При надсиланні коштів потрібне одне підтвердження. Можна встановити час затримки змішування, щоб підвищити конфіденційність. Є версія для мережі Tor.

Якщо вибрано кілька адрес отримання, то буде використана випадкова тимчасова затримка для кожного з них, інакше легко буде

відстежити використання мікшера. Сервіс має дуже хороші відгуки в мережі за якісну роботу, зручний інтерфейс та швидкі транзакції.



Рисунок – 2.15 Інтерфейс сайту криптомікшера coinomize.biz.

Криптоміксер UniJoin. Сайт: <https://unijoin.io>. Сервіс використовує для мікшування технологію CoinJoin. Підтримує зараз лише біткоїн, але в планах додати ще ефіріум, лайткоїн, USDT. Не зберігає жодних логів операцій.

Особливості: Комісія від 1 до 3% + комісія мережі. Мінімальна кількість варіюється. Створювати обліковий запис для роботи з мікшером не потрібно.

Інші популярні криптоміксери: Blindmixer, CryptoMixer, ChipMixer, MixTum, Anonymixer, Mixer.money, Mixtura [29–33] .

Якщо розглядати конкретні послуги, то в кожному також можна знайти недоліки. Наприклад, один не дозволяє використовувати розсилку з різних адрес, інший - не дає налаштувати відкладену транзакцію.

На що потрібно в першу чергу звертати увагу:

Репутація. Щоб не втратити монети, потрібно постаратися краще дізнатися про міксер, з яким вирішено взаємодіяти, почитати відгуки на форумах у даркнеті (наприклад, The Hub).

Блокчейн-аналіз для ідентифікації. Деякі з ресурсів для змішування біткоїнів особливим чином позначені, в результаті чого аналітики можуть пов'язати з ними Bitcoin-гаманці клієнтів. Зрозуміло, що в результаті клієнт може бути відстежений. Щоб перевірити, чи позначено ресурс, можна скористатися сайтом walletexplorer.com.

Розмір резерву. Він має бути великим. У разі, якщо транзакція більше, ніж пул монет сервісу, після здійснення мікшування свіжі монети нараховуватимуться частинами.

Швидкість мікшування залежить від обраної криптовалюти та загальної суми транзакції. Після залишення заявки монета пересилається в пул і чекає на підтвердження від майнерів, а потім переміщається на різні гаманці. Скільки гаманців, стільки і транзакцій – отже, розраховувати потрібно щонайменше на 5–6 біткоїн-перекладів за часом. Щоб зв'язок між адресами ще менше відстежувався, застосовується технологія відкладених транзакцій.

Більшість міксерів з метою підтримки конфіденційності не зберігають інформацію довго – максимум 3 діб. Адреса, яка генерується в самому міксері, діє лише добу та підходить виключно для переказів усередині сервісу. Як правило, забороняється приймати інші кошти на ту саму адресу.

Зрозуміло, послуги не вимагають підтвердження особистості і не проводять жодних типів KYC-процедур. Під час операції сервіс видає різні важливі відомості: гарантійний лист, код для підтвердження власності грошей, адресу криптовалютного гаманця – важливо випадково не закрити вкладки з цією інформацією, оскільки вона згодом стане в нагоді для повернення пересланих коштів.

Багато біткоїн-міксерів встановлюють мінімальну суму переказу. Потрібно бути уважними – якщо спробувати відправити суму меншу за нижній поріг, то гроші підуть як пожертвування в рахунок розробників.

Після перемішування є ризик отримати «брудні» BTC – такі, що були задіяні у злочинних справах або вкрадені. Біткоїни, позначені як «брудні», можуть принести проблеми: блокування акаунта на біржі і так далі.

Регулятори різних країн зараз приділяють дуже багато уваги роботі біткоїн-міксерів у рамках боротьби з відмиванням грошей, фінансуванням тероризму та кібер-злочинністю. Це одна з причин того, що сайти періодично закриваються, не витримуючи тиску, блокуються провайдерами та антивірусами.

Нюанси можуть відрізнятись, але в основному це працює так: кошти, які відправляє користувач, змішуються із коштами інших користувачів та самого сервісу, внаслідок транзакції неможливо відстежити в блокчейні.

Міксери стягують комісію, зазвичай, від 1 до 5% + комісія мережі. Її можна регулювати – чим вищі збори, тим сильнішим буде змішування.

Біткоїн міксери – важливий напрямок криптоіндустрії. Адже вже давно стало зрозуміло, що біткоїн не забезпечує достатньої анонімності, скоріше він псевдоанонімний, і правоохоронні органи вже навчилися способом пов'язати певні транзакції та гаманці з реальними особами.

Якщо Ви за стовідсоткову конфіденційність чи сумніваєтеся у походженні отриманих монет, то можете скористатися сервісами, про які розказано – міксери ретельно перемішують цифрові активи різних користувачів, забезпечуючи гідний рівень анонімності. Свої ризики тут теж є, тому не забудьте зважити всі плюси та мінуси перед застосуванням. Також у мережі є сотні шахрайських сервісів або клонів відомих сайтів, цього теж треба остерігатися.

2.2.3. Використання безпечних криптогаманців

Безпечні криптогаманці, відомі також як криптовалютні гаманці, є програмами або пристроями, що забезпечують зберігання, керування та безпеку криптовалютних активів. Вони використовуються для зберігання приватних ключів, необхідних для доступу до криптовалютних ресурсів, таких як баланси та транзакції.

Основна мета безпечних криптогаманців – забезпечити безпеку активів та конфіденційність користувачів. Вони надають захист від крадіжки, хакерських атак та втрати криптовалютних активів. Деякі безпечні гаманці володіють високим рівнем шифрування, багаторівневими автентифікаційними процедурами та можливістю зберігання криптовалютних активів офлайн (так званий «холодний сховище») для додаткової безпеки.

Існують різні типи безпечних криптогаманців:

Апаратні гаманці: Це фізичні пристрої, які зазвичай нагадують USB-накопичувачі або пристрої з вбудованим дисплеєм. Вони забезпечують зберігання приватних ключів в безпечному обладнанні середовищі та можуть бути використані для підпису транзакцій.

Гарячі гаманці: Це програми, які встановлюються на персональні комп'ютери або ноутбуки. Вони надають можливість зберігання приватних ключів в зашифрованому вигляді на комп'ютері користувача. Важливо використовувати надійне програмне забезпечення та забезпечити безпеку свого пристрою.

Мобільні гаманці: Це додатки, що встановлюються на мобільні пристрої, такі як смартфони або планшети. Вони забезпечують зручний доступ до криптовалютних активів, але вимагають обережності щодо безпеки пристрою та резервного копіювання приватних ключів.

Незалежно від типу безпечного криптогаманця, важливо виконувати деякі основні *принципи безпеки*:

- забезпечити безпечне зберігання приватних ключів;
- використовувати сильні паролі та двофакторну автентифікацію;
- робити резервні копії приватних ключів;
- оновлювати програмне забезпечення гаманця та операційну систему.

Вибір безпечного криптогаманця залежить від Ваших потреб, важливо оцінити його функціональність, репутацію, рецензії користувачів та рівень безпеки, перш ніж здійснити вибір [34–38].

Безпечний криптогаманець Electrum – це швидкий та легкий у використанні криптогаманець, що не потребує багато ресурсів. Він використовує віддалені сервери, що опрацьовують найскладніші операції біткойн-системи. Він також дозволяє вам відновити гаманець за допомогою секретної фрази (рис. 2.16).

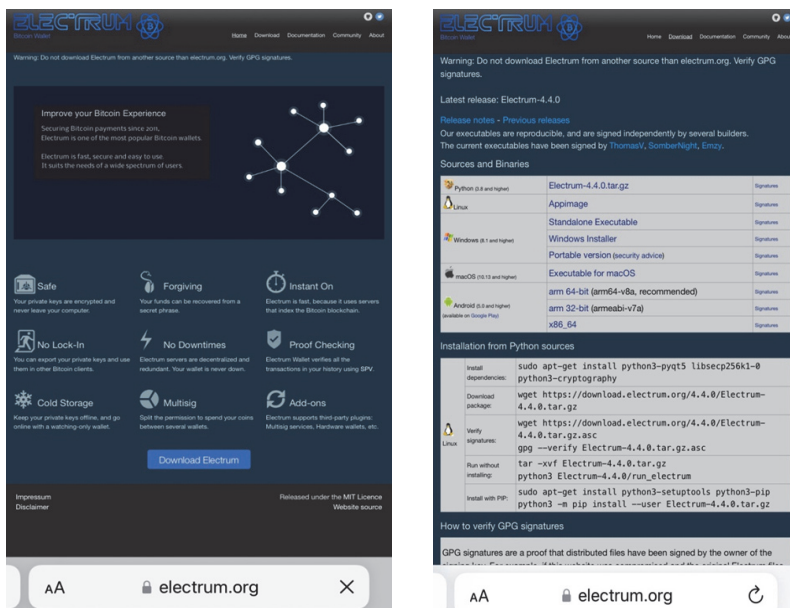


Рисунок – 2.16 Інтерфейс криптогаманця Electrum

Контроль грошей. Цей гаманець дає вам повний контроль над вашими біткоїнами. Це означає, що ніхто не в змозі заморозити чи втратити ваші кошти. Тим не менше, відповідальність за безпеку та резервне копіювання вашого гаманця повністю лежить на вас.

Спрощена перевірка. Гаманець використовує спрощену перевірку транзакцій за допомогою випадкового сервера зі списку. Це означає, що необхідно не так багато довіри до третіх сторін під час перевірки платежів. Однак, це не так безпечно як при використанні повного вузла, такого як Bitcoin Core.

Повна прозорість. Гаманець характеризується відкритим початковим кодом та фіксованою процедурою створення додатку. Це означає, що будь-який розробник у світі може провести аудит коду та впевнитись у тому, що виконуваний код не приховує ніяких секретів.

Двофакторна авторизація. Гаманець можна використовувати в умовах незахищеного середовища. Проте, цей сервіс потребує двофакторної авторизації. Це означає, що для того щоб викрасти ваші біткоїни, потрібен доступ одразу до декількох ваших пристроїв чи рахунків.

Базова конфіденційність. Запобігає шпигуванню за вашими платежами. Гаманець ускладнює шпигування за вашими балансами і платежами за

допомогою ротації адрес. Проте, вам все одно варто щоразу використовувати нову біткойн-адресу, коли ви подаєте запит на оплату.

Гаманець використовує центральні сервери для можливості прив'язки усіх ваших платежів та запам'ятовування вашої IP-адреси.

Гаманець дозволяє вам налаштувати та використовувати Тог в якості проксі для перешкодження прив'язці ваших платежів до вашої IP-адреси зловмисниками чи інтернет-провайдерами.

Повний контроль над комісіями. Цей гаманець дає вам повний контроль над комісіями. Це означає, що він дозволяє змінювати плату після надсилання коштів за допомогою RBF (Replace by fee) або CPFP (Child pays for parent). Цей гаманець також пропонує комісію на основі поточних умов мережі, щоб ваші операції були підтверджені своєчасно, не сплачуючи більше, ніж потрібно.

Анонімна криптовалюта Monero. Monero – криптовалюта з відкритим вихідним кодом, призначена для анонімних грошових транзакцій. На відміну від Біткойна, Monero використовує протокол CryptoNote, завдяки якому відбувається обфускація транзакцій. За даними на грудень 2017 року, Monero входить до десятки криптовалют з найвищою ринковою капіталізацією.

Простий режим. Призначений для найменш технічно підкованих користувачів, які хочуть, щоб використання Monero було максимально простим і швидким. Потрібно просто відкрити гаманець, під'єднатися до віддаленого вузла, відправити/отримати XMR, і все готово!

Просунутий режим. Передбачає всі просунуті функції. Ідеально підходить для досвідчених користувачів Monero, які віддають перевагу повністю контролювати свій гаманець і з'єднання з вузлом. Сторінка продавця дозволяє вам отримувати XMR за ваші товари або послуги.

Сумісність з апаратними гаманцями такими як Trezor і Ledger. Можливість оцінки у фіатній валюті всередині програми. Тепер, щоб дізнатися вартість ваших XMR у фіатній валюті, вам більше не потрібно отримувати актуальну інформацію з інших сервісів. Обрізання блокчейна. Недостатньо місця на диску? Скористайтеся обрізанням і завантажте 1/3 від усього блокчейна.

Верифікація. Настійно рекомендується перевіряти хеші завантаженого архіву. Це дає змогу переконатися в тому, що завантажені вами файли повністю збігаються з файлами, завантаженими групою розробників Monero. Не варто недооцінювати важливість цього кроку, оскільки пошкоджений архів може стати причиною втрати ваших коштів! Завжди слід перевіряти завантажувані вами файли! Завжди перевіряйте завантажувані файли!

Хеші, необхідні для перевірки завантажуваних файлів. Хеші SHA256 перераховані для зручності, список хешів, підписаний GPG (GNU Privacy Guard), розміщено за посиланням getmonero.org/downloads/hashes.txt, його слід розглядати як канонічний, з перевіркою підпису відповідним GPG ключем у вихідному коді.

- Доступні два керівництва, які допоможуть вам у цьому процесі перевірки: виконати верифікацію двійкових файлів Monero CLI/GUI у Windows (для початківців-початківців);

- за допомогою командного рядка виконати верифікацію двійкових файлів Monero CLI/GUI (для досвідчених користувачів).

Допомога та підтримка. Існує керівництво, яке допоможе розібратися з кожним розділом гаманця. Якщо у вас виникнуть питання або вам знадобиться більше інформації, то ви можете просто зв'язатися зі спільнотою. Команду розробників GUI можна знайти, використовуючи #monero-gui або ж зайшовши на сторінку Hangouts, де викладено більш повний список усіх контактів і чатів.

Безпечний криптогаманець Monero CLI. Гаманець з інтерфейсом командного рядка (CLI) з відкритим вихідним кодом, розроблений співтовариством Monero, є повністю безкоштовним у плані використання і підходить для розробників і технічно просунутих користувачів. CLI гаманець забезпечує повний контроль над вашим вузлом Monero і коштами. Його дуже зручно адаптувати під себе, і він містить найрізноманітніші засоби аналізу, а також HTTP і OMQ інтерфейс.

Локальний або віддалений вузол. Ви можете користуватися власною або загальнодоступною копією блокчейна

Tor/I2P транзакції. Забезпечує додатковий рівень анонімності

Вузол початкового завантаження. Під час скачування блокчейна буде використовуватися віддалений вузол. Це дасть вам змогу одразу почати використовувати Monero і переключитися на локальний вузол, після його синхронізації

Сумісність з апаратними гаманцями такими як Trezor і Ledger

RPC гаманець і демон включені в архів

Обрізання блокчейна. Недостатньо місця на диску? Скористайтеся обрізанням і завантажте 1/3 від усього блокчейна

Pay-for-RPC Нова функція дозволяє операторам вузлів отримувати винагороду за використання їхніх вузлів.

Мобільні та легкі гаманці. Cake Wallet, Feather, Monerujo – це мобільні або легкі гаманці. Ці гаманці підключаються до @віддалених вузлів і сканують блокчейн на вашому пристрої, не передаючи ключі вузлам. Вони забезпечують вищу конфіденційність, але вимагають більше часу для виконання синхронізації, оскільки відсутні блоки скануватимуться тільки при повторному відкритті гаманця.

Віддалена синхронізація (спрощений варіант). Гаманці MyMonero, Edge використовують ваш приватний ключ перегляду на віддаленому сервері, який постійно сканує ланцюжок блоків у пошуках ваших транзакцій. Цим типом гаманців можна скористатися без очікування завершення процесу синхронізації, але ваша конфіденційність може бути під загрозою, особливо, якщо ви не контролюєте віддалений сервер.

Апаратні гаманці. Апаратні гаманці – це криптографічно захищені пристрої, які допомагають зберегти ваші монети в безпеці. Наразі Monero підтримується Ledger Nano S / X і Trezor Model T.

2.3. Особливості виведення коштів з криптовалютної системи

Існує кілька шляхів для виведення коштів з криптовалютної системи. Основний метод виведення залежить від того, як ви зберігаєте свої криптовалютні активи та в якій формі вони знаходяться. Нижче перераховані декілька загальних способів виведення коштів:

Обмін на фіатні валюти: Ви можете скористатися криптовалютною біржею, що підтримує обмін на фіатні (традиційні) валюти, такі як долари, євро або інші національні валюти. На біржі ви можете продати свої криптовалютні активи і отримати кошти на свій банківський рахунок.

Виведення на банківський рахунок: Якщо у вас є криптовалютний гаманець, пов'язаний з вашим банківським рахунком, ви можете вивести кошти, переказавши їх на свій банківський рахунок через платіжну систему.

Використання платіжних карток: Деякі криптовалютні послуги пропонують платіжні картки, пов'язані з вашими криптовалютними активами. Ви можете виводити кошти з гаманця на ці картки і використовувати їх для покупок або зняття готівки з банкоматів.

Криптовалютні платіжні системи: Існують різні криптовалютні платіжні системи, які дозволяють виводити кошти в інші криптовалюти або прямо на платіжні картки.

Peer-to-peer (P2P) обмін: Ви можете використовувати платформи P2P для безпосереднього обміну криптовалютами з іншими користувачами. На таких платформах ви можете знайти покупців, які готові купити ваші криптовалютні активи за фіатні гроші або інші криптовалюти.

Перед виведенням коштів важливо ретельно перевірити безпеку вибраного методу та дотримуватися відповідних правил і обмежень, щоб уникнути можливих шахрайств або втрати активів.

2.3.1. Особливості роботи з криптовалютами в Україні

Законодавча база в Україні. На відміну від електронної валюти, біткойн, ефіріум та решта – це віртуальні валюти, які не мають фізичного виразу. Одиницею подібної валюти традиційно є так звані коїни, з англійської – монети; натомість ніяких монет у класичному сенсі не існує. Коїн є зашифрованою інформацією, яку неможливо скопіювати. Сьогодні в світі налічується близько 8300 криптовалют, найпопулярніші – Bitcoin та Ethereum. Донедавна правовий статус криптовалюти визначався виключно як «майно», але Верховна Рада у лютому 2022 року ухвалила закон «Про віртуальні активи», який було покликано легалізувати криптовалютний ринок в Україні [13]. Він набуває чинності з дня внесення та ухвалення змін до Податкового кодексу України. Цьому передувала ціла низка експериментальних законопроектів, серед яких:

- Проект Закону про обіг криптовалюти в Україні №7183 від 06.10.2017 [39];
- Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні №7183-1 від 10.10.2017 [40];
- Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами №2461 від 15.11.2019 [41];
- Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів №4004 від 01.09.2020 [42].

Віртуальні активи. Пояснювальна записка Закону України «Про віртуальні активи» визначала мету закону як надання учасникам віртуальних активів можливості користуватися банківськими послугами, виплачувати податки з отриманих доходів та отримувати юридичний захист в суді, коли їхні права порушуються. Також на меті в законотворців було забезпечити захист українських інвесторів під час інвестування на ринку віртуальних активів.

Саме цим документом визначається взагалі поняття та правовий статус віртуального актива. Відповідно до закону віртуальним активом визнається особливий вид майна, який є цінністю в електронній формі, існує в системі обігу віртуальних активів, та може знаходитись у цивільному обігу. Віртуальні активи можуть бути забезпеченими і незабезпеченими. Залежить цей критерій від посвідчення ним майнового або немайнового права, наприклад, права вимоги на якісь інші об'єкти цивільних прав.

Що важливо – забезпечення віртуального активу не тотожне забезпеченню віртуального зобов'язання. Незабезпечений віртуальний актив взагалі не посвідчує жодного майнового чи немайнового права. Також даний акт визначає деякі питання права власності та укладання угод із використанням активів такого типу в Україні. Даний законопроект – рамковий, він лише їх визначає та дозволяє. Застосування пропонується прописувати у додаткових питаннях.

Тепер варто трохи докладніше розкрити питання оподаткування та реальної необхідності його впровадження стосовно криптографічних валют на українських теренах. Наразі до Верховної Ради внесено проект закону №2461, який покликаний встановити чіткі правила оподаткування для продажу криптографічних активів, до яких також відносять і криптовалюти. Проект бере до уваги випадки так званого виводу активів у фіат (тобто продажу криптовалюти за реальні гроші, наприклад, за долари. Автори законопроекту відзначають, що український ринок віртуальних активів взагалі не може розвиватися через відсутність визначеності правового статусу віртуальних валют та токенів.

Також проект закону зазначає, що прибуток, який було отримано завдяки операціям із криптовалютою, буде розраховуватися окремо. Визначається же він як позитивна різниця між доходом від продажу та витратами від майнінгу (доцільне визначення містить проект Закону України «Про обіг криптовалюти» – обчислювальні операції, які здійснює майнер за допомогою власного та/або орендованого спеціалізованого обладнання, з метою забезпечення працездатності та безпеки системи блокчейн, та залежно від умов системи блокчейн отримує винагороду системи блокчейн) або купівлі активів. Законопроект визначає податок на такий прибуток у розмірі 18% для організацій та 5% для фізичних осіб. Натомість податком на додаткову власність (ПДВ) операції із купівлі та продажу криптографічної валюти не обкладаються.

