

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ**

КВАЛІФІКАЦІЙНА РОБОТА

**на тему: ВИЯВЛЕННЯ ТА ФІКСАЦІЯ КРИПТОВАЛЮТНИХ ГАМАНЦІВ
АНАЛІТИЧНИМИ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
У ПРОТИДІЇ ЗЛОЧИННОСТІ**

Виконав:

слухач 2-го курсу магістратури
факультету № 2 ННІПК
ШУТИЛО Сергій Вікторович

Науковий керівник:

доцент кафедри кібербезпеки та
інформаційного забезпечення
кандидат юридичних наук
Дмитро БЄЛИХ

Рецензент:

Доктортехнічних наук, доцент
Олексій БАЛТОВСЬКИЙ

Кваліфікаційна робота допущена до захисту

«__» _____ 2022 р., протокол № __.

Завідувач кафедри кібербезпеки та інформаційного забезпечення,
доктор юридичних наук, професор

Андрій БАБЕНКО

Одеса – 2022

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ ТА ТЕРМІНІВ	3
ВСТУП	5
РОЗДІЛ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН	
1.1. Загальна характеристика технології блокчейн та її місце в злочинній діяльності	9
1.2. Поняття та особливості криптовалют	14
1.3. Класифікація криптовалютних гаманців	22
Висновок до розділу І.	26
РОЗДІЛ ІІ. ВИЯВЛЕННЯ ТА ФІКСАЦІЇ КРИПТОВАЛЮНИХ ГАМАНЦІВ ПРАВООХОРОННИМИ ОРГАНАМИ	
2.1. Алгоритм виявлення криптовалютних гаманців на персональних комп'ютерах	28
2.2. Фіксація криптовалютних гаманців	46
Висновок до розділу ІІ.	48
ВИСНОВКИ	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	51
ДОДАТКИ	55

ПЕРЕЛІК

скорочень, умовних позначень та термінів

Blockchain (блокчейн)	побудований за певними правилами ланцюжок з формованих блоків транзакцій.
Bitcoin (біткоїн)	пірінгова платіжна система, яка використовує однойменну розрахункову одиницю і однойменний протокол передачі даних.
Bitcoin wallet	гаманець для збереження та передавання Bitcoin.
API	(англ. application programming interface) набір готових класів, процедур, функцій, структур і констант, що надаються додатком (бібліотекою, сервісом) або операційною системою для використання у зовнішніх програмних продуктах.
Криптовалюта	цифрові рахункові одиниці, облік яких децентралізований.
SWIFT	(англ. Society for Worldwide Interbank Financial Telecommunications) міжнародна міжбанківська система передачі інформації та здійснення платежів.
ARIS Objective Diagram	(англ. Architecture of Integrated Information Systems Objective Diagram) діаграма архітектури інтегрованої інформаційної системи.
DFD (IDEF0)	(англ. Data flow diagram) діаграма потоків даних.

Криптографія	наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.
Децентралізація	процес розподілу влади, фінансів або зусиль без втручання глобального керуючого органу.
Хешування	перетворення вхідного масиву даних довільної довжини в вихідний бітовий рядок фіксованої довжини.
Форк	(англ. Fork - «виделка», «вилка», «розгалуження») в розробці програмного забезпечення - процес розділення програмного проекту (зазвичай вільного) на два окремі проекти.
Майнінг (видобування)	(від англ. Mining - видобуток корисних копалин) - діяльність з підтримки розподіленої платформи і створення нових блоків з можливістю отримати винагороду в формі емітованої валюти і комісійних зборів у різних криптовалютах, зокрема в біткоінах.

ВСТУП

Актуальність теми дослідження. Зараз спостерігається стрімкий розвиток інтернет-технологій, а разом з ним великі корпорації та прості люди шукають нові можливості покращення системи грошового обігу, прискорення транзакцій платежів, збільшити надійності та ефективності операцій. Технологія блокчейн, на якій базується велика кількість технологічних розробок XXI віку, знайшла широкого застосування в багатьох сферах суспільства, таких як діяльність у сфері криптографії, криптовалюти так і застосування у державній сфері управління по всьому світу. Особливе це питання актуалізовалося після кризи в 2008 році, військового конфлікту 2014 року, а також зараз під час військового положення причиненого військовим нападом російської федерації на УКРАЇНУ.

Так, Україною було застосовано в сфері державного управління електрону платформу для реалізації арештованого майна «СЕТАМ». Тому поява технології блокчейн, яка дозволяє реалізовувати найстійкіші цифрові реєстри в світі, є логічним розвитком світу та прямо зараз ми спостерігаємо адаптацію технології блокчейн до традиційних секторів економік. Вже набрали популярність такі криптовалюти, які функціонують на основі технології блокчейн як: Bitcoin, Ethereum, Bitcoin Cash, Ripple та інші. Разом з технологіями злочинні угруповання також активно почали запроваджувати та використовувати технологію блокчейн у своїй протиправній діяльності, користуючись її особливостями такими як: скритність, децентралізація, легкість переводу та інші.

Тому питання розробки, пошуку та впровадження в діяльність співробітників правоохоронних органів методів та прийомів з виявлення та фіксації криптовалютних гаманців на сьогодні є найактуальнішим питанням.

З теоретичного погляду актуальність досліджуваного питання визначається тим, що більшість співробітників правоохоронних органів не отримали під час свого навчання в вищих навчальних закладах достатніх знань з методів, прийомів, джерел виявлення та фіксації криптовалютних гаманців у зв'язку зі застарілими навчальними планами навчання та стрімкого розвитку технологій, а підвищення

кваліфікації проводиться для груп кількістю 25-30 осіб, що не дає можливості в повному обсязі засвоювати матеріал даної тематики, оскільки велика чисельність групи на одного викладача або затягує освітній процес, або робить його не менш якісним.

З практичного боку зазначена проблема актуалізується тим, що правоохоронні органи неповністю виконують свою функцію в частині відшкодування заподіяної злочинцем шкоду у зв'язку з не накладенням арешту або не вилучення криптовалютних гаманців. А також тим, що в Україні не існують державних криптовалютних гаманців, що унеможлиблює переказ криптовалюти на них.

Стан наукової розробки теми. Слід зазначити, що проблематика криптовалют і блокчейну ще не увійшла до академічного дискурсу і поки активно обговорюється лише програмістами-розробниками, технічними експертами, майнерами, біржовими спекулянтами та ризиковими інвесторами.

Зв'язок роботи з науковими програмами, планами, темами.

Кваліфікаційна робота виконувалась по кафедрі кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ і, відповідно, до затвердженого напрямку загально-кафедрального наукового дослідження, що було визначено рішенням кафедри кібербезпеки та інформаційного забезпечення, а також Стратегії розвитку системи Міністерства внутрішніх справ України.

Мета й завдання дослідження. Мета роботи обумовлена актуальністю та ступенем розробленості обраної теми та полягає в визначенні сучасної ролі технології блокчейн в фінансових операціях, розкриття досвіту роботи з цією технологією та в розкритті існуючих на сьогодні методів та приймів з виявлення та фіксації криптовалютних гаманців правоохоронними органами. Відповідно до поставленої мети в роботі зосереджується увага на вирішенні таких **завдань**:

- визначити загальні особливості технології блокчейн, як найсучаснішу технологію розподіленого зберігання інформації;
- дослідити як технологія блокчейн використовується в злочинній діяльності;

- навести особливості найпопулярніших видів криптовалютних гаманців;
- проаналізувати сучасні практики виявлення та фіксації криптогаманців;
- узагальнити основні прийоми виявлення та фіксації криптогаманців;
- наглядно продемонструвати зовнішній вигляд криптовалютних гаманців.

Об'єктом кваліфікаційної роботи є технологія блокчейн, її застосування в протиправній діяльності та основи виявлення та фіксації такої діяльності.

Предметом дослідження стали прийоми виявлення та фіксації співробітниками правоохоронних органів криптовалютних гаманців, які використовуються в протиправній діяльності.

Методи дослідження. Методологічна база роботи ґрунтується на комплексі сучасних методів дослідження. Застосовувалися такі методи наукового пізнання: історико-правовий, діалектичний, порівняльно-правовий, формально-логічний, системно-структурного аналізу та синтезу. Дослідження та обґрунтування основних понять, що використані в роботі, виконані за допомогою діалектичного методу пізнання, дедуктивного методу (аналізу) та індуктивного методу (синтезу) вказаних визначень. Історико-правовий метод застосовувався при узагальненні наукових досліджень і аналізу наукової літератури з обраної проблематики. Використання порівняльно-правового методу дозволило дослідити досвід в інших країнах.

Наукова новизна отриманих результатів визначається тим, що кваліфікаційна робота є сучасним дослідженням, в якій:

- розглянуто технологію блокчейн, яка застосовується в протиправній діяльності;
- наведено основні криптовалюти та їх властивості з точки зору їх застосування в злочинній діяльності;
- визначено основні прийоми пошуку та фіксації криптовалютних гаманців.

Практичне значення одержаних результатів полягає в тому, що результати дослідження можуть бути використані в службовій діяльності співробітників правоохоронних органів, в навчальному процесі: при підготовці підручників, посібників та методичних рекомендацій; проведення тренінгів та семінарів; при

викладанні Інформаційно-телекомунікаційні системи, Актуальні проблеми протидії кіберзлочинам та Криміналістики; у різних формах підвищення кваліфікації практичних працівників.

Структура наукової роботи. Наукова робота складається зі вступу; переліку скорочень, умовних позначень; 2-х розділів, висновків, додатків (в кількості 17) та списку використаних джерел. Загальний обсяг роботи з додатками становить 107 сторінок.

РОЗДІЛ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН.

1.1 Загальна характеристика технології блокчейн та її місце в злочинній діяльності

Разом з появою нових фінансових інститутів, інструментів та форм взаємодії між людьми та за допомогою засобів комп'ютеризації пропонуються новітні криптографічні методи шифрування інформації, що полегшують регулювання та функціонування грошового обігу, зрозуміло, що злочинна діяльність також змінюється в цьому напрямку, тому співробітниками правоохоронних органів необхідно адаптувати свою тактику та методи боротьби зі злочинністю до потреб сьогодення. Перед тим як розглянути питання застосування злочинними елементами технології блокчейн у своїй протиправній діяльності необхідно з'ясувати перш за все, що саме таке блокчейн та чому він поширюється в кримінальному середовищі.

Технологія блокчейн є новою інформаційною технологією, яка набуває розвитку та використання у багатьох галузях тому числі і кримінальної. Після світової економічної кризи в 2008 році під псевдонімом Satoshi Nakamoto було опубліковано статтю «Bitcoin: A Peer-to-Peer Electronic Cash System» з описом концепції і принципів роботи платіжної системи у вигляді однорангової мережі [1]. Так вже у 2009 році було представлено протокол криптовалюти біткоїн та опубліковано код програми-клієнта. Ключова особливість запропонованої концепції полягала в тому, що онлайн-платежі між клієнтами здійснюються без центральної фінансової установи, яка виконує роль довіреної структури, з використанням криптографічних методів та публічної розподіленої бази даних [2].

По-перше технологія «блокчейн» або «розподіленого реєстру» вводить принципово іншу структуру децентралізованих платіжних систем, з криптографічними методами шифрування інформації. В основі криптовалют лежить технологія блокчейн (англ. Blockchain, Block chain¹ від block - блок, chain - ланцюг) – розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає [3]. Згідно проекту Закону України «Про обіг криптовалюти в

Україні» система блокчейн - децентралізований публічний реєстр усіх проведених криптовалютних транзакцій, які були проведені суб'єктом криптооперацій [19].

По-друге технологія блокчейн являє собою платформою віртуальної платіжної системи біткоїн. Тобто збудована база захищена до будь-якої підробки та переробки. Кожен блок містить часову мітку та посилання на попередній блок хеш дерева [4].

Як саме працює блокчейн на прикладі криптовалюти біткоїн (див. Додаток 1)

На сьогодні криптовалюти перетворились у визнаний платіжний засіб, віртуальну валюту, яку приймають великі та дрібні підприємства та корпорації. Наприклад за липень 2018 року капіталізація крипто валютного ринку збільшилась з 257,7 до 277,8 млрд доларів США (див. Додаток 2) [5]. Так, розповсюджена наступна схема злочинної діяльності, а саме злочинці наймають хакерів, які підробляють приватні ключі нотаріусів після чого роблять зміни в реєстрах, а потім вже проводиться рейдерський захват земель, будівель тощо. А якщо реєстр нотаріусів та інших державних структур був би побудовано за технологією блокчейн, подібні зміни було б неможливо здійснити. Це як позитивний приклад застосування технології блокчейн у протидії злочинності.

Унікальність методу блокчейн у:

1. Децентралізації. Інформація про блоки зберігається на всіх вузлах в мережі. Це видаляє необхідність наявності єдиного централізованого управління транзакціями. Інформацію про транзакції може перевірити будь-хто: жодної комерційної таємниці, всі операції видно всім.

2. Анонімності. Справжність транзакції і її виконання можна побачити завжди, тобто лише адресу, з якого виробляється транзакція або адресу кому вона призначена. Жоден з учасників групи не знає особистості інших, оскільки навіть під час переказу коштів бачить лише запис у вигляді набору цифр та букв [6]

3. Безпеці. Неможливість підробки блоку. За рахунок самого принципу роботи мережі це наймовірніше зробити. Для того щоб блок вважався справжнім з ним повинні погодитися 51% всіх існуючих вузлів.

4. Виключені подвійної витрати коштів. При відправленні коштів відразу можна побачити, що вони відіслані, але ці кошти не будуть зараховані на рахунок до тих пір, поки транзакція не потрапить в блок і не буде підтверджена. Приблизно в цей час зловмисник може ще раз відправити ці ж кошти до іншої людини, але Блокчейн не дозволить цього зробити. В нього присутні такий запобіжник, як мітки часу і транзакція, яка була відправлена раніше потрапить до блоку, а всі наступні, маючи інформацію про те, що гроші вже витрачені будуть відкинуті мережею.

5. Швидкості. Переказ криптовалюти за допомогою системи відбувається швидко, після підтвердження операції її неможливо скасувати та повернути переказ.

6. Гарантії. Оскільки кожна наступна сторінка-блок залежить від попередньої, якщо хтось захоче змінити дані вже «опечатаної» сторінки, йому також доведеться змінити зміст і шифр усіх наступних сторінок. А здійснити це самотужки, ураховуючи зростаючу складність обчислення кожного наступного коду, просто неможливо.

Тобто всі транзакції відбуваються напряму між користувачами. Ніякого головного сервера, який можна підключити, немає, а є лише мережа блокчейн, що складається з окремих суб'єктів. А спроби встановити анкетні данні власника криптогаманця через мережу досі не існує, тому інкогніто користувачів забезпечено, тобто всі ці параметри технічно дуже ускладнюють виявлення злочину не тільки правоохоронними органами України, а всього світу.

Існує безліч можливостей використовувати та впровадження технологію для електронного грошового обігу, документообігу та інших. Будь яка технологія має свої позитивні та негативні сторони, тому треба зважати на можливі загрози та слабкі сторони системи. Для прогнозування ефективності використання даної технології в Україні можливо застосувати SWOT аналіз.

На науковому рівні технології блокчейн розглядається в основному в технічному напрямку, а щодо впливу її на виникнення нових способів злочинної діяльності, або ще більш удосконалення існуючої злочинної діяльності не представлено широко в юриспруденції. Вивчення блокчейна з боку фахівців у

кримінології, кримінальному праві, кримінального процесу, криміналістики, економічної безпеки практично не проводиться.

Щодо законодавства України, то досі невизначений статус криптовалюти, як і основні поняття, що пов'язані з нею: блокчейн, токен, криптавалюта, майнінг [7].

За інформацією НБУ, СБУ та НПУ відсутність контролю за обігом криптовалют та анонімність розрахунків створює потенційні передумови для їхнього використання з метою легалізації коштів, отриманих злочинним шляхом, оплати заборонених до вільного обігу товарів (наркотиків, зброї), дають можливість фінансування тероризму, зокрема на окупованих територіях України.

Ще однією проблемою є випадки розголошення медичної таємниці пацієнтів. Технологія блокчейн є перспективним напрямком до реалізації захисту персональних даних блоків [31, с. 18-19].

Одже, технологія блокчейн може широко використовуватися в злочинній діяльності, а саме:

1. В якості грошових коштів при купівлі зброї, наркотичних засобів, порнографії та інших заборонених предметів, легалізація злочинних доходів, фінансування тероризму та ін.); створенні власної платіжної системи для злочинних цілей; у незаконній мережевій торгівлі отримана криптовалюта обмінюється на товарних біржах, потім перекладається на карти і знімається в банкоматі; використанні гаманця, на якій не знайомі один з одним люди переводять віртуальні гроші, потім та ж сума чужих BTC частинами повертається відправнику. Зв'язок між зловмисником і злочинними грошима таким чином розривається; фальшиві інтернет магазини імітують операційну діяльність

2. Криптовалюта як предмет злочинного посягання: розкрадання криптовалют з рахунків, інтернет-шахрайство, вимагання викупу у криптовалюті, шантаж у вигляді викупу у криптовалюті за розблокування державних сайтів, зараження шкідливим програмним забезпеченням ransomware (шифрує данні на усіх носіях в мережі та вимагає криптовалюту для відновлення доступу до даних;

3. Добича криптовалют шляхом зараження шкідливим програмним забезпеченням користувача, самовільне використання електроенергії на державних підприємствах та інше.

Так не можна стверджувати, що криптовалюти використовуються тільки для відмивання коштів, фінансування тероризму, торгівлі зброєю або наркотиками, оскільки всі дані про криптовалютні транзакції зберігаються у децентралізованому загальному доступі системи блокчейн. Зазначене дає більші можливості для регуляції з боку держави, та не створює проблем як з регуляцією обігу готівкових операцій. Наприклад, Податковою службою Сполучених Штатів Америки з 2015 року використовується програмне забезпечення, яке надає можливість відстежувати рух криптовалюти, визначати її походження та ідентифікувати власника, у Японії легалізована криптовалюта а контроль здійснює Агентство фінансових послуг.

Таким чином, технологія блокчейн є новою концепцією з високим потенціалом, відповідно потребує додаткових досліджень для її ефективного застосування у нових галузях, таких як кіберфізичні системи. Використання технології блокчейн кримінальними елементами в своїй злочинній діяльності неминуча, тому вже зараз необхідно вносити адекватні зміни в законодавство України, а також для ефективної протидії злочинності в сфері застосування блокчейна включити до навчальні планів підготовки правоохоронців відповідні навчальні дисципліни, курси, тренінги, а також розробити або придбати розробки в сфері аналізу транзакцій в мережі блокчейна для правоохоронних органів.

1.2. Поняття та особливості криптовалют

В попередньому пункті ми розглянули поняття технології блокчейн та дослідили її вплив на злочинну діяльність, але без розуміння працівниками правоохоронних органів, що саме таке криптовалюти, які властивості вони мають, який вигляд мають, а головне як особливість кожної криптовалюти впливає на її використання в злочинній діяльності, не можливо розглянути питання виявлення криптовалютних гаманців співробітниками будь-то НПУ, СБУ, НАБУ або САП.

Так, продовж свого розвитку гроші пройшли кілька етапів від появи, коли їх функції виконували випадкові товари, до поступового витіснення готівки з обороту. Черговим етапом розвитку грошей стала заміна традиційних грошей, які емітує держава на електронну криптовалюту (кібервалюту).

06 жовтня 2017 року в ВРУ зареєстровано законопроект №7183 «Про обіг криптовалют в Україні», який дає визначення криптовалютам та операціям з ними. Функціонування ринку криптовалют та їх похідних, відносини у сфері діяльності фінансових установ, що надають фінансові послуги на ринку криптовалют, щодо їх стосунків з клієнтами, саморегулюючими організаціями та Регулятором регулюються цим Законом, Законом України «Про фінансові послуги та державне регулювання ринків фінансових послуг» та іншими нормативно-правовими актами з питань регулювання ринків фінансових послуг, так стан нормативно-правової бази у даній сфері правового регулювання - питання регулюється Конституцією України, Кодексом України про адміністративні правопорушення, Законами України: «Про фінансові послуги та державне регулювання ринків фінансових послуг», «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», «Про ліцензування видів господарської діяльності», «Про збір на обов'язкове державне пенсійне страхування», «Про індустріальні парки», «Про інноваційну діяльність», «Про телекомунікації» [8-16].

Для всебічного розгляду питання правового статусу криптовалют приведемо деякі приклади її регулювання в інших країнах. Ураховуючи «незалежність» криптовалют від світових фінансових систем, ставлення до нього неоднозначне, а в багатьох країнах статус криптовалюти досі не визначений. Її кваліфікують як віртуальну валюту, грошовий сурогат, нематеріальну цінність, віртуальний товар тощо. Наприклад, у Китаї вона вважається віртуальним товаром, а не валютою, операції з біткоїнами заборонені для банків, але дозволені для фізичних осіб. В Австралії біткоїн розглядається як власність, а транзакції з ним - як бартер. Навіть в одній країні різні державні установи, міністерства, суди можуть ставитися до криптовалют по-різному. Приміром, у США біткоїни вважають лише віртуальною валютою, а ставлення до криптовалюти залежить від штату. У той же час Комісія з цінних паперів і бірж США двічі відмовилася допускати біткоїни на біржу [17]. Законодавство ЄС класифікує криптовалюту біткоїн як «цифрове представлення вартості, яке не підтверджено центральним банком або державним органом і не прив'язане до юридично встановлених валютних курсів, яке може використовуватися як засіб обміну для покупки товарів і послуг, їх передачі та зберігання і може купуватися в електронному вигляді». Крім цього, законодавство окремих держав по-різному трактує статус криптовалюти. Так, за законодавством Ізраїлю біткоїн не підпадає під юридичне визначення валюти ні як фінансове забезпечення, ні як оподатковуваний актив; у КНР та Японії біткоїн вважається віртуальним товаром, а не валютою, у Канаді – нематеріальним активом [28].

Також ми повинні пам'ятати за існування терористичної загрози в Україні, а криптовалюты надають додаткові можливості криміналітету та нашим ворогам. Так один з розробників клієнта мережі Bitcoin Гевін Андріс висловив занепокоєння тим, що деякі криптовалюты можуть бути шахрайськими [18].

Згідно проекту Закону «Про обіг криптовалюти в Україні» криптовалюта – це програмний код (набір символів, цифр та букв), що є об'єктом права власності, який може виступати засобом міни, відомості про який вносяться та зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду) [19]. За Вікіпедією криптовалюта (від англ.

Cryptocurrency) - вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту, таких як Proof-of-work та/або Proof-of-stake [20].

На сьогодні окрім криптовалютних бірж, обмінників та інтернет-ресурсів за допомогою криптовалюти вже можливо придбати квитки на літак, оплатити за оренду житла або за навчання в університеті. Зрозуміло, що криптовалюта ще не з'явилася в усіх куточках але вона стрімко розвивається. А все це привертає увагу злочинних угруповань. Тому найактуальнішим питаннями на сьогодні є визначення особливостей функціонування криптовалюти на сучасних фінансових ринках.

У зв'язку з високою анонімністю криптовалют наряду з традиційними методами розслідування необхідно застосовувати правоохоронними органами фінансовий аналіз та аналіз блокчейна. Так, відповідно до опублікованого дослідження аналітичної компанії Diar, різні відомства США витратили 5,7 млн доларів на аналітику криптовалютних транзакцій, зокрема, Імміграційна та Митна поліція США уклала з аналітичними компаніями 9 контрактів на 1,5 млн доларів. Крім того, компанія BIG Blockchain Intelligence Group, що спеціалізується на криптовалютном пошуку, оцінці ризиків і засобах для аналізу даних, відкрила 8-годинний курс для криптовалютних слідчих США [21]. Тому напевно і правоохоронні органи США конфіскували 500 BTC в 2017 році через спроби іранців обійти санкції США [22]. А також через недостатній рівень підготовки поліції Лондона для розслідування злочинів, пов'язаних з криптовалютами поліцейські пройдуть навчальні курси про криптовалютам [23]. Нажаль правоохоронні органи України такою підтримкою держави не користуються.

Щодо одного з видів злочинної діяльності, то розглянемо виявлення незаконних методів маніпулювання курсами криптовалют на біржах, а саме спуфінг, часте явище в криптовалютному сегменті. Суть полягає в штучному розміщенні великого замовлення на купівлю або продаж криптів на біржі (іноді суми досягають до 60 млн. дол США) за ціною істотно нижче або вище реально наявної вартості. При цьому сам заказ не закривається, а знімається з торгів ще до

здійснення угоди. Коли на біржі з'являється таке велике пропозиція, трейдери та торгові боти починають активно продавати або купувати валюту. Мошенник у цей час виявляє реальні замовлення, що дозволяє йому дорого продавати або купувати монети. На створеній ілюзії, наприклад, висока ціна курсу може піднятися.

Класифікація криптовалют:

1. За способом отримання. Криптовалюта одержуються за допомогою кріптодобичі (Майнінг), а випуск інших монет раніше стався в тому розмірі, в якому і був задуманий або наступний випуск монет не передбачується.

2. Кріптоалгоритмом хеширования, тобто способом, за допомогою якого здійснюється кодування значення. В подальшому саме його і намагаються підібрати кріптодобитчіки, задіюючи свої обчислювальні потужності.

3. Підтверджуючим механізмом. Механізм в ході кріптодобичі було виявлено точне вирішення проблеми (ключові механізми PoS і PoW).

4. Лімітами емісії. Ними обумовлюється, як багато ще монет має бути випущено і до якого терміну. Певні монети випускаються лише 1 раз.

5. За алгоритмом хеширування виділяють:

- **Script.** На ній працює лайткоїн, а також сіскоїн, днотс та інші альткоїни;
- **SHA-256.** Біткоїни і майже всі його форки функціонують саме на нем;
- **Equihash.** Тут можна згадати про Zcash, плюс біткоїни Голд;
- **Blake256.** Представники – Vcash та Decred;
- **CryptoNight.** Улюблена багатьма монета монери, а також Байткоїн працюють на ньому;
- **X11.** Яскравий представник - Dash.

6. За способом підтвердження:

- **Proof-of-Work.** Доказ роботи. Розмір винагороди залежить від того, наскільки потужним є обладнання Майнер. Головний алгоритм для всіх провідних криптовалют, в тому числі і Ефіріума, який найближчим часом може перейти на Proof-of-Stake;

- **Proof-of-Stake.** Доказ частки. Розмір винагороди залежить від кількості монет на гаманці. Менш енерговитратний алгоритм, але він схильний до чималих ризиків, зокрема, атаці 51%, тобто об'єднання власників монет для злому системи;
- **Proof-of-Importance.** Доказ важливості. Кількість монет на гаманці тут не найголовніше. Куди важливіше те, наскільки активний користувач, і скільки угод він заключив;
- **Proof-of-Activity.** Доказ активності. Симбіоз Proof-of-Stake і Proof-of-Work. Криптовалюта Dash працює на цьому алгоритмі;
- **Proof-of-Capacity.** Доказ обсягу. Потрібен для того, щоб визначити потужність [25].

Розглянемо основні особливості (властивості) головною криптовалюти – **біткоіна (BTC, Bitcoin)**. Ознаки біткоіна: передача, накопичення і збереження вартості. Проте у цієї валюти є як переваги, так і недоліки, які потрібно враховувати. До основних переваг біткоіна можна віднести: децентралізація (не контролюється ніким і ніхто не керує нею); універсальність (можна платити скільки завгодно, обміняти на будь-яку іншу криптовалюту, робити платежі або заощадження); анонімність (публічні адреси відкриті в блокчейні, але хто стоїть за ними — дізнатися з блокчейну неможливо); ефективність (економічна вартість у блокчейні менша, ніж у традиційних платіжних каналах, а швидкість транзакції — набагато вища, ніж у банківських платежів); безпека (криптопротокол дає гарантію, що гроші прийдуть до одержувача і при цьому надходити від платника); найбільша ліквідність в порівнянні з іншими криптовалютами; довіра спільноти до біткоіна більша, ніж до будь-якої іншої криптовалюти. Кожна транзакція використовується за допомогою засобів корегування віртуальних псевдонімів - називаються адресами біткоінів [24]. Адреса біткоін виглядає «1DSrfJdB2AnWaFNgSbv3MZC2m74996JafV». Він складається з рядка букв і цифр, що починається з «1» (число один). Для функціонування системи не потрібно створювати централізовані сховища даних. Їх функції забезпечують програми-клієнти, які з'єднуються в ланцюжок і утворюють самодостатній вузол. Біткоін є загальнодоступним і анонімним одночасно. Але список всіх криптовалют не

обмежується одним біткоіном, кожного дня з'являються та зникають десятки криптовалют. З огляду на те, що перша криптовалюта має відкритий програмний код, її почали використовувати для створення альтернативних грошових одиниць. Більшість з криптовалют є форком біткоіну. Тобто основою для створення таких валют став програмний код біткоіна.