Прогалинами у законі варто назвати відсутність якихось вказівок, які регулюють застосування спрощеної системи до таких операцій. На даний момент торгівля криптовалютою не заборонена для платників єдиного податку. Основна мета – це взагалі прибрати фактор впливу ПДВ та змінити податкову пільгу з 18%, вказаних загальним законодавством, на 5% протягом 4–5 років. Це спровоковано тим фактом, що ПДВ дійсно не працює так, як має, бо нема приймання-передачі товару у їхньому типовому значенні.

У той самий час влада планує контролювати розмір доходу двома основними способами. Якщо відбувається конвертація з фіатної, тобто реальної, валюти, у криптографічну, то критерієм контролю виступатиме різниця між виходом та входом у криптоактив. Натомість оподаткування доходу, який виникає під час операцій із використанням виключно криптовалют, можна реалізувати виключно за умови подання добровільного звіту суб'єктів та на підставі документальних підтверджень (чеків, виписок, довідок) від торгового майданчика, який контролював операцію.

Також законотворці мають на меті диференціювати податок на прибуток між фізичними та юридичними особами у відповідності із вимогами надання податкових звітностей: юридичним особам доведеться сплачувати податок або раз на квартал, або раз на півроку, а ФОПам (фізична особа-підприємець) – виключно раз на рік. Також для них буде особливе правило – сплачується 5% від обсягу.

Відношення влади до даних законодавчих метаморфоз загалом позитивне, бо, як вважається, цінність даних актів надвисока. Саме завдяки їм підвищується вагомість фінансової системи України, а також суттєво спрощується проведення фінансових потоків. Сьогодні це важливо, бо FATF (Financial Action Task Force on Money Laundering) – міжурядова організація, яка займається розробкою світових стандартів із протидії відмиванню злочинних доходів відносить українські банки до так званого «сірого» списку, на що мало не в першу чергу впливає саме відсутність чіткої законодавчої регуляції обороту криптографічних активів. У результаті для українських трейдерів закрито понад 20 бірж, серед яких американсько-британські Gemini та Coinbase, японська Bitflyer,

південнокорейська Korbit, бразильська Mercado bitcoin, мексикано-гібральтарська Bitso та інші. За міжнародним законодавством вони можуть надавати послуги виключно податковим агентам, якими українці, на превеликий жаль, не є.

Натомість вести в Україні свою діяльність, маючи за кордоном лише офіси, не припиняють не менш відомі Wirex та EXMO, тобто наша держава – це вигідна торговельна зона, ухвалення на якій законодавства із обороту віртуальних активів дасть загальний поштовх до еволюції усієї галузі фінтеху та криптоіндустрії як її випадку. Наслідком цього стане залучення масштабних інвестицій навіть у ті галузі економіки, які не мають жодного відношення до криптографії.

Ще однією вагомою причиною для переміщення криптовалютного питання у правове поле є проведення за допомогою «дітей блокчейну» величезної кількості незаконних операцій. Про це свідчить заява очільника Департаменту кіберполіції Олександра Гринчака, який повністю підтримував законодавчу ініціативу, адже це не лише поповнить бюджет, але й допоможе якомого ефективніше відстежувати незаконні операції, учасники яких користуються криптовалютою, а ними можуть бути будь-які злочини – від вимагання до работоргівлі та вбивства. За словами очільника, кіберполіція вже неодноразово піднімала дане питання та отримала підтримку від Верховної Ради та профільних комітетів.

Оподаткування криптовалютних операцій. Іноземний досвід доводить, що оподаткування криптовалютних операцій не лише приносить дохід до державного бюджету, але й вирішує проблеми кримінальних правопорушень, учасники яких проводять розрахунки за допомогою біткоїну, лайткоїну та інших їм подібних блокчейн-продуктів.

Наприклад, у Японії криптовалюти визнано повноцінними платіжними засобами та навіть прийнято особливий закон про криптовалютні платіжні послуги. Швейцарія пішла іншим шляхом, залишивши для токенів статус «майно» та оподатковуючи їх лише за даною ознакою.

Найбагатший досвід з цього питання, що не дивно, мають США (Сполучені Штати Америки). Там було прийняте водночас неочікуване та логічне рішення проблеми: криптовалюта визнається цінним папером та підпадає під юрисдикцію Державної комісії з цінних паперів і бірж. За цих обставин діяльність щодо операцій із криптографічними валютами у країні, на відміну від України, «занадто» врегульована, маючи купу обмежень. Найпоказнішим зразком того, як це працює у США, можна назвати ситуацію із токеном Gram на базі платформи TON (The Open Network). Павло Дуров тоді зміг пройти ICO та залучити інвестиції у розмірі понад півтора мільярди доларів, натомість Державна комісія з цінних паперів і бірж звернулася до суду та домоглася заборони випуску цієї валюти. У деяких країнах, у тому числі в Китайській Народній Республіці, криптовалютні операції взагалі поза законом – і це насправді найпростіший спосіб вирішення даної проблеми на тому етапі, коли

криптовалютними операціями не просякнутий певний сектор економіки, у тому числі тіньовий.

Налаштування системи оподаткування – це не єдиний чинник, який напряму впливає на саму можливість функціонування операцій з криптовалютою. Дуже важливо також, щоб великі фінансові структури підтримали розвиток крипторинку хоча б на початковому етапі, починаючи із впровадження блокчейну. Яку вигоду мають з цього банки? На сьогоднішній день усі подібні організації працюють із централізованими базами даних, які зберігаються або на фізичних серверах, або у хмарних сховищах. Для переходу на нову технологію доведеться створити розподілені бази, які зберігатимуться на пристроях учасників кожного ланцюжку. Це здешевить обслуговування, бо усю величезну систему банку зможуть контролювати одна-дві людини, а також підніме рівень безпеки. Щодо впровадження криптовалюти на даний момент у середовищі українських банків є лише теоретичні викладки, такі, як створення національної криптовалюти, яка зберігатиметься у децентралізованій мережі. Далі за усіх конкурентів у даному питанні, що не дивно, просунувся Монобанк, який планує налагодити інтеграцію із криптобіржею, аби дати своїм користувачам можливість проводити транзакції із застосуванням Bitcoin лише за допомогою карти.

Щодо решти банків – наразі у напрямку впровадження токенів готові рухатися лише декілька великих банківських структур, серед яких UniCreditBank та ПриватБанк. Саме останній наразі демонструє актуальні курси криптовалют, а також розміщує повну інструкцію, як купити біткоїн за допомогою додатку Приват24. Єдине обмеження на сьогодні для українців стосується об'єму транзакцій: більше 400.000 гривень обміняти на криптографічну валюту неможливо за допомогою жодного відомого сервісу на території нашої держави.

Відповідно до усього вищевикладеного можна упевнено сказати, що Закон України «Про віртуальні активи» дійсно важливий для вирішення проблеми визначення місця криптовалютних активів у системі цифрової економіки. Внаслідок його функціонування компанії зможуть реєструвати власний криптовалютний бізнес на наших теренах, а українські спеціалісти зможуть реалізовувати проекти в українській юрисдикції. Також даний закон буде сприяти усуненню певних ризиків, які стосуються роботи міжнародних блокчейн-компаній, а також залученню інвестицій з інших країн.

Як вивести USDT на карту і перевести в готівку. З початком війни багато українців вирішили убезпечити свій капітал і перевести гривні в долари. З огляду на обмеження купівлі валюти, було використано такий алгоритм: придбати криптовалюту за гривні, а потім вивести USDT через долари. За березень 2022 року громадяни України здійснили транзакції на 1,7 млрд дол, використовуючи іноземні системи платежів. У квітні сума зменшилася, але залишилася досить солідною: 0,9 млрд дол. (рис. 2.17).

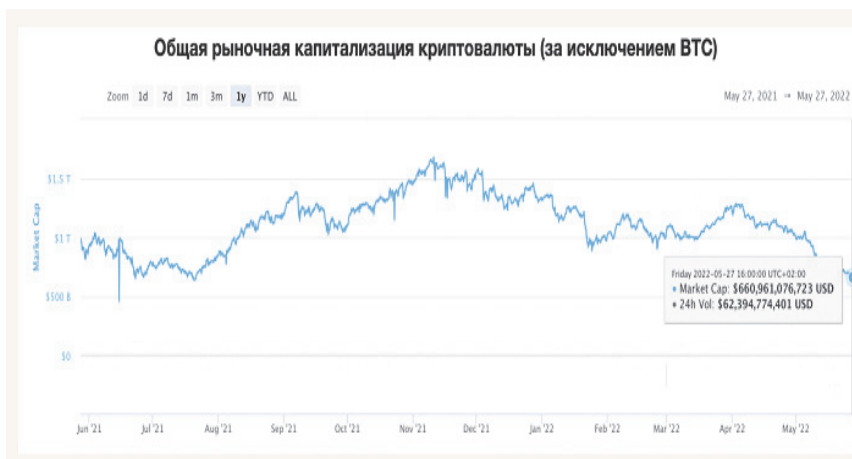


Рисунок – 2.17 Графік капіталізації криптовалют

Наскільки актуально змінювати криптовалюту в Україні у 2022 році. Інвестування в закордонні активи заборонено в період воєнного часу. Щоб унеможливити відтік гривні з країни, НБУ наприкінці квітня заборонив поповнення криптоакаунтів, брокерських рахунків і P2P-платежі в гривні. Наразі допускається протягом місяця купувати за долари і євро активи, рівноцінні 100.000 грн.

Проте інтерес до заробітку в криптовалюті не згасає, і для деяких суми в 3,3 тис. доларів/місяць (еквівалент 100.000 грн) є лише частиною прибутку.

Регулярно з'являються нові активи, збільшується потік вкладень у цифрові стартапи. Що з цього крупно «вистрілить» – поки що невідомо, проте досвідчені гравці не втрачають можливість «зробити ставку» на валюту, яка активно набирає обертів у перші тижні існування. Зароблені кошти виводять на карту або готівку.

Фахівці-практики віддають перевагу вкладенням у кілька активів (популярні Bitcoin, Ethereum, Waves, Litecoin, Dogecoin). Ті ж, хто поповнив криптопортфель USDT, можуть зараз обмінювати його на долари або гривні для повсякденних витрат, тому багатьох цікавить, як обміняти Tether на фіат.

Висока волатильність біткоїна, ефіріума призводить до того, що більшість, щоб уникнути втрат, трансформує основну цифрову масу в більш прийнятний грошовий актив: хочуть вивести на картку або готівку, купити золоті злитки та інше. Тому далі розповідаємо, як вивести USDT в Україні.

Способи обміну USDT на карту. Перевести віртуальні гроші в готівку пропонується кількома методами. Кожен обирає для себе найзручніший

варіант, виходячи з його надійності, швидкості та вигоди. Головне – ретельно проаналізувати доступні майданчики.

Обмінники криптовалют. Ними користується більшість. Онлайн-сервіси працюють з безліччю валют, а перевірити їхню надійність і курс пропонують моніторингові платформи.

Купити USDT за хорошим курсом може бути проблематично через високі ліміти або малий залишок потрібної криптовалюти в конкретному обміннику. Дані змінюються кожні 8–10 секунд, тому, поки заповнюєш форму, курс також може змінитися не у вигідний бік. Аналогічні проблеми виникають, коли хочеться вигідно продати USDT. Під час реєстрації час також займає перевірка надісланої користувачем інформації. Якщо обмінник працює в ручному режимі, може знадобитися тривалий час для завершення транзакції.

Із вдалих ресурсів для українців можемо назвати Changeit. Працює виключно з гривнею, за хорошим курсом, без прихованих комісій і в автоматичному режимі. Тому вивести USDT та іншу криптовалюту на банківську карту вдається без затримок.

Біржі. На відміну від обмінників, тут можна не тільки купити USDT або продати USDT, а й торгувати криптоактивами. За вдалого збігу обставин можна зайти з невеликою сумою, а вийти зі значним прибутком. Потрібно враховувати умови обміну USDT: резервні суми, запропонований курс, швидкість угоди, можливі бонуси. Біржі користуються популярністю у гравців. Після введення коштів їх одразу пускають в обіг, не оплачуючи додаткові відсотки.

Платіжні системи. Payeer, Perfect Money, PayPal та інші. ЕПС (електронні платіжні системи) зручні для того, щоб вивести USDT на бажаний платіжний інструмент, поповнити рахунок на біржі, виконати обмін, а також здійснити оплату за покупку. Деякі системи випускають картки дебетового типу для розрахунку в офлайн-магазинах, де конвертація в потрібну валюту виконується на касі автоматично.

P2P обмін. Користувачі здійснюють грошові операції між собою. Одна людина бажає продати USDT і оформляє ордер на певну кількість валюти. Інший має намір купити USDT, без відсотків від посередника.

Прикладом здійснення таких угод є валютний маркетплейс Binance. Зацікавлені сторони спілкуються в онлайн-чаті. Послуги у форматі ескроу допомагають проводити операції чесно і без претензій один до одного. Криптовалюта переводиться на тимчасовий рахунок. Вона надходить на рахунок покупця після того, як обидва контрагенти підтвердять проведення угоди. Далі залишається вивести USDT або використовувати за іншим призначенням.

Криптомати та офлайн обмін. Спеціальні термінали, що працюють виключно з цифровою валютою, називаються криптоматами. Вони надають клієнту доступ до електронного гаманця і здійснення обраної операції, згідно з наявним функціоналом.

Існують криптомати на окрему купівлю, тільки продаж або такі, що поєднують обидві дії. Останніми роками стало зручно використовувати термінали з оплатою за товари.

Щоб купити/продати USDT, потрібна ідентифікація клієнта кількома способами: за QR-кодом, відбитком пальця або телефонним номером.

Зі зручностей – швидкість проведення операцій. З недоліків – наявність криптоматів лише у великих містах (Київ, Львів, Івано-Франківськ, Харків), і в невеликій кількості. Кількість валют обмежена, а обміняти Tether на фіат можливо за курсом, який система вибирає сама з прийнятних варіантів. Не всіх влаштовує висока комісія (5%).

Як варіант – партнерська мережа офлайн обмінників від перевірених компаній, щоб здійснити обмін професійно і чесно.

Альтернативні способи. Є й інші, менш популярні способи обміну та виведення USDT.

Проведення угоди за готівку під час зустрічі з людиною, коли покупець обмінює свою цифрову валюту на гроші. Продавець може обдурити на поточному курсі або придумати махінацію з чужою віртуальною власністю. Такий спосіб продажу USDT рекомендується здійснювати тільки зі знайомими людьми.

Використання ботів у Телеграм. Оперативно, але не дуже надійно. Ви не можете точно знати, хто перебуває по той бік екрана. Орієнтуватися треба на відгуки, а краще – на перевірених друзями ботів.

Криптогаманці з додатковою опцією придбання. Вони допомагають купити USDT, але відрізняються підвищеним комісійним відсотком, на приклад: Trust Wallet, Exodus.

Особливості виведення криптовалюти на карту банку. Наразі складнощі пов'язані саме з придбанням кріпти у зв'язку з обмеженнями. Банк точно заборонить операцію через біржу. При виборі обмінника шанс все ж є, але залежить від схеми угоди.

Що стосується виведення, то воно здійснюється на будь-які суми – українська банківська система не забороняє вхідні гривневі або валютні перекази на картки.

Вивести USDT на карту банку можна 3-ма способами.

Через обмінник – попередньо перевіривши відгуки та курс. Щоб обміняти Tether USDT на фіат, знадобляться також біржі з функцією P2P. Будьте готові до високої комісії за угоду.

Телеграм-боти – потрібно бути дуже обережним і не «злити» гроші ошуканцям. На картку «Універсальна» роблять безоплатні зарахування сум, однак при виведенні потрібно платити відсоток. Тому нею зручніше розраховуватися за покупки, а не знімати готівку. Аналог «Для виплат» одноразово списує 0,5%, а переведення в готівку виконується без комісії.

Коли слід виводити USDT. USDT Tether (ребрендинг Realcoin, універсальна назва USDT), забезпечується фіатною доларовою «прив'язкою»

і не містить блоків транзакції. На відміну від стрибків біткоїна, обміняти Tether на фіат можна без жодного фінансового ризику.

Вивести USDT можна в будь-який час доби. Незважаючи на те, що забезпечення вважається найнадійнішим з позиції збереження курсу, потрібно свідомо підходити до потенційних ризиків.

Особливо якщо зберігання грошей або використання їх у тезерному вигляді в онлайн-проекті розраховане на тривалий термін.

Сьогодні зі 100% вартості Тезера реально забезпечено підтримкою готівкового долара тільки 75%, це означає, що надалі картина здатна змінитися. Не факт, що переведені в стейблкоїни тисячі доларів не перетворяться одного разу на сотні умовних одиниць.

2.3.2. Особливості роботи з криптоактивами в рф

Криптовалюта в рф є дуже популярним фінансовим інструментом, і питання, як її купити, стає актуальним для дедалі більшої кількості росіян.

Коли йдеться про інвестиції в криптовалюту, росіяни найчастіше стикаються з питаннями – яку криптовалюту купити?

Основні критерії, що надаються криптовалютою: поширеність (висока капіталізація); неможливість блокування гаманця; практичне застосування; законність.

Відомі способи купівлі криптовалюти в росії.

Купівля в P2P обміннику. P2P – спосіб укладання угоди між рівноправними користувачами платформи. У період, коли вартість біткоїну ще не перевищила позначку 20 000 USD, P2P платформи були одним з основних місць, де можна купити криптовалюту. З розвитком централізованих криптобірж метод P2P більше став використовуватися як засіб поповнення балансу.

Поетапний спосіб купівлі криптовалюти USDT через P2P обмінник. На P2P платформі у розділі «Купити» підбирається найкраще оголошення. При виборі варто звертати увагу на курс, ліміти та спосіб оплати. Наприклад, оголошення – купити USDT за курсом 75,70 з лімітами по угоді від 1.000 до 50.000 рублів, спосіб оплати – переказ по карті Сбербанк.

Відкриваємо угоду – Придбати 757 USDT за курсом 75,70 на суму 7.570 рублів, переказом по карті Сбербанк. Після відкриття угоди продавець буде сповіщений про те, що ви хочете купити USDT за заздалегідь обумовленими параметрами.

Продавець надсилає вам реквізити, куди необхідно відправити суму. В більшості випадків це номер картки або телефону, до якого прив'язана картка Сбербанку.

Далі ви здійснюєте переказ на вказану суму та натискаєте «Угода оплачена».

Як тільки продавець підтвердить надходження коштів, його криптовалюта буде зарахована на ваш рахунок.

Плюси: можливість купити по карті або за допомогою переказу зі зручних платіжних систем; покупка онлайн не виходячи з дому.

Мінуси: не вигідний курс; не завжди зручні мінімальні та максимальні ліміти на покупку; необхідність здійснювати грошовий переказ на карту незнайомої людини (банківські ризики); ризик отримання «брудної» криптовалюти.

Купівля з банківської картки іноземних банків. Такий спосіб слід розглядати як один з альтернативних, але, можливо, не найбільш загальнодоступний.

У зв'язку зі зростаючим санкційним тиском у 2022 році у громадян рф стали популярними «карткові тури», у яких люди подорожували до найближчих країн і відкривали банківські картки платіжних систем VISA та MasterCard, що призупинили роботу в росії. Основна мета відкриття таких карт – отримання можливості оплати різних міжнародних сервісів на кшталт Netflix, Spotify, YouTube тощо.

Якщо ви були одним із тих, хто відкривав собі картку за кордоном, то у вас є можливість купити криптовалюту на будь-якій біржі, яка підтримує спосіб поповнення рахунку за картками VISA або MasterCard.

Наявність такої картки не є панацеєю, тому що в умовах обмежень не всі крипто-платформи готові обслуговувати російських громадян через ризик потрапляння під вторинні санкції. На жаль, ці особливості роблять іноземні криптовалютні біржі не найкращим місцем, де можна купити криптовалюту.

Плюси: великий вибір криптовалюти для купівлі; спосіб підходить для тих, хто купує криптовалюту в невеликих обсягах.

Мінуси: висока вартість відкриття картки; необхідність їхати в іншу країну; необхідність повідомляти податкові органи про наявність рахунку в іноземному банку; складність у поповненні картки; великі комісії на купівлю з картки.

Купівля в криптовалютному гаманці. Купівля криптовалюти в криптогаманці є одним з найнадійніших способів, але при цьому супроводжується високими комісійними витратами, від 3,5 до 5%. Купити криптовалюту можна в таких мобільних гаманцях як Exodus, Trust Wallet тощо.