Розглянемо деякі особливості криптовалют з огляду на їх використання в противоправній діяльності злочинцями. Так, **ефіріум (ETH, Ethereum)** - це відкрита програмна платформа на базі блокчейн, завдяки якій розробники можуть створювати і розгортати децентралізовані додатки. Головна перевага ефіріума перед біткоіном полягає в тому, що для першого передбачена підтримка різних типів децентралізованих додатків. Дані транзакції біткоінів не просто дають право володіти монетами. Наприклад, нещодавно виконана зміна дозволяє відправляти заблоковані монети за певний період часу. Набір можливих інструкцій відомий як мова сценаріїв Bitcoin, і він навмисно обмежується обробкою транзакцій. Першою новинкою Ethereum було розширення цього набору інструкцій на повнофункціональній мові програмування, такий як JavaScript, що схожа на мову програмування Ethereum [26]. Ethereum став перш за все плацдармом для реалізації різних проектів [27]. У результаті чого з'явилося ICO –форма залучення інвестицій у вигляді продажу інвесторам фіксованої кількості нових одиниць криптовалюти, отриманих разовою або прискореною емісією.

Аналогічно іншим криптовалютам **монеро (XMR, Monero)** являє собою децентралізовану систему з вихідним кодом відкритого типу. Її головне завдання – забезпечувати проведення грошових транзакцій з підтриманням анонімності. Дана криптовалюта призначена не тільки для проведення операцій в повній анонімності, але також може застосовуватися в онлайн-іграх масового використання, також у віртуальних казино. Її користуються при грі в азартні ігри і змаганнях.

Основні особливості Monero:

- принцип кільцевої підписи за рахунок алгоритму Cryptonote;
- захист від майнінгу на окремих пристроях;
- висока ступінь анонімності;

- неможливо відстежувати транзакції;
- автоматичне змішування операцій в мережі;
- необмежена масштабованість;
- використання принципу Proof-of-work.

Ключовою перевагою Monero є найбільш висока в порівнянні з іншими криптовалютами анонімність, що гарантує повну захищеність проведених транзакцій. Наведемо приклад встановлення криптовалютного гаманця для криптовалюти монеро (Додаток 3).

Криптовалюта **даш (Dash)** - це децентралізована криптовалюта та відкрита платіжна система, яка покликана забезпечити високу анонімність транзакцій. До основним характеристикам криптовалюти Dash можна віднести:

- високу ступінь анонімності і швидкість транзакцій;
- децентралізоване управління та прийняття рішень.

Криптовалюта Dash багато в чому нагадує відомий всім Bitcoin, але в той же час має масу переваг. Одним з перших ключових відмінностей варто назвати унікальний алгоритм X11 Algo, що представляє собою дворівневу структуру, яка забезпечує високу анонімність і більш високий захист платежів. В той час коли транзакції через біткоїн можна відстежити за допомогою відповідних ключових точок і алгоритмів, Dash всі зв'язки між платежами та акаунтом стираються, виключаючи можливість будь-яких.

Все більше і більше нових криптовалют сьогодні роблять основний упор на анонімність, серед яких, наприклад Dash і Monero. Але є ще одна криптовалюта, яка не менш анонімна – це **зкэш (ZEC, Zcash)**, в основі, якої лежить метод доказу з нульовим розголошенням zk-SNARK. Це означає, що всі транзакції публікуються в загальнодоступному ланцюжку блоків і будь-хто може переконатися в тому, що переказ був виконаний, однак інформація про відправника, одержувача і суму переказу залишаються закритими. Таким чином, транзакція залишається повністю прихованою і відстежити що-небудь неможливо, метод доказу з нульовим розголошенням дає повну математичну гарантію анонімності.

Також заслуговують на увагу такі криптовалюти такі як **дашкоїн (DSH, Dashcoin)** - анонімна криптовалюта наступного покоління, так як мережевий код завжди оновлюється з мінімальними витратами на розробку і близькими до 0% помилками протоколів. **Поткоїн (POT, Potcoin)** представляє легальну індустрію марихуани, тобто розроблена криптовалюта саме для компаній, які спеціалізуються на виробництві та реалізації канабісу.

В цьому розділі було розглянуто найбільш популярні як серед населення так і серед кримінальних груп криптовалюти. Всього на сьогодні близько 3 000 криптовалют, зрозуміло, що всі описати займе не один десяток сторінок та вийде за межі нашого дослідження, тому деякі інші криптовалюти та їх особливості представлені в Додатку 5.

Отже, можна зробити висновок, що головними властивостями криптовалют є:

1. Обмеженість їх ресурсу, що запобігає інфляції криптовалют.
2. Захищеність даних від зовнішніх впливів та атак.
3. Анонімність користувачів системи. Саме це свого часу привернуло увагу до криптовалют з боку комп'ютерних шахраїв та кримінальних елементів.
4. Прозорість транзакцій, дані про кожна з яких доступні з будь-якого вузлу.
5. Відсутність контролю транзакцій з боку банків, податкових служб або інших наглядових органів держав.

Саме через ці переваги, а також внаслідок зменшення довіри до існуючого фінансового ринку, мінливості валютних курсів і нестійкості фінансових активів криптовалюти зайняли своє місце в сучасній злочинній діяльності.

1.3. Класифікація криптовалютних гаманців

Для дієвої протидії злочинності в питаннях крипто індустрії правоохоронними органами обов'язково необхідні знання щодо основних способах зберігання криптовалюти. Особливо це питання набуває актуальності при проведенні правоохоронними органами оглядів та обшуків, так як незнання як виглядають криптогаманці, як їх виявити та зафіксувати веде до втрати доказової бази та унеможливорює подальше відшкодування заподіяної шкоди.

Криптовалютний гаманець – це еквівалент фізичного гаманця в мережі криптовалют. Гаманець містить ваш приватний ключ (ключі), який дозволяє витратити криптовалюту, розміщені в блокчейні. Кожен такий гаманець показує баланс всіх активів, які він підтримує, і дозволяє робити транзакції в конкретних сумах конкретній людині [29].

Приватний ключ – це секретна інформація, яка підтверджує ваше право витратити криптовалюту за допомогою спеціального гаманця за допомогою криптографічного підпису. Ваш приватний ключ (ключі) зберігається на вашому комп'ютері, якщо ви використовуєте програмний гаманець і зберігається на віддалених серверах, якщо ви використовуєте інтернет-гаманець. Публічне сповіщення ключа може призвести до втрати ваших коштів. Варто дуже уважно зберігати приватні ключі ваших цифрових активів.

Існує кілька видів криптовалютних гаманців. Всі вони мають унікальний механізм забезпечення безпеки приватних ключів.

Види криптовалютних гаманців [30].

- | | |
|--------------|---------------------|
| - апаратні; | - онлайн гаманці; |
| - десктопні; | - паперові гаманці. |
| - мобільні; | |

Апаратні криптовалютні гаманці (див. Додаток 4)

Один з найбільш надійних способів зберігання криптовалюти пропонує саме апаратний гаманець. Пристрій нагадує флешку і зручний у використанні.

Щоб витратити криптовалюту через апаратний гаманець, потрібно спочатку підключити його до ПК, смартфона або планшета. Апаратні криптогаманці зберігають приватні ключі окремо від уразливого обладнання, підключеного до інтернету.

Робота з приватними ключами відбувається з віддаленого захищеного середовища всередині апаратного гаманця, що дозволяє зберігати їх в безпеці навіть при підключенні до ненадійного або зламаного ПК. Розробники передбачають факт викрадення апаратних гаманців, майже всі вони на випадок викрадення захищені вашим особистим PIN-кодом. Якщо гаманець вкрадений, загублений або пошкоджений, існує ініціалізація гаманця – створюється спеціальний код для відновлення, за допомогою якого завжди можна повернути доступ до своїх активів.

Переваги апаратного гаманця: простий спосіб безпечно зберігати криптовалюту, легко захистити і відновити гаманець, менше потенційних вразливостей, проста процедура настройки.

Виявити дані криптовалютні гаманці можливо під час проведення такої слідчо-розшукової дії як обшук, тому в додатку до наукової роботи № зображено найпопулярніші апаратні криптовалютні гаманці .

Десктопні криптовалютні гаманці (див. Додаток 5)

Десктопні (для комп'ютера) криптовалютні гаманці також пропонують високу ступінь безпеки для зберігання криптовалюти.

Гаманці для комп'ютера діляться на «товсті» і «тонкі». Товсті треба завантажувати з усім блокчейном, який буде постійно оновлюватися і, відповідно, займати все більше місця наприклад Bitcoin Core.

Після встановлення програми в діалоговому вікні повідомляється що буде завантажено весь ланцюжок блоків біткоін загальним розміром у 220 гігабайт, чим і забезпечується високий захист.

На відміну від товстих гаманців тонкі не потребують скачування всього блокчейну. При використанні тонкого гаманця рівень безпеки криптовалюта, що зберігається, знижується, оскільки всю інформацію, якої бракує, гаманцю необхідно брати зі сторонніх сервісів, яким доведеться довіряти.

Десктопні криптогаманці поділяються розроблені для однієї криптовалюти напр. Bitcoin Core та мультивалютні котрі підтримують дві і більше криптовалют.

Такі криптовалютні гаманці є досить важкими для виявлення на ПК для оперативних працівників поліції проте у даній науковій роботі наведено алгоритм дій завдяки якому будь який працівник поліції без допомоги працівника технічного відділу може виявити криптовалютний гаманець на персональному комп'ютері .

Мобільні криптовалютні гаманці (див. Додаток 6)

Використання мобільного криптогаманця – найзручніший спосіб розплачуватися криптовалютою в повсякденному житті. Він прекрасно підходить для тих, хто часто здійснює транзакції протягом дня. Доступ через додаток на смартфоні до цифрових активів забезпечує комфортну і швидку роботу з криптовалютою. Тому цей вид криптогаманців користується популярністю серед власників криптовалюти.

Однак варто пам'ятати, що мобільні гаманці не можуть забезпечити високу безпеку зберігання коштів, бо клієнт програми не спирається на локальний (скачаний на смартфон) блокчейн, а працює з віддаленими серверами. Проте для забезпечення безпеки окрім звичайного введення паролю працівник оперативного підрозділу може зіштовхнутись, з такими як сканування відбитку пальця, сканування обличчя також останнім часом розробники почали застосовувати сканування зіниці ока котре може бути використане для захисту мобільних криптовалютних гаманців.

Також важливо на якій операційній системі працює смартфон наприклад на смартфоні під управлінням ОС Android легше обійти систему безпеки із-за великої кількості помилок системи.

Онлайн криптовалютні гаманці (див. Додаток 7)

Онлайн-гаманці для криптовалют – це гаманці, які легко доступні при підключенні до Інтернету через будь-який пристрій. Грубо кажучи, це просто веб-сайт, якому користувач довіряє зберігання своїх коштів та здійснює певні маніпуляції з ними. Онлайн-гаманці зберігають приватні ключі в інтернеті. Доступність цих гаманців дозволяє простіше і швидше здійснювати транзакції. Один із прикладів такого це онлайн криптогаманець «Криптонатор». Так, гаманець Криптонатор - це мультивалютний онлайн-сервіс, який використовується для зберігання, обміну або покупки криптовалюта. Він підтримує 19 криптовалютних одиниць, серед яких: біткоіни (BTC), блеккоін (BLK), монери (XMR), піркоін (PPC), даш (DASH), праймкоін (XPM), редкоін (RDD), емеркоін (EMC), Zcash (ZEC), лайткоін (LTC), Ріплі (XRP) та інші (див. Додаток 8).

Однак це, мабуть, єдиний плюс таких гаманців. Фішинг (крадіжка особистих даних), шкідливе ПЗ, хакерські атаки – онлайн-гаманці схильні до багатьох ризиків.

Так як основним інструментом доступу до онлайн криптогаманця є браузер, результативність виявлення онлайн криптовалютного гаманця полягає у навиках, напрацюваннях та застосування чіткого алгоритму дій.

Паперові криптовалютні гаманці (див. Додаток 9)

Паперовий криптогаманець – документ, який містить копію приватного і публічного ключів. Здебільшого документ має кілька QR-кодів.

Сайти, що надають такі гаманці, генерують біткойн-адреси і створюють зображення, що містять два QR-коди: одну публічну адресу, яку можна використовувати для отримання криптовалюти; інший приватний ключ, яким необхідно скористатися для відправки криптовалюти.

Паперовий гаманець: приватні ключі не зберігається на комп'ютері або в мережі. Тому виявлення такої форми криптовалютного гаманця полягає в обшуку при якому оперативний працівник повинен звернути увагу і вилучити друкований аркуш паперу з відповідними атрибутами.

З усього вище наведеного ми можемо зробити такий висновок, що люди для зберігання великих сум віддають перевагу апаратним і десктопним гаманцям

оскільки вони найбільше заточені на забезпечення безпеки активів. Якщо ж потрібний швидкий доступ до свого гаманця тоді використовують мобільні та онлайн гаманці, однак останні не на стільки безпечні. Виявлення яких проводиться за допомогою використання програмних компонентів за чітким алгоритмом. Що ж стосується паперового варіанту тут складно в працівників поліції можуть з'явитися труднощі з їх виявлення адже вони не реєструються в електронному варіанті, але це залежить від сказати настільки такий гаманець зручний і безпечний. Він виглядає так, надрукований на папері QR-кодів, зручний він для тих хто звик тримати готівку поруч.

ВИСНОВКИ ДО РОЗДІЛУ I.

Технологія блокчейн вже увійшла в наше життя, є правове підґрає цього явища або нема, хочемо ми цього або ні, а правоохоронні органи повинні вже зараз забезпечувати охорону громадян від посягань в сфері використання криптовалют. Так, до особливостей застосування технології блокчейн та криптовалют необхідно віднести: високу ступінь анонімності; неможливість відстежувати транзакції; захищеність даних від зовнішніх впливів та атак; відсутність контролю транзакцій з боку банків, податкових служб або інших наглядових органів держав. Саме за ці властивості технологію блокчейн та криптовалют широко використовуються кримінальними елементами в своїй злочинній діяльності, тому необхідно вносити адекватні зміни в законодавство не тільки України, а і всім країнам світу, а також для ефективної протидії злочинності в сфері застосування технологій блокчейна включити до навчальні планів підготовки правоохоронців відповідні навчальні дисципліни, курси, тренінги, а також розробити або придбати розробки в сфері аналізу транзакцій в мережі блокчейна для правоохоронних органів.

Доведено, що на науковому рівні технологія блокчейн розглядається в основному в технічному напрямку, а щодо впливу її на виникнення нових способів злочинної діяльності або ще більш удосконалення існуючої злочинної діяльності шире в юриспруденції не представлено. Вивчення блокчейна з боку фахівців у кримінології, кримінальному праві, кримінального процесу, криміналістики, економічної безпеки практично не проводиться.

Сформульовано, що криптовалюты можуть використовуватися: в якості грошових коштів (при купівлі зброї, наркотичних засобів, порнографії та інше); як предмет злочинного посягання (розкрадання криптовалют з рахунків, інтернет-шахрайство, вимагання викупу в криптовалюті, шантаж та інше); для добичі криптовалют (шляхом зараження шкідливим програмним забезпеченням користувача, самовільне використання електроенергії на підприємствах та інше).

Наведено вичерпаний перелік нормативно-правових документів, які регулюють відносини в сфері технології блокчейн та криптовалют в Україні та приведені приклади як зазначена сфера регулюється в деяких країнах світу.

Сформовано перелік криптовалют з їх особливостями (властивостями), який дає чітке уявлення співробітникам правоохоронних органів про найбільш популярні криптовалюти (див. Додаток 10).

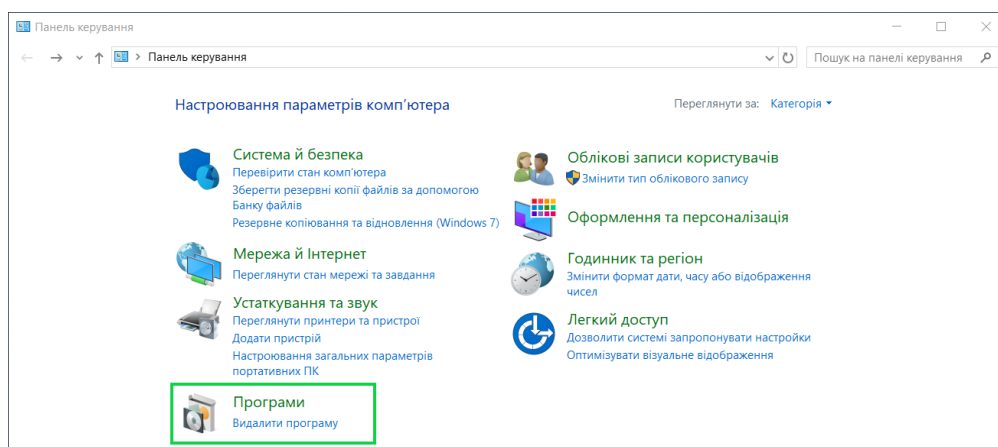
Надана класифікація криптовалютних гаманців, а саме: апаратні, десктопні, мобільні, онлайн гаманці та паперові гаманці та наглядно проілюстрований кожний вид гаманця, що облегшить їх пошук правоохоронцями при огляді або обшуку (див. Додатки 6-11).

РОЗДІЛ II. ВИЯВЛЕННЯ ТА ФІКСАЦІЇ КРИПТОВАЛЮНИХ ГАМАНЦІВ ПРАВООХОРОННИМИ ОРГАНАМИ

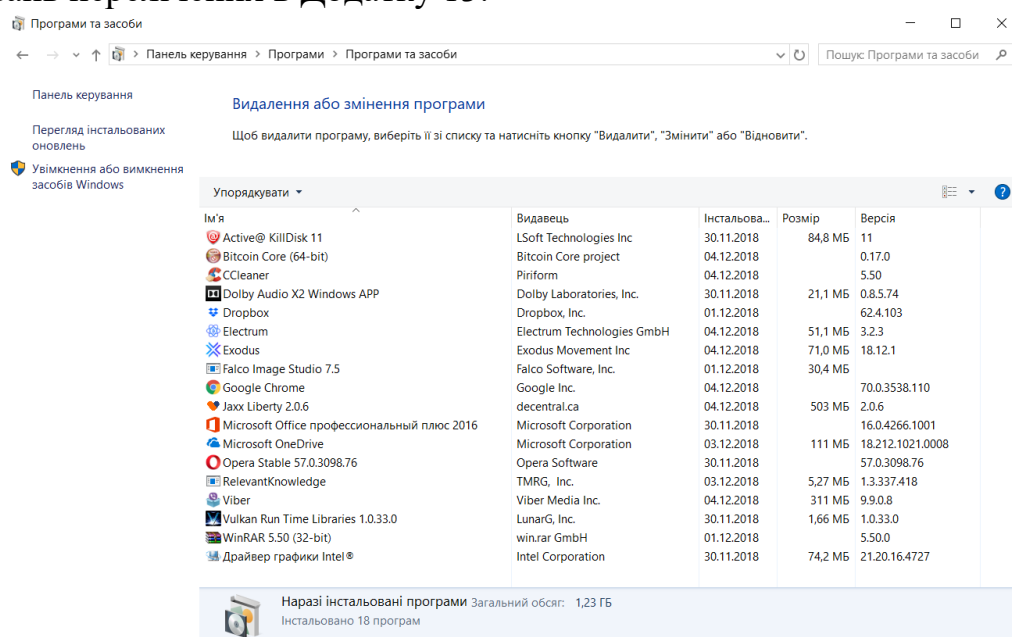
2.1. Алгоритм виявлення криптовалютних гаманців на персональних комп'ютерах

Для виявлення десктопних криптовалютних гаманців необхідно мати доступ до операційної системи персонального комп'ютера. Спочатку потрібно виконати певні налаштування пошуку системи.

Потрібно зайти до «панелі керування» та натиснути «видалити програму»



Перед користувачем вишикується весь список програм встановлених на даному персональному комп'ютері тут потрібно переглянути список на наявність найменувань перелічених в Додатку 13.



Із даного переліку ми знаходимо такі криптовалютні гаманці як «Bitcoin Core», «Electrum», «Exodus», «Jaxx».

Проте не завжди такий спосіб є ефективним оскільки:

- в операційній системі Windows для користувача не є проблемою приховати інсталювану програму.

В даному випадку слід користуватись програмами наприклад CCleaner.

- наявність портативних версій криптовалютних гаманців;
- криптовалютний гаманець був встановлений на іншому ПК відновлений з резервної копії (окремо від операційної системи);
- криптовалютний гаманець знаходиться на змінному носії (портативний HDD та SSD, USB, MicroSD).

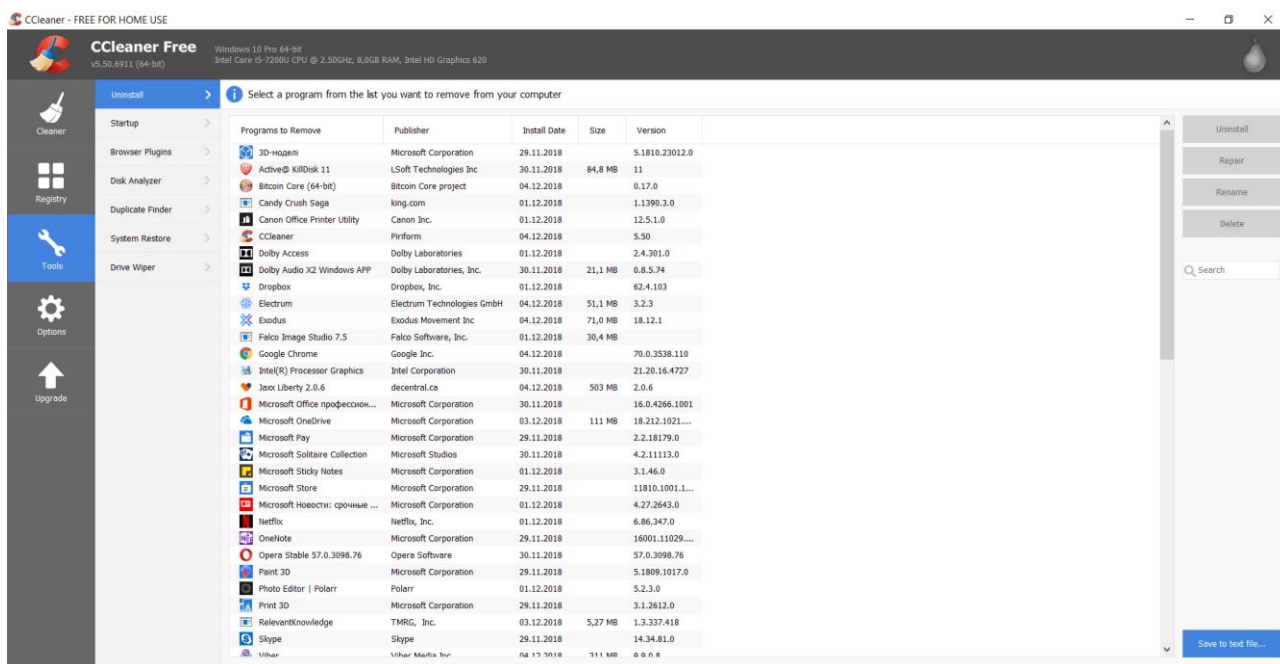
В цих випадках використовуємо прийоми пошуку використовуючи пошукову систему файлової системи, для покращення результатів пошуку можливе використання додаткових програм таких як Everything.

Прикладом програми для виявлення встановленого криптогаманця може слугувати CCleaner. Програма збирає інформацію про використання ПК, всіх встановлених програм та її основною метою є очищення ПК від інформації що накопичується при користуванні комп'ютером проте ми можемо використати ці функції та інструменти у своїх цілях. При правильному використанні її функцій, вони допоможуть оперативному працівнику виявити.

Щоб отримати повний перелік програм на ПК потрібно виконати наступні дії:

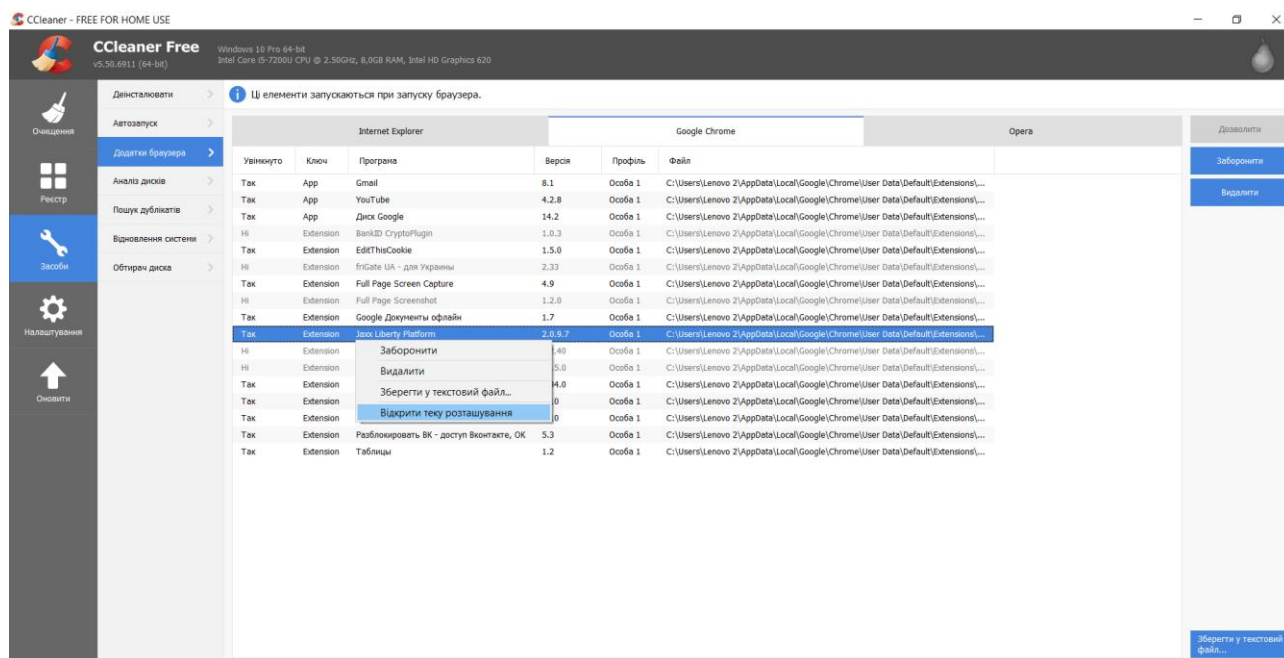
Засоби

Деінсталювати



Також програма має функцію пошуку, що допоможе скоротити час пошуку, але в цьому випадку потрібно мати перелік назв криптогаманців (див. Додаток 11)

Деякі криптовалюти гаманці мають розширення котрі встановлюються в браузер. За допомогою CCleaner ми можемо переглянути встановлені додатки на всіх браузерах. Для цього потрібно перейти в категорію «Додатки браузера»

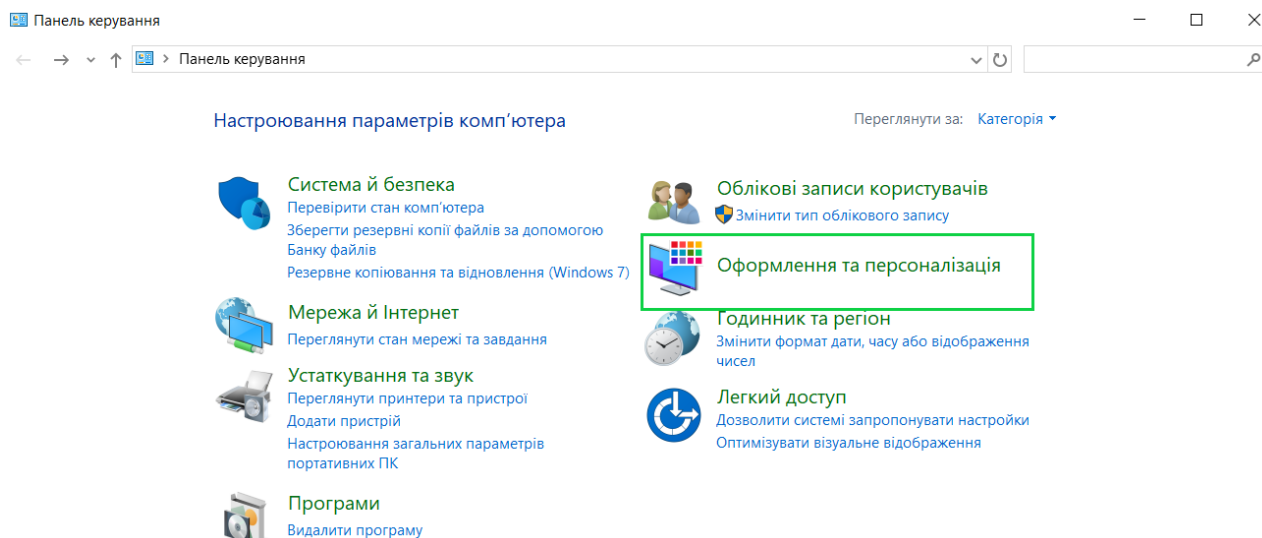


Після виявлення самої програми потрібно знайти власне головний файл гаманця.

Далі пошук буде відбуватись у файловій системі Windows.

Для того щоб розширити коло пошуку потрібно виконати наступні дії:

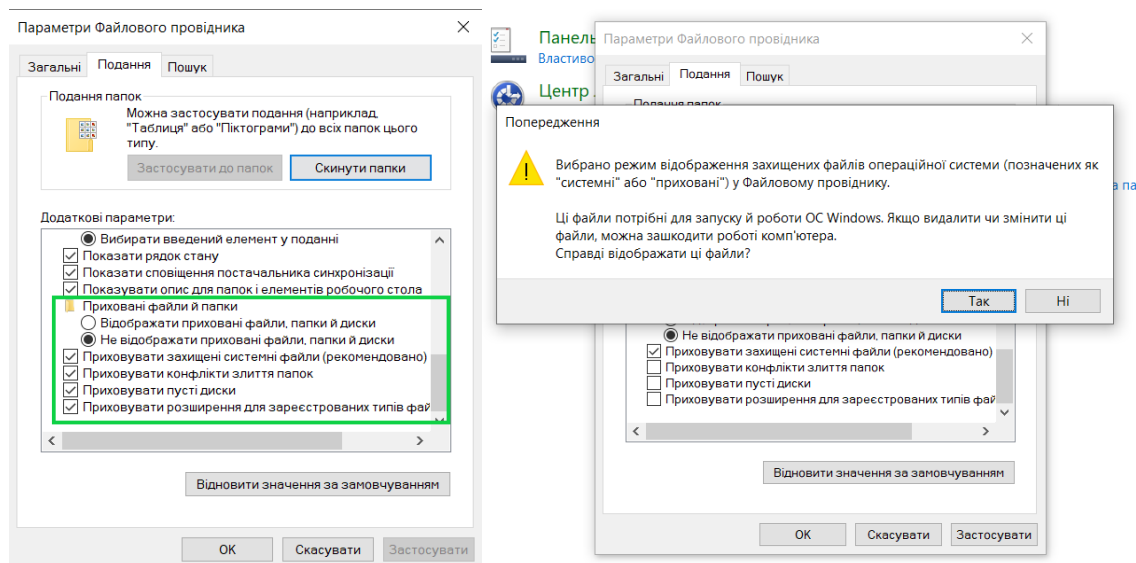
1. Зайти до панелі управління, перейти до категорії «оформлення та персоналізація»



2. В параметрах файлового провідника обрати категорію «Відображати приховані файли та папки» у діалоговому вікні спускаємось до кінця списку та деактивуємо:

- Приховувати розширення для зареєстрованих типів файлів
- Приховувати пусті диски
- Приховувати конфлікти злиття папок
- Приховувати захищені системні файли

Та в діалоговому вікні тиснемо «так»

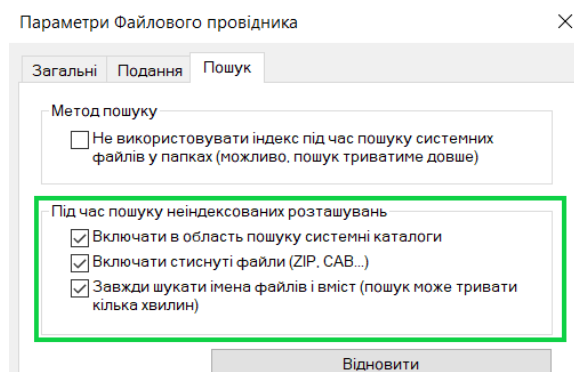


Також вибираємо «Відображати приховані файли й диски»

3. Здійснюємо перехід у вкладку «Пошук»

4. У вкладці активуємо:

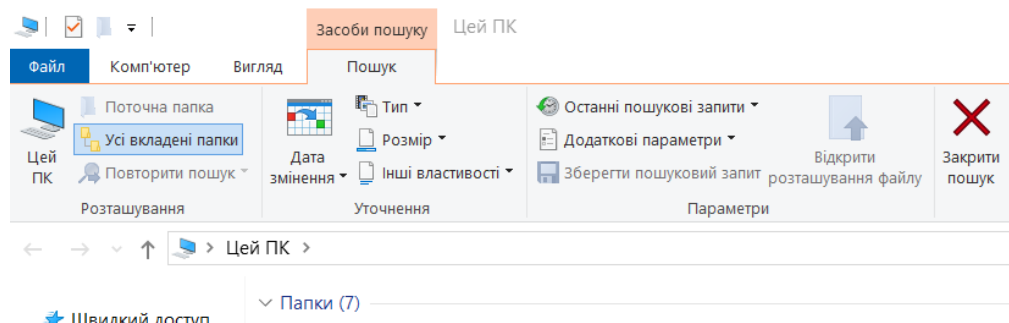
- включати стиснуті файли (ZIP, CAB...);
- завжди шукати імена файлів і вміст .



5. Тиснемо «застосувати» та «ОК»

Переходимо до провідника, найкраще для пошуку тиснути піктограму «Цей ПК» тоді пошук буде здійснюватися на всіх розділах жорсткого диску.

Інтерфейс файлового провідника пропонує деякий набір інструментів який дозволяє фільтрувати та налаштувати результати пошуку в залежності від потреб користувача.

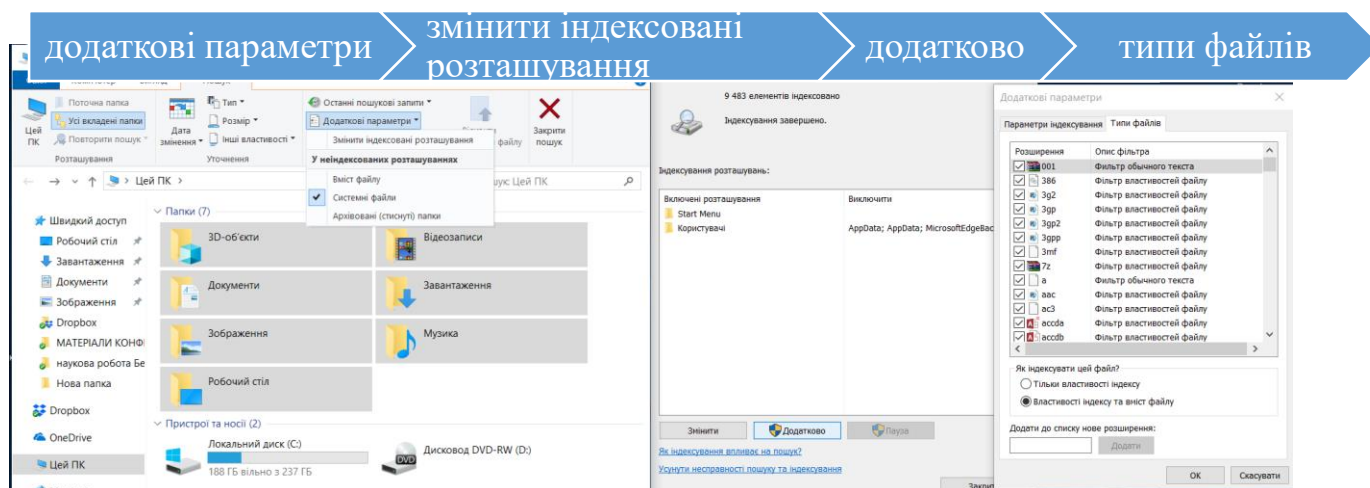


До цих інструментів входить:

- розташування (пошук тільки в поточній папці, пошук у вкладених папках, та клавіша для активації повторного пошуку);
- уточнення (дозволяє вибрати дату змінення, обрати тип файлу, обрати розмір шуканого файлу, та в інших властивостях обрати шлях, ім'я, теги та розширення файлу);
- у параметри пошуку дають можливість переглянути останні пошукові запити, налаштувати індексування, та вибрати пошук в неіндексованих розташуваннях, зберегти пошуковий запит та кнопка «відкрити розташування».

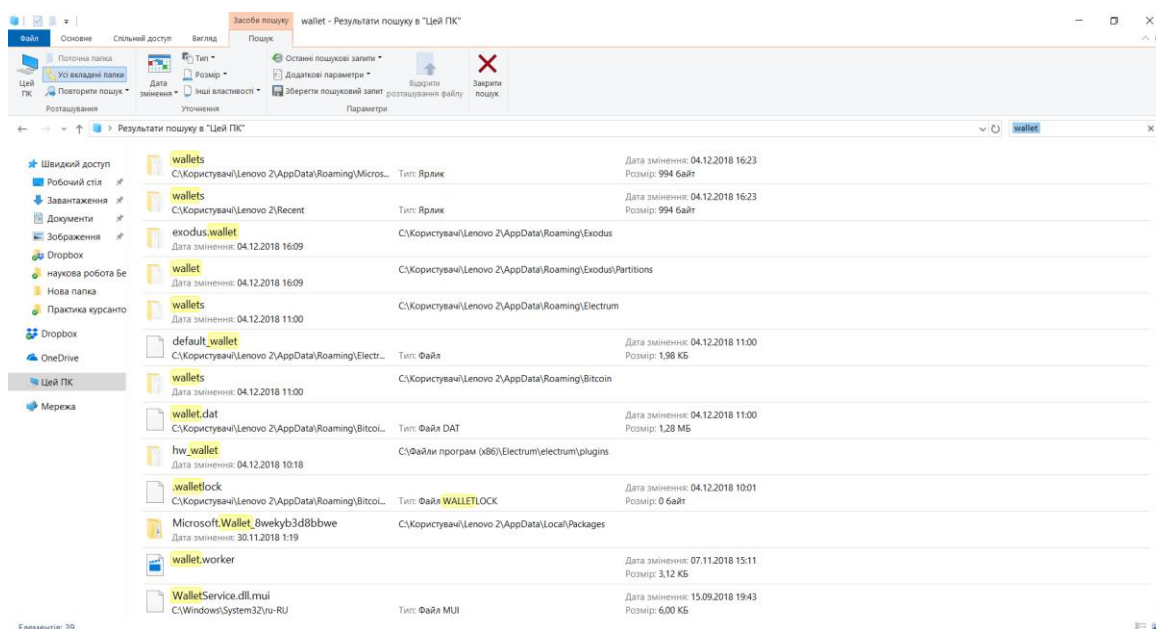
Для уточнення запитів пошуку користувач може скористатись пошуковими операторами (див. додаток 12).

Щоб впевнитись що пошук буде проведено у повній мірі потрібно перевірити чи включені до індексації всі типи файлів потрібно виконати наступні кроки в параметрах пошуку



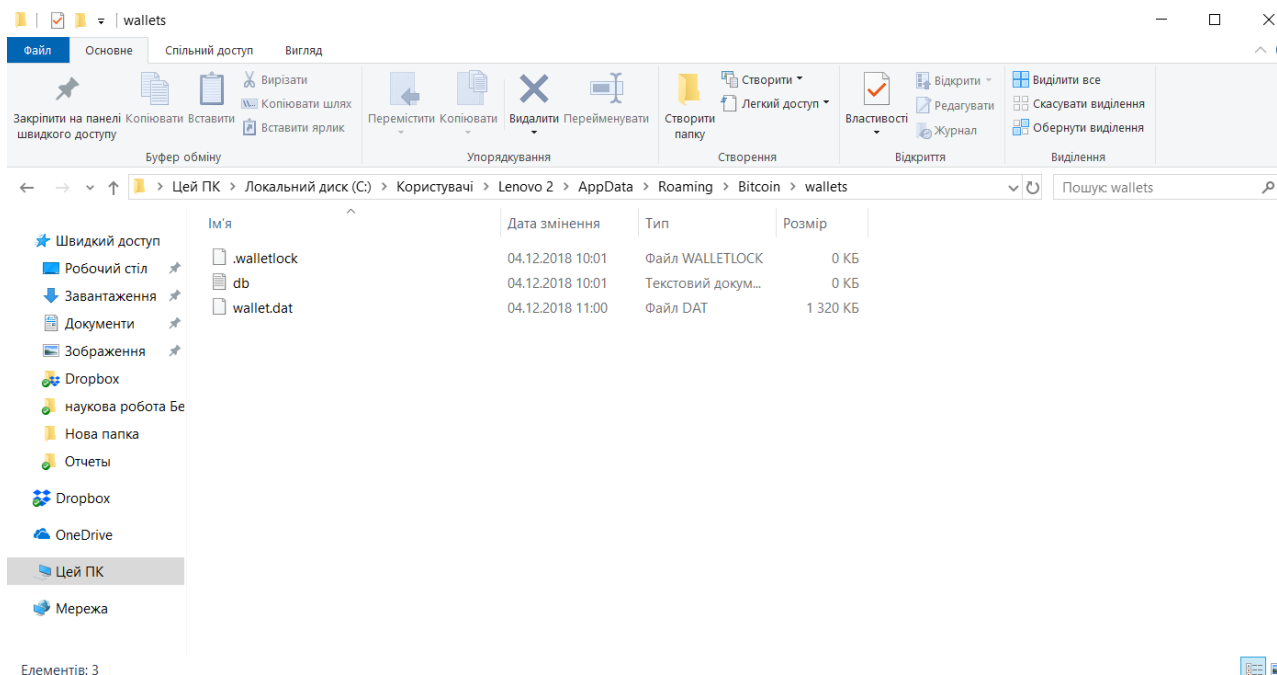
В даному вікні потрібно включити всі розширення до індексування [32].

Потім переходимо в провідник «Цей ПК» вводимо запит в пошукове поле наприклад «Wallet».



В результатах отримуємо 39 елементів серед яких є основні файли гаманця, основний файл у якому містяться вся інформація про рахунок, проведені транзакції. Саме цей файл є головною метою для підрозділів національної поліції, далі роботу продовжувати будуть працівники відділу технічного забезпечення.

Важливим моментом є визначення, від якого криптовалютного гаманця відноситься файл «wallet.dat». Тиснемо клавішу «відкрити розташування файлу».



Відбувається перехід до папки в якій розміщено файл. На рівні пошукового поля у центрі розташовано шлях до файлу «C:\Users\Lenovo 2\AppData\Roaming\Bitcoin\wallets» в шляху ми бачимо папку «Bitcoin» отже на ПК встановлено BitcoinCore.

Альтернативний варіантом пошуку є пошук за допомогою стороннього програмного забезпечення прикладом слугуватиме програма Everything це безкоштовна програма що здійснює миттєвий пошук файлів та папок за назвами.

Особливістю цієї програми є те що вона після встановлення та при першому запуску вона створює індекс для кожного файлу, папки у файлових системах NTFS та ReFS. За замовчуванням Everything індексує всі диски.

Для миттєвого пошуку в програмі потрібно здійснювати її запуск з правами адміністратора при запуску програма сама запропонує цей варіант.

Пошук можливо здійснити за допомогою звичайного пошуку та розширеного.

Розширений пошук пропонує користувачу більш розширений пошук за допомогою інструментів що його уточнюють

Расширенный поиск

Имена файлов содержат...

все эти слова:

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

точную фразу:

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

любые эти слова:

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

кроме этих слов:

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

Слово или фраза внутри файла: ⚠

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

Тип содержимого:


Местоположение:

Тут присутні такі елементи як пошук всіх слів (одне та більше), пошук за точною фразою, пошук за наявністю одного з кількох слів, та обмежити пошук виключенням назв в результатах. Також під кожним пошуковим полем знаходяться прапорці активація яких дозволяє враховувати регістр, окреслити пошук тільки цілими словами, враховувати діакритику [33].

Нижче програма дає змогу налаштувати пошук за:

- місцем розташування;
- досить широкі налаштування дати;
- фільтри файлів, вибір типу файлів, атрибути.

Расширенный поиск

Слово или фраза внутри файла: 

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику


Тип содержимого: Автоопределение


Местоположение: Обзор...

☒ С вложенными папками

Дата изменения: 06.12.2018 по 06.12.2018

Размер: МБ по МБ

Дата создания:  06.12.2018 по 06.12.2018

Дата последнего доступа:  06.12.2018 по 06.12.2018

Дата изменения в базе данных: 06.12.2018 по 06.12.2018

Фильтр: Всё


Тип: (все файлы и папки)

Расширение:

☐ Учитывать регистр ☐ Учитывать диакритику

OK Отмена

Расширенный поиск

Атрибуты: 

☐ Архивный

☐ Сжатый

☐ Устройство

☐ Папка

☐ Зашифрованный

☐ Скрытый

☐ Обычный

☐ Неиндексированный

☐ На отключённом носителе

☐ Только чтение

☐ Точка повторной обработки

☐ Разрежённый файл

☐ Системный

☐ Временный

Регулярное выражение:

☐ Учитывать регистр

Длина имени файла: по

☐ Учитывать путь

Вложенность папок: по

Число запусков: по

Дата запуска: 06.12.2018 по 06.12.2018

Папки с вложенной папкой или файлом, содержащем в имени:

OK Отмена

расширенный поиск

Дата запуска:
 по


Папки с вложенной папкой или файлом, содержащем в имени:

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

Папки с этим количеством вложенных папок и файлов:
 по

Папки с этим количеством файлов:
 по

Папки с этим количеством вложенных папок:
 по

Дубли: 
☐ Имя
☐ Дата изменения
☐ Дата создания
☐ Дата последнего доступа
☐ Размер
☐ Атрибуты

Файл со списком файлов содержит:

☐ Учитывать регистр ☐ Только целые слова ☐ Учитывать диакритику

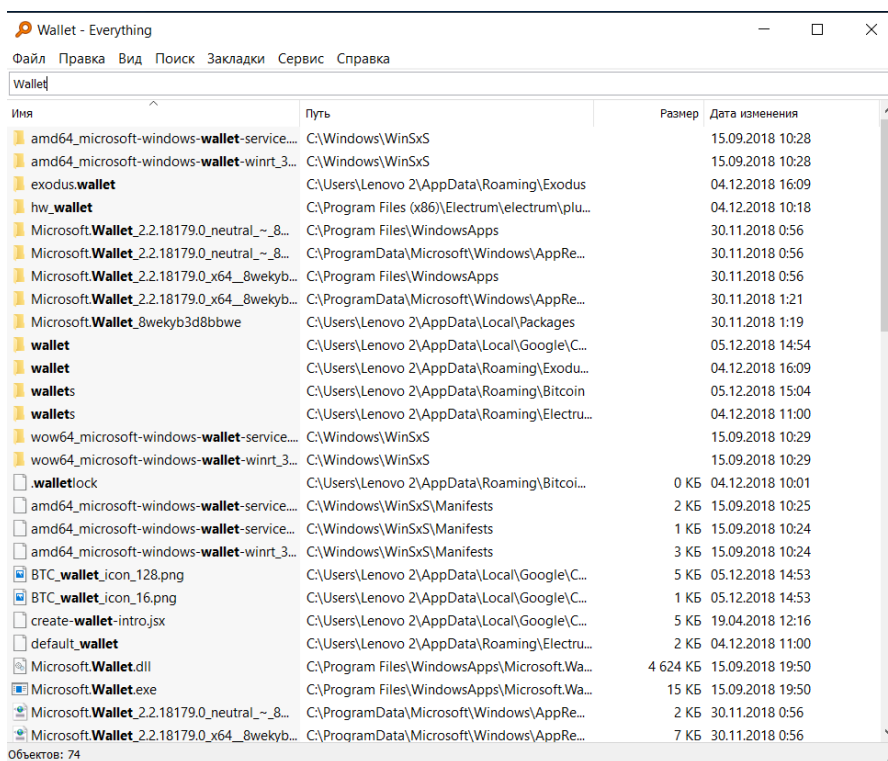
Поиск файлов из списка:

☐ Учитывать регистр ☐ Учитывать диакритику

Дополнительные параметры поиска:

Окрім налаштувань розширеного пошуку програма має пошукові оператори, символи підстановки, макроси, модифікатори, функції та інші інструменти уточнення запиту (див. Додаток 13).

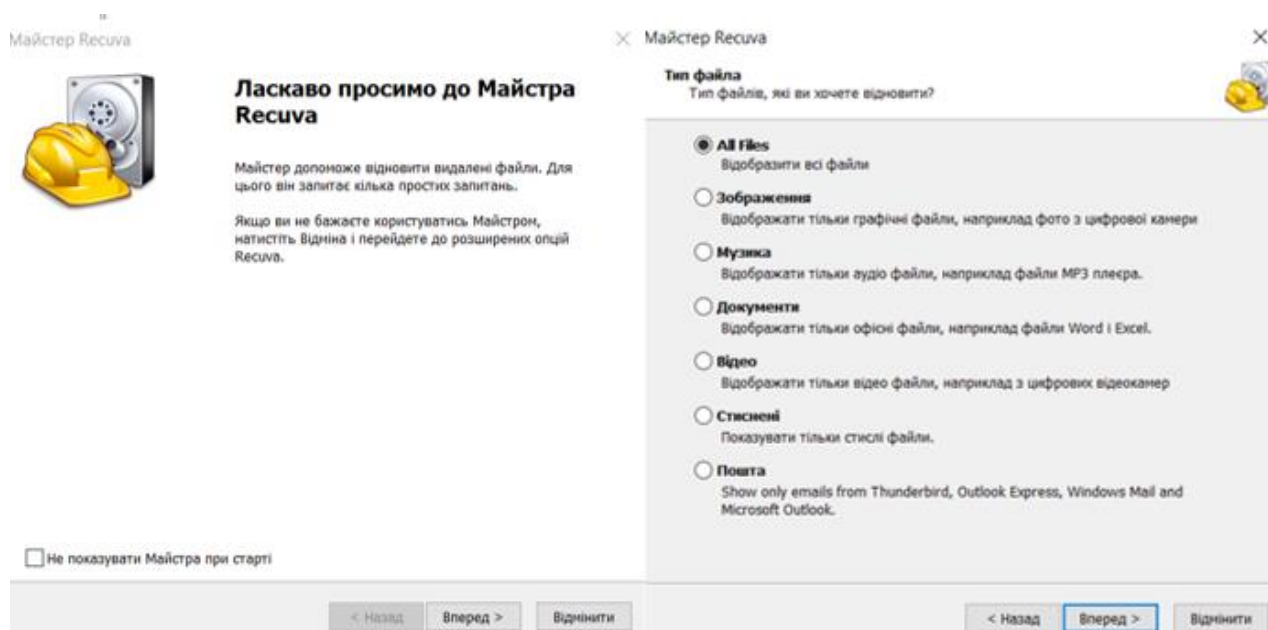
Введемо простий запит «Wallet» програма запропонує файли всіх типів, далі працівнику поліції потрібно виділити важливе зі всіх результатів.



Отримавши результати ми отримуємо папки та файли “wallet” та виявляємо такі криптогаманці як Exodus, Bitcoin, Electrum.

У випадках коли криптогаманець видалили з комп’ютера це не означає що він втрачений назавжди. За допомогою додаткового програмного забезпечення ці файли можна відновити за приклад візьмемо програму «Recuva».

Програма досить легка у користуванні потрібно виконати наступні кроки: Запускаємо програму та вибираємо відобразити всі файли у розділі «тип файла»



1. Наступне вікно «місцезнаходження файлу» тут ми знову вибираємо перший пункт «Шукати усюди на даному комп’ютері»

Майстер Rescuva

Місцезнаходження файла
Де були файли?☒ **Невпевнений**

Шукати усюди на даному комп'ютері

☐ **На мої медіа-картці**

Шукати видалені файли на будь-яких зйомних дисках (крім CD та флопі)

☐ **У Мої Документи**

Пошук у теці документів

☐ **У Корзині**

Шукати видалені файли з Кошика

☐ **Специфічне розміщення**

C:\

Огляд...

☐ **On a CD / DVD**

< Назад

Вперед >

Відмінити

< Назад

Старт

Відмінити

Дякуєм, Rescuva готова шукати
ваші файли

Після закінчення пошуку, ви побачите список знайдених файлів. Відмітьте файли, які ви бажаєте відновити і натисніть кнопку Відновити.

Виберіть, якщо попереднє сканування не дало результатів. Майте на увазі, що на великих дисках може зайняти більше години часу.

☒ Дозволити Покращене Сканування

Натисніть Старт для початку пошуку

2. Особливу увагу звертаємо на прапорець «дозволити покращене сканування» без його активації ми не отримаємо потрібного результату.

Scan

Аналіз 1 з 4 дисків

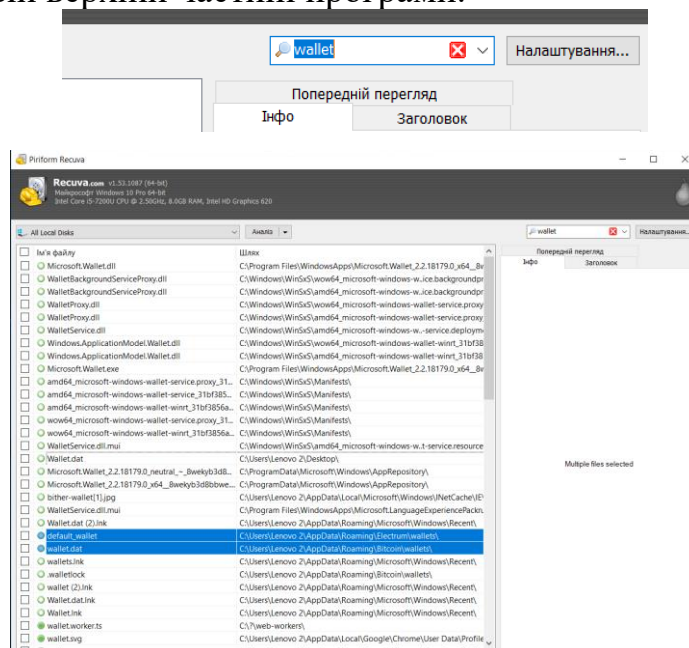
Стан 1 з 3: Сканувати носій на видалені файли

Поточний прогрес: 0%, 131922 файл(ів) знайдено

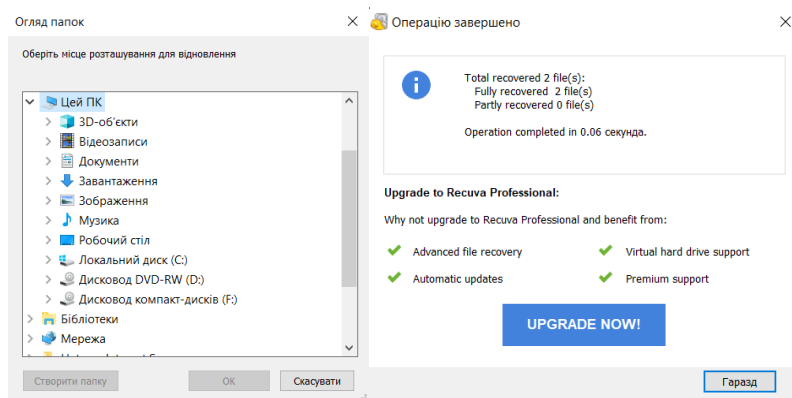
Підрахунок часу, що залишився...

Відмінити

3. Чекаємо закінчення сканування та отримуємо результати у виді списку Пошук серед такої кількості файлів триватиме довго, тому зручніше скористатись пошуком. Пошукова система шукає збіги по назвах серед аналізованих файлів, вона розташована у правій верхній частині програми.



Отримуємо збіги із пошуковим запитом `default_wallet` та `wallet.dat` відновлюємо ці файли для цього тиснемо клавішу відновити.