Якщо у вас є криптовалютний гаманець фірми Ledger, то функціонал додатка Ledger Live дає змогу купувати криптовалюту прямо в додатку. Із запропонованих способів: MoonPay (VISA, MasterCard, SEPA); Coinify (VISA, MasterCard, SEPA); BTC Direct (VISA, MasterCard, Maestro, SEPA).

Плюси: безпечна купівля невеликих обсягів цифрових активів; можна вивчити принципи роботи блокчейна на невеликих сумах.

Мінуси: дуже високі комісії за обмін (можуть досягати до 5%); не підтримуються карти MIP і карти VISA, MasterCard, випущені в рф.

Купівля в Телеграм-ботах. Спосіб купівлі криптовалюти в Телеграмі був одним із найпопулярніших способів у період 2017–2020 року. Наразі цей спосіб став неефективним з точки зору швидкості обробки транзакції.

Криптовалюту в телеграмі можна купити або через сервіс, який обробляє заявки вручну, або через P2P-бота. Раніше колись популярний спосіб купівлі криптовалюти через телеграм був поширеним, але в міру зростання популярності телеграма з'явилося багато шахрайських сервісів, які негативно позначилися загалом на цьому методі купівлі.

Плюси: усі операції проходять у зручному месенджері.

Мінуси: не завжди вигідний курс; багато шахрайських і не перевірених ресурсів.

Купівля криптовалюти за готівку в обміннику. Одне з найпопулярніших і найпоширеніших місць, де можна придбати криптовалюту, є обмінники. Перевірені обмінники можна знайти на різних сайтах агрегаторів, найпопулярнішим з них є бестчендж. Кожен обмінник, розміщений на сайті-агрегаторі, проходить повну верифікацію і перевірку на сумлінність.

Лева частка обмінників, розміщених на найбільших агрегаторах, є надійними, але відомі й випадки, коли всупереч репутаційним ризикам адміністрація здійснювала шахрайські дії. Також варто зазначити, що існують різні шахрайські схеми, де фігурантами є обмінники, найчастіше ця схема відома як «трикутник». Якщо хочете випробувати цей спосіб купівлі криптовалюти, будьте уважні й обачні під час вибору обмінного пункту.

Плюси: зрозумілий і традиційний спосіб; великий вибір обмінників.

Мінуси: не завжди вигідний курс; невеликий, але все ж таки присутній ризик шахрайства.

Приклад. Купівля криптовалюти на Veribit. Покрокова Інструкція.

Крок 1 – Реєстрація на біржі Veribit. Переходимо на сторінку реєстрації Veribit (<https://veribit.com/register>). Вводимо необхідну інформацію, реєструємося і підтверджуємо пошту.

Крок 2 – Верифікація акаунта. Щоб мати можливість повноцінно використовувати платформу Veribit і захистити свій акаунт необхідно пройти верифікацію. Для проходження верифікації необхідно: ввести Прізвище Ім'я та По-батькові (необов'язково); завантажити селфі; завантажити лицьовий і зворотний бік документа. Пройти верифікацію можна на Державний паспорт, Закордонний паспорт або Водійське посвідчення.

Крок 3 – Поповнення рублевого балансу. Рублевий баланс можна поповнити двома найпоширенішими способами: готівкою в офісі (комісія становить 0%, лімітів немає); за допомогою банківської карти (комісія становить 2,7%, ліміти від 2.500 до 50.000 рублів); в розділі Veribit P2P.

Крок 4 – Купівля криптовалюти. Купівля криптовалюти здійснюється в розділі «Біржа». Для прикладу здійснимо операцію з купівлі USDT. Якщо ви хочете виконати швидку купівлю, то купуйте, використовуючи ринкову заявку, але якщо ви хочете виставити свою ціну, то необхідно активувати «Лімітна» і виставити заявку зі своїми параметрами.

Виставляємо параметри: Тип «Ринкова»; кількість 1.000 USDT; перевіряємо всі параметри і якщо ціна влаштовує натискаємо кнопку купити; перед здійсненням угоди з'явиться вікно для додаткового підтвердження. Після угоди ваш баланс поповниться USDT, які можна вивести через мережу ERC-20, TRC-20 і BEP-20.

Отже, індустрія криптовалют розвивається дуже стрімко, а тому на ринку з'являється безліч цікавих рішень і способів інвестування в криптовалюту.

Якщо говорити про швидкі та безпечні способи поповнення, то це, безумовно, купівля криптовалюти безпосередньо в холодних гаманцях. Але якщо ви хочете купити криптовалюту дешево без додаткових переплат і з високим рівнем безпеки, то її слід купувати на платформі біржі типу Veribit.

Перевагою платформ типу Veribit є відсутність комісій на поповнення та виведення готівкою. Такими перевагами активно користуються трейдери, які використовують різні арбітражні стратегії. Платформа дає можливість купити криптовалюту за рублі з найнижчими комісіями.

Незважаючи на невизначений статус криптовалюти в рф, нічого незаконного в її купівлі немає. Тобто можна спокійно купувати і продавати цифрові монети або інвестувати в них.

Криптові біржі які на сьогодні працюють в рф: KuCoin, Gate.io, Lbank, Bybit, OKX.

На сьогоднішній день російський закон не забороняє купувати криптовалюту на зарубіжних ринках ні фізичним, ні юридичним особам. Заборонено лише випускати криптовалюту на майданчиках рф та використовувати як засіб платежу всередині країни.

Також через сервіс Bitbanker можна купити за рублі BTC, ETH і USDT. Для цього потрібно зареєструватися, пройти KYC, поповнити баланс і купити криптовалюту. Поповнити баланс рублями можна через P2P або готівкою через офіси в Москві та Дубаї.

З початком повномасштабного вторгнення рф на території України ЄС ухвалив новий пакет санкцій, до якого потрапили популярні у росіян Тінькофф і Альфа-банк. Слідом за цим перекази за допомогою карт цих банків перестала приймати «Золота корона». А найпопулярніша криптобіржа Binance з посиланням на обмеження Євросоюзу і зовсім заборонила російським користувачам купувати і продавати долари та євро.

Переказувати можна тільки невеликі суми, список країн, у яких можна отримати переказ, обмежений. Але час і війна постійно вносять свої корективи.

Внаслідок останнього пакета санкцій ЄС проти Тінькоффа і Альфа-банку їхні картки перестала приймати платіжна система «Золота корона», яка весь минулий рік постачала грошима більшу частину росіян, які виїхали з країни.

Найімовірніше, заборона боляче вдарить по бізнесу «Золотої корони», тому що її основний конкурент, Unistream, картки санкційних банків продовжує приймати. Також їхніми картками все ще можна відправити переказ у платіжній системі Contact, що належить Qiwi.

Через «Золоту корону», як і раніше, можна відправити гроші з картки банку, який поки що не потрапив під санкції, наприклад – Райффайзенбанку. Користувачі також знайшли ще кілька способів: завести віртуальні картки Ozon або «Яндекса» (обидві компанії встигли обзавестися банківськими ліцензіями, тому що будували великі плани на фінтех, більша частина з яких тепер уже навряд чи здійсниться). Для переказу потрібно буде спочатку відправити гроші на віртуальну карту, а потім за допомогою «Золотої корони» відправити за кордон.

SWIFT (Society for Worldwide Interbank Financial Telecommunications: дорого і не завжди надійно. Незважаючи на всі пакети санкцій проти банківського сектору, виводити гроші з рф за допомогою SWIFT-переказів усе ще можна без великих проблем, кажуть учасники ринку та фінансові консультанти. Щоправда, для цього знадобиться рахунок у закордонному банку, відкрити такий без особливих проблем можна в Казахстані, Вірменії або Грузії, а ось для рахунку в країнах ЄС знадобиться вид на проживання або довгострокова віза.

Головним банком для таких переказів все ще залишається російська «дочка» австрійського Райффайзенбанку. На неї, за даними FT, зараз припадає до 50% всіх платежів між росією і рештою світу. Понад 60% прибутку всієї групи торік припало саме на росію і білорусь. Російська «дочка» заробила 2 млрд євро – це в п'ять разів більше, ніж рік тому. Через це, за даними FT, у банку навіть почалися проблеми в США: зараз американська влада розслідує його роботу в росії. Але, так чи інакше, цей спосіб виведення грошей для росіян все ще доступний.

Щоправда, російський банк весь час змінює умови для SWIFT-переказів: з 6 березня мінімальна сума вихідного переказу у валюті піднялася до \$10.000. Ще наприкінці грудня вона була вдвічі меншою.

Комісія за переказ становитиме 2–3% від суми переказу, але мінімум \$200 і максимум \$300. За купівлю валюти в банку доведеться заплатити ще 3%. Також доведеться заплатити комісію банку-посередника, у середньому \$10–70. Нарешті, варто пам'ятати, що якщо ви не встигнете швидко зробити переказ і на вашому рахунку залишиться понад \$10.000, то за їхнє зберігання теж доведеться заплатити 0,5–1% щомісяця. Це, досить дороге вікно можливостей для росіян скоро може закритися.

Австрійські засоби масової інформації (ЗМІ) дізналися про передбачувану схему виходу Райффайзенбанку з росії. Так, банк може обміняти свої російські активи на активи Сбербанку в Європі. Деталі угоди поки обговорюються і ще не зрозуміло, чи відбудеться обмін у принципі. Однак, з огляду на увагу американських регуляторів, вихід банку з росії – це, швидше за все, питання часу.

SWIFT-переказ можна зробити і в інших російських банках. За підрахунками РБК (РосБізнесКонсалтинг), такі послуги зараз пропонують близько 40 організацій. Але є нюанс: у більшості з них транскордонні перекази у валюті фактично поставлено на паузу, зрозуміти це можна тільки в результаті спілкування з підтримкою. Серед банків, які все-таки надають таку послугу – Газпромбанк (комісія 3%, мінімум 30.000 рублів, максимум – 60.000) або китайський Бенк оф Чайна (0,3% усередині мережі і вище – в інші банки). Є ще банки, які готові переказувати валюту, але тільки в дуже обмежений набір країн, серед яких зазвичай немає так званих «недружніх».

Але у SWIFT-переказів з російських банків є одна велика проблема: періодично вони підвисають і губляться. У Telegram уже утворилося кілька великих чатів, у яких обговорюють ці проблеми. Судячи з них, найчастіше перекази підвисають через банки-кореспонденти, через які транзакція йде з банку-відправника в банк-одержувач. Йому для проведення платежу окремо можуть знадобитися документи, що підтверджують походження коштів – причому ці документи, найімовірніше, доведеться надавати самому користувачеві, розшукавши контакт банку-кореспондента. Банк-одержувач, до речі, теж варто повідомити про переказ заздалегідь, щоб не виникло непередбачених ситуацій. Також, щоб дізнатися заздалегідь, чи приймає конкретний закордонний банк SWIFT-перекази з росії, варто перевірити його в сервісі Ohmswift: там користувачі збирають актуальну статистику щодо транзакцій. Там же можна відстежити SWIFT-переказ за номером.

Рублеві перекази: дешевше, але довше. Ще один робочий спосіб переказувати гроші за кордон через банки – рублеві перекази. Працює це так: у «дружній» країні відкривається банківський рахунок у банку, що приймає рублеві перекази. Популярна локація для такої схеми – Казахстан. По-перше, тому що відкрити рахунок там можна і віддалено: на це знадобиться приблизно два місяці і до 60 тисяч рублів за послуги посередника. По-друге, там є біржа, а отже, можна міняти рублі на валюту за більш-менш хорошим курсом. Для такого способу підійдуть і Вірменія, Узбекистан, Киргизстан та інші країни, куди можна відправити переказ у рублях. Туди відправляються рублі, які потім міняються на долари і вже із закордонного рахунку за допомогою SWIFT відправляються далі.

Наприклад, у Freedom Bank, це казахстанський банк брокера Freedom Finance, можна відкрити рахунок за російською сім-карткою й отримати мультивалютний рахунок, де будуть і рублі, і долари з євро. Такий переказ вийде дешевше, ніж SWIFT безпосередньо з росії. Якщо для останнього комісія складе до 4% від переказу, то тут на весь ланцюжок вийде близько 1,5%, оцінює експерт. Але й документів знадобиться набагато більше: адже за відкриття рахунку і рух коштів по ньому (якщо за рік сума переказів перевищить 600.000 рублів) доведеться звітувати перед федеральною податковою службою. Також варто пам'ятати, що банки не дуже люблять транзитні перекази, попереджають експерти.

Криптовалюти: ризиковано і проблематично. Перекази за допомогою криптовалют все ще залишаються популярним способом для виведення грошей з росії.

Після заборони Binance, найпопулярнішої криптобіржі світу, росіянам заборонили купувати і продавати через свій р2р-сервіс долари та євро. Це означає, що купити за рублі USDT, а потім продати стейблкоїни за долари або євро і вивести гроші на закордонний рахунок, тепер не спрацює.

Новина насправді не жахлива. По-перше, російські користувачі все ще можуть купувати стейблкоїни за рублі. Після купівлі той самий USDT можна вивести на власний гаманець і продати в іншому місці: наприклад, у фізичному обміннику в країні проживання або в онлайн-обміннику. По-друге, росіянам усе ще доступний цілий набір інших популярних криптобірж, які не вводили нових обмежень. Наприклад, OKX або KuCoin.

Ще один спосіб, доступний росіянам із видом на постійне проживання або довгостроковими візами в європейських країнах – завести криптокарту і розплачуватися за повсякденні витрати прямо нею.

На практиці виведення за допомогою криптовалюти зручніше використовувати для невеликих переказів до \$2–3 тисяч. Якщо таким способом переказувати великі суми, то їхнє походження буде складно пояснити, щоб завести на банківський рахунок.

Однак і для цієї проблеми знайшлося рішення: більшість великих обмінників криптовалют готові надавати послуги з «відмивання» грошей. Популярними локаціями для цього стали Туреччина та Дубай. Там після обміну крипто на фіат одержувачу грошей допоможуть створити фейковий контракт на розробку програмного забезпечення (ПЗ) або рекламні послуги на потрібну суму. З цих грошей заплатять податки, для них зберуть усі підтверджувальні документи. Далі їх можна виводити в інші країни.

Також під час купівлі та продажу криптовалют на великі суми можна зіткнутися з шахрайством, оскільки цей ринок, по суті, ніким не регулюється.

Для виведення криптовалют в росії потрібно дотримуватися певних правил і процедур. Ось кілька кроків, які можна виконати:

1. Відкрийте електронний гаманець, що підтримує виведення грошей в російських рублях. Найбільш популярним сервісом є Qiwi Wallet, але є й інші варіанти, такі як Yandex.Money, WebMoney та інші.
2. Підключіть двофакторну автентифікацію та перевірте свою особу, щоб виконати фінансові операції.
3. Переведіть криптовалюту з вашого гаманця на біржу, яка підтримує виведення грошей в російських рублях. Наприклад, такими біржами є Binance, EXMO, Livecoin та інші.
4. Обміняйте криптовалюту на російські рублі на біржі.
5. Виведіть рублі на свій електронний гаманець, що підтримує виведення грошей на картку або банківський рахунок.

6. Переведіть гроші з гаманця на свою картку або банківський рахунок.

Важливо пам'ятати, що процедура виведення грошей може бути пов'язана з певними комісійними витратами, які залежать від вибраного сервісу та кількості переведених грошей. Також слід звернути увагу на податкове законодавство росії щодо оподаткування криптовалютних операцій.

Якщо ви маєте криптовалюту і хочете її перевести у фіатні гроші в росії, ви можете скористатися одним з наступних способів:

Криптовібіржі: Ви можете продати свою криптовалюту на одній з багатьох криптобірж в росії, таких як Binance, Bitmex, Bitforex, и т.д. Для цього вам потрібно буде створити обліковий запис на криптобіржі, підключити свій банківський рахунок і продати свою криптовалюту за фіатні гроші.

Обмінники: Ви можете скористатися послугами криптовалютних обмінників, таких як BestChange, для обміну своєї криптовалюти на фіатні гроші. Ці обмінники пропонують різні методи оплати, такі як банківські перекази, платіжні системи, карти Visa/Mastercard та інші.

Приватний продаж: Ви можете знайти особу, яка бажає придбати вашу криптовалюту, і продати її безпосередньо. Цей спосіб може бути менш безпечним, ніж інші методи, тому слід бути дуже обережним при здійсненні такої угоди.

Незалежно від того, який спосіб Ви виберете, слід пам'ятати про необхідність дотримуватися правил інвестування в криптовалюту та регулятивних вимог в росії.

2.3.3. Виведення криптоактивів з території третіх країн

Сфера товарів та послуг. Завдяки можливостям, які відкривають законодавство деяких країн, зараз на Заході криптоплатежі приймають безліч компаній – від стільникового зв'язку до іпотечних платежів.

Цей список поповнюється буквально щотижня. Наприклад, у Microsoft можна купувати ігри та програми (саме вони стали одними з перших, хто впровадив цей спосіб у 2014 році), у магазинах Whole Foods можна оплачувати продукти харчування, в AT&T – оплачувати мобільний зв'язок. Практично всі послуги групи компаній Virgin можна оплачувати криптою: від мобільного зв'язку (Virgin Mobile) до та польотів у космос (Virgin Galactic).

У *Ванкувері*, самому просунутому з точки зору інтеграції криптовалют місті Канади, витратити свої блокчейн-гроші можна в кафе та ресторанах (Rouge Bistro, Steamrollers Burritos та ін), в зоомагазинах (Lead Mate та Zyza Yoga Clothing&Active Wear) або на організацію заходів чи весілля (Man About Town Entertainment).

У *Швейцарії* розрахуватися криптою можна навіть у McDonalds. Але це не перша країна, де мережа швидкого харчування надала таку

можливість: раніше 2021 року понад 19 ресторанів почали приймати оплату в біткойні в Сальвадорі .

Країни *Латинської Америки* стоять особняком. Там, на відміну від США та Європи, криптоплатежі стали популярні не від хорошого життя, а через те, що крипта стала єдиним способом хоч якось упоратися з економічною кризою та інфляцією. Наприклад, у *Венесуелі* до 30% мешканців – безробітні, а середньорічна інфляція у 2018 році сягала 1.370.000%. Саме в цій країні зараз налічується понад 5.000 (1.000 лише у столиці Каракасі) організацій, які приймають цифрові валюти, і цей ринок постійно зростає. Можливість оплати криптою є практично у всіх сферах – кафе, мед. послуги, оренда готелів та автомобілів, поповнення мобільного зв'язку та інтернет-послуг, купівля авіаквитків, електроніки, продовольчих/непродовольчих товарів (рис. 2.18) .

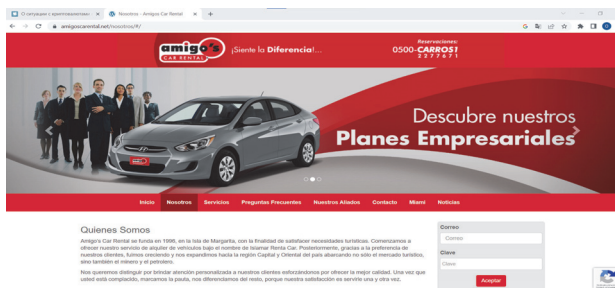


Рисунок – 2.18 Компанія Amigos Car Rental (Венесуела) приймає оплату в криптовалюти

Фактично резиденти країн Заходу та деяких країн Близького Сходу та Азії можуть оплачувати товари та послуги криптовалютами навіть тоді, коли продавець не приймає оплату у крипті. Для цього існує безліч способів конвертації криптовалюти у фіат ще на стороні покупця – таким чином, криптовалютами можна оплачувати практично все що завгодно. Крипто-дебетові (або передплатені) карти пропонують великі централізовані біржі типу Binance чи Crypto.com, а також сервіси на кшталт BitPay чи Revolut, Wirex чи Wise. Свою повномасштабну систему конвертації криптовалюти у фіат тестують і найбільші платіжні системи, наприклад, VISA. На жаль, сьогодні ці інструменти доступні лише резидентам конкретних країн (ЄС та США).

Податки та державні послуги. У місті Лугано у *Швейцарії*, де криптовалюти визнані офіційним платіжним засобом, поряд із фастфудом можна сплатити й податки. Загалом до системи платежів вже приєдналося понад 60 продавців товарів та послуг, включаючи державні послуги (рис. 2.19).