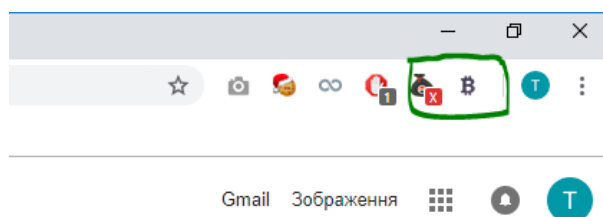
Вказуємо шлях відновлення та тиснемо «ок» далі файл передаємо працівникам відділу технічного забезпечення.

Виявлення слідів діяльності користувача з криптовалютними програмами та додатками в браузері

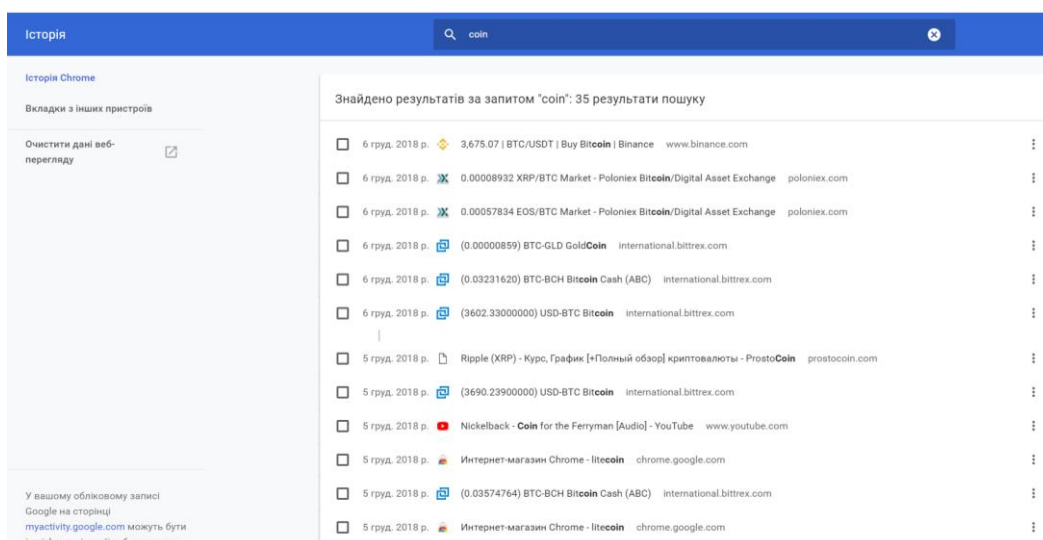
Браузер це програма без якої неможливо користування комп'ютером, особливо проведення маніпуляцій з криптовалютами. Користуючись браузером користувач залишає сліди своєї діяльності які на потрібно звертати увагу та вміти правильно їх виявляти.

Першочергово потрібно переглянути які браузери встановлені на ПК.

Одним із найрозповсюдженішим браузером є Chrome щоб отримати максимум інформації перевіряємо додатки, історію, кеш, збережені паролі.

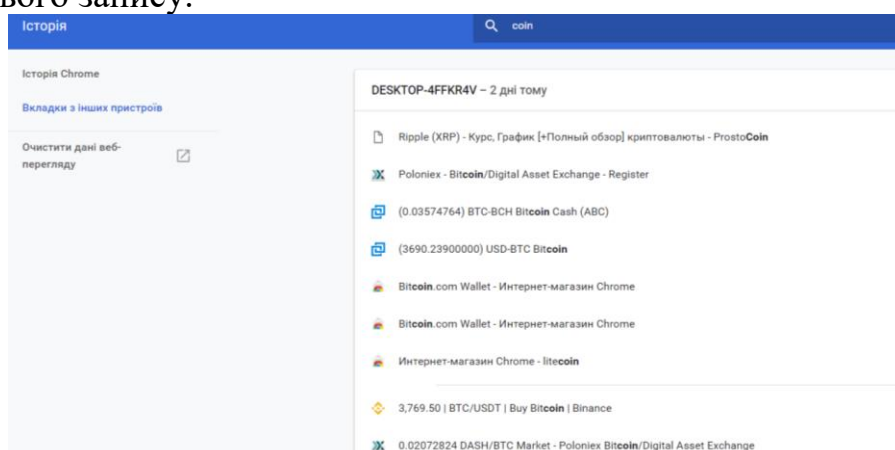


Додатки за звичай розташовані зверху біля акаунту та налаштувань, на даному скриншоті ми бачимо два додатки Jaxx, та BitcoinCore. Комбінацією клавіш `ctrl+h` переходимо до історії. Перед користувачем відкрилась історія браузера проте якщо переглядати її всю це займе багато часу, для його заощадження ми можемо використати пошук по історії. У верхній частині сторінки історія розміщене пошукове поле в яке вводимо запит наприклад «coin»

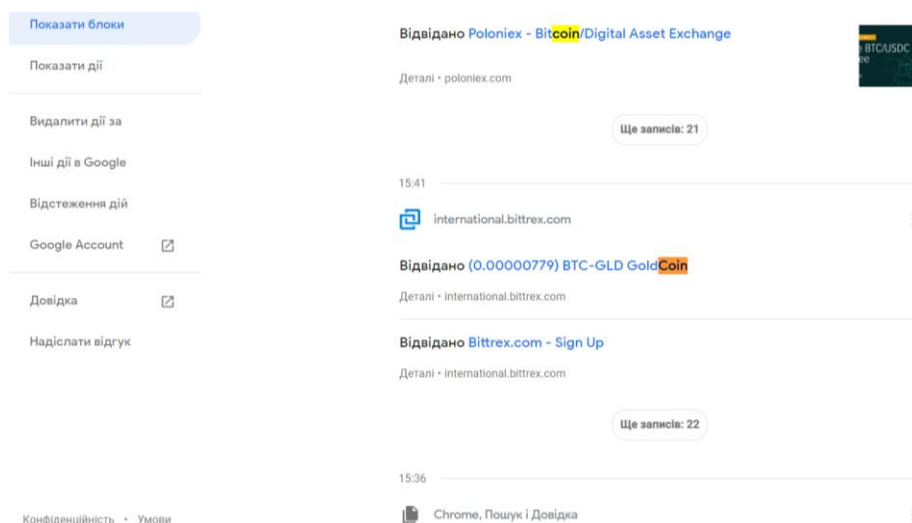


В результатах бачимо відвідані сторінки користувачем за певний час. Бачимо відвідувані сайти (біржі) www.binance.com, <https://poloniex.com/>, <https://international.bittrex.com/>

Також ми можемо переглянути вкладки з інших пристроїв під'єднаних до цього облікового запису.

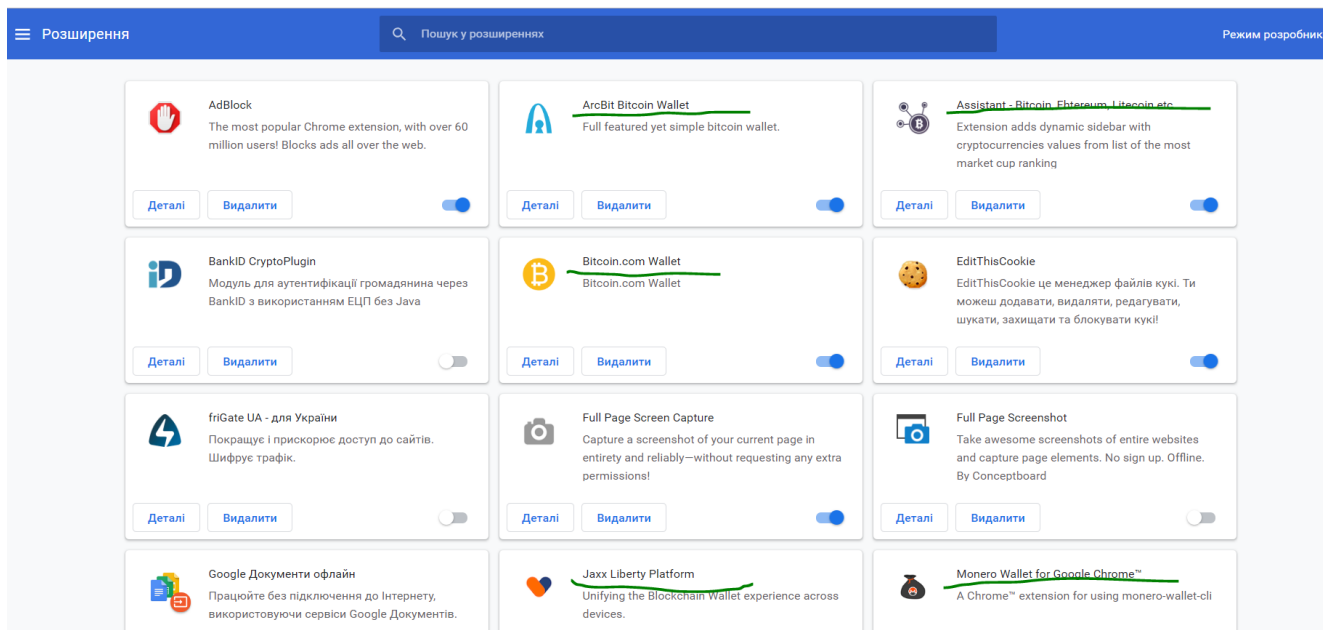


У лівому нижньому куті сторінки є посилання на іншу (детальнішу форму історії)

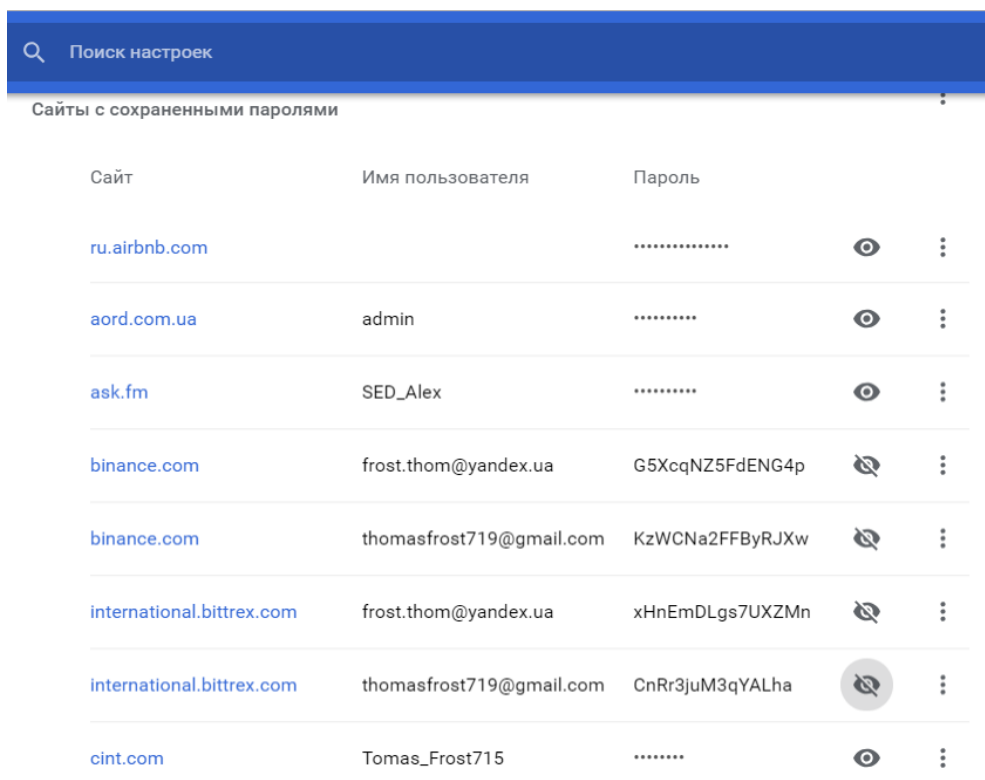


Для того щоб тут здійснити пошук найкращим варіантом буде натиснути клавішу F3 та ввести запит до пошукового поля вверху вікна. Оскільки в історії були

виявлені переходи до магазину Chrome із запитом скачати криптовалютні гаманці переходимо до додатків і виявляємо додатки криптовалютних гаманців.



Наступним кроком слід перевірити браузер на збережені паролі для цього потрібно перейти



На даній сторінці налаштувань зібрано паролі для функції автозаповнення, щоб побачити пароль потрібно активувати клавішу збоку «показати пароль» котра має піктограму у вигляді ока.

Відновлення слідів діяльності користувача в браузері

У випадку якщо користувач досить обережний та видалив історію, паролі, кеш вийшов з облікових записів її можливо відновити кількома методами:

Метод 1: За допомогою DNS

(Domain Name System) операційної системи тимчасово зберігає запити пошуку та видаляє їх після перезавантаження комп'ютера. Коли видаляється історія пошукових запитів, кеш DNS не видаляється. Це означає, що можна побачити всі імена доменів на які були здійснені переходи.

Це швидкий, але він має певні мінуси.

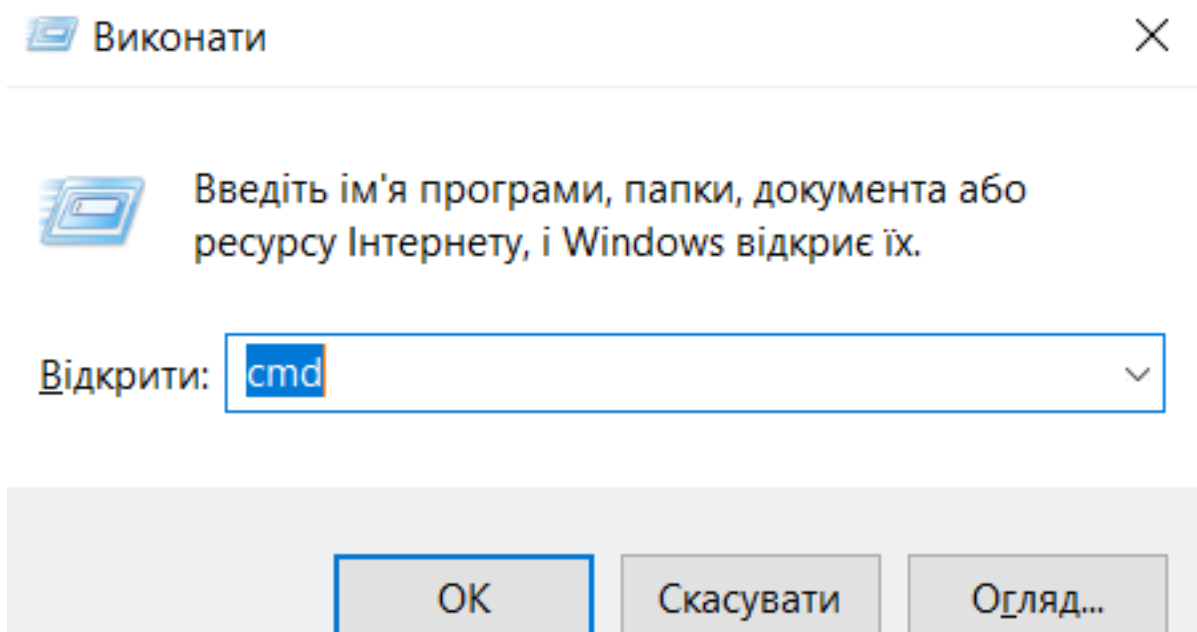
- він відновлює інформацію за досить короткий термін;
- бувають випадки коли цей метод показує недостовірну інформацію.

Так як в кеші зберігаються всі з'єднання комп'ютера з Інтернетом, не тільки з браузера: в тому числі з додатків, реклами, антивірусної програми і т.д.;

- будь-який додаток з'єднується з чимось в інтернеті, це також буде відображено як пошук сайту. Тому буде важко визначити де пошук здійснювався користувачем, а де іншими додатками комп'ютера.

Щоб відновити історію з кешу DNS необхідно зробити наступне:

1. Запустити інструмент «Виконати» (Windows + R) і введіть в ньому команду «cmd» та виконати її.



2. Ввести у вікні Командного рядка команду `ipconfig /displaydns` та виконати її.

```

Командний рядок
Microsoft Windows [Version 10.0.17763.134]
(c) Корпорація Майкрософт (Microsoft Corporation), 2018. Усі права захищено.

C:\Users\Lenovo 2>ipconfig /displaydns

Настройка протокола IP для Windows

r6---sn-bpb5oxu-vqne.googlevideo.com
-----
Имя записи. . . . . : r6---sn-bpb5oxu-vqne.googlevideo.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 1403
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : r6.sn-bpb5oxu-vqne.googlevideo.com

Имя записи. . . . . : r6.sn-bpb5oxu-vqne.googlevideo.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 1403
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . . : 185.158.209.17

Имя записи. . . . . : ns1.google.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 1403
Длина данных. . . . . : 4
Раздел. . . . . : Дополнительно
  
```

Результатом виконання даної команди, користувачеві будуть показані всі сайти, на які було здійснено перехід, включаючи з'єднання додатків комп'ютера.

Але будуть відображені тільки адреси веб-сайтів, а не сторінки на які здійснювався перехід.

Метод 2: За допомогою програм для відновлення даних

Відновлення історії браузера можливе за допомогою таких програм як Resuva, Netman Internet Spy

Для відновлення історії браузера за допомогою програми «resuva» потрібно точно знати яку папку сканувати та які файли відновлювати у кожного браузера ці файли відрізняються за назвою та розташуванням:

У **Google Chrome** ці файли мають такий локальний шлях:

C:\Користувачі\ (Ім'я користувача) \AppData\Local\Google\Chrome\User
Data\Default\local storage

У **Mozilla Firefox**:

C:\Користувачі\ (Ім'я користувача) \AppData\Roaming\Mozilla\Firefox\
Profiles\<profile folder>

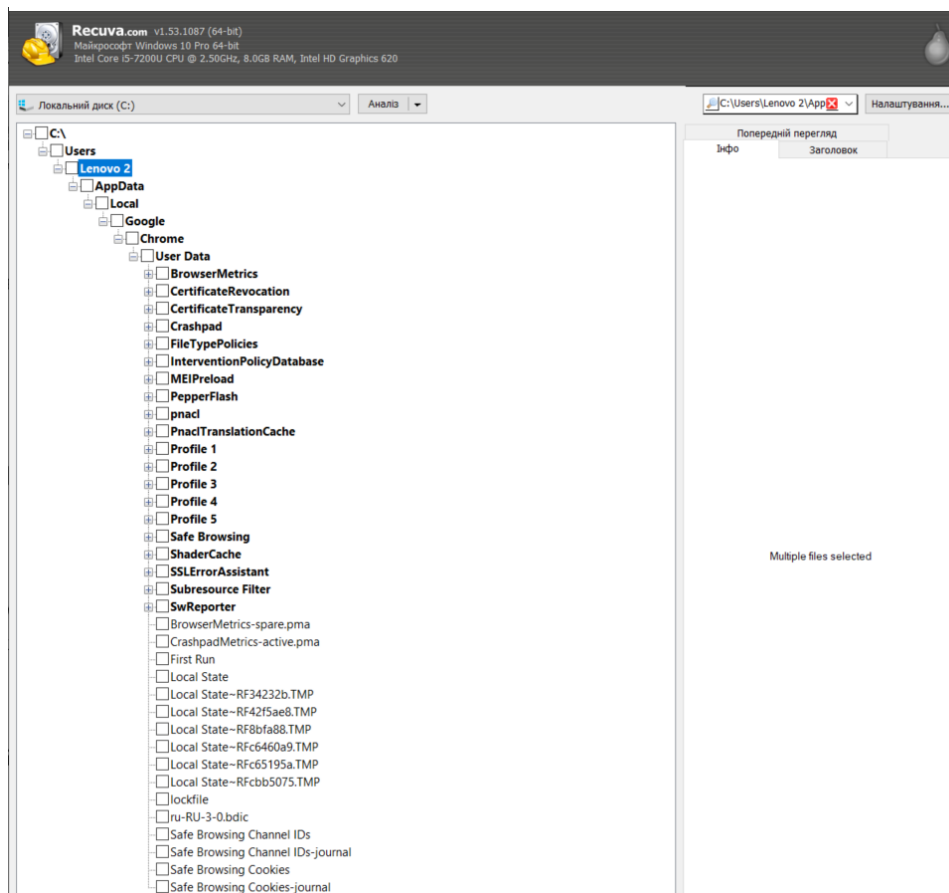
У **Microsoft Edge**:

C:\Користувачі\ (Ім'я користувача) \AppData\Local\Microsoft\

Алгоритм пошуку залишається майже незмінним змінюється тільки те що вказується папка яку потрібно аналізувати

У пошукове поле прописуємо шлях папки яку потрібно аналізувати.

Тиснемо клавішу аналіз та чекаємо деякий час.



Після чого відновлюємо файли в папку з якої їх видалили. Після чого ми отримаємо доступ до видаленої історії через браузер.

2.2. Фіксація криптовалютних гаманців

Фіксація доказів та електронних виявлених криптовалютних гаманців проводиться за допомогою технічних та програмних засобів. Для фіксації криптовалютного гаманця можна використати стандартні програми операційної системи windows такі як «знімок екрану» «захоплення фрагментів», «запис дій користувача».

Найпростіший способом фіксації є знімок екрану - це зображення того, що бачить користувач на екрані монітора. Для того щоб створити знімок всього екрану в операційній системі Windows потрібно натиснути на клавіатурі клавішу та для активного вікна `Alt+PrintScreenSysRq` після натискання клавіші знімок буде автоматично направлений до буфера обміну Windows потім користувачу потрібно запустити будь-який фоторедактор, вставити цей знімок комбінацією клавіш `Ctrl+V` до файлу та зберегти його з відповідною назвою та форматом.

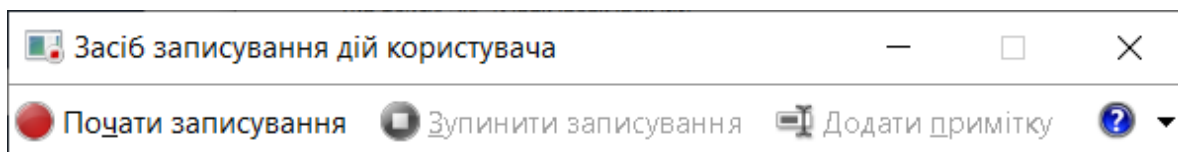
Рекомендовано зберігати знімки за допомогою стандартної програми paint так як вона є системним компонентом операційної системи та не потребує встановлення (див. Додаток 14).

Функція захоплення екрану дає можливість зробити знімок всього екрану, прямокутної або довільної форми, на відміну від першого способу інструмент дає змогу зберегти знімок у форматах PNG, GIF або JPEG (див. Додаток 15).

Засіб записування дій користувача

Стандартний інструмент, котрий покрокова описує та фіксує знімками екрану активність пристроїв вводу інформації таких як миша, клавіатура, вказує дату та час, надає інформацію про операційну систему в якій здійснено запис.

Для використання цього інструменту потрібно натиснути на клавішу «почати записування».



Далі виконувати дії щодо виявлення криптовалютних гаманців. По завершенню натиснути клавішу зупинити записування, потім зберегти. Файл формату MHTML збережеться в архіві який з легкістю можливо запустити на іншому ПК (див. Додаток 16).

На відміну від стандартних інструментів операційної системи Windows стандартного програмного забезпечення додаткове пропонує більший спектр функцій наприклад програмне забезпечення Bandicam Screen Recorder дозволяє записати дії користувача на відео, при цьому має велику функціональність.

Для використання програму потрібно встановити на ПК та запустити. На головному екрані присутні такі варіанти запису як:

- «прямокутна ділянка» - зйомка буде проводитись тільки тієї частини екрану, яку окреслив користувач. В даному режимі користувачеві потрібно обрати місце та розмір ділянки запису та натиснути «почати запис».
- «Весь екран» захоплення буде проводитись на всьому екрані.
- «Навколо курсора» буде знімати частину навколо курсора.
- «Запис з пристрою» цей режим захоплює інформацію з зовнішніх пристроїв з веб-камери, смартфонів, IPTV

Для початку запису потрібно виконати наступні дії:

1. Обрати пристрій-камеру з якої буде проводитись зйомка;
2. Натиснути клавішу «почати запис».

Також для початку та зупинки запису, можна користуватись клавішами клавіатури F12 та для захоплення зображення F11.

Під час захоплення екрану можливо додати звук з мікрофону, додати ефекти курсора та зображення з веб-камери під час запис (див. Додаток 17).

ВИСНОВКИ ДО РОЗДІЛУ II.

В розділі було наглядно продемонстровано алгоритм виявлення криптовалютних гаманців на персональних комп'ютері та в додатках до наукової роботи надано візуалізація основних криптовалютних гаманців (див. Додатки 6-13).

Розглянуті сучасні практики виявлення та фіксації криптогаманців, а також інструменти уточнення пошуку за допомогою програми Everything. Наведено методи відновлення видаленої історії браузера, а саме за допомогою DNS та програм (наприклад Rescuva, Hetman Internet Spy)

Всі переховані інструменти, методи та прийоми в свою чергу дають правоохоронним органам знання щодо зовнішнього виду криптогаманців, їх особливостей, що в свою чергу полегшить їх виявлення та подальше використання в якості доказової бази у кримінальному провадженні або засобу відшкодування коштів потерпілій стороні.

ВИСНОВКИ

Дана кваліфікаційна робота є сучасним дослідженням, яке зібрало в собі основні положення щодо технології блокчейн і криптовалюти та їх місця в злочинній діяльності, а також прийоми, методи та інструменти виявлення та фіксації криптовалютних гаманців.

Так, до особливостей застосування технології блокчейн та криптовалют необхідно віднести: високу ступінь анонімності; неможливість відстежувати транзакції; захищеність даних від зовнішніх впливів та атак; відсутність контролю транзакцій з боку банків, податкових служб або інших наглядових органів держав. Саме за ці властивості технологію блокчейн та криптовалюти широко використовуються кримінальними елементами в своїй злочинній діяльності, тому необхідно вносити адекватні зміни в законодавство не тільки України, а і всім країнам світу, а також для ефективної протидії злочинності в сфері застосування технологій блокчейна включити до навчальні планів підготовки правоохоронців відповідні навчальні дисципліни, курси, тренінги, а також розробити або придбати розробки в сфері аналізу транзакцій в мережі блокчейна для правоохоронних органів.

На прикладі криптовалюти біткоїн продемонстровано як саме працює технологія блокчейн (див. Додаток 1). Сформульовано, що криптовалюти можуть використовуватися: в якості грошових коштів (при купівлі зброї, наркотичних засобів, порнографії та інше); як предмет злочинного посягання (розкрадання криптовалюти з рахунків, інтернет-шахрайство, вимагання викупу в криптовалюті, шантаж та інше); для добичі криптовалют (шляхом зараження шкідливим програмним забезпеченням користувача, самовільне використання електроенергії на підприємствах та інше).

В роботі наведено вичерпаний перелік нормативно-правових документів, які регулюють відносини в сфері технології блокчейн та криптовалют в Україні та приведені приклади як зазначена сфера регулюється в деяких країн світу.

Наведена класифікація криптовалютних гаманців, а саме: апаратні, десктопні, мобільні, онлайн гаманці та паперові гаманці та наглядно проілюстрований кожний вид гаманця, що облегшить їх пошук правоохоронцями при огляді або обшуку (див. Додатки 6-11). А також перелік основних запитів, які повинен зробити правоохоронець для виявлення криптовалютного гаманця на персональному комп'ютері.

Розглянуті та практично продемонстровані сучасні практики виявлення та фіксації криптогаманців, а також інструменти уточнення пошуку за допомогою програми Everything. Наведено методи відновлення видаленої історії браузера, а саме за допомогою DNS та програм (наприклад Recuva, Hetman Internet Spy).

Список використаних джерел

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: <https://bitcoin.org/bitcoin.pdf>
2. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014. 298 p.
3. Блокчейн. URL: <https://uk.wikipedia.org/wiki/Блокчейн>
4. Blockchain.Investopedia. Процитовано 19 March 2016. «Based on the Bitcoin protocol, the blockchain database is shared by all nodes participating in a system».
5. Ежемесячный анализ рынка криптовалют и ICO. URL: <https://anycoin.news/2018/08/08/ico-crypto-july>
6. Ісмаїлов К.Ю., М.Г. Романюков Вплив розвитку інформаційного суспільства на принципи засекречування. *Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції: збірник наукових статей за матеріалами доповідей Всеукраїнської науково-практичного семінару 23.03.2018 року*. Львів: ЛьВДУВС, 2018. С. 141-146.
7. Ісмаїлов К.Ю., Д.В Крівега., М.Г. Романюков Проблеми нормативно-правового регулювання обороту криптовалюти : сучасний світовий досвід та перспективи для України. *Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.)*. Одеса: Одеський державний університет внутрішніх справ, 2017. С. 74-76.
8. Конституція України. URL: <http://zakon0.rada.gov.ua/laws/show/254к/96-вр>
9. Кодекс України про адміністративні правопорушення. URL: <http://zakon3.rada.gov.ua/laws/show/80731-10>
10. Про фінансові послуги та державне регулювання ринків фінансових послуг: Закон України. URL: <http://zakon2.rada.gov.ua/laws/show/2664-14>
11. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню

розповсюдження зброї масового знищення: Закон України. URL: <http://zakon3.rada.gov.ua/laws/show/1702-18>

12. Про ліцензування видів господарської діяльності: Закон України. URL: <http://zakon2.rada.gov.ua/laws/show/222-19>

13. Про збір на обов'язкове державне пенсійне страхування: Закон України. URL: <http://zakon3.rada.gov.ua/laws/show/400/97->

14. Про індустріальні парки: Закон України. URL: <http://zakon2.rada.gov.ua/laws/show/5018-17>

15. Про інноваційну діяльність: Закон України. URL: <http://zakon2.rada.gov.ua/laws/show/40-15>

16. Про телекомунікації: Законом України. URL: <http://zakon.rada.gov.ua/laws/show/1280-15>

17. Bitcoin та Blockchain, що це таке і як працює в Україні та світі. URL: <https://hromadske.ua/posts/shcho-take-bitcoin>

18. Molly Wood Here's why Bitcoin is the future of money. Cnet. 2013. 29

19. Про обіг криптовалюти в Україні: проекту Закону України URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684

20. Криптовалюта. URL: <https://inlnk.ru/xvnkXG>

21. В США открылись первые курсы для крипто-следователей. URL: <https://bitnovosti.com/2018/12/04/v-ssha-otkrylis-pervye-kursy-dlya-kripto-sledovatelej>

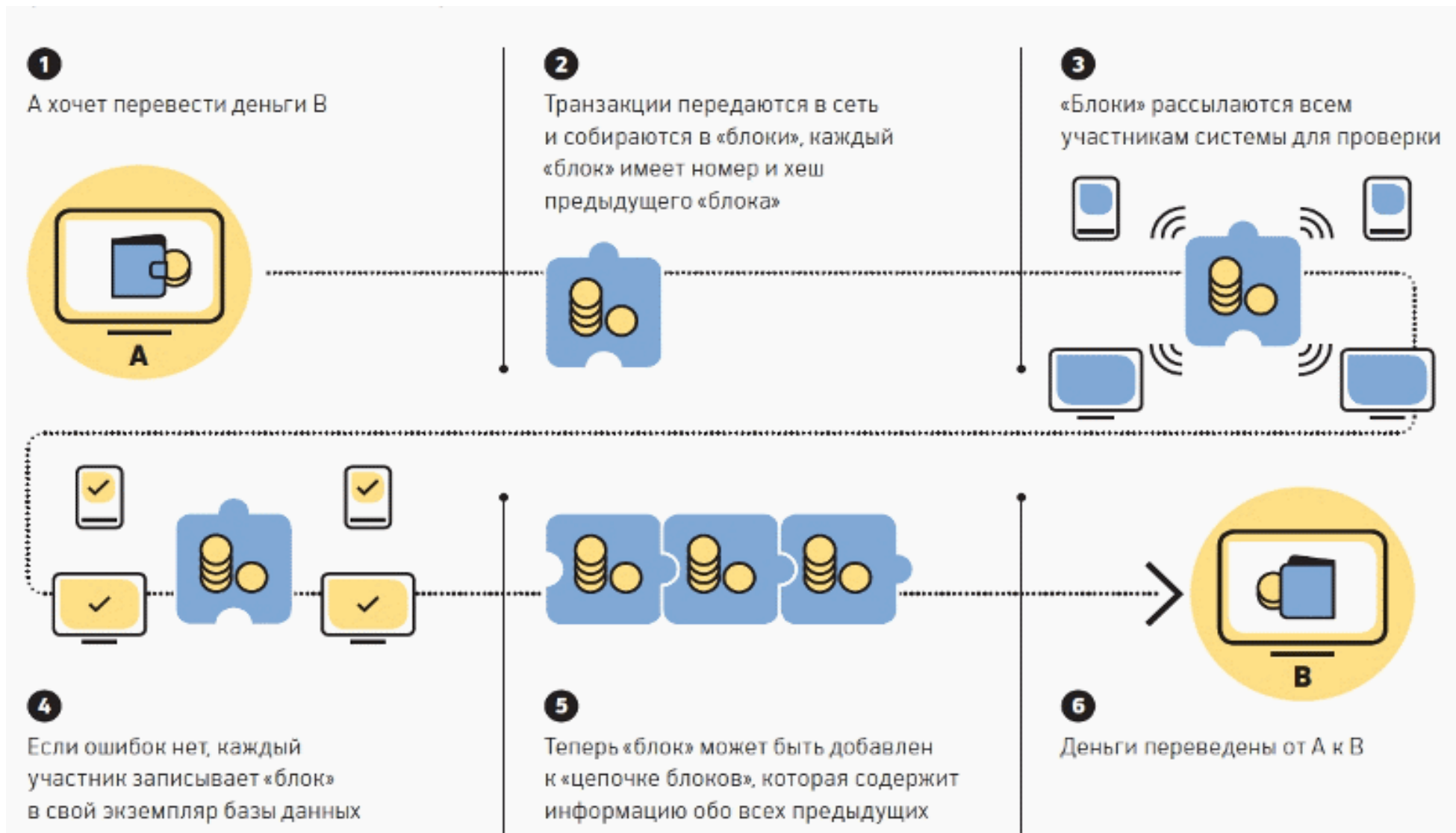
22. ICE: преступники «уязвимы» при конвертации криптовалют в фиат. URL: <https://bitnovosti.com/2018/10/04/ice-prestupniki-uyazvimy-pri-konvertatsii-kriptovalyut-v-fiat>

23. Лондонские полицейские пройдут обучающие курсы о криптовалютах URL: <https://bitnovosti.com/2018/07/23/londonskie-politseyskie-projdut-obuchayushhie-kursy-o-kriptovalyutah/>

24. Karame O.G., Androulaki E., Capkun S. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. URL: <https://eprint.iacr.org/2012/248.pdf>

25. Какие криптовалюты существуют. URL: <https://1ethereum.ru/kakie-est-kriptovalyuty/#i-3>
26. Биткоин VS Ethereum: сравнение криптовалюты. URL: <https://golos.io/ru-golos/@junglebitcoin/bitcoin-vs-ethereum-sravnenie-kriptovalyuty>
27. История биткойна: краткий экскурс в прошлое и будущее криптовалют. URL: <https://geektimes.ru/post/294881>
28. В НБУ пояснили, який статус Bitcoin має в Україні. URL: <https://www.segodnya.ua/economics/finance/v-nbu-obyasnili-kakoy-status-imeet-bitcoin-v-ukraine-1046544.html>
29. Криптовалютные кошельки. URL: <https://inlnk.ru/MjJ7An>
30. Огляд криптовалютних гаманців. URL: <https://stocx.org/cryptovalyutni-gamantsi>
31. Бедрій Т.А., Андрієнко І.С. Медична таємниця: окремі аспекти. *Проблемні питання правоохоронної та правозахисної діяльності в контексті Євроінтеграційних тенденцій: матеріали Міжнародної курсантсько-студентської науково-практичної конференції (м. Одеса, 29.03.2018 р.)*. Одеса, Видавничий дім «Гельветика», 2018. С. 18-21.
32. Search indexing in Windows 10: FAQ. URL: <https://support.microsoft.com/en-gb/help/4098843/windows-10-search-indexing-faq>
33. Voidtools. URL: <https://www.voidtools.com/ru-ru/faq>
34. Криптовалюта як якісно новий платіжний інструмент та перспективи її інтеграції у світову фінансову систему. URL: https://www.dnu.dp.ua/docs/visnik/fmecon/program_5e4b83104fa49.pdf
35. Гордієнко С. Доктринальні положення інформаційної безпеки України в умовах сучасності. *Юридичний вісник*. 2019. № 3. URL: <https://lexinform.com.ua/dumka-eksperta/doktryni-polozhennya-informatsijnoyi-bezpeky-ukrayiny-v-umovah-suchasnosti>
36. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. № 2. С. 200-203.

СХЕМА ЯК ПРАЦЮЄ БЛОКЧЕЙН НА ПРИКЛАДІ КРИПТОВАЛЮТИ



*Додаток 1 продовження***ЯК САМЕ ПРАЦЮЄ БЛОКЧЕЙН НА ПРИКЛАДІ КРИПТОВАЛЮТИ БІТКОІН**

1. Користувач «А» має намір переказати певну суму до користувача «Б». Вони відкривають біткоїн-гаманці та стають учасниками блокчейн-мережі.
2. При відкриванні гаманця користувач отримує його номер, що є публічним кодом і зазначається для здійснення фінансових операцій.
3. Після заповнення відомостей про переказ (сума, номер гаманця отримувача), транзакція скеровується до блокчейн-мережі, де очікує на інші транзакції, щоб сформувався блок.
4. Блоку привласнюється номер і майнери обчислюють для нього хеш - спеціальний код, що містить відомості про цей та попередній блоки (див. Додаток2).
5. Блок розсилається до всіх учасників мережі та вони перевіряють дані.
6. Якщо помилки не знайдено, то кожен учасник додає блок до свого екземпляру розподіленої бази даних.
7. Блок додається в кінець ланцюжка блоків і містить інформацію про попередній блок, який відповідно містить інформацію про блок, що перед ним і так далі до початкового блоку в ланцюжку. Транзакція вважається підтвердженою. Виробляється закритий код для кожної транзакції блоку.
8. Відповідь про підтвердження транзакції разом із закритим ключем надходить до учасника «Б». Користуватися грошима з гаманця – обміняти на іншу валюту, здійснити покупку або переказ можна лише знаючи закритий код.

Додаток 2

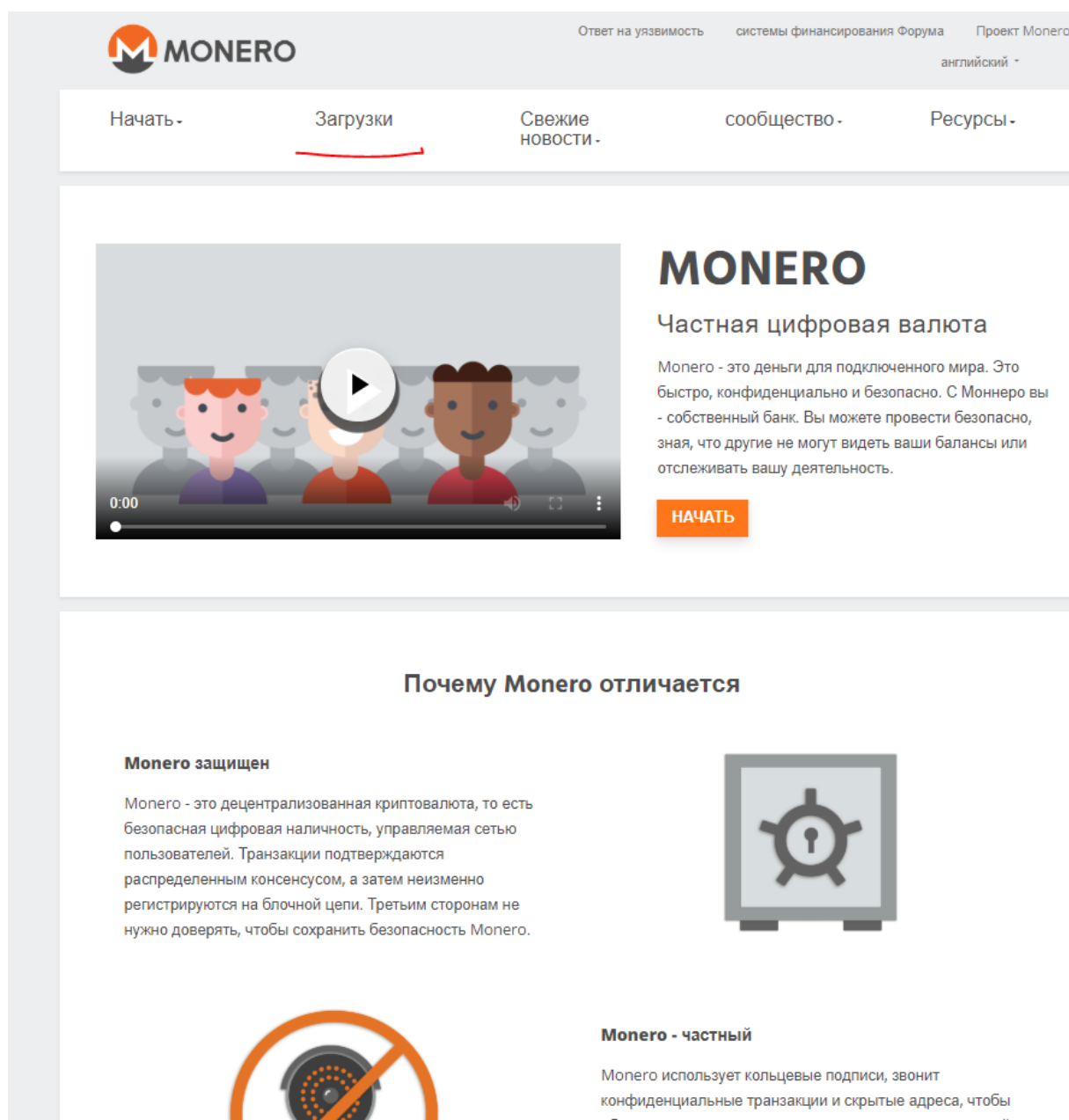
**ДИНАМІКА
КАПІТАЛІЗАЦІЇ КРИПТОВАЛЮТНОГО РИНКУ
квітень-серпень 2018 року**

#	Name of Parameter	1-Apr-18	1-May-18	MoM, %	1-June-18	MoM, %	1-July-18	MoM, %	1-Aug-18	DoD, %	5-Aug-18	DoD, %
1	Total market capitalization, USD billion	263,9	423,2	60,4%	331,3	-21,7%	257,7	-22,2%	277,8	7,8%	253,8	-8,6%
2	Altcoin market capitalization, USD billion	145,2	265,8	83,1%	203,2	-23,6%	147,9	-27,2%	144,3	-2,4%	132,9	-7,9%
	Altcoin dominance, %	55,0%	62,8%	-	61,3%	-	57,4%	-	51,9%	-	52,4%	-
3	Bitcoin price, \$	7 003,1	9 251,5	32,1%	7 500,7	-18,9%	6 411,7	-14,5%	7 769,0	21,2%	7 031,1	-9,5%
	Bitcoin market capitalization, USD billion	118,7	157,4	32,6%	128,0	-18,6%	109,8	-14,2%	133,5	21,6%	120,9	-9,5%
	Bitcoin dominance, %	45,0%	37,2%	-	38,6%	-	42,6%	-	48,1%	-	47,6%	-
4	Ethereum price, \$	397,3	670,5	68,8%	578,7	-13,7%	455,2	-21,3%	433,9	-4,7%	407,4	-6,1%
	Ethereum market capitalization, USD billion	39,1	66,5	69,8%	57,7	-13,1%	45,7	-20,8%	43,8	-4,1%	41,2	-6,0%
	Ethereum dominance, %	14,8%	15,7%	-	17,4%	-	17,7%	-	15,8%	-	16,2%	-
5	Bitcoin Cash price, \$	688,0	1 348,6	96,0%	995,7	-26,2%	749,2	-24,8%	780,0	4,1%	696,1	-10,8%
	Bitcoin Cash market capitalization, USD billion	11,7	23,1	96,6%	17,1	-25,9%	12,9	-24,5%	13,5	4,4%	12,0	-10,7%
	Bitcoin Cash dominance, %	4,4%	5,5%	-	5,2%	-	5,0%	-	4,8%	-	4,7%	-
6	Litecoin price, \$	116,9	148,3	26,9%	118,0	-20,4%	81,5	-30,9%	80,4	-1,4%	73,4	-8,7%
	Litecoin market capitalization, USD billion	6,5	8,4	27,9%	6,7	-19,8%	4,7	-30,4%	4,6	-0,6%	4,2	-8,6%
	Litecoin dominance, %	2,5%	2,0%	-	2,0%	-	1,8%	-	1,7%	-	1,7%	-
7	Volume (24h) 4 crypto, USD billion**	6,4	11,8	84,2%	7,7	-35,0%	7,1	-7,1%	7,5	5,4%	5,6	-25,7%
	Market cap 4 crypto, USD billion	189,7	279,7	47,5%	226,9	-18,9%	186,7	-17,7%	207,9	11,4%	190,9	-8,2%
	ZAK-4 crypto index	3,4%	4,2%	-	3,4%	-	3,8%	-	3,6%	-	2,9%	-
	4 crypto dominance, %	71,9%	66,1%	-	68,5%	-	72,4%	-	74,8%	-	75,2%	-
8	Volume (24h) 8 crypto, USD billion**	7,2	16,0	121,3%	9,2	-42,4%	8,2	-10,5%	8,7	5,2%	6,4	-25,9%
	Market cap 8 crypto, USD billion	208,7	319,5	53,1%	255,9	-19,9%	205,9	-19,5%	228,2	10,8%	209,3	-8,3%
	ZAK-8 crypto index	3,5%	5,0%	-	3,6%	-	4,0%	-	3,8%	-	3,1%	-
	8 crypto dominance, %	79,1%	75,5%	-	77,2%	-	79,9%	-	82,1%	-	82,5%	-

ПОРЯДОК СКАЧУВАННЯ ТА УСТАНОВКИ ГАМАНЦЯ ДЛЯ КРИПТОВАЛЮТИ MONERO

Якщо ви хочете скачати гаманець, то ваші дії наступні:

1. Перейти за посиланням <https://getmonero.org/> на офіційний сайт і зайти в розділ Завантажень;



Додаток 3 продовження


2. Ви побачите великий перелік варіантів для завантаження, залежно від типу і характеристик встановленої операційної системи на ПК або мобільному пристрої;

Загрузки

Если вам нужна помощь в выборе правильного приложения, нажмите [здесь](#), чтобы получить быстрый ответ, а затем выберите соответствующий выпуск для вашей операционной системы ниже.

Примечание. Хэши SHA256 перечислены в загружаемых файлах для удобства, но список хэшей, подписанных GPG, находится в файле getmonero.org/downloads/ashes.txt и должен рассматриваться как канонический, при этом подпись проверяется соответствующим ключом GPG в исходный код (в / utils / gpg_keys).

[Windows](#)
[макинтош](#)
[Linux](#)
[Рука \(v7 & 8\)](#)
[Источник и блокировка](#)
[Мобильные и светлые аппаратные средства](#)



Windows, 64-разрядная

Windows, 64-разрядная

Текущая версия: 0.13.0.4 Beryllium Bullet

SHA256 Хэш (GUI):


ff1b1467dc6252462e5e7818485857ad2ee253712670ff7f5716aa57241577c7

Windows, только 64-разрядные средства командной строки

Текущая версия: 0.13.0.4 Beryllium Bullet

SHA256 Hash (CLI):

d809acd1ed688a4567716cf199c75b51e696a022e6953df3642a8922a48a734a



Windows, 32-разрядная

Windows, 32-разрядная

Текущая версия: 0.13.0.4 Beryllium Bullet

SHA256 Хэш (GUI):


50feee5c42c7342140a7e5c95a88d330262bebf3b844817e4d9e4be86787795b

Windows, только 32-разрядные средства командной строки

Текущая версия: 0.13.0.4 Beryllium Bullet

SHA256 Hash (CLI):

f2034f3dc125097c3ae50dff5b0a46798863fab60da8e4f35e4cb8d7d2202741



Mac OS X, 64-разрядная версия

Mac OS X, 64-разрядная версия

Текущая версия: 0.13.0.4 Beryllium Bullet

SHA256 Хэш (GUI):

c425f1b984cf00ffd1a9f1322e5da876aa07c106e975ca9fe08ee0a2d2956335

Mac OS X, только 64-разрядные средства командной строки

Текущая версия: 0.13.0.4 Beryllium Bullet

SHA256 Hash (CLI):

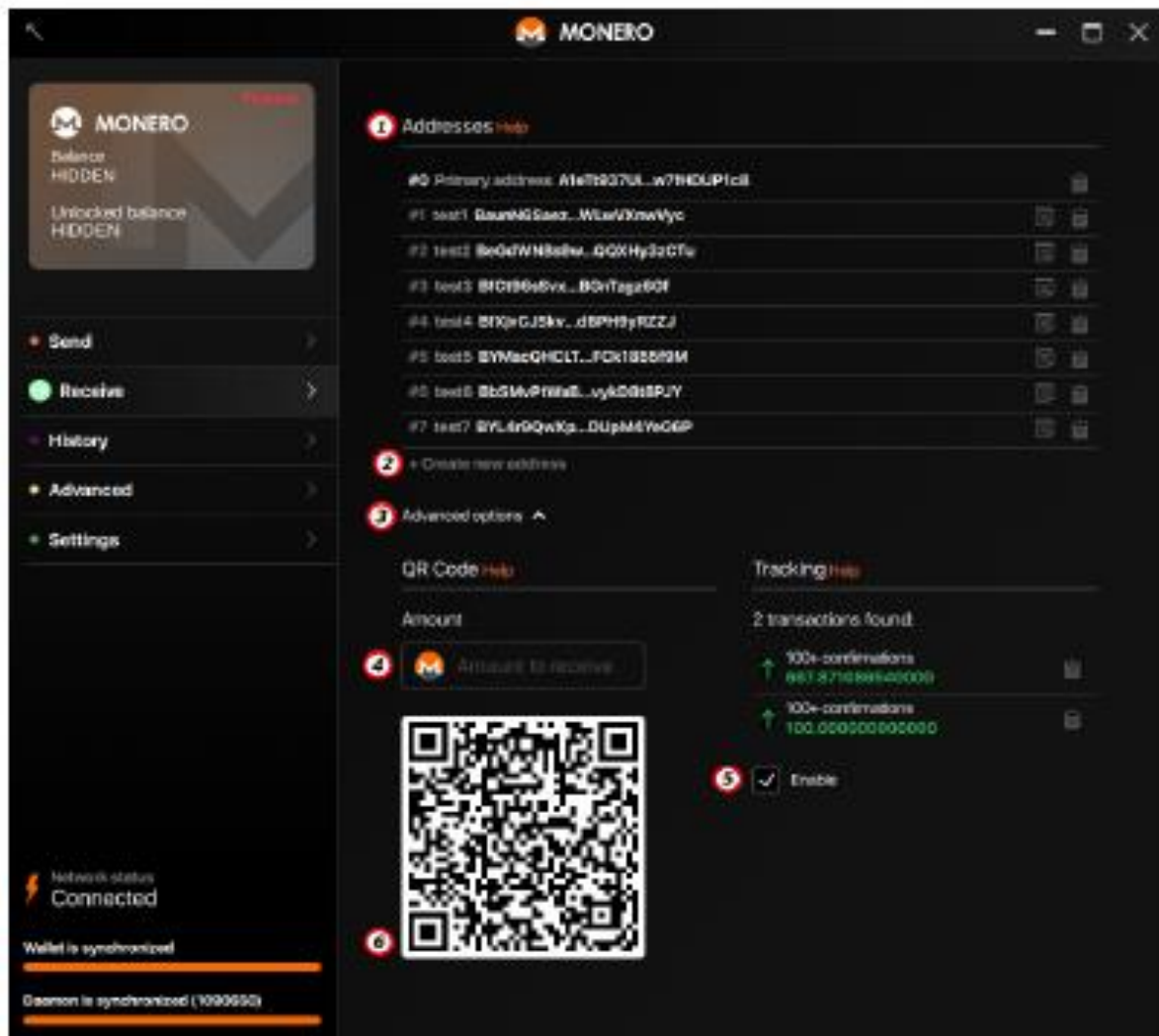
dd859659bf46a11f4bb2de5bddca7c19038758024e32eb7979bc6bf29ef72e56

Додаток 3 продовження

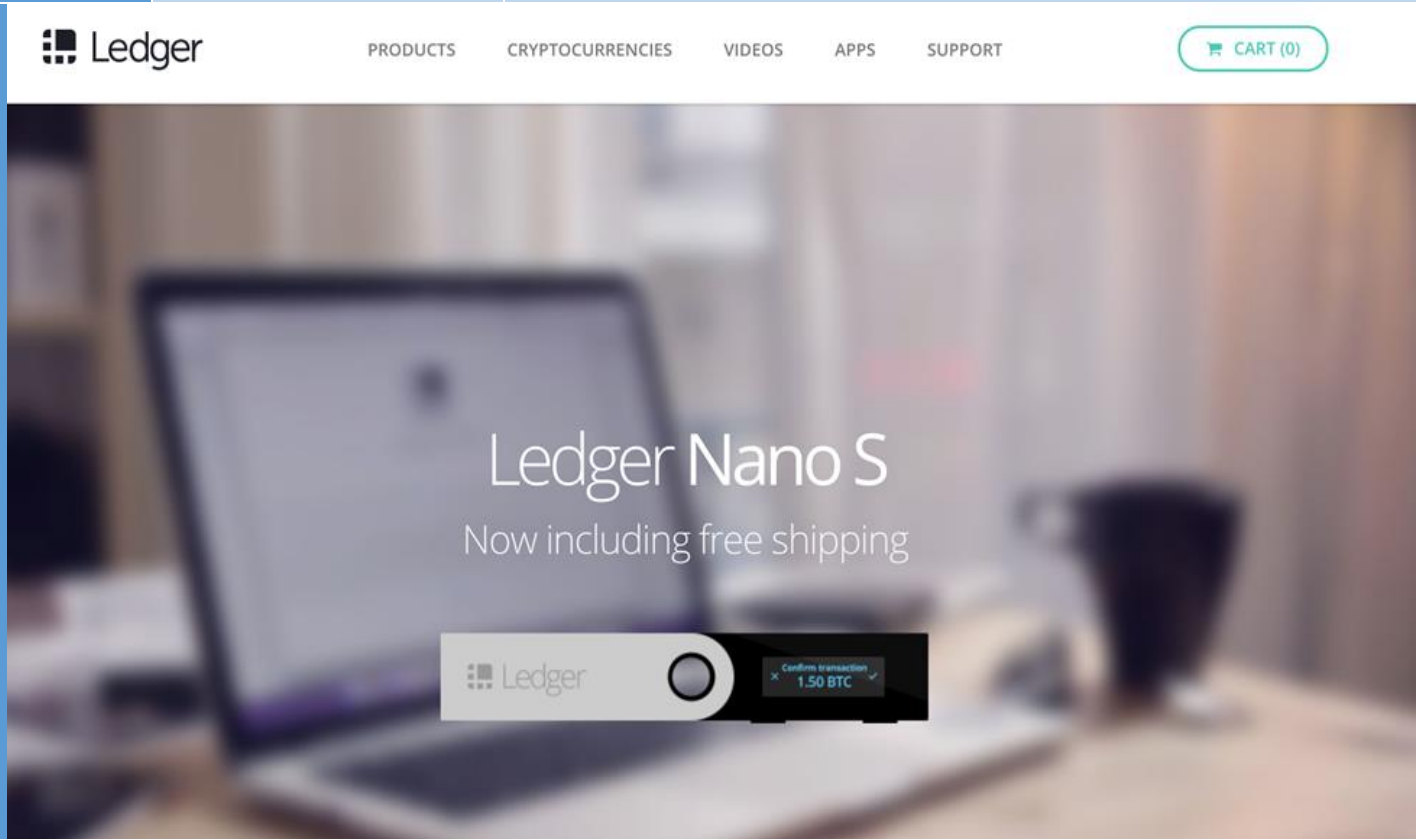
3. Ви вибираєте один з варіантів і чекаєте, поки завантажувється інсталяційний архів з файлами.