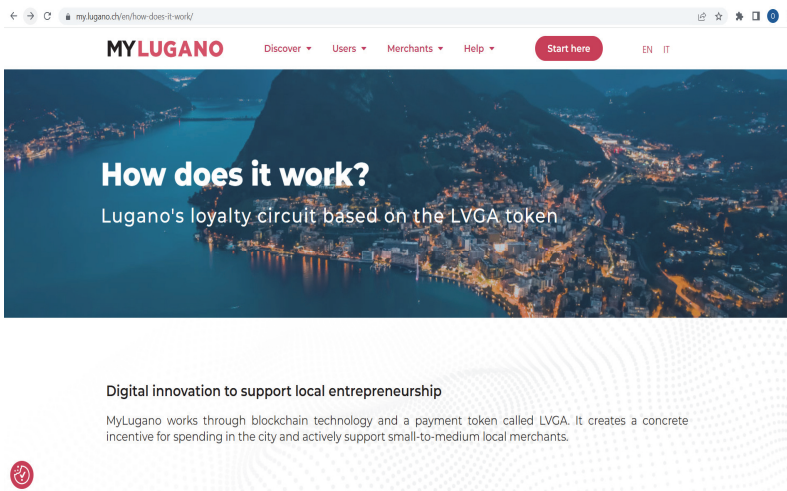


Рисунок – 2.19 Сайт м. Лугано у Швейцарії пропонує розрахунки в криптовалюті

У *Нью-Йорку* державні органи можуть на законних підставах приймати платежі у криптовалюті. Більше того, у деяких штатах США платежі в крипті приймають навіть деякі ресурсопостачальні організації.

Нещодавно жителі 37 міст *Аргентини* отримали можливість розплатитися биткоїном у громадському транспорті. А завдяки інтеграції з платіжними системами, аргентинці можуть платити за комунальні послуги будь-яким криптовалютним гаманцем, включаючи Binance, Bitso, Buenbit, Byubit, Ripio та Lemon. До оплати приймаються стейблкоїни – у тому числі DAI та USDT.

Подорожі. На окрему увагу заслуговує сфера туризму. Індустрія туризму, будучи одним із найбільших бенефіціарів світу без фінансових кордонів, активно розвивається у цьому напрямі.

Один із найяскравіших прикладів – криптовалютна туристична агенція Travalala.com, на якому за криптовалюту можна забронювати квитки та готелі. Загалом у сервісі понад 200.000 активних користувачів на місяць, і практично 80% вибирають для оплати саме криптовалюту. Більше того, нещодавно вони оголосили про запуск децентралізованого сервісу з оренди нерухомості, який має скласти конкуренцію самому Airbnb.

Багато сервісів (не тільки пов'язані з подорожами) містять інформацію про можливість оплатити послуги або товари криптоплатами внизу сторінки (рис. 2.20). Однак найнадійніший спосіб зрозуміти, чи приймає той чи інший сервіс оплату в криптовалюті – дійти до етапу оплати та вибрати з переліку доступних оплат за допомогою BitPay або аналогічних сервісів.

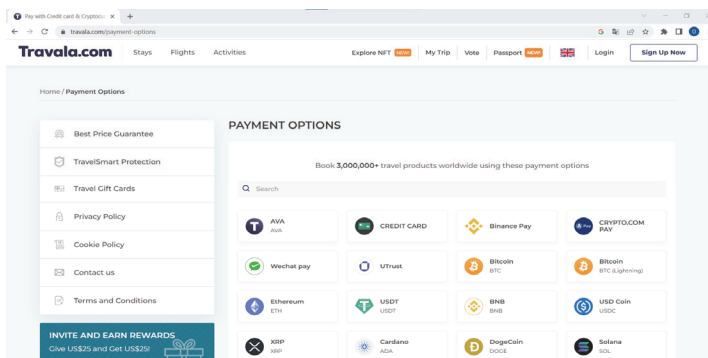


Рисунок – 2.20 Список платіжних сервісів, що працюють на сайті travala.com

З інших помітних агентств та агрегаторів можна звернути увагу на Cryptoturismo, Flight Centre, GetYourGuide та Crypto Cruise Deals .

Оплату в криптовалюті приймають і окремі авіаперевізники, наприклад AirBaltic і Virgin Airlines , а також оператори приватних літаків Cielo Aviation, Fast Private Jet і JetFinder.

Нерухомість. Навіть консервативний ринок нерухомості не став винятком: дедалі більше країн дозволяють купувати нерухомість з використанням крипти. Це швидше, ефективніше та вигідніше в порівнянні з традиційними банківськими розрахунками, а значить дозволяє залучати ширшу аудиторію клієнтів (рис. 2.21).

Таїланд – одна з перших азіатських країн, що легалізували криптовалюту: держава дозволяє покупцям нерухомості здійснювати платежі цифровими грошима. Проте інвестори зобов'язані звертатися за послугами місцевих акредитованих агентств нерухомості, які приймають віртуальні валюти.

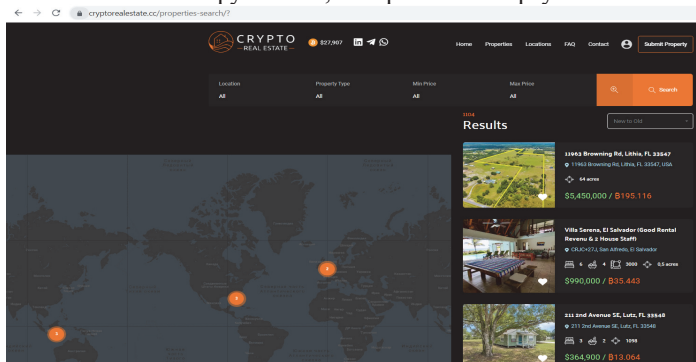


Рисунок – 2.21 Сайт Crypto Real Estate (купівля нерухомості за криптовалюту)

Криптовалютний ринок *Об'єднаних Арабських Еміратів* виріс у кілька разів за останні два роки і, за прогнозами, зросте вдесятеро протягом наступних кількох років. В ОАЕ можна купувати будинки, вілли, квартири та будівлі, використовуючи крипту через уповноважені агенції.

Центробанк ОАЕ ще не визначив криптовалюти як законний платіжний засіб, проте крипто-транзакції між фізичними особами та деякими регульованими агентствами нерухомості дозволені.

У *Туреччині* також деякі агентства нерухомості приймають криптовалютні платежі, а в країні, як і раніше, діє програма «золотої візи»: вкладення в нерухомість сумою понад 400.000 доларів дозволять отримати дозвіл на проживання.

Уряд *Португалії* дозволив купувати нерухомість з використанням криптовалюти: прийняті закони класифікують купівлю нерухомості за віртуальні гроші як бартерні. Раніше операції потрібно було здійснювати з обміном цифрових грошей на фіатні.

Чорногорія вважається найбільшою фінансово-ліберальною державою на Балканах – у країні відсутні особливі вимоги до криптовалютних угод, включаючи купівлю нерухомості. В останні роки Чорногорія прагне стати великим криптоцентром регіону та приймає низку законів для легалізації та спрощення обороту криптовалюти.

У *Грузії* також можна купити нерухомість із використанням криптовалюти, але цифрові гроші не регулюються в країні. Тому остаточна сума купівлі, внесена до реєстру власності, має бути зазначена у фіатному еквіваленті. Купівля нерухомості з розрахунком у крипті може здійснюватись лише через ліцензовані агентства нерухомості.

Ринок праці: криптоплатежі для бізнесу. Поки що більшість криптовалютних транзакцій в результаті конвертується у фіат. Однак багато бізнесів не тільки приймають оплати у криптовалюти, а й використовують її для виплати зарплат співробітникам.

Яскравий приклад – Аргентина. За останній рік кількість компаній, які оплачують роботу співробітників у криптовалюти, збільшилась на 340%. Тепер Аргентина – це країна з найвищим % виплат зарплат у цифрових активах. Криптовалюти стали одним із найдієвіших способів забезпечити стабільну та надійну роботу бізнесу в умовах економічної турбулентності (рис. 2.22).

Якщо раніше фіат на крипту міняли так, то сьогодні це не обов'язково. Ще більше криптоплатежі поширені при розрахунках із фрілансерами, з якими сьогодні працюють усі: від бутикових агентств до міжнародних корпорацій. Щороку дедалі більше віддалених виконавців переходять на крипту, відмовляючись від роботи з фіатними грошима.

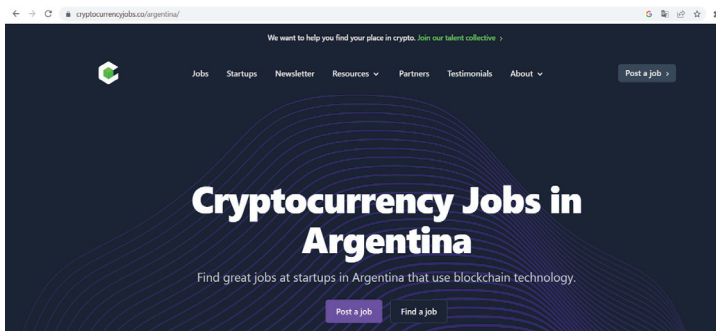


Рисунок – 2.22 Сайт пошуку роботи з оплатою криптовалютою

Ось деякі майданчики, де можна знайти виконавців, які приймають криптовалюту:

P2payer-Freelance – міжнародний мультимовний маркетплейс фріланс-послуг. Майданчик пропонує не тільки зручний пошук та функціонал для взаємодії замовників та виконавців, а й механізми узгодження вартості послуг.

Freelancehunt – перша в російськомовному сегменті біржа з оплатою роботи фрілансерів криптою.

Freelance for Coins – міжнародна фріланс-біржа, на якій можна знайти виконавців різних спеціальностей з оплатою в криптовалютах. Більшість завдань пов'язані з перекладами, написанням текстів, дизайном і програмуванням.

Cryptocurrency Jobs – ресурс для пошуку віддалених співробітників та фрілансерів. На платформі розміщуються заявки працювати від провідних криптокомпаній світу.

Bitcoinjobs – одна з найпопулярніших платформ з великою кількістю роботодавців та виконавців.

Однак для компаній за простим на вигляд запитом «виплатити зарплату» стоїть величезна робота із систематизації, організації та обробки криптоплатежів. Для безпечної та стабільної роботи з клієнтами та підрядниками бізнесу важливо мати «під капотом» потужний та надійний інструмент.

Тим, хто вже перейшов на розрахунки в криптовалютах, варто звернути увагу на сервіс криптобухгалтерії MFPay – він допомагає бізнесу організувати зручні розрахунки криптовалютів з підрядниками, партнерами і клієнтами. Буквально в кілька кліків можна налаштувати власну систему та керувати всіма платежами у криптовалюті. У MFPay можна виставляти та оплачувати рахунки, вести облік платежів, зберігати та структурувати контрагентів.

ВИСНОВКИ ДО РОЗДІЛУ 2

Україна має ряд обмежень та регулювань щодо вводу-виводу криптовалют. Це може включати обов'язкову ідентифікацію, обмеження кількості та сум переказів, а також потребу відповідності до фінансового моніторингу.

Кріптоміксери (також відомі як міксери або туманні мережі) використовуються для змішування та анонімізації транзакцій криптовалют. Однак, використання неперевіраних кріптоміксерів може належати до нелегальних діяльностей та створювати ризики для користувачів.

Легітимні криптовалютні біржі та платіжні сервіси, що відповідають вимогам регулювання та фінансового моніторингу, можуть стати надійними каналами для вводу-виводу криптовалют в Україні.

Для забезпечення безпеки та мінімізації ризиків необхідно активно вдосконалювати освіту та свідомість користувачів щодо правил використання криптовалют, захисту приватності та використання надійних сервісів.

Україна може співпрацювати з міжнародними організаціями та іншими країнами для розв'язання спільних проблем, таких як боротьба зі шахрайством, відмивання грошей та фінансуванням тероризму.

Загалом, використання криптовалют в Україні вимагає уважного вивчення нормативного середовища, обережного вибору платіжних сервісів та бірж, а також підвищеної свідомості користувачів.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Наведіть особливості купівлі криптовалют.
2. Наведіть алгоритм поповнення криптогаманця кредитною картою.
3. Наведіть особливості поповнення криптогаманця через термінали самообслуговування.
4. Наведіть особливості поповнення криптогаманця в криптообміннику.
5. Які є способи купівлі криптовалют?
6. Які особливості здійснення фінансових операцій з використанням криптовалют?
7. Які особливості використання анонімних віртуальних кредитних карт?
8. Які особливості використання криптоміксерів для підвищення анонімності платежів? Наведіть приклади популярних криптоміксерів.
9. Які особливості використання безпечних криптогаманців? Наведіть приклади популярних анонімних криптовалют.
10. Розкрийте особливості виведення коштів з криптовалютної системи.
11. Розкрийте особливості роботи з криптоактивами в Україні.
12. Розкрийте особливості роботи з криптоактивами в рф.
13. Розкрийте особливості виведення криптоактивів з території третіх країн.
14. Наведіть основні проблеми пов'язані з кібербезпекою використання криптовалют.
15. Надайте характеристику законодавчої бази в Україні щодо обігу криптовалют.

РОЗДІЛ 3

КІБЕРБЕЗПЕКА ПРИ ВИКОРИСТАННІ КРИПТОВАЛЮТ

В розділі розглянуті такі питання як псевдонімність криптовалют, безпечні криптовалюти, кібербезпека співробітника, використання анонімної операційної системи типу Live USB TAILS, використання анонімної віртуальної операційної системи Whonix.

3.1. Поняття псевдонімності криптовалют

Псевдонімність в криптовалютах означає можливість приховати реальні ідентифікатори осіб, які здійснюють транзакції, за допомогою використання псевдонімів або випадково згенерованих адрес. Це дозволяє забезпечити певний рівень конфіденційності та анонімності.

В криптовалютах з псевдонімністю, таких як Bitcoin, Ethereum і багато інших, транзакції записуються в публічний реєстр, відомий як блокчейн. У блокчейні зберігається інформація про адреси відправників та отримувачів та суми транзакцій. Однак, реальні ідентифікатори або особиста інформація не пов'язані прямо з цими адресами.

При використанні псевдонімів або випадково згенерованих адрес для кожної транзакції у криптовалюті можна забезпечити певний рівень анонімності. Це ускладнює можливість прослідкування та ідентифікації реальних осіб за адресами та транзакціями.

Проте варто зазначити, що псевдонімність не є повною анонімністю. В деяких випадках за допомогою аналізу блокчейну, вивченням громадських даних та інших методів можливе встановлення зв'язку між псевдонімами та реальними особами.

Деякі криптовалюти, такі як Monero та Zcash, пропонують більш високий рівень приватності та конфіденційності, за допомогою використання різних протоколів та технологій, що дозволяють приховати дані про адреси та суми транзакцій.

В будь-якому випадку, рівень псевдонімності та анонімності використання криптовалют залежить від кожної конкретної криптовалюти та способів використання.

3.2. Безпечні криптовалюти

Безпечні криптовалюти, такі як Monero, є ті, що надають підвищений рівень приватності та конфіденційності в порівнянні з іншими криптовалютами, такими як Bitcoin (рис. 3.1). Основна мета таких

криптовалют – забезпечити анонімність та приховати дані про адреси, суми транзакцій та інші деталі.

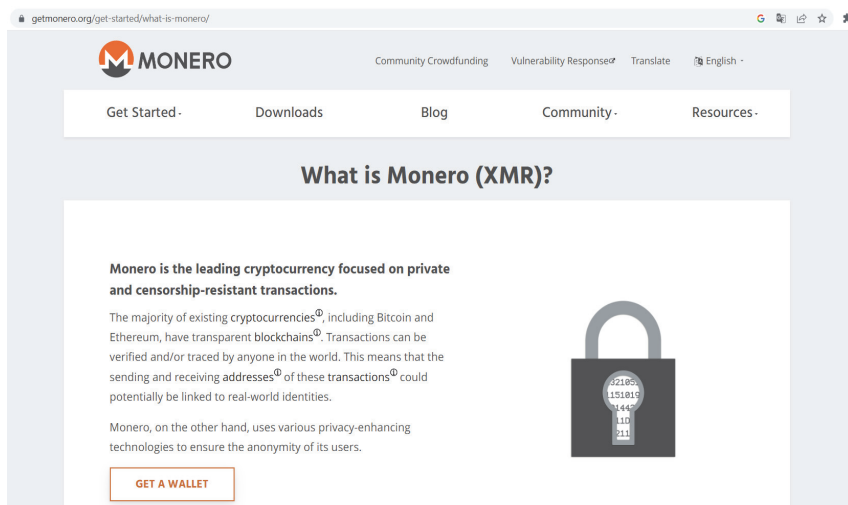


Рисунок – 3.1 Сайт криптовалюти Monero

Monero, заснований на протоколі CryptoNote, є однією з найпопулярніших безпечних та приватних криптовалют. Основні особливості Monero, що забезпечують приватність, включають:

Приховані адреси: кожна транзакція Monero має унікальну одноразову адресу, що ускладнює прослідкування транзакцій та встановлення зв'язку між адресами.

Кільцеві підписи: використання кільцевих підписів у Monero дозволяє забезпечити псевдонімність, перекриваючи сліди транзакцій.

Кільцеві конфіденційні транзакції (RingCT): цей протокол дозволяє приховати суми транзакцій, що робить їх нечитабельними для сторонніх спостерігачів.

Додатковий рівень шифрування: Monero використовує симетричне шифрування для забезпечення конфіденційності даних у блокчейні.

Всі ці технології та протоколи, що використовуються в Monero, спрямовані на забезпечення приватності та конфіденційності користувачів. Втім, важливо пам'ятати, що абсолютна анонімність не гарантується, і в деяких випадках можуть виникати технічні або правові обмеження.

Для створення криптогаманця Monero Ви можете використовувати офіційний гаманець Monero, відомий як «Monero GUI Wallet».

Ось кроки, які можна виконати для створення гаманця Monero:

Крок 1: Завантажте програмне забезпечення Monero GUI Wallet з офіційного сайту Monero (<https://www.getmonero.org/downloads/>). Оберіть відповідну версію для своєї операційної системи (Windows, macOS, Linux).

Крок 2: Після завантаження програмного забезпечення встановіть його на свій комп'ютер, вибравши відповідну версію для своєї операційної системи.

Крок 3: Після встановлення відкрийте Monero GUI Wallet. Ви побачите початковий екран зі створенням нового гаманця.

Крок 4: Виберіть "Create a new wallet" (Створити новий гаманець) і натисніть "Continue".

Крок 5: Виберіть "Standard wallet" (Стандартний гаманець) і натисніть "Continue".

Крок 6: Виберіть "Create a new wallet file" (Створити новий файл гаманця) і натисніть "Continue".

Крок 7: Виберіть назву та розташування для вашого нового гаманця Monero. Введіть надійний пароль, який буде використовуватись для доступу до гаманця, і натисніть "Continue".

Крок 8: Запишіть мнемонічну фразу, яка буде використовуватись для відновлення гаманця у разі втрати доступу до нього. Збережіть цю фразу в безпечному місці і ніколи не діліться нею з іншими людьми.

Крок 9: Ваш гаманець Monero створений! Ви побачите головний екран зі своїм адресою Monero та іншою інформацією.

За допомогою Monero GUI Wallet ви зможете отримувати, зберігати та надсилати Monero (XMR), а також здійснювати різні операції з вашими коштами. Важливо пам'ятати про безпеку, резервні копії та використання сильного пароля для захисту вашого гаманця Monero.

Крім Monero, існує кілька інших криптовалют, які відомі своїм підвищеним рівнем безпеки та приватності. Ось кілька з них:

Zcash (ZEC) – є криптовалютою, яка забезпечує приватність за допомогою протоколу zk-SNARKs. Вона дозволяє користувачам здійснювати повністю анонімні транзакції, приховуючи дані про адреси відправників, отримувачів та суми транзакцій.

Dash (DASH) – використовує технологію PrivateSend, яка забезпечує змішування транзакцій. Це дозволяє приховувати походження коштів та забезпечує певний рівень приватності.

Verge (XVG) – використовує комбінацію різних протоколів, таких як TOR і I2P, для забезпечення анонімності транзакцій та IP-приховування.

Grin (GRIN) – є криптовалютою, заснованою на протоколі Mimblewimble, який дозволяє стискати транзакційні дані та приховувати деяку інформацію, таку як адреси та суми.

Це лише кілька прикладів криптовалют, які приділяють особливу увагу безпеці та приватності. Варто пам'ятати, що рівень безпеки та приватності може різнитися в залежності від криптовалюти та її протоколів. Також важливо розуміти, що незалежно від рівня безпеки, використання криптовалют потребує деяких заходів обережності та безпеки з боку користувача.

3.3. Особливості забезпечення кібербезпеки та анонімності співробітника

Використання криптовалют пов'язане зі зберіганням та керуванням цифровими активами, тому забезпечення безпеки є критично важливим. Деякі рекомендації, як забезпечити безпеку при використанні криптовалют:

Вибір безпечного гаманця: Використовуйте надійні криптогаманці з хорошою репутацією та сильною системою безпеки. Ретельно перевіряйте рецензії та рекомендації від користувачів перед використанням гаманця.

Нижче ви знайдете список перевірених та безпечних криптогаманців, популярних серед трейдерів та інвесторів з усього світу. За допомогою рейтингу ви зможете вибрати найкращий криптовалютний гаманець.

Ledger Nano X. Апаратний мультивалютний гаманець компанії Ledger, яка займається створенням криптовалютних сховищ з 2014 року. Фактично це невеликий Bluetooth-пристрій для зберігання криптографічних ключів, яким можна керувати зі смартфона або підключатися до комп'ютера по USB.