Установка гаманця Monero відбувається наступним чином:

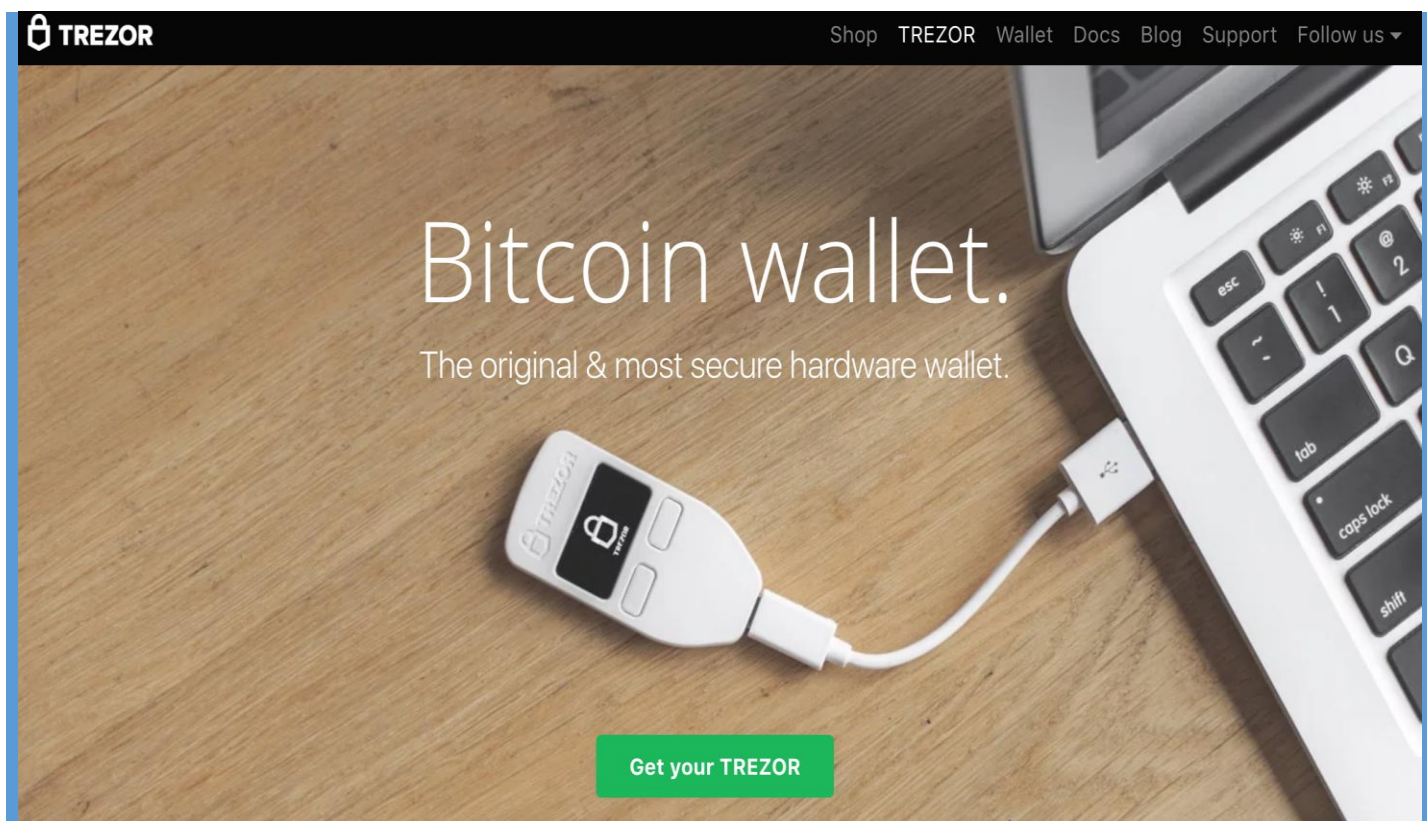
1. завантажити інсталяційний архів і відкрити його;
2. слідувати всім командам, які з'являтимуться на екрані;
3. чекаєте завершення процесу інсталяції.



НАЙПОПУЛЯРНІШІ АПАРАТНІ КРИПТОВАЛЮТНІ ГАМАНЦІ

№ п/п	назва	Підтримувані криптовалюти
1	Ledger	ARK, Sealthcoin, Stratis, PIVX, Ubiq, Expense, Posw, Vertcoin, Dogecoin, Dash Qtum, Viacoin, Komodo, NEO.
		
<p>Особливості:</p> <ul style="list-style-type: none"> ❖ Заводський ключик. ❖ Принцип криптографії, створений для банківського пластику (EAL5 +). ❖ Багаторівневу систему підтвердження операції. ❖ Спеціально розроблену ОС під Ledger з набагато більш просунутим принципом охорони, ніж класичні. 		
2	Trezor	Bitcoin (BTC), Ripple (XRP), Ethereum (ETH), Bitcoin Cash (BCH), Stellar (XLM), EOS (EOS), Litecoin (LTC), Tether (USDT), Cardano (ADA), Monero (XMR), Tron (TRX), Dash (DASH), NEM (XEM), Ethereum Classic (ETC), Zcash (ZEC), Tezos (XTZ), Bitcoin Gold (BTG)

Додаток 4 продовження



Особливості:

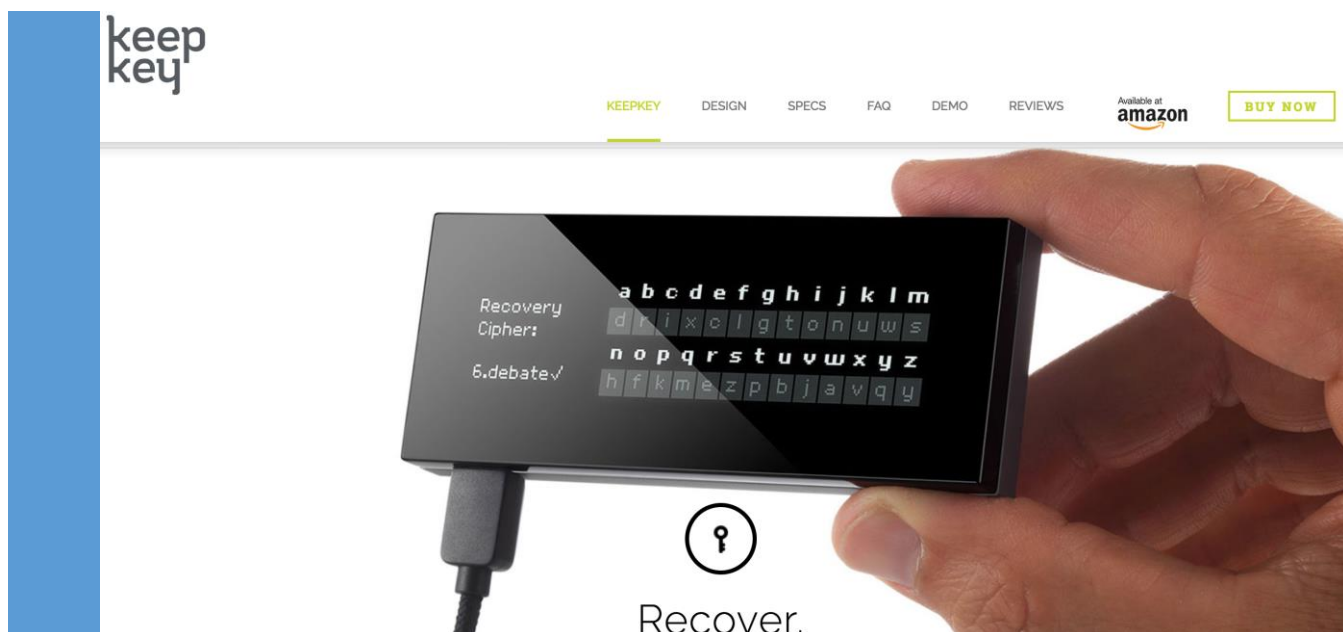
- ❖ Високого рівня захист криптовалюти паролем.
- ❖ Багаторівневе підтвердження дій. Унікальне програмне забезпечення дозволяє підписувати транзакції і здійснювати інші маніпуляції з рахунком оффлан.
- ❖ Може працювати зі сторонніми сервісами і зберігати різні валюти різні валюти. Навіть якщо втратили пароль до портмоне передбачена функція відновлення доступу.

3

Keep Key

Bitcoin, Bitcoin Cash, Bitcoin Gold, Dash, Doge, Ethereum, Litecoin, OxBitcoin, Ox, Aelf, Aeternity, Aragon, Augur, Basic Attention Token, Bancor, Binance, Civic, CyberMiles, Crypto.com, Dai, Decentraland, DigixDAO, District0x, Edgeless, FirstBlood, FunFair, Gifto, Gnosis, Golem, ICONOMI, iExec, IOST, Maker, Matchpool, Melon, Metal

Додаток 4 продовження



Recover.

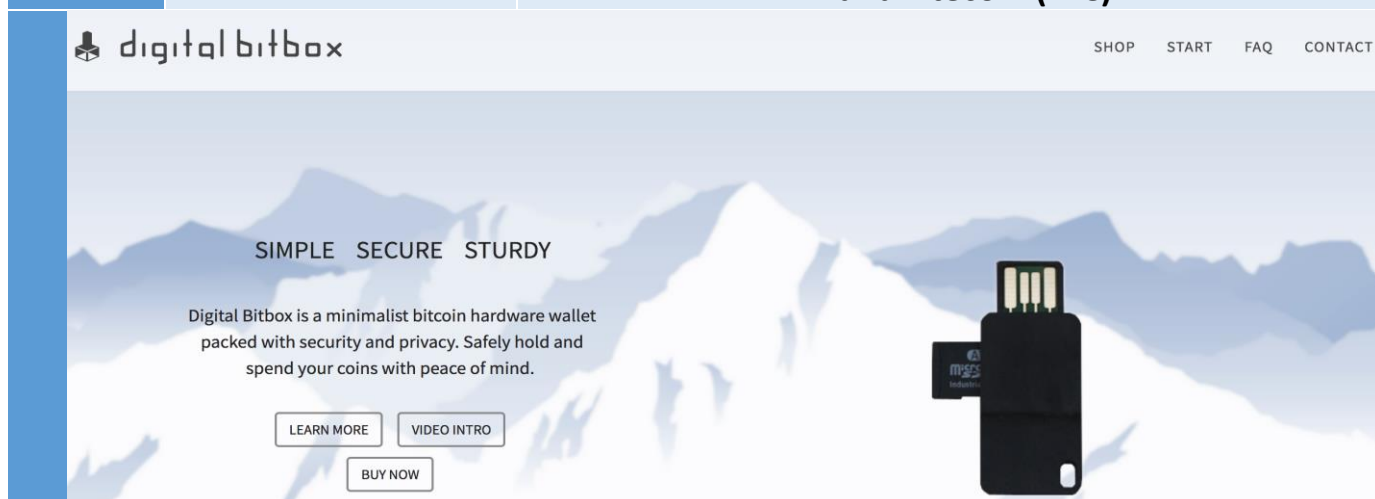
Особливості:

- ❖ Кеер Кієй виграє з естетичної точки зору, а також може похвалитися корисною особливістю – повідомляє власники, якщо була спроба поставити сторонню прошивку.

4

Digital Bitbox

Bitcoin (BTC), Ethereum (ETH, ETC, and ERC20 tokens), and Litecoin (LTC).



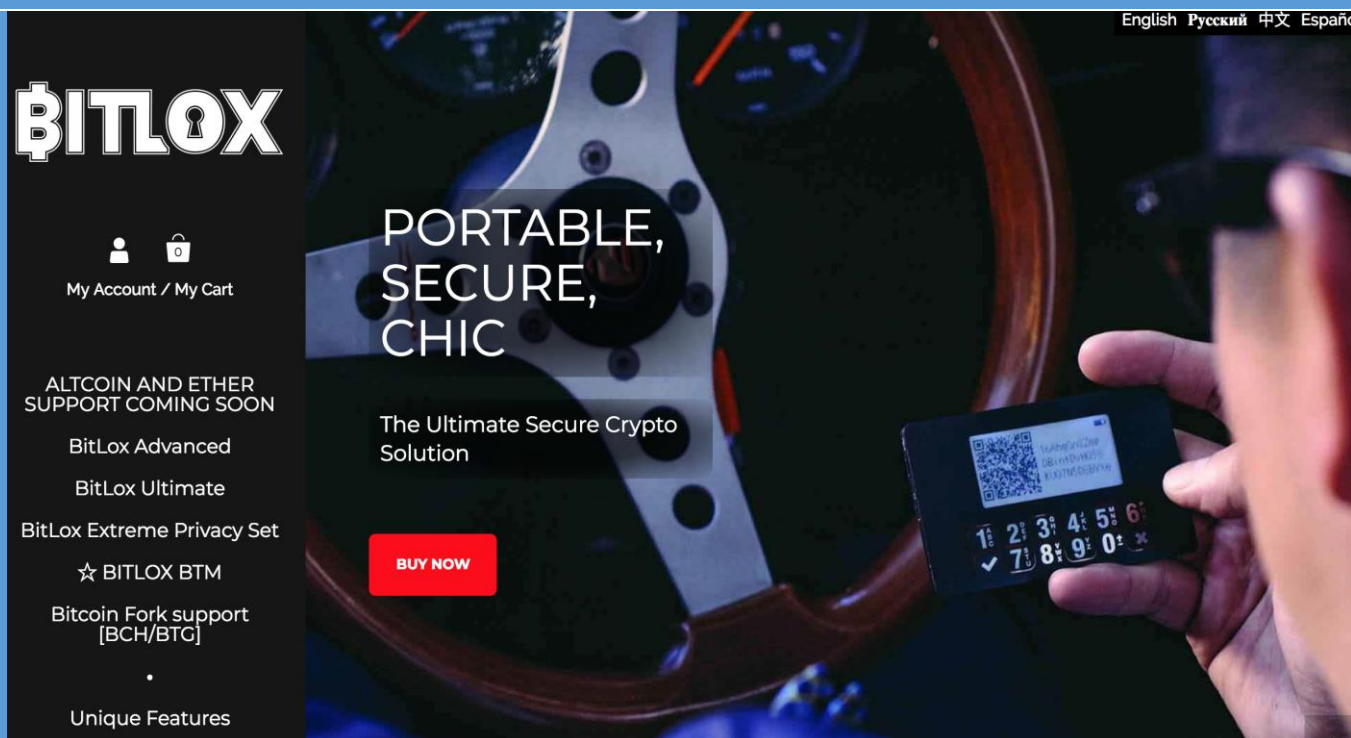
Особливості:

- ❖ Підтримує систему Tails, що забезпечує захист і конфіденційність.
- ❖ Також анонімність гарантує ПО Tor.
- ❖ Ключі зберігаються на чіпі захищеному від фізичного пошкодження і хакерського злому (військових технологій)
- ❖ При втраті ключа його можна відновити завдяки microSD де зберігається його копія.

Додаток 4 продовження

5

Bitlox

Bitcoin, Litecoin, Dogecoin;, Namecoin;, Testnet;, Ethereum;, Dash.

Особливості:

- ❖ Його товщина 4 мм і він запросто поміститься в кишені класичного портмоне. Також оснащений кнопковим набором та екраном, здатним відображати QR коди, а для більшої безпеки запитує пін-кодів кілька.

6

BitStash

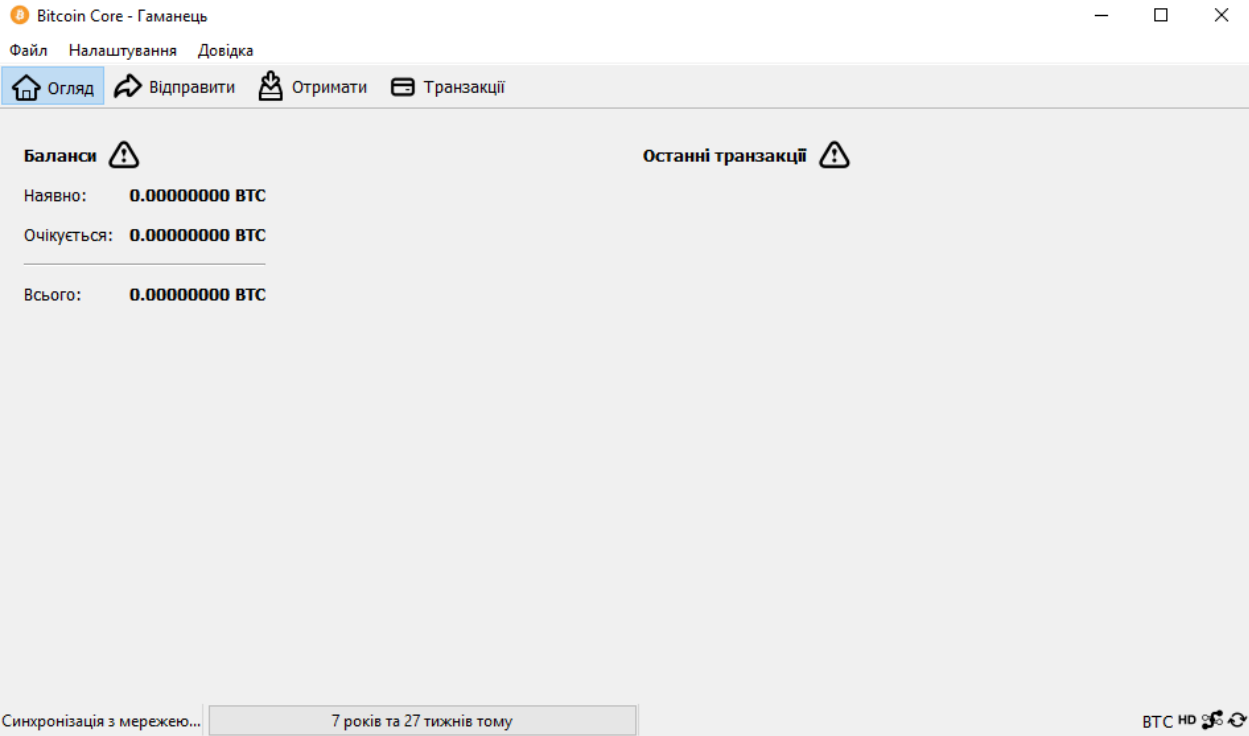
Ethereum



Особливості:

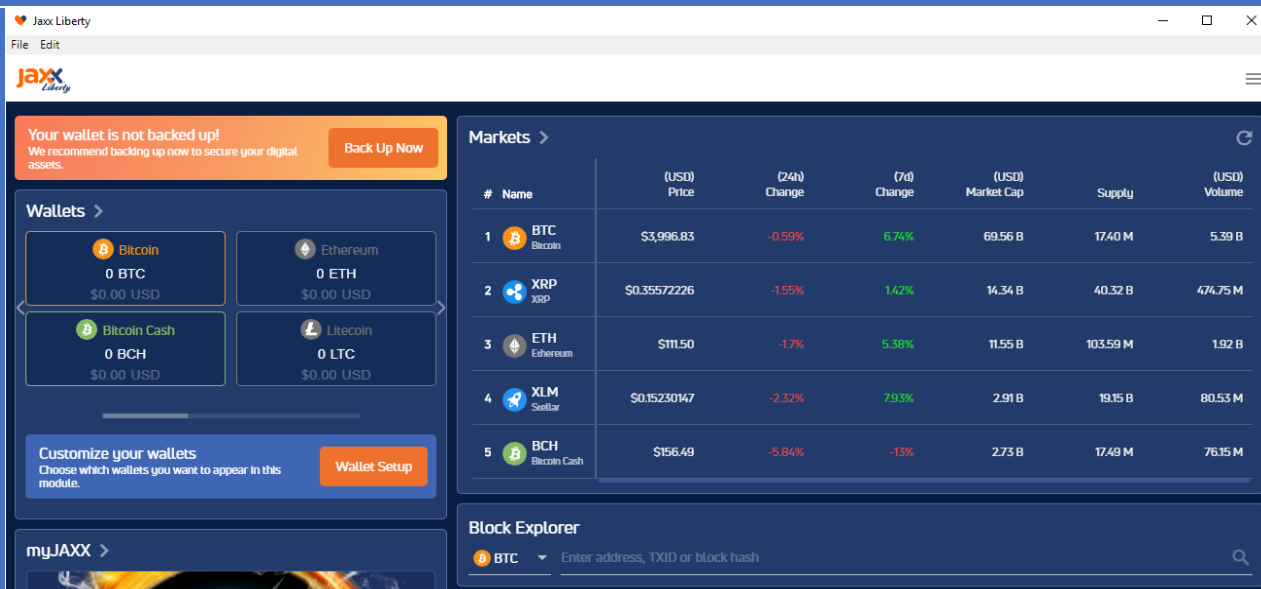
- ❖ Щоб схвалити транзакцію застосовується потрійний підхід кольорова і текстова капчи, а також PIN-код.
- ❖ Навіть на відстань в нього можна стерти всю інформацію.

ДЕСКТОПНІ КРИТОВАЛЮТНІ ГАМАНЦІ

№ п/п	назва	Підтримуванні криптовалюти
1.	BitcoinCore	Bitcoin(BTC)
		
	<p>Особливості:</p> <ul style="list-style-type: none"> ➤ генерують пари публічних (біткоїн адрес) приватний ключ та/або seed фрази; ➤ віддають секретні дані власнику та дозволяють робити резервні зашифровані копії файлу з секретними даними; ➤ показують баланс на біткоїн рахунках; ➤ формують рахунки для прийому біткоїнів та транзакції для передачі біткоїнів ➤ формують рахунки для прийому біткоїнів та транзакції для передачі біткоїнів; ➤ створення цифрового підпису текстового повідомлення приватним ключем від обраної біткоїн адреси; ➤ дозволяють імпортувати біткоїн адреси холодних гаманців. 	

Додаток 5 продовження

2. Jaxx Bitcoin, BitcoinCash, Ethereum, Golem, EthereumClassic, Litecoin, Zcash, Dash, Eos, Dao, Bancor, Augur, Testnet, Iconomi, BlockchainCapital, Quantum.



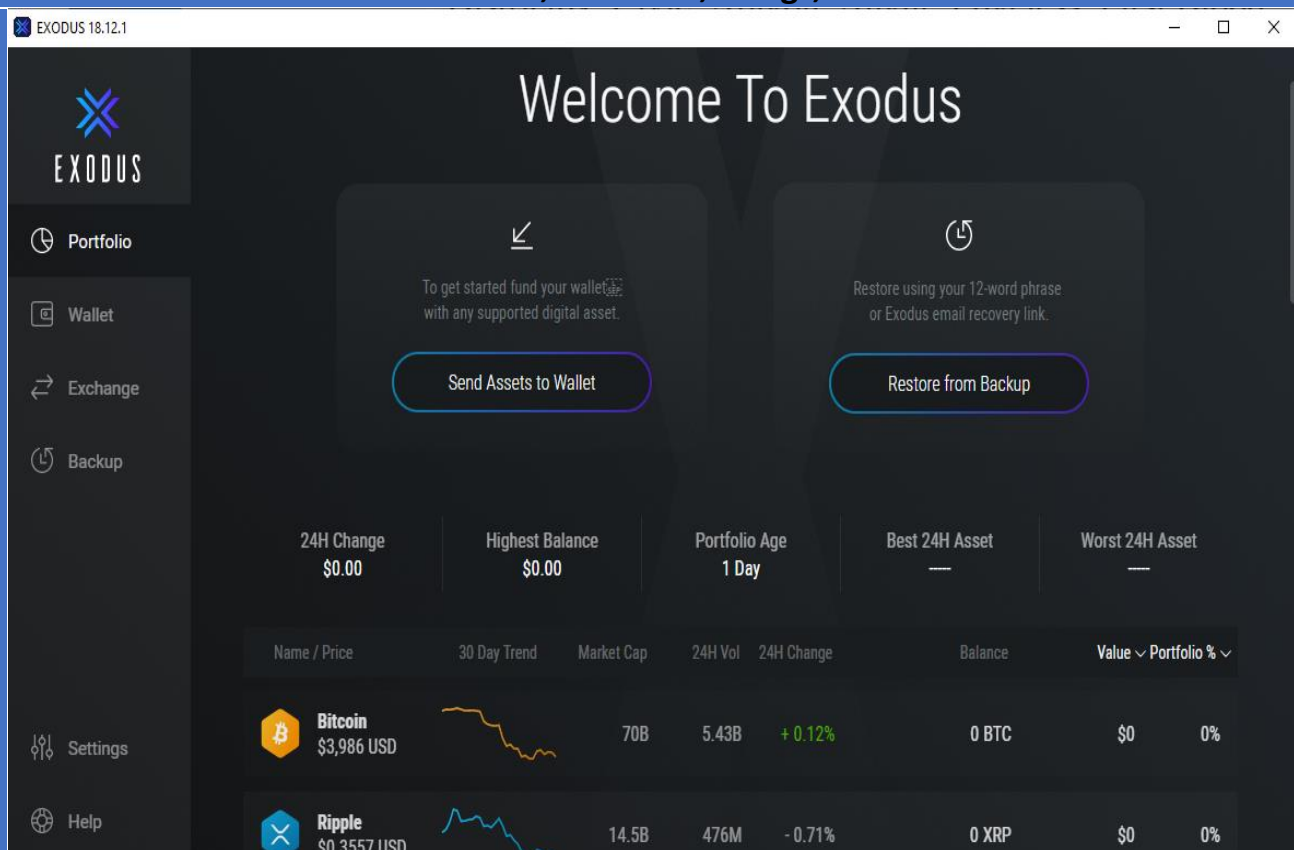
Особливості:

- Безпека зберігання даних. Приватний ключі і коди зберігаються не на центральних серверах, до яких в теорії будь-хто може отримати доступ, а на стороні користувача, тобто на його особистому комп'ютері (смартфоні, планшеті) в програмних файлах встановленого Jaxx.
- Додатковий захист. Jaxx пропонує користувачеві встановити PIN-код на гаманець. Його потрібно вводити кожен раз в момент входу і в інших випадках, коли мова йде про доступ до секретних даних.
- Відновлення доступу за допомогою мнемо-фрази з 12 слів. Фраза генерується при створенні гаманця і дозволяє в разі втрати ключа відновити доступ до грошей.
- Можливість створення резервної копії. Стандартний елемент системи безпеки, що дозволяє створювати резервні копії гаманця для запису, наприклад, на флешку.
- Можливість використовувати Jaxx на різних пристроях. Користувач може об'єднати Jaxx, наприклад, на комп'ютері і на смартфоні. Дані синхронізуються.
- Відкритий код. Jaxx позиціонується як opensource-проект, а це значить, що будь-який бажаючий може побачити програмний код гаманця і переконатися в його надійності.

Додаток 5 продовження

3 Exodus

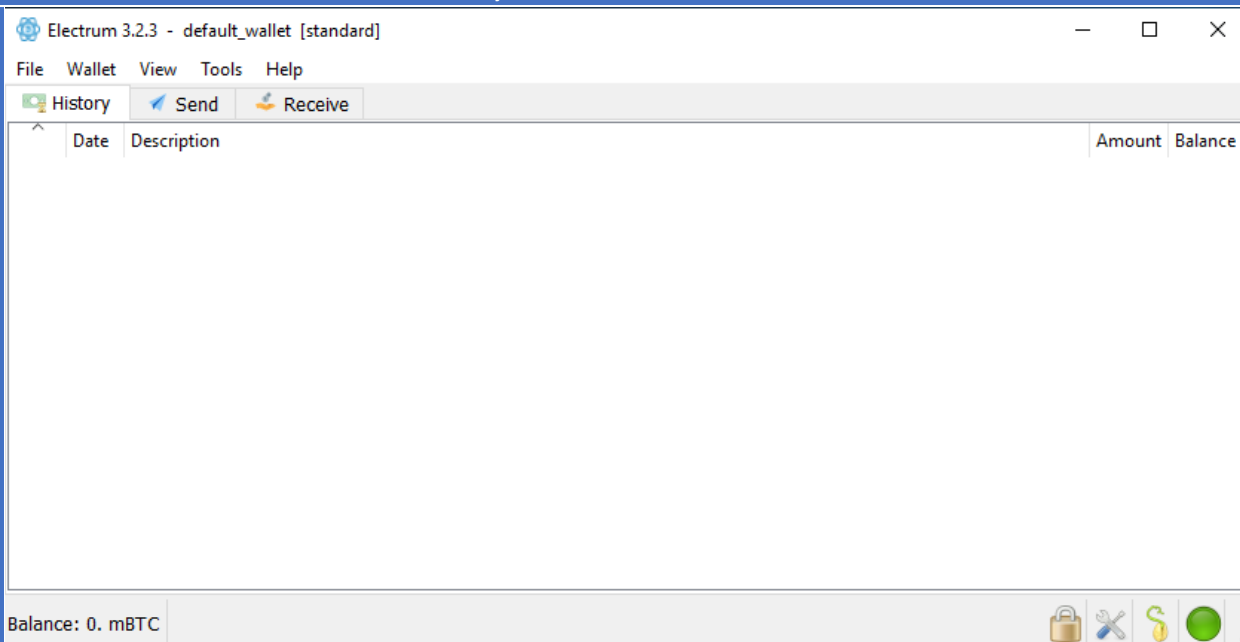
Bitcoin и Bitcoin Cash, Ethereum и Ethereum Classic, Litecoin, Dash, EOS, Bitcoin Gold, Bancor, BAT, Gnosis, Decred, Golem, MatchPool, Salt, 0X, District0x, Civic, Aragon, Augur, Edgeless, First Blood, Fun Fair, Status, iExecRLC, We Trust, Wings, Numeraire и OmiseGo.



Особливості:

- Простота і зручність. Щоб освоїти Exodus, потрібно всього кілька хвилин;
- Гаманець може зберігати не тільки біткойни, але і більше 15 інших монет;
- Інтеграція з біржею ShapeShift дозволяє обмінювати монети прямо в інтерфейсі гаманця;
- Доступні версії програми для Windows, Mac і Linux;
- Прекрасний дизайн, який нікого не залишить байдужим.

4 Electrum Bitcoin, Dash

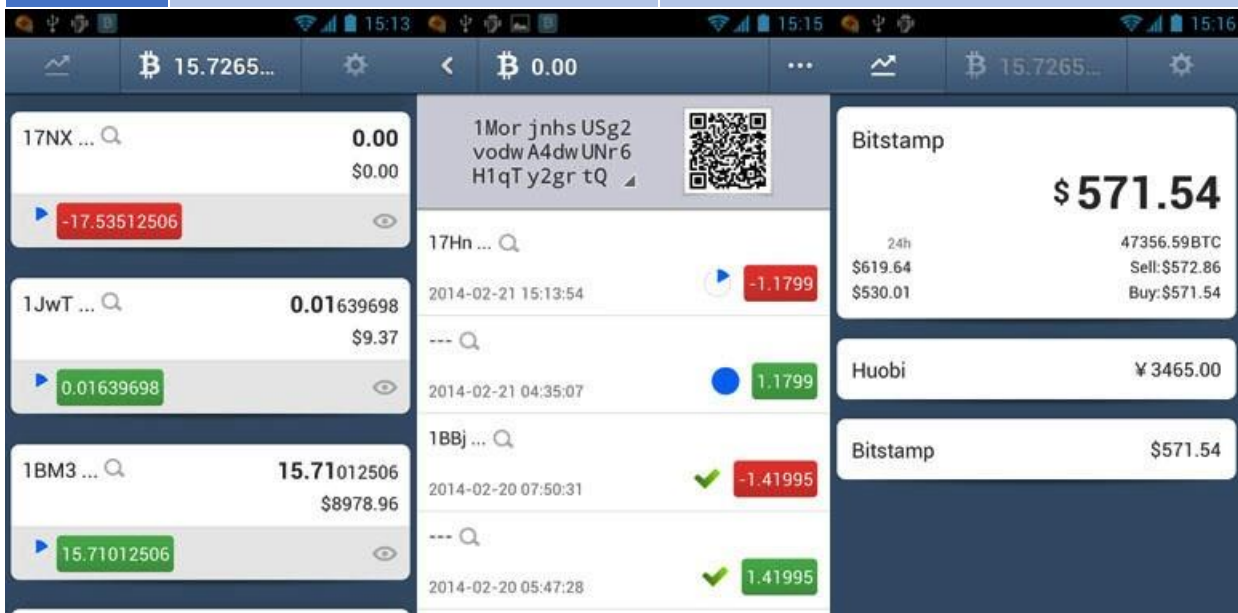


Особливості:

- Це швидкий та легкий у використанні гаманець, що не потребує багато ресурсів. Він використовує віддалені сервери, що опрацьовують найскладніші операції біткоїн-системи. Він також дозволяє вам відновити гаманець за допомогою секретної фрази.

МОБІЛЬНІ КРИПТОВАЛЮТНІ ГАМАНЦІ

№ п/п	назва	Підтримувані криптовалюти
1.	Bither	Bitcoin(BTC)



The screenshot displays the Bither mobile application interface. At the top, there's a status bar with the time 15:13 and various icons. Below it, a navigation bar shows the Bitcoin price at 15.7265... and a balance of 0.00 BTC. The main screen is divided into three sections. The left section shows a list of transactions with details like '17NX ...', '1JwT ...', and '1BM3 ...', along with their respective values and timestamps. The middle section displays a QR code for a transaction and a list of transactions with their details. The right section shows exchange rates for Bitcoin on various platforms, including Bitstamp, Huobi, and Bitstamp, with prices like \$571.54 and ¥3465.00.

Особливості:

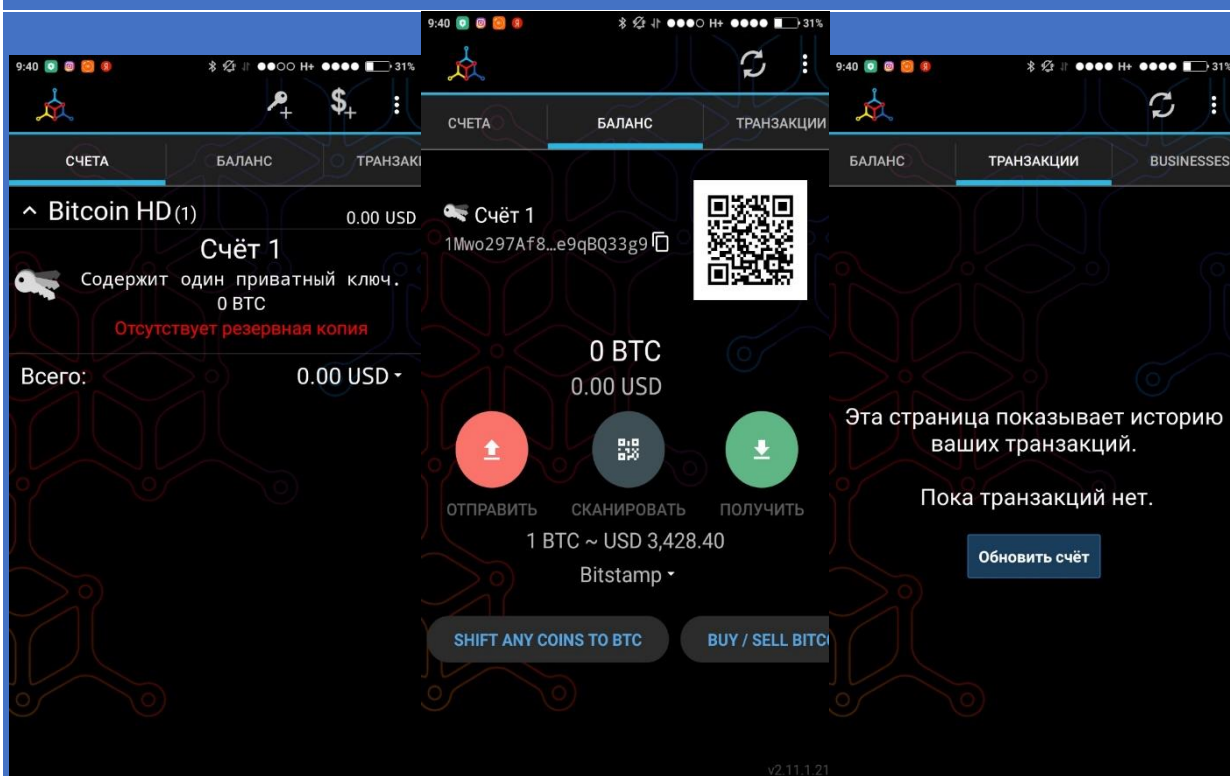
- ❖ Можливість контролю власних коштів - зберігання криптовалюта здійснюється при повному контролі коштів власником. Ніхто крім вас не зможе заморозити ваші гроші або здійснити операції з ними. Однак ніколи не забувайте про організацію належного рівня безпеки та про резервне копіювання;

- ❖ Процедура спрощеної перевірки - в програмному забезпеченні гаманця Bither застосовується спрощена процедура перевірки транзакцій прямо в мережі Bitcoin. Це не вимагає надання третім особам надмірної кількості інформації про учасників перекладу, проте рівень безпеки набагато нижче порівняно з іншими програмами, наприклад, Bitcoin Core;

- ❖ Прозорість - вихідний код програми публікується розробниками у відкритому доступі, тобто кожен бажаючий може перевірити цей код. У будь-якому випадку, щоб встановити гаманець Bither, необхідно довірити розробникам додатку свої персоналізовані дані, що також потрібно при оновленні версії програми - створення вихідного коду відбувається за іншою схемою, відмінною від фіксованої процедури Bitcoin Core.

2. Mycelium

Ontology, Bitcoin Gold, Ripple

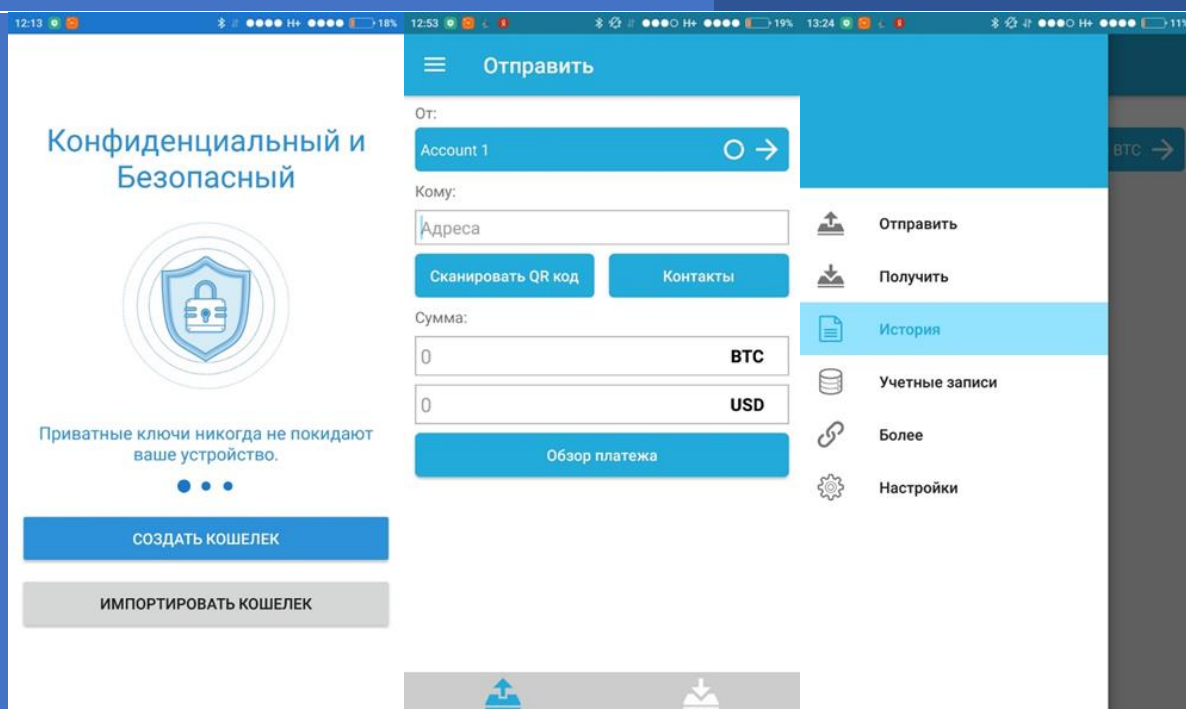


Особливості:

- ❖ Повний контроль над приватними ключами з боку користувача;
- ❖ Підключення до блокчейн через спеціальні суперноди;
- ❖ Інтеграція з популярними сервісами (Trezor, Ledger, Cashila, Coinapult);
- ❖ Відкритий вихідний код;
- ❖ Ієрархічні детерміновані адреси;
- ❖ Мультивалютне відображення балансу.

3. ArcBit

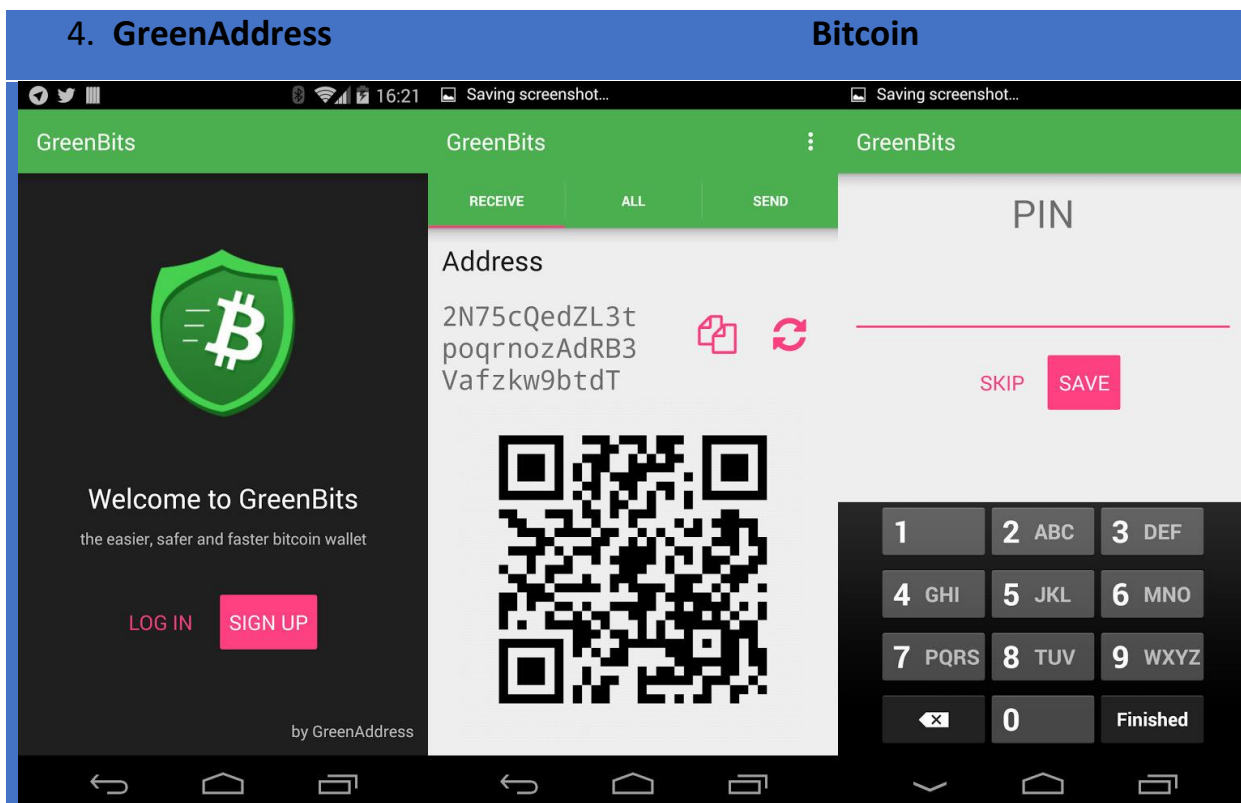
Ripple, Quark, NXT, Namecoin



Особливості:

- ❖ Простий інтерфейс.
- ❖ Можливість інтеграції з Tor для виключення відстеження.
- ❖ Функція динамічної комісії.
- ❖ Наявність базового функціоналу (відправка прийом, сканери і т.д.)

Додаток 6 продовження



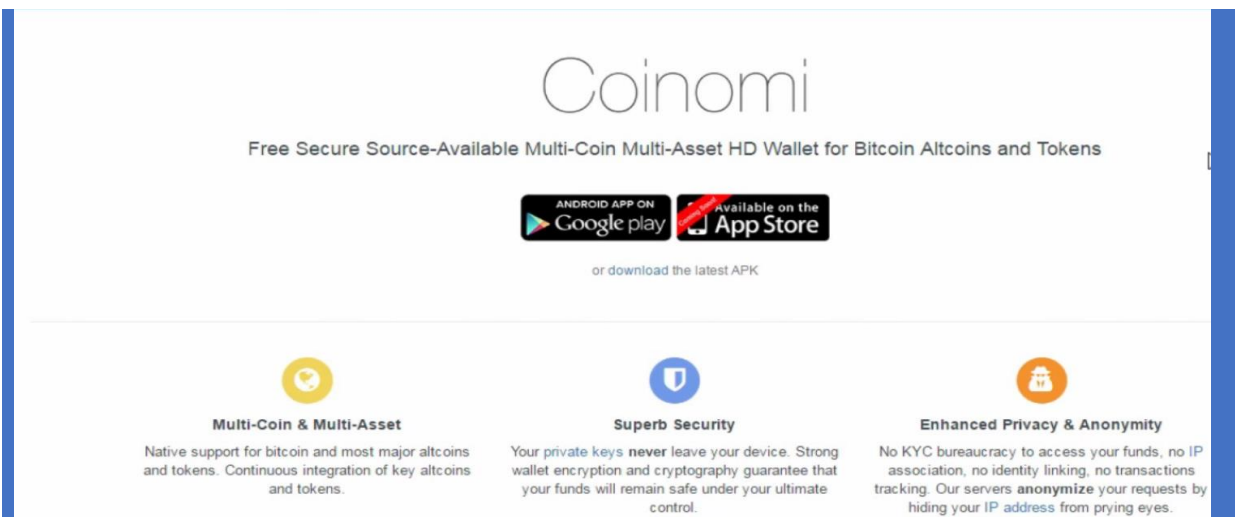
Особливості:

- ❖ Неперевершена ступінь захисту гаманця, включаючи 4 різні дворівневі аутентифікації.
- ❖ Адреса постійного платежу, який можна розмістити публічно
- ❖ Відкритий вихідний код.

ОНЛАЙН КРИПТОВАЛЮТНІ ГАМАНЦІ

№ п/п	назва	Підтримувані криптовалюти
1.	Криптонатор (Cryptonator)	Bitcoin BTC, Bitcoin Cash BCH, Dash DASH, Ethereum ETH, Litecoin LTC, Monero XMR. Ripple XRP. Zcash ZEC
<div> <div> <h2>Удобный криптовалютный кошелек</h2> <p>Получайте, отправляйте и обменивайте Биткоин и другие криптовалюты. Быстро, удобно, безопасно. Доступ к персональному счету доступен круглосуточно, из любой точки планеты, как с компьютера, так и со смартфона.</p> </div> <div>  </div> </div>		
<p>Особливості:</p> <ul style="list-style-type: none"> ❖ Мультивалютність. ❖ Швидкий обмін без комісії між гаманцями ❖ Возможность настройки интерфейса кошелька. ❖ Захист двухфакторной аутентификацией і можливість підключення довірених IP. ❖ Російськомовний інтерфейс ❖ Робота з ЯД і банківськими картами ❖ Великий і докладний довідковий центр 		
2.	Coinomi	Bitcoin, Ethereum, Litecoin, Ethereum Classic, Bitcoin Cash и Bitcoin Gold, Dash, Stratis, Tether, ZCash; Dogecoin, Litecoin Cash, Novacoin, Bitcore, Credo, Dentacoin,

Додаток 7 продовження



Особливості:

❖ **Конфіденційність.** На стороні розробника застосовується система шифрування, яка «перемішує» IP-адреси і адреси гаманців відправників і одержувачів. У сукупності зі створенням десятків адрес для кожного користувача це практично не залишає можливості його ідентифікувати ні в криптовалютній мережі, ні в загальній мережі, де ідентифікатором є IP.

❖ **Безпека.** Як запевняють розробники, всі ключі і паролі генеруються і зберігаються на стороні користувача. При зломі мережі Coinomi, якщо він раптом станеться, це не дозволить шахраям отримати доступ до гаманців і засобів на них.

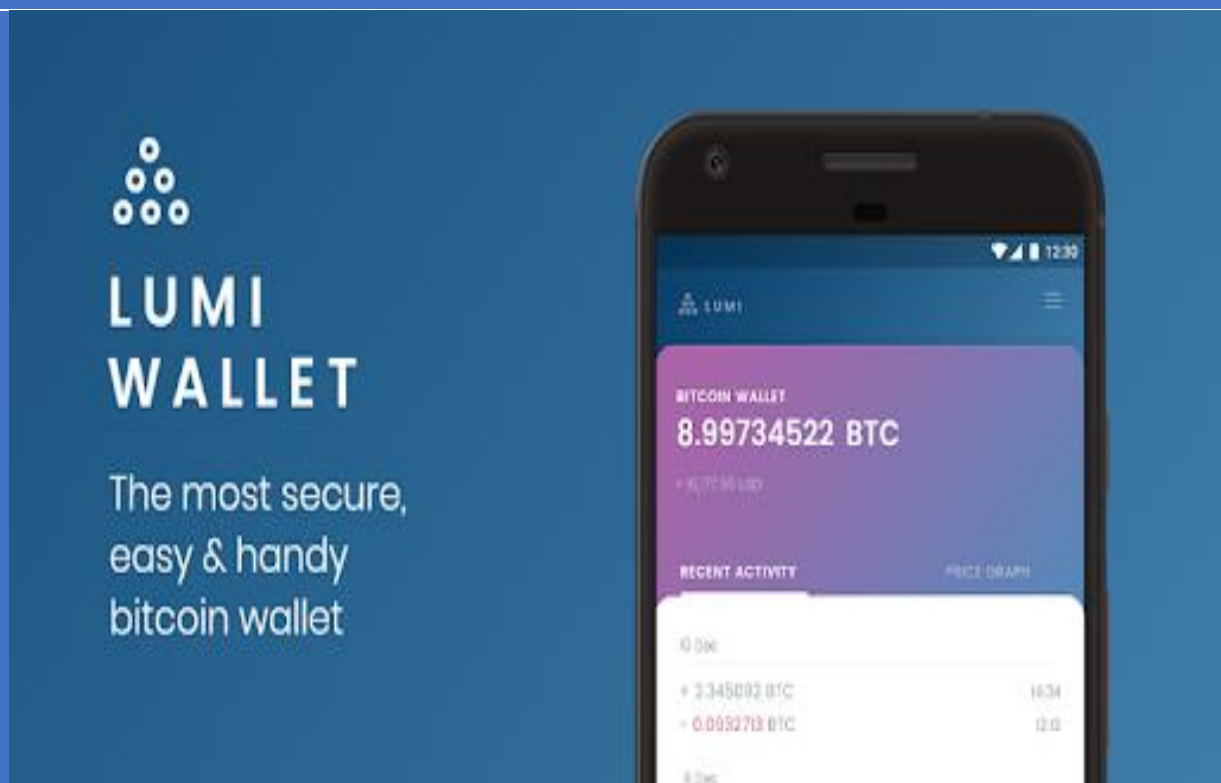
❖ **Комісії.** Coinomi пропонує користувачеві оптимальну на момент транзакції комісію, яка розраховується, виходячи з поточної черги в мемпуле. Якщо користувач вважає її завищеною, він має право її змінити і виставити ту, яку готовий заплатити за транзакцію.

❖ **Швидкість обміну валют.** Два сервісу працюють швидше, ніж один: інтеграція ShapeShift і Changelly прискорює проведення обмінних операцій в порівнянні з гаманцями, де встановлений тільки ShapeShift. Обмін проводиться протягом декількох хвилин навіть в дні ажіотажу.

❖ **Coinomi гаманець простий.** У ньому немає додаткових фінансових інструментів типу графіків, введення, виведення та обміну фіатних грошей, він не передбачає можливості посилення захисту за допомогою двофакторної аутентифікації або мультіпідписі транзакцій (відправлення грошей з підтвердженням 2-3 ключами). У нього мінімалістичний дизайн, мінімум налаштувань. Все це робить програму легкою і не вимагає великої кількості оперативної пам'яті, що для мобільного додатка важливо.

*Додаток 7 продовження***3. Lumi**

Bitcoin, Ethereum, Tronix,
Ethibits, Loopring, Populous
VeChain, ICON, Binance,
Network.

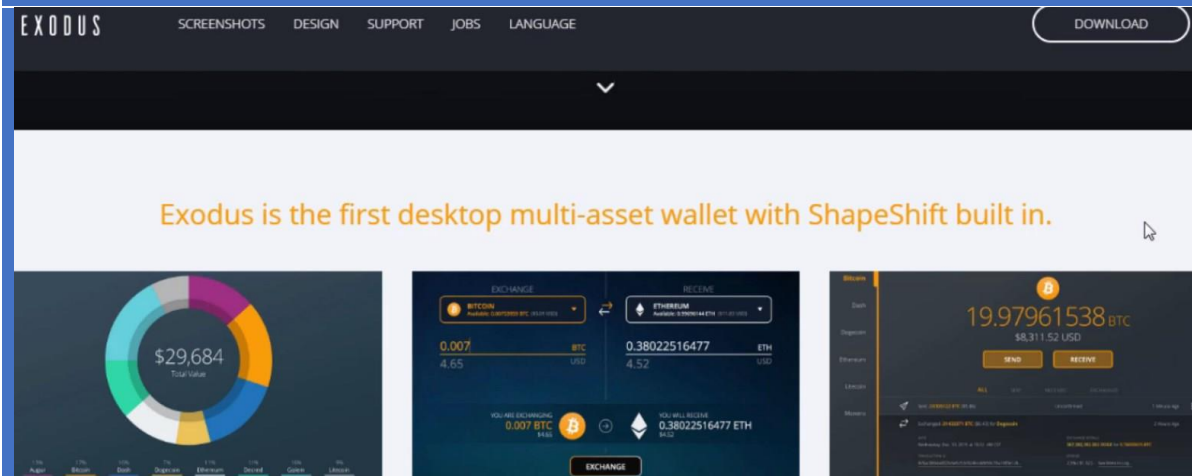
**Особливості:**

- ❖ Lumi - це безпечний, простий у використанні біткоїн-гаманець, який підходить як для нових, так і для просунутих користувачів. Він об'єднує зручний дизайн і функціональність високого класу. Приватні ключі знаходяться під контролем клієнта, вони ніколи не відправляються і не зберігаються за межами вашого пристрою. Немає необхідності надавати особисту інформацію і не потрібна реєстрація. Простота, зручність у використанні і швидкий монтаж роблять додаток простим у використанні. Ви можете відправляти і отримувати біткоіни всього за кілька кліків. У разі втрати пристрою або будь-яких інших обставин ваш гаманець можна відновити за допомогою 12-річної мнемонічною фрази.

Додаток 7 продовження

4. Exodus

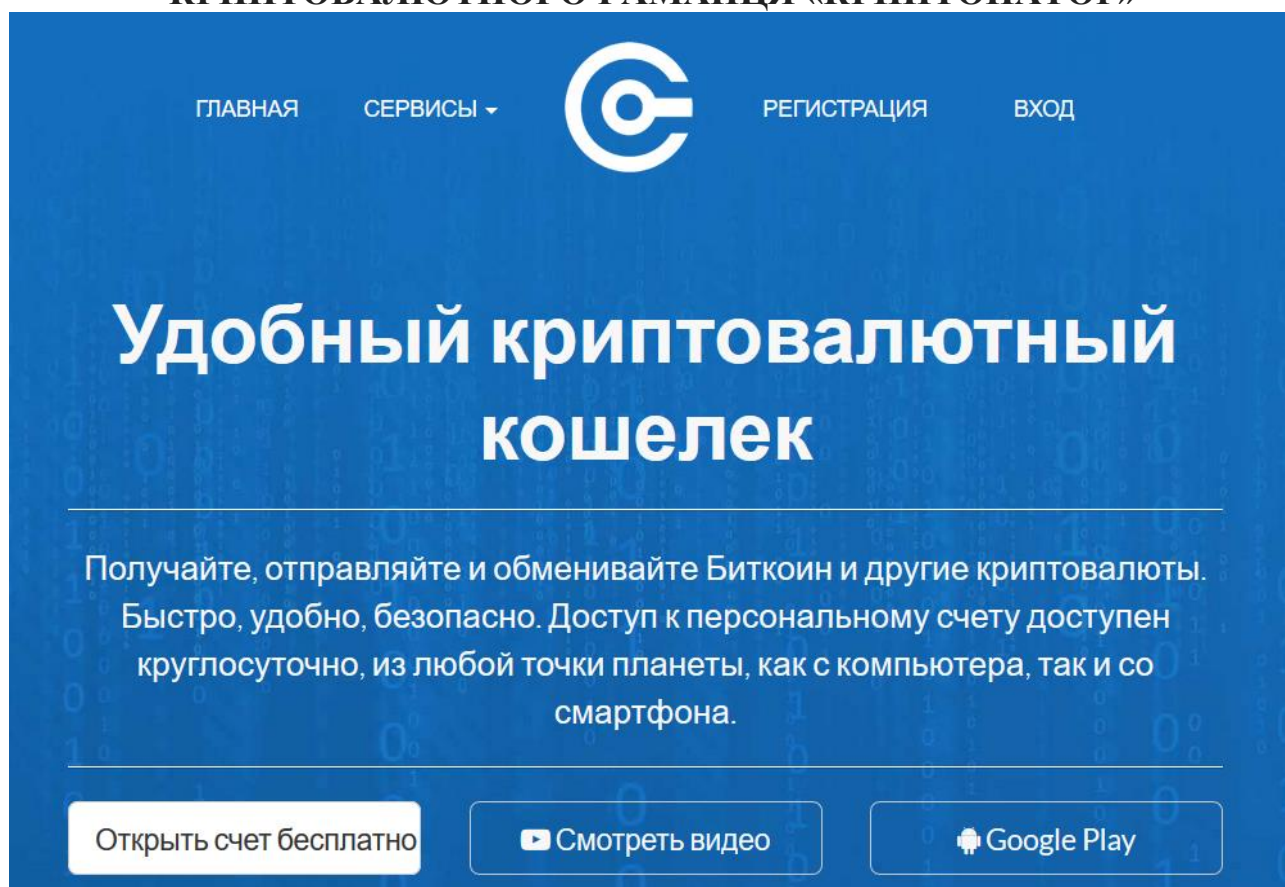
Bitcoin и Bitcoin Cash, Ethereum и Ethereum Classic, Litecoin; Dash, EOS, Bitcoin Gold Bancor, BAT, Gnosis.