Exodus. Мультивалютний гаманець доступний у вигляді програми для комп'ютерів, розширення для браузерів та мобільного формату. Exodus має зручний інтерфейс та підійде для новачків. Він підтримує сотні криптовалют і дозволяє не тільки зберігати, а й купувати, продавати та обмінювати кошти.

MetaMask. Гаманець для криптовалюти у вигляді браузерного розширення для роботи з ETH та іншими токенами на базі блокчейну Ethereum. MetaMask підтримує взаємодію зі смарт-контрактами, він сумісний з апаратними гаманцями та DApps (децентралізованими додатками).

Atomic Wallet. Підтримує понад 350 валют та токенив. Сервіс пропонує не лише гаманець для зберігання, але також купівлю та обмін коштів. Для роботи з ним можна використовувати програму для Windows, macOS та Linux, а також мобільний додаток.

Guarda Wallet. Безкоштовний універсальний гаманець криптовалюти, користувачі якого можуть отримати доступ до своєї криптовалюти на ПК. Він підтримує понад 400 тисяч цифрових активів. Користувачі Guarda можуть переміщувати криптовалюту на холодне зберігання за допомогою інтеграції з гаманцем апаратного Ledger. Guarda (рис. 3.2).

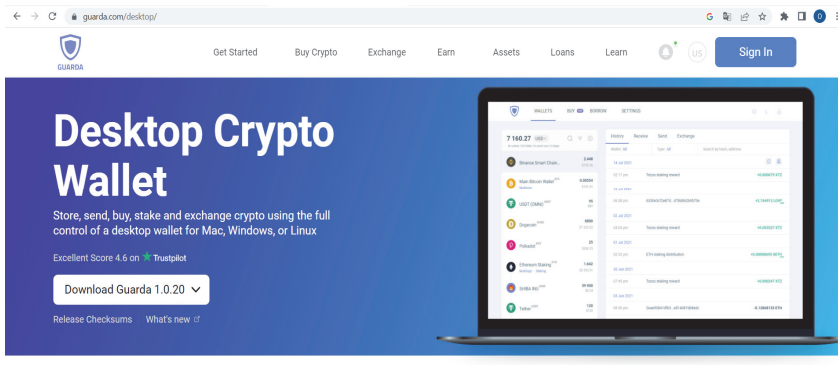


Рисунок – 3.2 Сайт криптогаманця *Guarda Wallet*

Jaxx Liberty. Підтримує десятки цифрових активів. Гаманець працює на Android, iOS, macOS, Windows, Linux та Google Chrome. Усі приватні дані зберігаються локально на пристрої.

Trust Wallet. Обходить по функціоналу всі некастодіальні онлайн-гаманці. А його токен наразі є одним з найбільш обговорюваних на ринку, що підтверджує інтерес та довіру аудиторії до цього криптогаманця.

MyEtherWallet (MEW). Один з найпопулярніших і надійних сервісів для роботи з блокчейном Ethereum. Він дозволяє приймати та відправляти кошти на рахунок, обмінювати валюти, а також отримувати пасивний дохід через стейкінг.

Mycelium Wallet. Мобільний крипто гаманець, який пропонує додатковий рівень безпеки за рахунок використання ієрархічної детермінованої (HD) структури та двофакторної аутентифікації.

Trezor One. Апаратний крипто гаманець, який підтримує велику кількість валют. Trezor One активується за допомогою програми для комп'ютера. Пристрій підключається до ПК на Windows, macOS та Linux, а також до Android смартфонів за допомогою USB.

Зберігання приватних ключів: приватні ключі використовуються для доступу до криптовалютних активів, тому забезпечення їх безпеки є надзвичайно важливим. Зберігайте приватні ключі в надійних місцях, таких як апаратні гаманці або безпечні електронні пристрої. Не розголошуйте свої приватні ключі нікому і не зберігайте їх у відкритому вигляді на комп'ютері чи в хмарних сервісах.

Двофакторна аутентифікація: Використовуйте двофакторну аутентифікацію (2FA) для своїх криптовалютних гаманців та обмінних платформ. Це додатковий шар захисту, який вимагає підтвердження вашої особи через додатковий пристрій або код.

Оновлення програмного забезпечення: Регулярно оновлюйте програмне забезпечення вашого криптогаманця та комп'ютера, щоб уникнути

вразливостей безпеки. Важливо використовувати офіційні та актуальні версії програм.

Фізична безпека: Забезпечте фізичну безпеку своїх криптовалютних пристроїв та інших засобів зберігання. Уникайте використання загальнодоступних комп'ютерів або мереж Wi-Fi, якщо вони не є безпечними.

Перевірка посилань: Уникайте кліків на підозрілі посилання, особливо у електронних повідомленнях або повідомленнях в соціальних мережах. Це можуть бути фішингові атаки, спрямовані на крадіжку ваших криптовалютних активів або приватних ключів.

Резервне копіювання: Регулярно робіть резервні копії своїх криптовалютних гаманців та приватних ключів. Зберігайте ці резервні копії в безпечних місцях, віддалених від потенційних ризиків.

Дослідження перед участю: Перед вкладанням коштів в нові криптовалюти або проекти, ретельно досліджуйте їх, перевіряйте команду, технологію та репутацію. Уникайте підозрілих або недостовірних проектів.

Загалом, свідомий підхід до безпеки, дотримання вищезгаданих рекомендацій та постійний контроль над своїми криптовалютними активами допоможуть забезпечити їх безпеку.

Забезпечення повної анонімності: при використанні криптовалют може бути складним завданням, оскільки багато блокчейн-технологій, на яких ґрунтуються криптовалюти, є публічними та трасують всі транзакції. Однак, існують деякі заходи, які можна прийняти для покращення рівня анонімності. Нижче наведено кілька рекомендацій:

Використання анонімних гаманців: оберіть криптогаманці, які дозволяють вам зберігати та пересилати криптовалюту з більшим рівнем анонімності. Наприклад, деякі гаманці забезпечують змішування транзакцій, що робить їх важкими для відстеження.

Анонімні гаманці без верифікації – найактуальніший варіант зберігання криптовалюту, починаючи з моменту її появи. Такі гаманці належать до децентралізованих або некастодіальних.

Перераховані сервіси не вимагають від користувача реєстрації або верифікації та не зберігають його ключі або інші особисті дані. Однак, якщо ви скористаетесь ними для купівлі криптоактивів з картки, то втратите анонімність, адже картка прив'язана до вашої особистості. Нижче наведені найпоширеніші криптогаманці:

Trust Wallet – зручний мобільний гаманець від біржі Binance;

Metamask – найкращий гаманець-розширення для доступу до децентралізованих додатків і протоколів через браузер;

Binance Wallet – розширення для роботи з мережами BNB Beacon Chain, BNB Smart Chain і Ethereum;

Ledger, Trezor, SafePal та інші – апаратні гаманці для холодного зберігання криптовалют;

imToken – мультивалютний мобільний гаманець із підтримкою 12 блокчейнів і всіх розміщених на них монет;

Token Pocket – інший мультивалютний мобільний гаманець, доступний також у вигляді браузерного розширення;

MathWallet – гаманець, що підтримує 100+ блокчейнів, працює з браузера і з мобільних пристроїв;

Atomic Wallet – мультиплатформний сервіс, дає можливість зберігати 300+ монет і токенів;

Jaxx – один із найстаріших і перевірених гаманців, доступний на різних пристроях;

Exodus – зручний децентралізований криптогаманець із підтримкою 180+ криптоактивів;

Bitcoin Core – офіційний гаманець для BTC, якій є найбезпечнішим програмним сховищем для біткоіна;

Wasabi – гаманець для біткоіна з вбудованими функціями додаткової конфіденційності (рис. 3.3):

MyEtherWallet – гаманець для ETH, токенів ERC20, NFT.

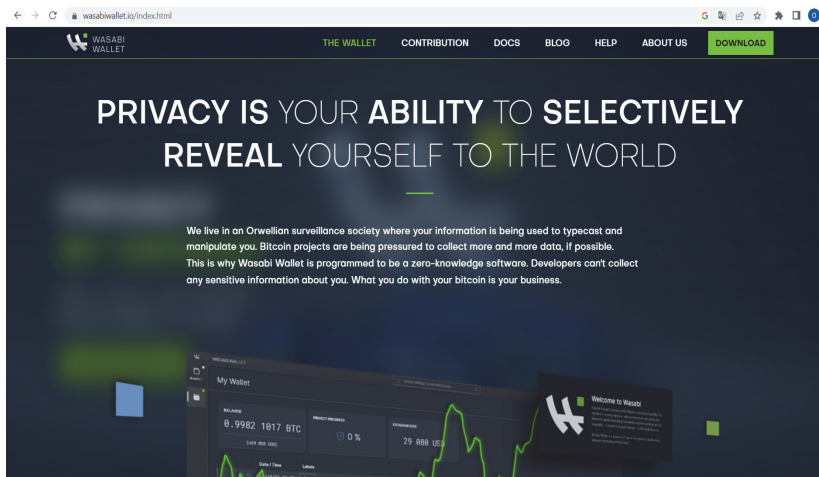


Рисунок – 3.3 Сайт криптогаманця *Wasabi*

Некастодіальні децентралізовані сервіси – єдиний по-справжньому безпечний спосіб зберігання криптовалют. Хоч би які гарантії та обіцянки не давали централізовані гаманці й біржі, їх дотримуються рівно до того моменту, доки у світі не трапляється якогось масштабного потрясіння, санкцій, урядових заборон.

Використання анонімних криптовалют: деякі криптовалюти, такі як Monero (XMR) або Zcash (ZEC), мають вбудовані функції конфіденційності,

які дозволяють приховати деталі транзакцій, такі як сума та адреси відправника та отримувача (рис. 3.4).

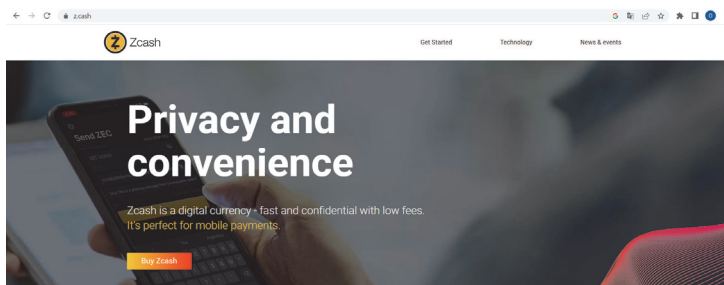


Рисунок – 3.4 Сайт криптовалюти Zcash (ZEC)

Використання децентралізованих бірж: деякі децентралізовані біржі дозволяють торгувати криптовалютами без необхідності реєстрації акаунта, що може покращити рівень анонімності.

Децентралізована біржа – це додаток для торгівлі криптоактивами, в якому обмін та інші операції відбуваються за допомогою смарт-контрактів без використання централізованої торгової системи. Користувачі здебільшого отримують доступ до DEX або через веббраузер, або за допомогою додатків для смартфонів (рис. 3.5).

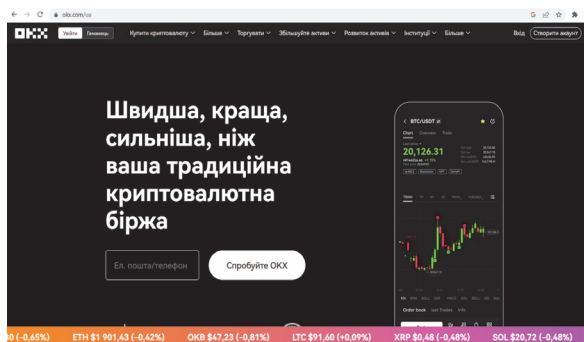


Рисунок – 3.5 Сайт DEX-крипобіржі OKX

Принципова відмінність децентралізованих бірж від централізованих у тому, що вони не зберігають кошти користувачів і не контролюють угоди. Кошти переказують безпосередньо з гаманця користувача, який той підключає до децентралізованої платформи.

Також DEX не мають процедури верифікації користувачів (KYC), тобто угоди можна виконувати повністю анонімно, що часто використовується шахраями.

Децентралізовані біржі стали найважливішим елементом галузі децентралізованих фінансів (DeFi). Станом на початок 2023 року, згідно даних coinmarketcap, існує майже 300 децентралізованих бірж, які працюють на декількох десятках блокчейнів – найпопулярніші з них є:

- *OKX* – децентралізована криптобіржа з понад 340 токенами;
- *Uniswap* – популярна децентралізована біржа для DeFi;
- *PancakeSwap* – найкращий DEX для відкриття нових криптовалют;
- *SushiSwap* – швидкозростаюча DEX для криптофермерства;
- *dydx* – провідна децентралізована криптобіржа для денної торгівлі;
- *Curve Finance* – найкращий DEX для стейкінгу криптовалют DeFi;
- *Kine Protocol* – розширений DEX для криптотрейдингу та ставок;
- *ApolloX* – торгуйте децентралізованими ф'ючерсами на біткоїн.

Використання VPN та IP-анонімізаторів: використання віртуальних приватних мереж (VPN) та інших IP-анонімізаторів може приховати вашу реальну IP-адресу під час використання криптовалютних сервісів. Найкращі VPN для криптовалют:

- *ExpressVPN* – максимальна швидкість передачі даних та розширені функції безпеки для торгівлі криптовалютою, надається 30-денна гарантія повернення грошей;

- *CyberGhost* – сервери NoSpy відрізняються підвищеною продуктивністю та забезпечують безпеку ваших угод, хоча політика конфіденційності не пройшла незалежний аудит;

- *Private Internet Access* – вбудований блокувальник реклами, засобів відстеження та шкідливого ПЗ на криптовалютних сайтах, але швидкість нижча, ніж у ExpressVPN та CyberGhost (рис. 3.6);

- *PrivateVPN* – бюджетний VPN із високопродуктивною серверною мережею, що дозволяє стабільно користуватися ринком криптовалют, але набір функцій відрізняється залежно від клієнта;

- *IPVanish* – необмежену кількість підключень для торгівлі з усіх ваших пристроїв, але компанія має підозріле минуле.



Рисунок – 3.6 Сайт VPN сервісу *Private Internet Access*

Використання нових адрес: використовуйте нові криптовалютні адреси для кожної транзакції, щоб ускладнити спроби прослідкування ваших дій.

Важливо пам'ятати, що повна анонімність використання криптовалют є складним завданням, і не завжди можна досягти повного рівня конфіденційності. Також варто враховувати правові аспекти і рекомендації країни, в якій ви проживаєте, оскільки анонімне використання криптовалют може мати обмеження або регуляції.

Загальний алгоритм використання криптогаманця. Створення та використання анонімного криптогаманця може варіюватися залежно від конкретного гаманця та протоколу, на якому він базується. Проте основні кроки можуть бути наступними:

Крок 1: Завантаження і встановлення гаманця. Виберіть анонімний криптогаманець, який відповідає вашим вимогам до приватності та безпеки. Завантажте програму гаманця з офіційного джерела, якщо вона доступна. Переконайтеся, що ви завантажаєте програму з надійного джерела, щоб уникнути можливості отримання підробленої версії.

Крок 2: Створення нового гаманця. Зазвичай у гаманці є опція створення нового гаманця. Виберіть цю опцію і дотримуйтеся інструкцій на екрані для генерації нового гаманця. Зазвичай процес включає створення зашифрованого приватного ключа, який буде використовуватися для доступу до вашого гаманця, а також генерацію публічного ключа для отримання платежів.

Крок 3: Збереження резервних копій. Дуже важливо зберегти резервну копію вашого приватного ключа. Це дає вам можливість відновити доступ до вашого гаманця, якщо ви втратите приватний ключ або забудете пароль. Збережіть резервну копію у безпечному місці, відокремленому від комп'ютера або пристрою, на якому встановлений гаманець.

Крок 4: Використання гаманця. Після створення гаманця ви зможете використовувати його для отримання та відправлення криптовалюти. Гаманець зазвичай надає вам унікальну адресу, яку ви можете використовувати для отримання платежів. Ви також зможете підписувати та відправляти транзакції за допомогою вашого приватного ключа.

Крок 5: Дотримання правил безпеки. Використовуючи анонімний криптогаманець, важливо дотримуватися правил безпеки. Зберігайте свій приватний ключ в безпечному місці і не розголошуйте його нікому. Використовуйте надійний пароль для захисту вашого гаманця. Оновлюйте програму гаманця, коли з'являються нові версії з виправленнями помилок та поліпшеннями безпеки.

Зверніть увагу, що це загальні кроки, і кожен криптогаманець може мати власні особливості та процедури. Для кожного конкретного гаманця рекомендується докладно ознайомитися з документацією та інструкціями, що надаються розробниками гаманця.

3.4. Особливості використання анонімної операційної системи Live USB TAILS

Операційна система (ОС) Tails (The Amnesic Incognito Live System) розроблена з огляду на забезпечення максимальної приватності та анонімності користувачів (рис. 3.7).

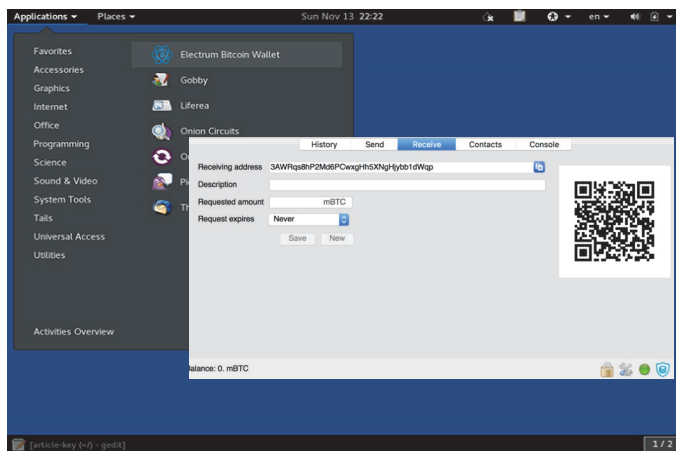


Рисунок – 3.7 Процес завантаження додатку криптогаманця Electrum – меню операційної системи TAILS

Деякі з технологій, які використовуються в Tails для досягнення анонімності, включають:

Tor: Tails використовує Tor (The Onion Router) для забезпечення анонімного інтернет-з'єднання. Тор перенаправляє ваш трафік через декілька вузлів мережі, маскуючи вашу реальну IP-адресу та шифруючи ваше з'єднання. Це допомагає забезпечити приватність та анонімність при використанні Інтернету.

Заборона запису: Tails працює в режимі «amnesic», що означає, що всі зміни, внесені під час роботи з операційною системою, автоматично видаляються при вимкненні комп'ютера. Це допомагає уникнути залишків інформації про ваші дії та захищає вашу приватність.

Захист даних: Tails використовує криптографічні методи для захисту ваших даних. Він автоматично шифрує всю інформацію на вашому пристрої за допомогою інструментів шифрування, таких як LUKS (Linux Unified Key Setup) або eCryptfs. Це допомагає захистити ваші дані від несанкціонованого доступу.

Захист від атак: Tails включає набір інструментів для захисту від різних типів атак. Це включає захист від фішингу, використання шифрованих з'єднань та запобігання відстеженню.

Додаткові інструменти: Tails містить додаткові інструменти для забезпечення приватності та анонімності, такі як інструменти для роботи з криптовалютами та інструменти для видалення метаданих з файлів.

Важливо враховувати, що анонімність – це складне поняття, і вона залежить від багатьох факторів. Використання Tails може допомогти забезпечити додатковий рівень приватності та анонімності, але важливо розуміти, що жодна система не є абсолютною. Завжди дотримуйтесь найкращих практик безпеки та приватності при роботі з криптовалютами та інтернетом.

Tails є безпечною та приватною операційною системою, яка може бути використана для роботи з криптовалютами.

Ось кроки, які ви можете виконати для використання Tails для роботи з криптовалютами:

Крок 1: Завантажте Tails з офіційного веб-сайту Tails (<https://tails.boum.org/>) на безпечний комп'ютер або на USB-накопичувач.

Крок 2: Після завантаження Tails перевірте цілісність завантаженого файлу за допомогою перевірки контрольної суми або підпису. Це забезпечить, що ви отримали автентичну копію Tails.

Крок 3: Створіть загрузочний USB-накопичувач за допомогою завантаженого файлу образу Tails та інструменту для створення загрузочного накопичувача, такого як Rufus або Etcher. Слідуйте інструкціям на веб-сайті Tails для правильного створення загрузочного накопичувача.

Крок 4: Після створення загрузочного накопичувача вставте його в комп'ютер, з якого ви хочете запустити Tails, та перезавантажте комп'ютер.

Крок 5: При запуску комп'ютера виберіть загрузку з USB-накопичувача. Tails автоматично завантажиться з USB-накопичувача без збереження жодних слідів на комп'ютері.

Крок 6: Після завантаження Tails виберіть свою мову та налаштування мережі.

Крок 7: Використовуйте Tails для роботи з криптовалютами, встановлюючи відповідне програмне забезпечення, таке як криптогаманці, наявні в Tails або завантажені з офіційних джерел.

Крок 8: Перед використанням криптовалютних гаманців в Tails рекомендується ознайомитись з інструкціями й рекомендаціями, наданими розробниками конкретного гаманця. Дотримуйтесь правил безпеки, таких як створення надійних паролів і зберігання резервних копій приватних ключів.

Крок 9: Після завершення роботи з Tails вимкніть комп'ютер та вийміть USB-накопичувач. Таким чином, не залишиться слідів вашої діяльності на локальному комп'ютері.

Важливо пам'ятати, що безпека й анонімність залежать не тільки від використання Tails, але й від правильного вибору та налаштування криптогаманців та виконання відповідних безпекових заходів під час роботи з криптовалютами.

Для використання криптогаманця *Electrum* в операційній системі *Tails* потрібно виконати наступні кроки:

Крок 1: Запустіть *Tails* на своєму комп'ютері, вставивши USB-накопичувач з *Tails* і перезавантаживши комп'ютер.

Крок 2: Після завантаження *Tails* підключіться до мережі Інтернет, якщо цього вимагає ваша конфігурація.

Крок 3: Відкрийте веб-браузер у *Tails* і завантажте офіційний веб-сайт *Electrum* (<https://electrum.org/>).

Крок 4: Завантажте версію *Electrum*, яка відповідає операційній системі *Tails* (зазвичай Linux версія).

Крок 5: Після завершення завантаження відкрийте файл збірки *Electrum* (зазвичай .AppImage) і виконайте його.

Крок 6: З'явиться вікно встановлення *Electrum*. Імпортуйте свій гаманець, якщо ви вже маєте його, або створіть новий гаманець, слідуючи інструкціям на екрані.

Крок 7: Виберіть параметри безпеки для свого гаманця, включаючи налаштування пароля, шифрування і резервного копіювання гаманця. Дотримуйтесь рекомендацій безпеки, наданих *Electrum*.

Крок 8: Після налаштування гаманця ви зможете використовувати *Electrum* для перегляду балансу, отримання і відправлення криптовалюти, проведення транзакцій тощо.

Важливо пам'ятати, що під час роботи з криптогаманцем *Electrum* в *Tails* необхідно дотримуватися правил безпеки, таких як збереження приватного ключа в надійному місці і створення резервних копій.

3.5. Особливості використання анонімної віртуальної операційної системи Whonix

ОС *Whonix* також спрямована на забезпечення максимальної приватності та анонімності для користувачів (рис. 3.8).

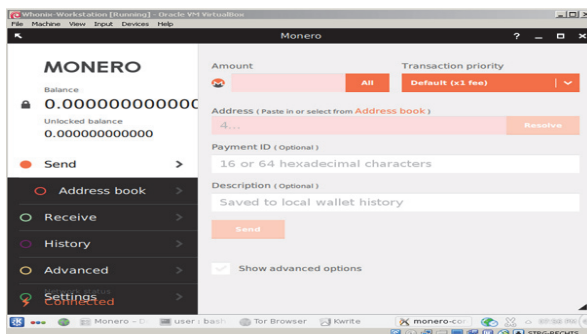


Рисунок – 3.8 Інтерфейс криптогаманця Monero (версія для ОС Whonix)

Деякі з технологій, які використовуються в Whonix, включають:

Tor: Whonix використовує Tor (The Onion Router) для маршрутизації мережевого трафіку через різні вузли, забезпечуючи анонімність та захист приватності. Всі з'єднання, що йдуть через Whonix, автоматично маршрутизуються через Тор-мережу, що допомагає захистити вашу реальну IP-адресу та забезпечити анонімне переглядання Інтернету.

Віртуалізація: Whonix використовує технологію віртуалізації, щоб розділити функції Тор-мережі від вашої основної операційної системи. Основна система (наприклад, Qubes OS або VirtualBox) використовується для запуску Whonix-Gateway, який обробляє всю мережеву активність через Тор. Захищена система Whonix-Workstation використовується для роботи з програмами та додатками, що вимагають мережевого з'єднання через Тор.

Ізоляція: Whonix забезпечує ізольоване середовище для перегляду Інтернету та роботи з програмами. Це означає, що всі програми і додатки запускаються в ізольованому середовищі, що міститься у віртуальній машині, і не мають прямого доступу до вашої основної операційної системи або інших даних на вашому комп'ютері. Це допомагає запобігти витоку інформації та захистити вашу приватність.

Захист від витоку DNS: Whonix використовує конфігурацію мережі, щоб уникнути витоку DNS-запитів через незахищені канали. Всі DNS-запити перенаправляються через Тор-мережу, що допомагає зберегти ваші DNS-запити приватними та анонімними.

Це лише деякі з технологій, які використовуються в Whonix для забезпечення анонімності та приватності. Важливо ретельно ознайомитися з документацією та інструкціями, наданими розробниками Whonix, щоб коректно налаштувати та використовувати систему з усіма її можливостями. Whonix є безпечною операційною системою, яка забезпечує анонімність та приватність при роботі в Інтернеті.

Щоб використовувати операційну систему Whonix для роботи з криптогаманцем Monero, слід виконати наступні кроки:

Крок 1: Завантажте дві віртуальні машини Whonix-Whonix-Gateway і Whonix-Workstation – з офіційного веб-сайту Whonix (<https://www.whonix.org/>). Дотримуйтесь інструкцій з завантаження та налаштування Whonix.

Крок 2: Після завантаження налаштуйте Whonix-Gateway і з'єднайте його з мережею Тор.

Крок 3: Налаштуйте Whonix-Workstation і з'єднайте його з Whonix-Gateway. Це забезпечить безпечний тунель для вашого Інтернет-з'єднання через мережу Тор.

Крок 4: Встановіть криптогаманець Monero на Whonix-Workstation. Ви можете завантажити його з офіційного веб-сайту Monero (<https://www.getmonero.org/>), слідує інструкціям для Linux.

Крок 5: Після встановлення криптогаманця Monero на Whonix-Workstation відкрийте його і налаштуйте або імпортуйте свій гаманець.

Слідуйте інструкціям, наданим розробниками Monero, для правильного налаштування та безпечного використання гаманця.

Крок 6: Запустіть Whonix-Workstation та забезпечте з'єднання з мережею Tor перед використанням криптогаманця Monero. Впевніться, що ваша з'єднання з Інтернетом забезпечується через мережу Tor для забезпечення анонімності та приватності.

Крок 7: Використовуйте криптогаманець Monero на Whonix-Workstation для перегляду балансу, отримання і відправлення криптовалюти, проведення транзакцій тощо. Пам'ятайте про правила безпеки та збереження свого приватного ключа в безпечному місці.

Важливо пам'ятати, що Whonix забезпечує анонімність та приватність, проте безпека вашого гаманця Monero залежить від правильного налаштування, виконання безпекових заходів та дотримання рекомендацій безпеки, наданих розробниками Monero.

Розробники Monero рекомендують дотримуватись наступних рекомендацій для забезпечення безпеки криптогаманця:

Завантажуйте офіційний криптогаманець: Завжди завантажуйте криптогаманець Monero з офіційного джерела, такого як офіційний веб-сайт Monero. Уникайте використання посилань з ненадійних джерел або неперевірених джерел, оскільки це може призвести до втрати коштів або компрометації вашої безпеки.

Захистіть свій приватний ключ: Приватний ключ є основою доступу до вашого криптогаманця і коштів. Забезпечте його безпеку, використовуючи надійні методи, такі як криптографічне шифрування, паролі або апаратне збереження (наприклад, апаратні гаманці).

Зберігайте резервні копії: Регулярно створюйте резервні копії свого гаманця і зберігайте їх у безпечному місці. Це дозволить вам відновити доступ до своїх коштів в разі втрати або пошкодження гаманця.

Оновлюйте гаманець: Слідкуйте за випусками оновлень криптогаманця Monero і завжди оновлюйте його до останньої версії. Оновлення часто містять виправлення безпекових уразливостей і покращення безпеки.

Уникайте публічних Wi-Fi мереж: Уникайте використання ненадійних або публічних Wi-Fi мереж для доступу до свого криптогаманця або здійснення фінансових операцій. Ці мережі можуть бути небезпечними і вразливими до атак, що можуть призвести до втрати коштів.

Використовуйте двофакторну аутентифікацію: Увімкніть двофакторну аутентифікацію для свого криптогаманця Monero, якщо це підтримується. Це надасть додатковий шар захисту для вашого облікового запису.

Дотримуйтеся безпеки комп'ютера: Забезпечте безпеку свого комп'ютера або пристрою, на якому працюєте з криптогаманцем. Встановіть антивірусне програмне забезпечення, оновлюйте операційну систему та програмне забезпечення, уникайте небезпечних веб-сайтів та завантажень.

Будьте обережними зі своїми персональними даними: Уникайте розголошення свого приватного ключа, інформації про гаманець або інших особистих даних. Не довіряйте підозрілим повідомленням, електронним листам чи запитам, які можуть мати на меті шахрайство або компрометацію вашої безпеки. Ці рекомендації допоможуть вам підвищити безпеку вашого криптогаманця Monero та забезпечити безпечну роботу з цією криптовалютою.

ВИСНОВКИ ДО РОЗДІЛУ 3

Криптовалюти в Україні піддаються ризику кібератак, які можуть спрямовуватися на обман користувачів, викрадення коштів або компрометацію приватних ключів. Забезпечення безпеки криптогаманців та інших засобів збереження має велике значення.

Зловмисники використовують фішинг та соціальний інжиніринг, щоб отримати доступ до особистих даних та приватних ключів користувачів. Популярними методами є підробка веб-сайтів обміну або гаманців, відправка шкідливих посилань та запитів на введення конфіденційної інформації.

Україна ще не має повноцінної регуляторної бази щодо криптовалют, яка б встановлювала стандарти безпеки та захисту прав користувачів. Це створює необхідність самостійної освіти та обережного підходу до використання криптовалют.

Користувачам криптовалют потрібно бути осведомленими про основні принципи кібербезпеки, використання надійних гаманців та обережність при взаємодії з підозрілими веб-сайтами або повідомленнями.

Криптовалюти, як Монепо, надають певний рівень анонімності та приватності користувачів. Проте, в сучасних умовах, з'явилися технології, які можуть допомогти відслідковувати транзакції та ідентифікувати користувачів.

Розвиток безпечних інфраструктур, таких як безпечні обмінники та гаманці, є важливим для забезпечення безпеки криптовалютних операцій та захисту від кіберзлочинців.

Загалом, використання криптовалют та анонімного використання в Україні вимагає уважного управління ризиками та свідомого підходу до забезпечення кібербезпеки. Постійна освіта користувачів, співпраця зі спеціалістами з кібербезпеки та розвиток надійних сервісів можуть допомогти створити безпечне середовище для використання криптовалют.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Розкрийте поняття псевдонімності криптовалюти.
2. Розкрийте поняття безпечні криптовалюти.
3. Наведіть зразки безпечних криптовалют.
4. Наведіть особливості криптовалюти Monero.
5. Наведіть особливості криптовалюти Zcash.
6. Наведіть особливості забезпечення кібербезпеки та анонімності співробітника.
7. Наведіть зразки безпечних криптогаманців.
8. Наведіть зразки безпечних криптобірж.
9. Наведіть зразки криптоміксерів.
10. Наведіть зразки VPN сервісів. Як забезпечується анонімність з використанням цих сервісів?
11. Наведіть основні рекомендації безпечної роботи з криптовалютами.
12. Наведіть недоліки та переваги використання анонімних криптооперацій.
13. Наведіть особливості використання анонімної ОС Live USB TAILS.
14. Наведіть особливості використання анонімної віртуальної ОС Whonix.

РОЗДІЛ 4

РОЗСЛІДУВАННЯ ЗЛОЧИНІВ В СФЕРІ КРИПТОВАЛЮТ

В розділі досліджуються питання стану та перспектив розслідувань злочинів з використанням криптовалют, а також технології розслідувань.

4.1. Основні типи злочинів з використанням криптовалют

Криптовалюти – вже давно використовують, як інструмент для злочинців. Основні типи злочинів, які можуть бути пов'язані з використанням криптовалют, включають наступні:

- *відмивання грошей* – криптовалюти можуть використовуватись для приховання походження злочинно здобутих коштів, змішування їх та перетворення у легальні активи;
- *шахрайство з криптовалютами* – включає фальшиві ICO, підставне представництво криптопроектів, фішинг, підробку гаманців та інші схеми обману;
- *крадіжка криптовалют* – незаконний доступ до гаманців або криптобірж з метою викрасти криптовалюту.
- *використання криптовалют у злочинах* – злочинці можуть використовувати криптовалюту для оплати товарів або послуг, пов'язаних зі злочинними діями, наприклад, незаконні наркотики або зброя;
- *розповсюдження зловмисного програмного забезпечення* – криптовалюти можуть використовуватись для оплати викупу в результаті атак типу «рансомвар».

Наведемо кілька прикладів викритих злочинів в сфері криптовалют в Україні до вересня 2021 року.

У 2019 році у Львові була проведена спільна операція правоохоронних органів США, Польщі та України, під час якої було затримано чотирьох осіб за створення інтернет-форуму, призначеного для злочинців з обміну злочинної інформації та продажу зловмисного програмного забезпечення. Учасники форуму обмінювались досвідом щодо викрадення грошей з банківських рахунків, крадіжки криптовалют та інших злочинів.

У 2020 році правоохоронці Києва затримали групу злочинців, які створили фальшивий криптовалютний обмінник та обманом виводили кошти у криптовалюті з рахунків жертв.

У 2021 році СБУ оголосила про припинення діяльності кількох інтернет-ресурсів, які використовувалися для виготовлення та поширення зловмисного програмного забезпечення з метою викрадення криптовалютних активів.

Важливо зазначити, що злочини в сфері криптовалют є реальною загрозою, і правоохоронні органи продовжують активно боротися з ними. При цьому користувачі криптовалют повинні бути уважними, дотримуватися основних заходів безпеки та вживати заходів для захисту своїх активів.

Приклад фінансування сепаратизму через нелегальні криптообмінники в Україні.

За інформацією правоохоронного органу, виявлена мережа підпільних криптообмінників, які дозволяють проводити анонімні платежі та системно виводити тіньові кошти та переводити їх в готівку. Послугами цих онлайн-обмінників здебільшого користувалися фізичні особи. Зокрема люди, які отримували кошти із заборонених в Україні електронних гаманців країни-агресора.

Зокрема, йдеться і про організаторів масових акцій протесту напередодні Дня Незалежності України. Саме через такі мережі вони отримували фінансування для оплати «послуг» провокаторів. Мережа функціонувала від початку 2021 року та надала послуги з переказу понад 1.000 клієнтам.

Зловмисники щомісяця переказували через таку мережу майже 30 млн гривень. За «послуги» отримували 5–10 % від суми переказу.

Правоохоронним органом розпочато кримінальне провадження за ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення» та ст. 209 «Легалізація (відмивання) доходів, одержаних злочинним шляхом» Кримінального кодексу України (КК України)).

В Україні розслідування злочинів, пов'язаних з криптовалютами, зазвичай здійснюють наступні правоохоронні органи:

- *СБУ* – займається боротьбою з кіберзлочинами, включаючи використання криптовалют для незаконних цілей, таких як кібершахрайство та викрадення коштів;

- *Національна поліція* – також займається розслідуванням кіберзлочинів в Україні, включаючи злочини, пов'язані з криптовалютами, такі як крадіжка криптовалют або шахрайство з її використанням.

Ці органи співпрацюють між собою та з іншими міжнародними партнерами для ефективного розслідування злочинів, пов'язаних з криптовалютами. Важливо підтримувати злагоджену роботу з огляду на глобальний характер криптовалют та їх перетинання між країнами.

Також до вересня 2021 року були звіти про деякі злочини в сфері криптовалют в росії:

У липні 2020 року було затримання підозрюваних у крадіжці криптовалют на суму понад 600 мільйонів рублів (близько 8 мільйонів доларів США). Злочинці використали соціальну інженерію, щоб отримати доступ до обмінних гаманців жертв.

У травні 2021 року було оголошено про арешт чотирьох осіб у росії, які були зв'язані із злочинним обігом близько 1,5 мільярда рублів (приблизно 20 мільйонів доларів США) криптовалюти. Вони звинувачувалися у використанні фінансових пірамід для обміну криптовалюти на рублі та на здійснення нелегальних операцій.

В росії розслідування злочинів, пов'язаних з криптовалютами, зазвичай здійснюють наведені нижче правоохоронні органи:

- *Міністерство внутрішніх справ російської федерації (МВД рф)* – відповідно до юрисдикції МВД рф, поліція займається боротьбою з кіберзлочинами, включаючи злочини, пов'язані з використанням криптовалют;

- *Федеральна служба безпеки російської федерації (ФСБ рф)* – має компетенцію у сфері національної безпеки, в тому числі у сфері кібербезпеки та боротьби з кіберзлочинами, включаючи злочини з використанням криптовалют;

- *Прокуратура російської федерації* – також займається контролем та наглядом за правоохоронними органами у розслідуванні злочинів, включаючи ті, що пов'язані з криптовалютами;

- *Центр «Е-кримінал»* – є частиною МВД рф і спеціалізується на розслідуванні кіберзлочинів, у тому числі тих, що пов'язані з криптовалютами;

- *Федеральна податкова служба (ФНС)* – займається контролем за використанням криптовалют у фінансових операціях та розрахунках, включаючи оподаткування доходів, отриманих у криптовалюті;

- *Федеральна служба з контролю за обігом наркотиків (ФСКН)* – може здійснювати розслідування випадків, коли криптовалюти використовуються для нелегальних операцій, таких як купівля наркотиків через даркнет;

- *Центральний банк російської федерації* – також спостерігає за використанням криптовалют та може брати участь у розслідуванні злочинів у цій сфері;

- *Федеральна служба зв'язку, інформатизації та масових комунікацій (роскомнадзор)* – цей орган контролює інформаційний простір, включаючи діяльність в інтернеті, де також можуть виникати злочини з використанням криптовалют.

Ці органи співпрацюють між собою і з іншими відповідними службами для забезпечення ефективного розслідування злочинів, пов'язаних з криптовалютами, та забезпечення додержання законів та правопорядку в цій сфері.

Покарання за скоєння фінансових злочинів, пов'язаних з криптовалютами, в російській федерації може варіюватися залежно від конкретного типу злочину та ступеня його тяжкості. Зазвичай ці злочини підпадають під статті Кримінального кодексу рф, пов'язані з

кіберзлочинами, фінансовими злочинами або економічними правопорушеннями.

Ось кілька прикладів покарань, які можуть застосовуватися за скоєння фінансових злочинів, пов'язаних з криптовалютами, в росії:

- *відшкодування завданих збитків* – злочинцю може бути накладено зобов'язання відшкодувати завдані збитки потерпілим, які виникли в результаті кіберзлочину з використанням криптовалют;

- *позбавлення волі* – за більш тяжкі злочини, такі як крадіжка великих сум криптовалют, може передбачатися покарання у вигляді позбавлення волі на певний строк;

- *фінансові санкції* – злочинець може бути оштрафований або стягнуто інші фінансові санкції, що мають на меті покарати за злочин та зміншити економічний збиток;

- *заборона на роботу з криптовалютами* – у разі засудження за злочини з криптовалютами злочинець може бути позбавлений права працювати з криптовалютами або займатися пов'язаною діяльністю.

Ці покарання можуть бути застосовані в поєднанні з іншими заходами, які передбачені законодавством росії. Важливо зазначити, що покарання можуть бути змінені або доповнені згідно з рішенням суду в кожному конкретному випадку.

4.2. Стан та перспективи розслідувань злочинів з використанням криптовалют

Нові технології, продукти та пов'язані послуги мають потенціал до стимулювання фінансових інновацій та ефективності й покращення фінансових послуг, але вони також створюють нові можливості для злочинців та терористів у відмиванні їх доходів або фінансуванні їх незаконної діяльності.

Віртуальні активи (криптоактиви) використовують інноваційні технології для швидкої передачі вартості по всьому світу та мають багато потенційних переваг, включаючи швидше та дешевше здійснення платежів.

Засновані на віртуальних валютах платіжні продукти та послуги створюють ризики відмивання грошей і фінансування тероризму в значних обсягах. Ця технологія дозволяє здійснювати анонімні перекази коштів в міжнародному масштабі.

Переваги криптовалют – наступні:

- відкритий код алгоритму дає змогу добувати криптовалюту кожному;
- анонімність транзакцій (інформація про власника криптогаманця відсутня, є тільки номер гаманця);
- відсутність єдиного цифрового банку;
- відсутність контролю за транзакціями та платежами.

- гроші зберігаються децентралізовано, тобто на гаманцях мільйонів користувачів у всьому світі – є одночасно і її недоліками та сприяють значній вразливості цього фінансового інструменту у сфері спекуляцій та використання для злочинних операцій, таких як торгівля людьми, контрабанда наркотиків, фінансування тероризму тощо.

Віртуальні валюти (криптовалюти), що забезпечують анонімність як користувачів, так і операцій, дозволяють швидко переводити незаконні доходи з однієї країни до іншої, широко використовуються у кримінальному світі та мають попит. Віртуальна валюта може бути або конвертованою в національну (або «фіатну») валюту або ж неконвертованою.

Валюти, що видаються низкою адміністраторів комп'ютерних ігор, є неконвертованими, оскільки можуть використовуватися лише в контексті гри (наприклад, гри Warhammer).

Віртуальні валюти на зразок біткоіна можуть конвертуватися у фіатні валюти. Тому саме конвертовані віртуальні валюти зазвичай потрапляють до поля зору злочинців та як наслідок правоохоронців.

Оскільки криптовалюти значною мірою анонімні, зручні та глобальні за своєю природою, деякі найбільші злочинні угруповання у світі зацікавлені у їх використуванні як способу відмивання коштів.

Анонімність, пов'язана з віртуальними активами, також приваблює злочинців, які використовують такі активи для відмивання доходів від низки злочинів, таких як торгівля наркотиками, незаконна контрабанда зброї, шахрайство, ухилення від сплати податків, кібератаки, ухилення від санкцій, експлуатація дітей та торгівля людьми.

15 Рекомендація FATF вимагає, що з метою протидії легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення (ВК/ФТ/ЗМЗ), ринок надання віртуальних послуг повинен мати належний рівень регулювання, надавачі віртуальних послуг мають бути зареєстровані та отримати ліцензії, а також щодо них впроваджено належний рівень нагляду (моніторингу).

Євросоюз вживає різні масштабні заходи для боротьби з відмиванням коштів та фінансуванням тероризму, зокрема щодо більш ретельного контролю транзакцій в криптовалюті.

Традиційною технологією відмивання коштів в цій сфері є придбання за «злочинні» кошти різних видів віртуальних активів (криптовалют) та на наступному етапі за допомогою різних бірж та спеціальних сервісів-міксерів подрібнити початкові монети та конвертувати їх в інші криптовалюти.

Таким чином кошти можуть пройти сотні адрес, ускладнюючи відстеження початкового власника. Принцип роботи подібних сервісів простий, вони беруть криптовалюту у різних клієнтів, «перемішують» її, в кінцевому результаті виходить «мікс», який не дозволяє відстежити власника грошей.

У 2021 році британська поліція конфіскувала рекордну кількість криптовалют на загальну суму \$408 мільйонів в рамках розслідування про відмивання коштів. Один з майданчиків торгів криптовалютою був причетний до відмивання коштів.

Віртуальні валюти можуть бути пов'язані зі злочинами:

- віртуальна валюта сама по собі може бути викрадена або одержана шахрайським способом;
- віртуальна валюта може бути використана для забезпечення анонімності під час купівлі таких речей, як наркотики або вогнепальна зброя;
- віртуальна валюта може застосовуватися в ході шантажу, наприклад, коли від компанії або установи вимагають сплатити викуп у віртуальній валюті за видалення шкідливого програмного забезпечення з комп'ютерної системи;
- віртуальну валюту можуть застосовувати для відмивання доходів від організованої злочинності та корупції, зокрема, в цілях швидкого переміщення активів через кордони.

Типові приклади розслідувань щодо відмивання злочинних доходів через віртуальні активи наведено нижче.

Проведення підозрілих транзакцій з використанням віртуальних валют. Держфінмоніторингом, з врахуванням інформації, отриманої від іноземного підрозділа фінансової розвідки (ПФР), банківських установ та баз даних, виявлено групу громадян України, які проводили підозрілі транзакції з використанням віртуальних валют рис. 4.1).

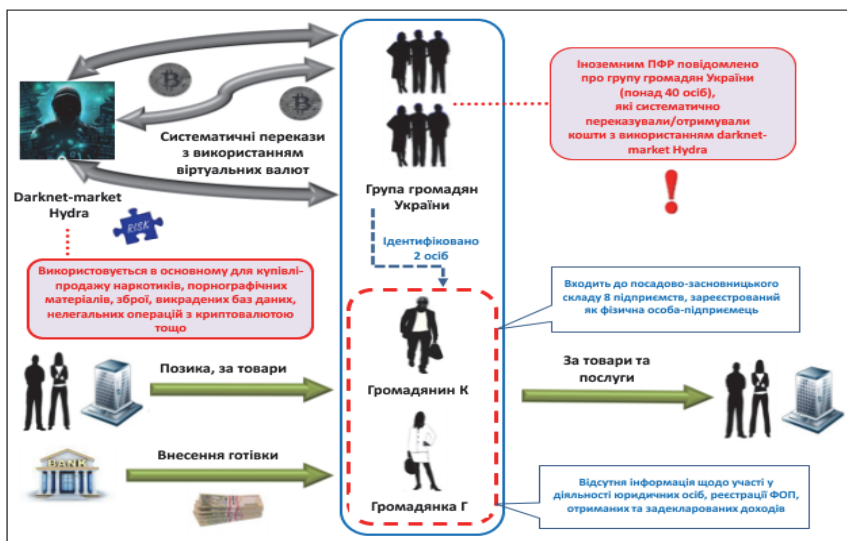


Рисунок – 4.1 Схема проведення підозрілих транзакцій з використанням віртуальних валют

Так, іноземним ПФР повідомлено про групу громадян України (понад 40 осіб), які систематично переказували/отримували кошти з використанням darknet-market Hydra. Привертає увагу, що зазначений інтернет-ресурс використовується в основному для купівлі-продажу наркотиків, порнографічних матеріалів, зброї, викрадених баз даних, нелегальних операцій з криптовалютою тощо.

В ході фінансового розслідування ідентифіковано дві особи з даної групи громадян. Слід зазначити, що громадянин «К» входить до посадово-засновницького складу 8 підприємств, а також зареєстрований як фізична особа-підприємець. Водночас стосовно громадянки «Г» відсутня будь-яка інформація щодо участі у діяльності юридичних осіб, реєстрації як суб'єкта підприємницької діяльності, отриманих та задекларованих доходів, а також сплачених податків.

Держфінмоніторингом від банківських установ отримано ряд повідомлень про фінансові операції проведені за участю громадянина «К» та громадянки «Г», в тому числі пов'язані з використанням готівкових коштів, які, не виключено, отримані від незаконних операцій протизаконного інтернет-ресурсу. Правоохоронним органом здійснюється досудове розслідування.

Вчинення кіберзлочинів з використанням послуг користуванні крипто біржі Binance. За інформацією правоохоронного органу, виявлена транснаціональна злочинна діяльність групи осіб, які використовуючи віддалене кероване шкідливе програмне забезпечення, отримали доступ до «AD» (ActiveDirectory – віддалене керування комп'ютером в ОС Microsoft) серверів корейських компаній.

У подальшому злочинці встановили програму-вимагач «Clor» для блокування інформації та подальшого витребування викупу за розблокування інформації. Внаслідок кібератаки на чотирьох корейських компаніях було заблоковано 810 внутрішніх серверів та персональних комп'ютерів.

В ході розслідування встановлено, що вказана кібератака здійснювалась із сервера, який закріплений за IP-адресою, яка фактично знаходиться у м. Харків.

Встановлено, що до вчинення кримінального правопорушення причетна Фізична особа, яка має у користуванні криптогаманці на біржі Binance, та на які надходили кошти за розблокування інформації.

В ході розслідування встановлено, що Фізична особа має відношення до вчинення фінансових операцій та інших угод з грошовими коштами та іншим майном, здобутих відомо злочинним шляхом, та не маючи офіційних доходів, які співрозмірні з його видатками, купує у свою приватну власність транспортні засоби, цінне нерухоме майно, земельні ділянки та інше.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 209 (Легалізація (відмивання) майна, одержаного злочинним шляхом), ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.

Заволодіння ідентичності аккаунту на крипто біржі «Binance». Правоохоронним органом встановлено, що Фізична особа здійснила несанкціоноване втручання в роботу персонального комп'ютера потерпілого, що призвело до втрати грошових коштів. Так, злочинці використовуючи аккаунт потерпілого на крипто біржі «Binance», заволоділи криптовалютою на суму 60.000 доларів США.

Створення онлайн-ресурсів для відмивання коштів та фінансування тероризму (сепаратизму) через віртуальні активи. СБУ заблокувала діяльність злочинного угруповання, яке займалося відмиванням та незаконним переведенням коштів, у тому числі з використанням криптовалют.

Так, організатори створили низку онлайн-ресурсів (сайти, телеграм-канали), які дозволяли користувачам конвертувати криптовалюту у готівку в особливо великих розмірах (на понад 240 млн. грн).

Даним сервісом користувались також особи, які підтримують тероризм та сепаратизм. Дані транзакції здійснювались через заборонені іноземні електронні платіжні системи. Для відмивання коштів злочинці інвестували в нерухомість, земельні ділянки та дорогоцінні метали.

Використання криптовалюти як розрахунок за наркотичні засоби. В Одеській області СБУ виявлено функціонування нарколабораторії, яка займалась виготовленням амфетаміну. Злочинці також здійснювали контрабандне постачання МДМА (напівсинтетична психоактивна сполука амфетамінового ряду) з Нідерландів.

Для проведення розрахунків злочинці активно використовували криптовалюту Bitcoin. Необхідна сума в Bitcoin розміщувалась в електронний гаманець продавця, якому за допомогою системи знеособлених чатів «Джаббер» повідомлявся електронний код для отримання доступу для коштів.

Для купівлі Bitcoin клієнти, які мали намір придбати наркотичні засоби або психотропні речовини, з використанням банківських карт українського банку за допомогою різноманітних іноземних сайтів придбавали криптовалюту.

Використання криптовалюти для сепаратистських акцій, терористичних, диверсійних та екстремістських актів. У Хмельницькій області в рамках кримінального провадження, розпочатого за ст. 110 «Посягання на територіальну цілісність і недоторканність України» КК України, СБУ викрито факт отримання винагороди у вигляді криптовалюти Bitcoin жителем регіону за виконання злочинних доручень співробітників спецслужб іноземної держави.

Розслідування фінансових злочинів – досвід криптобіржі Binance. Технологія блокчейн, яка використовує децентралізовані бази даних та відповідає за всі криптовалютні транзакції, є абсолютно прозорою, тому дозволяє публічно відстежувати грошові потоки та розслідувати нелегальну активність. Як саме це відбувається всередині найбільшої криптобіржі Binance?

У вересні 2021-го до команди Binance долучився новий начальник відділу боротьби з фінансовими злочинами Binance Тигран Гамбарян. Попередні 15 років фахівець працював у американських правоохоронних органах, 10 з яких він провів у підрозділі з розслідування кіберзлочинів (IRS-CI) у службі внутрішніх доходів Міністерства фінансів США.

Окрім розслідування справ, пов'язаних з національною безпекою, крадіжкою особистих даних, ухиленням від сплати податків та інших, Гамбарян також працював над одними з перших випадків злочинів, пов'язаних з криптовалютами [43].

Зокрема, експерт працював над гучною справою забороненої анонімною торговою платформою Silk Road, зламом першої найбільшої біткоїн-біржі Mt.Gox та закриттям російської криптоплатформи BTC-e. У межах розслідування роботи одного з найбільших піратських веб-сайтів у світі KickassTorrents, створеного групою розробників з Харкова, Гамбарян також співпрацював з українськими правоохоронними органами.

Вже під час роботи у Binance спеціаліст долучився до викриття схеми фінансування російських окупантів в Україні за допомогою криптовалют. Фахівці з'ясували, що з початку 2022-го нелегальні проросійські групи у різних країнах, багато представників яких є у санкційних списках, зібрали для військових угруповань окупантів близько \$4,2 млн.

Як змінилась ситуація зі злочинами з використанням криптовалют після повномасштабного російського вторгнення? – Глобально, ми не спостерігали сильного зростання нелегальної активності з використанням криптовалют після лютого 2022-го.

Однак, що стосується безпосередньо України та росії – нещодавно ми співпрацювали з українськими правоохоронними органами, і нам вдалося ідентифікувати декілька злочинців, що використовували криптовалюту для фінансування російських військових угруповань.

Здебільшого ми працюємо як і раніше, займаємось моніторингом транзакцій, відслідковуємо використання криптовалют з подальшими розслідуваннями можливої незаконної діяльності.

Як часто трапляються підозрілі транзакції та скільки з них вам вдалось заблокувати? – Немає точних цифр, але можна говорити, що мова йде про тисячі заблокованих транзакцій, пов'язаних з ймовірною нелегальною активністю.

Binance – це найбільша криптовалютна біржа, тому ми маємо зважати на загальний об'єм транзакцій. Сьогодні ми є найбільшим обробником криптовалютних транзакцій у світі, і кількість наших користувачів у рази більша, ніж у інших платформах.

Паралельно з власними моніторинговими системами ми також користуємось послугами провідних компаній з аналізу блокчейнів, таких як Elliptic Ltd., Chainalysis, TRM Labs для пошуку та ідентифікації ризикових транзакцій.

Окремо ми розгортаємо нові інструменти для моніторингу фіатних транзакцій, в яких також використовуються міжнародні фінансові бази даних.

Як саме Binance працює з тимчасово окупованими територіями і визначає їх? — Загалом, цими питаннями займається наша команда із дотримання санкцій.

З технічної точки зору, у нас є системи, які дозволяють відстежувати, з якого місця користувачі використовують свої акаунти. Завдяки цьому ми можемо ідентифікувати заборонені та нелегальні транзакції.

В Україні ми тісно співпрацюємо з правоохоронними органами, маємо доступ до контактних баз і, коли це треба, ми дійсно можемо надати глибоку допомогу для виявлення будь-яких небезпечних транзакцій. Як це було з фінансуванням російських військових через криптовалюту. Але так роблять далеко не всі криптовалютні платформи.

Наскільки важливо криптобіржам співпрацювати з правоохоронними органами? — Річ у тім, що Binance повністю працює за стандартом KYC (обов'язкова ідентифікація особистості клієнтів). Цим займаються тисячі людей, лише у моїй команді працює близько 330 людей.

Є криптобіржі, і навіть в Україні, які часто з негативної точки зору обговорюють те, що ми робимо. Але часто вони самі навіть не збирають KYC-дані і фактично не знають, ким є їхні клієнти, з якою метою вони користуються послугами тощо.

Тому не всі криптоплатформи працюють таким чином і не всі можуть допомагати правоохоронцям та тим, хто займається розслідуваннями в цій сфері. Тим паче, не у всіх є така кількість експертів з моніторингу, як у нас.

Звісно подібний моніторинг залежить від об'єму ресурсів, і сьогодні Binance є лідером у цій площині.

Чи дійсно криптовалюта є зручним фінансовим інструментом для кіберзлочинців? — Якщо криптовалютна платформа належним чином виконує свою роботу, ідентифікує користувачів, моніторить транзакції — у неї є більше можливостей для контролю нелегальної діяльності, ніж у традиційних фінансових інституцій. До прикладу, великий банк не може контролювати вхідні та вихідні потоки коштів так, як це може робити криптовалютна біржа.

Сучасні інструменти для аналізу роблять публічною будь-яку транзакцію, і ми одразу можемо побачити переміщення декількох мільйонів доларів. Ми не часто чуємо про подібні історії з банками, оскільки банки просто не можуть контролювати грошові потоки на такому рівні.

Публічний блокчейн дозволяє нам використовувати дуже ефективні інструменти моніторингу та розслідування транзакцій на рівні правоохоронних органів.

Сьогодні можна точно сказати, що криптовалюта не є зручним інструментом для фінансових злочинців чи підсанкційних користувачів, які намагаються переказувати великі суми коштів таким чином. Ми відразу зможемо помітити це та заморозити кошти.

При цьому, люди поняття не мають, що відбувається з великими фіатними транзакціями всередині банків, куди відправляються гроші тощо. Склався певний наратив, що криптовалюта – це інструмент для шахраїв, але фінансові злочини у набагато більших масштабах здійснюються у фіатній валюті, завдяки дорогоцінним металам, цінним паперам та будь-яким іншим активам. І їх набагато складніше відстежити.

Як легалізація криптовалют в Україні допоможе запобігати фінансовим кіберзлочинам та крадіжці цифрових активів? – Українські правоохоронні органи були більш ніж адаптовані до розслідувань нелегальної діяльності з використанням криптовалют.

Але впровадження нових рівнів нормативних регулювань, як це відбувається в Україні, залучає не тільки більшу кількість користувачів, але і більшу кількість компаній, що зацікавлені у побудові легального бізнесу.

Мене дійсно вражає те, як Україна пристосована до використання криптовалют. Локальні команди Binance також зробили свій внесок у це.

Нові норми регулювання цієї індустрії не лише дозволять ефективніше боротись з нелегальною активністю, але і допоможуть захистити пересічних користувачів, наприклад, від наслідків банкрутства криптокомпаній чи будь-яких негараздів з використанням цифрових активів.

4.3. Технології розслідування злочинів з використанням криптовалют

Розслідування злочинів в сфері криптовалют може відрізнитися в різних країнах залежно від законодавства та правоохоронних органів. Проте, загалом, такі злочини розслідуються за допомогою комплексного підходу, який включає в себе наступні кроки:

1) *збір доказів* – поліція та інші правоохоронні органи збирають інформацію про злочинців, зокрема, про їхні криптовалютні адреси та транзакції;

2) *аналіз даних* – зібрані дані піддаються аналізу для встановлення зв'язків між різними адресами та транзакціями, що може допомогти виявити осіб, які здійснювали злочин;

3) *співпраця з криптобіржами та сервісами* – у деяких випадках правоохоронні органи можуть співпрацювати з криптобіржами та сервісами, які надають послуги з обміну криптовалют, для відстеження транзакцій та встановлення осіб, які здійснюють операції з криптовалютами;

4) *проведення обшуків та арештів* – якщо існує достатньо доказів, то правоохоронні органи можуть провести обшук в приміщеннях, які належать підозрюваним, та здійснити їх арешт;

5) *судове переслідування* – після збору достатньої кількості доказів та проведення розслідування, справу можуть передати до суду для розгляду.

Збирання доказів про злочини в сфері криптовалют може бути складним процесом, оскільки це вимагає спеціалізованих знань і технічних навичок. Однак, в основному, процес збору доказів подібний до

традиційного процесу збору доказів. Нижче наведено кілька загальних кроків, які можуть включатися до процесу збору доказів про злочини в сфері криптовалют.

1. *Збір інформації.* Перший крок – зібрати інформацію, що стосується злочину. Це можуть бути дані з різних джерел, таких як розмови з потенційними свідками, записи відеоспостереження або соціальні мережі.

2. *Аналіз даних.* Для аналізу зібраних даних можуть використовуватися різноманітні інструменти, наприклад, програмне забезпечення для аналізу текстів або відеоаналітики.

3. *Збір електронних доказів.* При злочинах, що стосуються криптовалют, можуть використовуватися електронні докази, такі як транзакції в блоці, адреси гаманців, записи інтернет-трафіку, логи серверів та інше. Для збору цих доказів можуть використовуватися спеціальні інструменти, такі як блокчейн-аналізатори або інструменти відкритої розвідки.

4. *Експертиза.* Експерти можуть бути залучені для аналізу зібраних доказів, щоб встановити їх доказову цінність і з'ясувати, які інші докази можуть бути необхідні.

5. *Подання доказів.* Після збору і аналізу доказів вони можуть бути використані для подання в суді.

Для збору доказів про злочини в сфері криптовалют використовується різноманітне програмне забезпечення залежно від конкретної ситуації та завдання. Нижче наведено деякі з найбільш поширених програмних засобів, які використовуються в розслідуваннях:

- *блокчейн-аналітика* – це програмне забезпечення, що дозволяє відстежувати рух криптовалют у блокчейні, що є основою більшості криптовалют, воно може використовуватися для виявлення злочинів, таких як відмивання грошей, обман та фінансування тероризму;

- *програмне забезпечення для аналізу даних* – це програмне забезпечення дозволяє аналізувати великі обсяги даних, що містяться в електронних гаманцях, обмінниках криптовалют та інших джерелах, для виявлення злочинів та зловживань;

- *хакерські засоби* – це програмне забезпечення, що дозволяє отримувати доступ до комп'ютерів, мобільних пристроїв та інших електронних пристроїв, що використовуються злочинцями для здійснення злочинів в сфері криптовалют;

- *програмне забезпечення для відновлення даних* – це програмне забезпечення дозволяє відновлювати втрачені дані з комп'ютерів та інших електронних пристроїв, воно може бути корисним при розслідуванні крадіжок криптовалют, якщо злочинці зберігали ключі доступу до гаманців на своїх пристроях.

- *програми кібербезпеки* – це програмне забезпечення, що дозволяє виявляти та захищати комп'ютерні системи.

Для блокчейн-аналітики існує багато програм і інтернет-послуг. Ось деякі з них:

Blockchain Explorer – це програма для дослідження блокчейну, яка надає доступ до інформації про транзакції, блоки та адреси в мережі. Вона дозволяє переглядати транзакції в режимі реального часу та проводити аналіз транзакцій.

Bitquery – це інструмент аналізу даних, який дозволяє аналізувати транзакції, блоки та адреси в мережі. Він надає доступ до глибоких даних про транзакції та дозволяє здійснювати аналіз на основі різних параметрів.

Crystal Blockchain Analytics – це програма, що дозволяє відстежувати походження криптовалютних транзакцій та виявляти підозрілі операції. Вона забезпечує засоби для виявлення фінансових злочинів, таких як відмивання грошей та фінансування тероризму.

Chainalysis – це комплексний інструмент для аналізу блокчейну, який надає детальну інформацію про транзакції, адреси та гаманці в мережі. Він дозволяє виявляти підозрілі транзакції та ідентифікувати користувачів мережі.

CoinTracking – це програма для відстеження портфеля криптовалют, яка дозволяє вести облік транзакцій та аналізувати рухи на ринку. Вона надає засоби для аналізу прибутку та витрат, статистики портфеля та іншої корисної інформації.

WalletExplorer – це програма для аналізу гаманців криптовалют, яка дозволяє відстежувати транзакції та ідентифікувати користувачів.

Робота з Blockchain Explorer. На його головній сторінці є пошукова система. Можемо ввести адресу гаманця, зміст якого ми хочемо перевірити, номер транзакції, курс якої ми хочемо відстежувати, або ім'я токена, випущеного в мережі ethereum (зазвичай у стандарті ERC20), про який ми хочемо дещо дізнатися. Ми почнемо з цієї останньої дії (рис. 4.2).

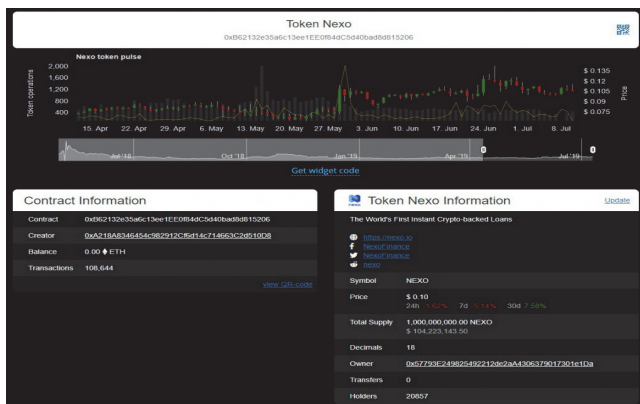


Рисунок – 4.2 Інформаційна сторінка токена Нехо у провіднику блокчейну

Входимо в пошукову систему Nexho і перейдіть на сторінку з повною інформацією про цей токен.

У центрі інформаційної сторінки ви можете побачити графік зміни ціни токена. Вгорі, під його назвою, а також у таблиці зліва, є інформація про номер контракту (контракт), або унікальний ідентифікатор даного токена в мережі блокчейна. Багато токенів можуть мати однакові імена. Для БД блокчейна важлива адреса договору.

Інвестор, коли хоче передати цей токен, або на вашому гаманці, і за замовчуванням цей токен відсутній у БД гаманця, він повинен надати інформацію про себе символ токена (в даному випадку NEXO), адресу його контракту та кількість десяткових знаків, які він поділяє (десятичні знаки в таблиці праворуч).

Інша цікава інформація, яку ми можемо знайти на цій сторінці кількість перекладів, зроблені за допомогою цих токенів за всю історію їх існування (Транзакції), всього кількість токенів в обігу (Total Supply) та їх поточна ринкова капіталізація, а також кількість портфелів на яких токени зберігаються зараз (Holders).

У провіднику блокчейну у нас є можливість запідозрити які гаманці найбагатші в даному типі токенів. Для цього перейдіть на вкладку «Тримачі». Як виявилось, два найбільші портфелі Nexho мають майже 60% від усіх токенів. Власники портфоліо нам невідомі, за адресою у них немає свого імені або назви компанії (рис. 4.3).

Transfers	Issuances	Holders
Token Nexho Holders		
20,857 total		
1	0x65b0b8ec4947ed32a500d74e5 ...	392,746,771.50545 NEXO \$ 40,933,363.13
2	0x11111111111111111111111111111111 ...	208,333,330.99359998 NEXO \$ 21,713,154.63
3	0x22222222222222222222222222222222 ...	98,437,500.00 NEXO \$ 10,259,465.69
4	0x57793e249825492212dc2aa430 ...	86,145,831.00 NEXO \$ 8,978,389.31
5	0xc3333333333333333333333333333333 ...	33,333,332.00 NEXO \$ 3,476,104.64
6	0x00ee047a66d5c0f27587a615591 ...	27,247,015.00 NEXO \$ 2,830,769.55
7	0x44444444444444444444444444444444 ...	13,749,996.000000002 NEXO \$ 1,433,067.81
8	0xfec00675a79c07527b53d83dd ...	9,620,362.8896231 NEXO \$ 1,002,664.48
9	0xc763cba7c24d8995aad891500b ...	7,999,898.00 NEXO \$ 833,774.52
10	0x6748f50f86b0fcafe8ad62b222 ...	5,859,150.7601433 NEXO \$ 610,659.11
10		
Summary of page is 883,473,188.1488165 NEXO, which is 88.32% of Nexho total supply		

Рисунок – 4.3 Список найбагатших портфелів даного токена в провіднику блокчейна

Однак, трохи більше запитуючи і шукаючи інформацію про розподіл токенів, іноді можна визначити, що, наприклад, даний пул токенів в даний час виключений з обігу так званих холодний гаманець і використовуватиметься тільки в наступні роки проекту... або портфель належить платформі даного проекту тому він збирає ресурси багатьох тисяч користувачів. Те саме стосується і портфельів криптовалютних бірж, які зазвичай лопаються по швах з погляду вмісту накопичених коштів.

Як ви перевіряєте статус та історію нашого портфолію у провіднику блокчейну?

Як і раніше, ми знайшли інформаційну сторінку про токени NEXO, те саме зараз ми йдемо в бік нашого портфолію набравши в пошуковій системі на EThplorer його адресу. Адреса гаманця Мережа ethereum складається з 0x на початку та символів 40, включаючи цифри та літери. Перейшовши до нашого портфолію в блокчейні, адреса нашого портфолію відображається на білій панелі у верхній частині. Нижче наведено графік обміну його вартості (рис. 4.4).

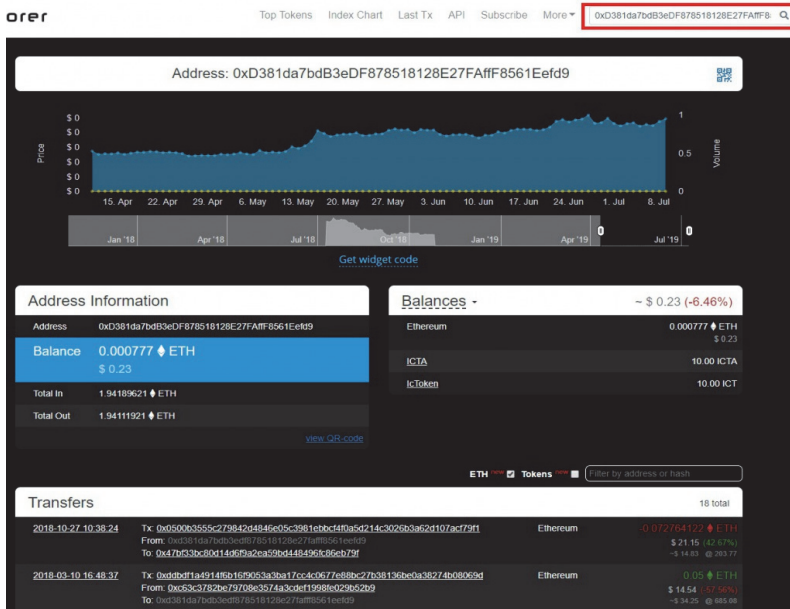


Рисунок – 4.4 Стан та історія портфолію в мережі ефіріум

У таблиці зліва інформація про поточну кількість збережених ефірних монет (для мене `0,000777` ЕТН зі значенням `0,23$`). Нижче наводиться сума ЕТН, яка в історії портфеля увійшла та вийшла з нього.

У таблиці праворуч сальдо або баланс рахунку. Показує кількість збережених ЕТН та токенів. У стовпці зліва – назва токена, праворуч – його номер.

Нижче ми маємо переказ або історія переказів. Ми знайдемо там інформацію про дату транзакції, її номер (Tx), адресу, з якої було відправлено токен або ефір, та адресу призначення. Правильні імена токенів, їх кількість та значення під час передачі і сьогодні.

ВИСНОВКИ ДО РОЗДІЛУ 4

Використання криптовалют може створювати виклики для правоохоронних органів, оскільки транзакції можуть бути анонімними та важкими для відстеження. Це ускладнює розслідування злочинів, таких як відмивання грошей, фінансування тероризму та наркотрафіку.

Розслідування криптовалютних злочинів потребує глибоких технічних знань та експертизи. Відстеження транзакцій, аналіз блокчейну та ідентифікація користувачів можуть вимагати спеціалізованих інструментів та ресурсів.

Криптовалюти не мають меж, тому розслідування злочинів в сфері криптовалют часто вимагає співпраці міжнародних правоохоронних органів та обміну інформацією між країнами. Відсутність єдиних стандартів та юрисдикційних викликів можуть ускладнювати цей процес.

Ефективне розслідування криптовалютних злочинів потребує наявності експертів з криптовалют, кібербезпеки та сфери права. Вони мають бути оснащені необхідними знаннями та ресурсами для виконання своїх обов'язків.

Швидкий розвиток криптовалютного сектору вимагає постійного оновлення та розширення законодавства, щоб регулювати цю сферу та дозволити правоохоронним органам боротися з криптовалютними злочинами. Створення ефективних правових рамок може сприяти розслідуванню та засудженню злочинців.

Усі ці аспекти свідчать про складність розслідування злочинів в сфері криптовалют та необхідність спільних зусиль з боку правоохоронних органів, експертів та міжнародної співпраці для забезпечення безпеки та боротьби з кримінальною діяльністю.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Наведіть основні типи злочинів, які можуть бути пов'язані з використанням криптовалют.
2. Наведіть приклади викритих злочинів в сфері криптовалют в Україні.
3. Наведіть приклад фінансування сепаратизму через нелегальні криптообмінники в Україні.
4. Які правоохоронні органи в Україні здійснюють розслідування злочинів, пов'язаних з криптовалютами?
5. Наведіть приклади викритих злочинів в сфері криптовалют в рф.
6. Які правоохоронні органи в рф здійснюють розслідування злочинів пов'язаних з криптовалютами?
7. Яке передбачається покарання за скоєння фінансових злочинів пов'язаних з криптовалютами в рф?
8. Наведіть 15 рекомендацію FATF щодо протидії ВК/ФТ/ЗМЗ.
9. З якими типами злочинів можуть бути пов'язані віртуальні валюти?
10. Наведіть типові приклади розслідувань щодо відмивання злочинних доходів через віртуальні активи.
11. Наведіть приклад злочину – проведення підозрілих транзакцій з використанням віртуальних валют.
12. Наведіть приклад злочину – вчинення кіберзлочинів з використанням послуг користуванні криптобіржі Binance.
13. Наведіть приклад злочину – заволодіння ідентичності аккаунту на криптобіржі «Binance».
14. Наведіть сучасні технології розслідування злочинів з використанням криптовалют
15. Наведіть зразки програмного забезпечення для блокчейн-аналітики.

ВИСНОВКИ

Цей посібник створений з метою надати читачам основні знання та рекомендації щодо використання криптовалют в Україні в умовах збройної агресії росії. Посібник містить важливу інформацію, яка може допомогти вам зрозуміти сутність криптовалют та їх можливості в таких непростих часах.

В умовах збройної агресії росії проти України, криптовалюти можуть відігравати важливу роль як інструмент фінансової незалежності та захисту. Вони забезпечують можливість зберігання активів поза контролем централізованих фінансових систем, що є особливо актуальним у періоди нестабільності.

Проте, використання криптовалют вимагає від користувачів пильності та обережності. Важливо дотримуватися найкращих практик з кібербезпеки, використовувати надійні гаманці та обмінники, а також добре розуміти ризики, пов'язані з волатильністю криптовалютних ринків.

Крім того, необхідно враховувати правові аспекти використання криптовалют в Україні. Уряд встановив ряд правил та регуляцій, що стосуються криптовалютних операцій, тому важливо бути в курсі останніх змін та дотримуватися відповідних правил.

Нехай цей посібник стане вашим надійним джерелом інформації та практичних порад щодо використання криптовалют в умовах збройної агресії. Ми сподіваємося, що він допоможе вам зробити свідомі та безпечні рішення щодо ваших фінансових операцій та захисту ваших активів. Пам'ятайте, що знання – це сила, а правильне використання криптовалют може стати одним із інструментів, що сприятимуть вашій фінансовій незалежності та стійкості у цей важкий період.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке криптовалюта: пояснюємо простими словами. URL: <https://forklog.com.ua/exclusive/shho-take-kryptovalyuta-poyasnyuyemo-prostymy-slovamy> (дата звернення 12.09.2023).
2. Що таке криптовалюта? – Вадим Попов, директор з маркетингу Bitcoin-агентства KUNA. URL: <https://www.radiosvoboda.org/a/details/28742278.html> (дата звернення 12.09.2023).
3. Solomon, M. G., Danial, K., Laurence, T., Kent, P., Bain, T. (2022). Cryptocurrency All-in-One For Dummies. Велика Британія: Wiley. URL: <https://www.google.pl/books/edition/Cryptocurrency All in One For Dummie s/> (дата звернення 12.09.2023).
4. Hoffman, N. (2017). Cryptocurrency: The Ultimate Guide to The World of Cryptocurrency and How I Became a Crypto Millionaire in 6 Months. (n.p.): CreateSpace Independent Publishing Platform. URL: <https://www.google.pl/books/edition/Cryptocurrency/> (дата звернення 25.09.2023).
5. Lesiv, O. (2019). Introduction to the World of Cryptocurrency: Getting Started with Bitcoin. Сполучені Штати Америки: Blurb Books. URL: <https://www.google.pl/books/edition/Introduction to the World of Cryptocurr e/> (дата звернення 25.09.2023).
6. Derausseau, R. (2019). The Everything Guide to Investing in Cryptocurrency: From Bitcoin to Ripple, the Safe and Secure Way to Buy, Trade, and Mine Digital Currencies. Сполучені Штати Америки: Adams Media. URL: <https://www.google.pl/books/edition/The Everything Guide to Investing in Cry/> (дата звернення 30.09.2023).
7. The Bitcoin Investor: A Complete Guide to Cryptocurrency Investing. (2018). (n.p.): Michael Gonzalez. URL: <https://www.google.pl/books/edition/The Bitcoin Investor A Complete Guide to> (дата звернення 30.09.2023).
8. Закон України «Про валюту та валютні операції». URL: <https://zakon.rada.gov.ua/laws/show/2473-19#Text> (дата звернення 30.09.2023).
9. Закон України «Про фінансові послуги та державне регулювання ринків фінансових послуг». URL: <https://zakon.rada.gov.ua/laws/show/2664-14#Text> (дата звернення 02.10.2023).
10. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». URL: <https://zakon.rada.gov.ua/laws/show/361-20#Text> (дата звернення 02.10.2023).
11. Роз'яснення Національного банку України щодо правомірності використання в Україні «віртуальної валюти/криптовалюти» Bitcoin. URL:

<https://zakon.rada.gov.ua/laws/show/n0435500-14#Text> (дата звернення 06.10.2023).

12. Спільна заява фінансових регуляторів щодо статусу криптовалют в Україні // Національний банк України – 30.11.2017. URL: <https://bank.gov.ua/ua/news/all/spilna-zayava-finansovih-regulyatoriv-schodo-statusu-kriptovalyut-v-ukrayini> (дата звернення 06.10.2023).

13. Закон України «Про платіжні послуги». URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text> (дата звернення 12.10.2023).

14. Закон України «Про віртуальні активи». URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (дата звернення 12.10.2023).

15. Офіційний сайт Центрального банку росії. URL: www.cbr.ru (дата звернення 05.08.2023).

16. Федеральний закон «Про валютний регулювання та валютний контроль» від 10.12.2003 №173-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_45458/ (дата звернення 18.10.2023).

17. Офіційний сайт Міністерства фінансів росії. URL: www.minfin.ru (дата звернення 18.10.2023).

18. Федеральный закон от 31.07.2020 №259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты рф». URL: <https://habr.com/ru/articles/515538/> (дата звернення 23.10.2023).

19. Офіційний сайт криптообмінника Changelly. URL: <https://changelly.com/> (дата звернення 23.10.2023).

20. Офіційний сайт криптообмінника ShapeShift. URL: <https://shapeshift.io/> (дата звернення 28.10.2023).

21. Офіційний сайт криптообмінника Binance. URL: <https://www.binance.com/> (дата звернення 28.09.2023).

22. Офіційний сайт криптообмінника Coinmama. URL: <https://www.coinmama.com/> (дата звернення 28.10.2023).

23. Офіційний сайт криптообмінника LocalBitcoins. URL: <https://localbitcoins.com/> (дата звернення 28.10.2023).

24. Офіційний сайт криптобіржі Binance. URL: <https://www.binance.com/> (дата звернення 30.10.2023).

25. Офіційний сайт криптобіржі Coinbase. URL: <https://www.coinbase.com/> (дата звернення 30.10.2023).

26. Офіційний сайт криптобіржі Kraken. URL: <https://www.kraken.com/> (дата звернення 30.10.2023).

27. Офіційний сайт криптобіржі Bitfinex. URL: <https://www.bitfinex.com/> (дата звернення 25.09.2023).

28. Офіційний сайт криптобіржі Huobi. URL: <https://www.huobi.com/> (дата звернення 28.09.2023).

29. Офіційний сайт криптоміксеру Wasabi Wallet. URL: <https://www.wasabiwallet.io/> (дата звернення 13.10.2023).

30. Офіційний сайт криптомікзера Samourai Wallet. URL: <https://samouraiwallet.com/> (дата звернення 13.10.2023).

31. Офіційний сайт криптомікзера ChipMixer. URL: <https://chipmixer.com/> (дата звернення 18.10.2023).

32. Офіційний сайт криптомікзера Blender.io. URL: <https://blender.io/> (дата звернення 18.10.2023).

33. Офіційний сайт криптомікзера SmartMixer. URL: <https://smartmixer.io/> (дата звернення 30.09.2023).

34. Офіційний сайт криптогаманця Ledger. URL: <https://www.ledger.com/> (дата звернення 16.09.2023).

35. Офіційний сайт криптогаманця Trezor. URL: <https://trezor.io/> (дата звернення 16.09.2023).

36. Офіційний сайт криптогаманця MetaMask. URL: <https://metamask.io/> (дата звернення 18.09.2023).

37. Офіційний сайт криптогаманця Exodus. URL: <https://www.exodus.io/> (дата звернення 21.09.2023).

38. Офіційний сайт криптогаманця Atomic Wallet. URL: <https://atomicwallet.io/> (дата звернення 21.09.2023).

39. Проект Закону про обіг криптовалюти в Україні № 7183 від 06.10.2017. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684 (дата звернення 21.09.2023).

40. Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні №7183-1 від 10.10.2017. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710 (дата звернення 26.09.2023).

41. Законопроект про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами №2461 від 15.11.2019. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423 (дата звернення 12.10.2023).

42. Проект Закону №4004 від 01.09.2020 про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771 (дата звернення 12.10.2023).

43. «Криптовалюти – вже давно невідповідний інструмент для злочинців» – Тигран Гамбарян, Binance. URL: <https://www.epravda.com.ua/publications/2023/01/31/696489/> (дата звернення 14.10.2023).

Навчальне видання

Лисецький Ю.М., Зайцев О.В., Богун А.М.

ОСНОВИ ВИКОРИСТАННЯ КРИПТОВАЛЮТ У ФАХОВІЙ ДІЯЛЬНОСТІ

Навчальний посібник

Літературний редактор, коректор – Д.О. Кашперська
Комп'ютерна верстка, макетування – А.О. Брем
Дизайн обкладинки – Д.О. Кашперська
Технічний редактор – В.Ю. Бихун

Підп. до друку 25.12.2023. Формат 64х90/16.
Папір офсетн. Друк цифровий.
Ум. друк. арк. 8,25. Наклад 200 прим. Зам. № 25/12

Видавець Бихун В.Ю.
Видавництво «ЛІАТ & К»
вул. Леонтовича, 9, к. 18, м. Київ, 01054
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
ДК № 5366 від 26.06.2017 р.
тел./факс: +38 044 235 000 9
моб.: +38 050 310 22 04
e-mail: lk@ukr.net