Особливості:

- ❖ Основна перевага Exodus полягає в тому, що він добре працює. А саме - швидко, без зависань, особливих затримок і помилок переводить і конвертує гроші.
- ❖ Exodus жодного разу не був зламаний. Скарг на зломи окремих гаманців теж мало, що свідчить про хорошу програмної захисту гаманця як з боку розробників, так і з користувальницької боку
- ❖ Техпідтримка Exodus відрізняється професійністю і оперативністю. Проблеми окремих користувачів вирішуються найчастіше за день або кілька днів, в залежності від складності. Взагалі, індивідуальні проблеми виникають рідко і найчастіше пов'язані або з тим, що користувач не оновив програму до останньої версії, або (рідше) з несумісністю програми з операційною системою або технічними параметрами комп'ютера.
- ❖ Новачкам допомагають оперативно, є досить інформативний FAQ. Правда, у всього цього є один недолік: інформація - виключно англійською, і спілкуватися з фахівцями теж доведеться англійською.
- ❖ Дизайн - окрема гордість Exodus. Мало які гаманці можуть похвалитися наявністю серед розробників такого дизайнера, як Кастальоні, і Exodus по праву вважається гаманцем для користувачів, яким важлива естетика. «Родзинка» цього проекту - діаграми, що дають користувачеві уявлення про стан рахунку. Крім того, гаманець пропонує кілька сучасних тем і стилів.

**ПРОЦЕДУРА
РЕЄСТРАЦІЇ ТА ОСОБЛИВОСТІ ВИКОРИСТАННЯ ОНЛАЙН
КРИПТОВАЛЮТНОГО ГАМАНЦЯ «КРИПТОНАТОР»**



Процедура реєстрації

Открыть новый счет

Управляйте криптовалютами с единого счета

Личный счет

Счет для магазина

Email

Пароль

Открыть счет

1. Переходимо в пункт «Реєстрація».
2. Після цього нас перекидає на нову сторінку, де необхідно вказати дані, а саме електронну пошту і пароль.
3. Буде запропонована тест. Ввести її дуже просто.
4. Натискаємо кнопку «Відкрити рахунок».

Додаток 8 продовження

5. Перевірте свою електронну пошту і підтвердить всі дані, а також саму реєстрацію

6. Номер телефону обов'язково вказувати. Ось і ви це зробите, а також підтвердить всі свої дії. Справа в тому, що зайти на платформу без цих відомостей не вдасться.

Выберите какие кошельки следует показывать в разделе БАЛАНС.

Bitcoin	<input type="checkbox"/> ВКЛ <input checked="" type="checkbox"/> ВЫКЛ
Blackcoin	<input type="checkbox"/> ВКЛ <input checked="" type="checkbox"/> ВЫКЛ
Dash	<input type="checkbox"/> ВКЛ <input checked="" type="checkbox"/> ВЫКЛ
Dogecoin	<input checked="" type="checkbox"/> ВКЛ <input type="checkbox"/> ВЫКЛ

Відразу ж варто сказати, що нічого важкого в роботі немає. Інтерфейс і інші функції зрозумілі на інстинктивному рівні, тому їх освоїть буквально кожен.

Після того, як ви пройшли реєстрацію, будете автоматично спрямовані на вкладку «Мій рахунок». Тут вже надається все, що потрібно для роботи. Для цього лише потрібно натиснути.

Вибираємо, наприклад, «Криптовалютный гаманець». Нас направляють на сторінку, де ми маємо можливість створити валлет для підтримуваної крипти. Робиться це дуже просто. Є повзунок навпроти кожної валюти. Переводимо його в положення «Вкл» і готово.

Вищеподані елементи є головними інструментами для заробітку на Криптонатор, шляхом покупки або продажу. У випадку, коли потрібно буде купити що-небудь, достатньо перейти на «Відправити». Тут все просто: вказуємо адресу гаманця інтернет-магазину або окремого користувача. Досконалу транзакцію вже неможливо буде повернути назад, тому будьте максимально уважні.

Присутня ще вкладка «Заплатити». Можна сказати, що вона має той же ресурс, що і «Надіслати», тільки мова йде про рублевий гаманець. Платите за комунальні, інтернет, ігри і т. д. Такий собі онлайн-банкінг на окремій платформі.

Окрему увагу заслуговує вкладка «Історія». Тут можна переглянути всі раніше зроблені операції по ваших рахунках. Є зручний фільтр, а також сортування даних.

Щоб вивести якусь кількість криптовалюти, спочатку потрібно її обміняти на долари або євро, рублі. Сам переклад здійснюється зручним для вас способом. Достатньо лише вибрати із запропонованих.

Додаток 8 продовження

The screenshot shows the main interface of the Cryptonator website. At the top, there is a navigation bar with links: ГЛАВНАЯ, СЕРВИСЫ (with a dropdown arrow), a logo, РЕГИСТРАЦИЯ, and ВХОД. Below the navigation bar, the title 'Калькулятор и конвертер криптовалют' is displayed. The main area features a conversion tool with two dropdown menus: 'ИЗ' (From) set to 'Bitcoin (BTC)' and 'В' (To) set to 'US Dollar (USD)'. Below these is a text input field labeled 'Укажите сумму' (Specify the amount) with a small icon to its right. Underneath the input field is a numeric keypad with buttons for digits 0-9, a decimal point, and a 'del' button.

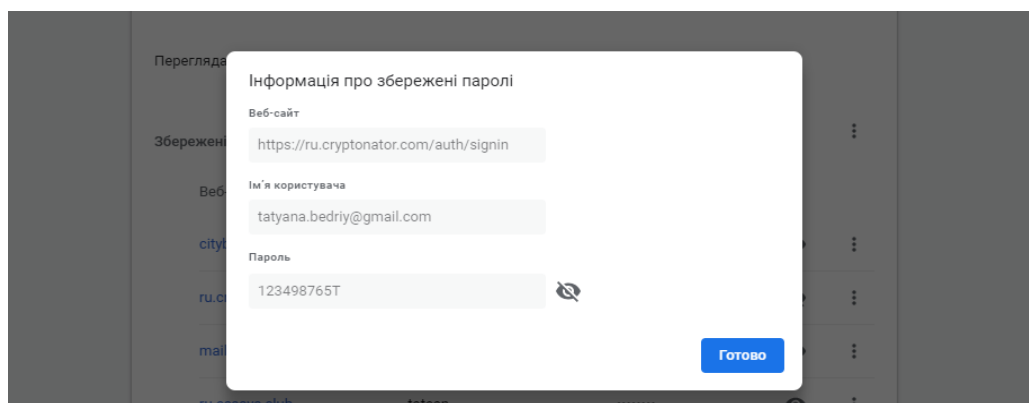
Функції гаманця Криптонатор ще не закінчуються. Що ж він може запропонувати ще:

1. Калькулятор конвертер. Вже з назви стає зрозуміло, що це і як працює. Функціонує дуже просто. Вказуємо крипто-монету, і на що ми будемо її міняти. Всі дані відображаються в режимі реального часу. Дуже зручно і практично.

2. Списки бірж. Унікальна функція, так як дає нам можливість взаємодіяти з різними біржами. Наприклад, хочемо подивитися, на яких біржах можна працювати з Блеккоїном. Користуємося фільтрами.

3. Всі зміни, що пов'язані з курсом крипти. Так, це також можливо. Таким чином, ви будете першим, хто дізнається про різні зміни. До речі, інформація оновлюється кожні 30 секунд, так що затримки мінімальні.

Якщо при реєстрації чи вході до свого криптогаманця ви зберегли Email та Пароль його потім легко можна буде знайти перейшовши до «Налаштувань» та відкрити вкладку паролі



ПЕРЕЛІК САЙТІВ ГЕНЕРАТОРІВ ПАПЕРОВИХ КРИПТОГРАФІЧНИХ ГАМАНЦІВ

1. <https://www.bitaddress.org/>



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet Paper Wallet Bulk Wallet Brain Wallet
Vanity Wallet Split Wallet Wallet Details

Generate New Address
Print

Bitcoin Address



SHARE

1Ju8Wy8VdMXw3bM4wcL9NMEo9r17WcZRpc

Private Key



SECRET

L48bFFVvapxdq9sxxWcrrv2jvJ9NPXtCwEenCMDwCEVMZ58exqKo



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet Paper Wallet Bulk Wallet Brain Wallet
Vanity Wallet Split Wallet Wallet Details

Hide Art? ☐
Addresses to generate:
Generate
Print

BIP38 Encrypt? ☒
Passphrase:
Addresses per page:

Bitcoin Address



Load & Verify

1FjLcZiWEEXxQabMFgy57nwKb9E3VYbXTe

Private Key



Spend

SPRmBuYtYCS4nRkKqstCFU8ZAK\$
3erXoUyWuYdY1szv6mZoyAabJa

Додаток 9 продовження



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet	Paper Wallet	Bulk Wallet	Brain Wallet
Vanity Wallet	Split Wallet	Wallet Details	

Step 1 - Generate your "Step1 Key Pair"

Step 1 Public Key:
 043D42350383A81FE5DF0F6306ED881C8D86F44F14D995513EFB99DC37EAE9EBE82A86
 CDB2A00A3A379DDC12E444C89E470FFD248F8E64BCC8D9B7640F2DB1F33C

Copy and paste the above into the Your-Part-Public-Key field in the Vanity Pool Website.

Step 1 Private Key:
 FAA65E7488EEFD4456781D0FD4C2A950B9024B6A14A1C135A8A8F8129FF70BD5

Copy and paste the above Private Key field into a text file. Ideally save to an encrypted drive. You will need this to retrieve the Bitcoin Private Key once the Pool has found your prefix.

1. <https://walletgenerator.net/>

WalletGenerator.net
 Universal Open Source Client-Side Wallet Generator

Оберіть валюту: Bitcoin

Один гаманець | Паперовий гаманець | Кілька гаманців | Розумний гаманець | Детальніше про гаманець | Пожертвувати

Публічна адреса

 194uN5qnbGQupmaFM9yZHb4uc3pYzUThVq

Приватний ключ (формат імпорту гаманця - WIF)

 5KWhGVQ6MG2Bid8CmNnEL548FnNBs383njr73LiLJHwCA8317Zn

ДЛЯ ПОШИРЕННЯ СЕКРЕТНИЙ (ЗАХОВАТИ)

Крок 0. Дотримуйтесь рекомендацій "Пам'ятки безпеки"

Насамперед завантажте цей сайт з [Github](#), розархівуйте його і безпосередньо з вашого комп'ютера відкрийте файл index.html. Це достатньо просто сховати деякий шкідливий код у 6000+ рядків javascript, щоб поціпити ваш приватний ключ, але ви ж не хочете довідатися, що ваші кошти вкрадено. Контроль версії кода дозволяє набагато простіше перевірити діючу програму. Для забезпечення додаткової безпеки, відключіть доступ до Інтернету під час створення вашого гаманця.

Крок 1. Створіть нову адресу

Оберіть вашу валюту й клацніть на кнопку "Створити нову адресу".

Крок 2. Роздрукуйте паперовий гаманець

Клацніть на закладку "Паперовий гаманець" та роздрукуйте сторінку якнайкращіше. Ніколи не зберігайте сторінку як PDF файл, щоб роздрукувати її згодом, бо файл швидше буде зламаний хакерами ніж клаптик паперу.

Додаток 9 продовження


WalletGenerator.net
 Universal Open Source Client-Side Wallet Generator

Оберіть валюту : Bitcoin

Один гаманець | Паперовий гаманець | Кілька гаманців | Розумний гаманець | Детальніше про гаманець | Пожертвувати

Зашифрувати за допомогою BIP38? ☐ Парольна фраза:
 Randomly generate OR Enter your own WIF private key



Private



Public

- Внести гроші на паперовий гаманець: відправте кошти на публічну адресу.
- Перевірити стан рахунку: введіть публічну адресу гаманця в оглядач блокчейна (для біткойна це blockchain.info).
- НІКОЛИ НІКОМУ НЕ ПОКАЗУЙТЕ ПРИВАТНИЙ КЛЮЧ**, аж поки ви не зберетесь імпортувати кошти з цього гаманця на інший будь-який гаманець.

Кількість : Дата :
 Нотатки :


Підтримати WalletGenerator.net Завантажити (репозиторій на GitHub)



Copyright WalletGenerator.net. Авторські права на JavaScript включено у джерела. Гарантії не надаються.

ОСОБЛИВОСТІ КРИПТОВАЛЮТ

Назва криптовалюти	Алгоритм хешування	Алгоритм консенсуса	Особливості
Bitcoin (BTC) 	SHA-256	PoW	<p>Перша криптовалюта в світі. Обмін на звичайні валюти відбувається анонімно через онлайн-сервіс обміну цифрових валют, інші платіжні системи, обмінні пункти або безпосередньо між зацікавленими сторонами. Повна децентралізація. Ретельно захищений від злому і копіювання за допомогою різних криптографічних (шифрувальних) методів захисту. Не регулюється жодним регулятором. Кількість монет обмежена.</p>
Ethereum (ETN) 	Dagger-Hashimoto	PoW	<p>Це перша платформа, яка дала можливість укладати «розумні контракти» смарт-контракти будь-якої складності та стежити за виконанням умов угоди. У протоколі Ethereum і блокової ланцюга зберігається інформація про стан рахунків, стан всіх програм після транзакції. Використовується для розрахунку між людьми, а також для обміну різними ресурсами і біржовими активами. Перекази здійснюються в лічені секунди в будь-який час доби. Всі транзакції захищені криптографією. Транзакції конфіденційні та анонімні. Інтерес до платформи проявили: Microsoft, IBM., ВТБ и Сбербанк, ЮНІСЭФ. Повністю децентралізована.</p>

Додаток 10 продовження

<p>Ripple (XRP)</p> 	відсутня	RPCA	<p>Має централізацію. Використовується, як більш досконалий варіант міжбанківських переводів. Система має додаткові параметри безпеки і краще захищена від злону, ніж Bitcoin. кожна транзакція може бути звернена в зворотному напрямку. На гаманцях зберігається повна історія транзакцій. Система повністю анонімна — ніякого заповнення декларацій. Кожен користувач системи Ripple має можливість переглянути інформацію за операціями обміну, а також продажу/купівлі криптовалюти, зафіксовану на будь-якому гаманці.</p>
--	----------	------	--

<p>Bitcoin Cash (BCH)</p> 	SHA-256	PoW	<p>Збільшений розмір блоку на відміну від біткоіну, що збільшило швидкість транзакцій і зменшило комісійні та XRP. Діють нові стандарти безпеки: система захищена від атак зі стирання і повторних відтворень, що додатково захистило в мережі транзакції. При переказах вхідне значення транзакції підписується, для підвищення безпеки криптогаманців. На відміну від Bitcoin, в Bitcoin Cash не передбачені миттєві перекази коштів.</p>
<p>EOS</p> 	Використовує платформу Ефіріум	DPoS	<p>Виділяється дуже високою швидкістю транзакцій і низькими комісіями. Ціна міняється на кожному етапі продаж. Відрізняється прогресивною технологією, порівняно з іншими валютами.</p>



Додаток 10 продовження



Litecoin (LTC) 	Scrypt	PoW	Відрізняється більш швидким часом появи блоку в мережі, емісія обмежена 84 млн. монет.
Stellar (XLM) 	відсутня	SCP	Використовується для грошових операцій онлайн. Об'єднує в себе криптовалютну біржу, гаманці та монети. Володіє найбільшою швидкістю транзакцій.
Cardano (ADA) 	Використовує платформу Ефіріум	PoS	Єдиний криптовалютний гаманець, який підтримує ADA і дозволяє здійснювати перекази на адреси інших криптогаманців.
ІОТА 	відсутня	Tangle	Відсутність майнерів в мережі, її вузли самі відправляють і підтверджують транзакції, комісії відсутні. Дозволяє об'єднати у своїй мережі безліч електронних пристроїв для управління та використання їх.

Додаток 10 продовження

TRON (TRX) 	SHA-256	PoS	З самого початку розробники проекту орієнтовані на створення азартних ігор. Але зараз TRON розглядають як онлайн-казино, YouTube і Steam на одній платформі. При цьому всі вони представлені у вигляді децентралізованої системи.
Tether (USDT) 	Omni Layer	Proof-of-Reserve	Криптовалютне втілення традиційних валют, випущених на блокчейне біткоіна компанії Tether Limited. Кожна одиниця Tether підкріплена одиницею відповідної її валюти на рахунку компанії.
NEO 	відсутня	dBFT+PoS	Китайський Efirium, за запевненням розробників, володіє значно більшими можливостями. Підтримується владою Китаю.
Dash 	X11	PoA	Мастерноди формують додатковий рівень мережі з серверів, що працюють разом із другом в кластерах, які називаються кваррами. Забезпечується робота нових видів децентралізованих сервісів, таких як миттєві транзакції, приватність і децентралізоване керування. Системи захищені від загрози відповідних атак на мережу.

Додаток 10 продовження

Monero (XMR) 	CryptoNight	PoW	Одна з найбільш анонімних криптовалют. На відміну від більшості монет, у її блокуванні самими користувачами регулюється можливість перегляду транзакцій адрес та кількості переданих засобів за допомогою транзакцій.
Binance Coin (BNB) 	відсутня	відсутня	Токени були випущені криптовалютною біржею Binance для підтримки та розвитку своєї платформи. Використовується в тому числі для оплати комісій в біржі.

NEM 	blockchain	PoI	Вийшли на оновлення Catapult, що значно розширює можливості цієї криптовалюти, значно збільшує швидкість транзакції та захищеність мережі.
VeChain (VEN) 	Використовує платформу Ефіріум	PoS	Платформа, створена з метою об'єднання та внесення в єдину мережу всіх даних про товари, що дозволяє за допомогою звичайного сканера QR-коду отримати повну історію продукту, починаючи від дати та місця виробництва та завершуючи шлях, яким товаром потрапив на прилад.

Додаток 10 продовження

Ethereum Classic (ETC) 	Dagger-Hashimoto	PoW	Представляє собою початково збір блоків Ethereum. Після виявлення уразливості DAO, був проведений хардворк, в результаті якого з'явився Ефіріум (у якому відкатили всі зміни блокуєня в стан, попередня виявлена уразливість) та Ethereum Classic (в якому блокчейн залишився без змін.) Має ті самі можливості, що і Ethereum.
Qtum 	Використовує платформу Ethereum	IPoS	Платформа, призначена об'єднати кращі характеристики Bitcoin та Ethereum. По факту є р2р-мережею, цифровою валютою та віртуальною машиною.
Ontology (ONT) 	Використовує платформу Ethereum	airdrop	Являється багаторівневою мережею, що дозволяє різним компаніям перекладати свою діяльність в блокчейн. Реалізована на платформах NEO, Ethereum, EOS
Zcash (ZES) 	Equihash	PoW	Якщо порівняти конфіденційність біткоіни з Zcash, то у другій більш високий рівень захисту даних. Учасники мережі користуються публічними платежами і нічого приховують, - анонімність гарантовано. Швидкість. Формування хеш в платформі Zcash вимагає мінімального часового проміжку. На відміну від біткоіни, переклади криптовалюта відбуваються миттєво. З мінусі підтримується тільки операційну систему Linux.

СПИСОК
НАЗВ КРИПТОВАЛЮТНИХ ГАМАНЦІВ

№	Назва гаманця
1.	Bitcoin Core
2.	Copay
3.	Jaxx
4.	Electrum
5.	Exodus
6.	MyCrypto
7.	Neon Wallet
8.	KeepKey
9.	MSigna
10.	Morpheuswallet
11.	Litecoin Core Client
12.	Agama
13.	Toast
14.	Electron Cash
15.	CoinSpace
16.	Daedalus
17.	StellarTerm
18.	Stellar Desktop Cliem
19.	Stargazer
20.	Ledger
21.	Morpheus
22.	Emerald
23.	Bitcoin Knots
24.	MultiBit
25.	Qtum Core
26.	Qtum Electrum
27.	Armory
28.	BitGo
29.	Green Address
30.	mSIGNA

ІНСТРУМЕНТИ УТОЧНЕННЯ ПОШУКУ ЗА ДОПОМОГОЮ ПРОГРАМИ EVERYTHING

ОПЕРАТОРИ:		
	пробіл	AND ('i')
		OR (або')
	!	NOT ('ні')
	< >	Дужки
	" "	Знайти точну фразу
СИМВОЛИ ПІДСТАНОВКИ (ШАБЛОНИ):		
	*	Нуль або більше символів
	?	Один символ
МАКРОС:		
	quot:	Символ подвійні дужки ("")
	apos:	Символ апострофа ('')
	amp:	Символ амперсанда (&)
	lt:	Знак 'менше' (<)
	gt:	Знак 'більше' (>)
	#<n>:	Буквений юнікодний символ з кодом <n> в десятковому вигляді
	#x<n>:	Буквенный юникодный символ с кодом <n> в 16-ковий вигляд
	audio:	Пошук аудіофайлів
	zip:	Пошук архівів
	doc:	Пошук документів
	exe:	Пошук виконуваних файлів
	pic:	Пошук графічних файлів
	video:	Пошук відеофайлів
	ascii:	Дозволити швидке ASCII-порівняння регістрів букв
	case:	Розрізняти регістри букв
	diacritics:	Розрізняти діакритичні знаки
	file:	Тільки файли
	folder:	Тільки папки
	noascii:	Заборнити швидке ASCII-порівняння регістрів
	nocase:	Не розрізняти регістр бу

	nodiacritics:	Не розрізняти діакритичні знаки
	nofileonly:	Не розрізняти тільки файли
	nofolderonly:	Не розрізняти тільки папки
	nopath:	Не зважати на шлях
	noregex:	Заборонити регулярні вирази.
	nowfn:	Відключити зіставлення тільки цілих імен файлів
	nowholefilename:	Відключити зіставлення тільки цілих імен файлів
	nowholeword:	Відключити зіставлення тільки цілих слів
	nowildcards:	Заборонити символи підстановки (шаблони)
	noww:	Відключити зіставлення тільки цілих слів
	path:	Зіставляти шлях і ім'я файлу.
	regex:	Дозволити регулярні вирази.
	utf8:	Заборонити швидке ASCII-порівняння регістрів букв.
	wfn:	Зіставляти тільки цілі імена файлів
	wholefilename:	Зіставляти тільки цілі імена файлів
	wholeword:	Зіставляти тільки цілі слова
	wildcards:	Дозволити символи підстановки (шаблони)
	ww:	Зіставляти тільки цілі слова
ФУНКЦІЇ:		
	album:<текст>	Знайти носій по альбому в метаданих
	ansicontent:<текст>	Знайти ANSI- файл що містить зазначений текст
	artist:<текст>	Знайти носій по виконавцю в метаданих.
	attrib:<атрибути>	Знайти файли і папки із зазначеними файловими атрибутами
	attribdupe:	Знайти файли і папки з однаковими атрибутами

attributes:<атрибути>	Знайти файли і папки з зазначеними файловими атрибутами.
bitdepth:<кольоровість >	Знайти зображення тільки з роздільною число біт на піксель.
child:<имя_файла>	Знайти папки, що містять файли з відповідними ім'ям.
childcount:<кол-во>	Знайти папки, що містять зазначену кількість підпапок і файлів.
childfilecount:<кол-во>	Знайти папки, що містять зазначену кількість файлів.
childfoldercount:<к-во>	Знайти папки, що містять зазначену кількість підпапок
comment:<текст>	Знайти носій по коментарю в метаданих
content:<текст>	Знайти файл міститься в ньому тексті.
count:<макс>	Обмежити кількість результатів до зазначеного максимуму
dateaccessed:<дата>	Знайти файл і папки із зазначеною датою останнього доступу
datecreated:<дата>	Знайти файли і папки із зазначеною датою створення
datemodified:<дата>	Знайти файли і папки із зазначеною датою зміни
daterun:<дата>	Знайти файли і папки із зазначеною датою запуску
da:<дата>	Знайти файли і папки із зазначеною датою останнього доступу
dadupe:	Знайти файли і папки з однаковою датою останнього доступу
dc:<дата>	Найти файлы и папки с указанной датой создания

dcdupes:	Знайти файли і папки із зазначеною датою створення
dimensions:<w>X<h>	Знайти зображення із зазначеними шириною і висотою.
dm:<дата>	Найти файлы и папки с указанной датой изменения
dmdupes:	Найти файлы и папки с одинаковой датой изменения
dr:<дата>	Найти файлы и папки с указанной датой запуска
dupes:	Знайти файли з однаковими номерами
empty:	Знайти пусті папки
endwith:<текст>	Імена файлів (включаючи розширення), що закінчується текстом.
ext:<список>	Знайти файли з відповідним розширенням в зазначеному(розділеного крапкою з комою) списку розширень.
filelist:<iф1 iф2 ...>	Знайти список імен файлів
filelistfilename:<імя>	Знайти файли і папки, що належить вказаного файлу-списку.
frn:<frn>	Знайти файли і папки з зазначеним номером FRN (File Reference Number).
fsi:<індекс>	Знайти файли і папки в зазначеному внутрішньому індексі файлової системи з базою
genre:<текст>	Зайти носій в метаданих
height:<висота>	Знайти зображення з вказаною висотою (в пікселях)
infolder:<шлях>	Знайти файли і папки за вказаним шляхом, включаючи підпапки

len:<длина>	Знайти файли і папки з іменами зазначеної довжини
namepartdupe:	Знайти файли і папки з однаковою частиною імені
orientation:<тип>	Знайти зображення з альбомної або книжкової орієнтації (landscape или portrait)
parent:<шлях>	Найти файли і папки за вказаним шляхом, виключаючи підпапки.
parents:<кількість >	Знайти файли і папки з вказаною кількістю батьківських папок.
rc:<дата>	Знайти файли і папки із зазначеною датою зміни в базі даних Everything.
recentchange:<дата>	Знайти файли і папки із зазначеною датою зміни в базі даних Everything.
root:	Знайти файли і папки, які не мають батьківських папок
runcount:<число>	Знайти файли і папки, запущені вказану кількість разів.
shell:<ім'я>	Знайти папки з відомою оболонкою, включаючи підпапки і файли.
size:<размер>	Знайти файл зазначеного розміру (в байтах).
sizedupe:	Знайти розміри які дублюються.
startswith:<текст>	Імена файлів, що починаються з вказаного тексту.
title:<текст>	Знайти носій за назвою метаданих
track:<число>	Знайти медіафайли з зазначеним номером треку
type:<тип>	Знайти файли і папки зазначеного типу.

	utf16content:<текст>	Знайти файл міститься в ньому тексті в UTF-16
	utf16becontent:<текст>	Знайти файл міститься в ньому в UTF-16 Big Endian
	utf8content:<текст>	Знайти файл міститься в ньому в тексті в UTF-8
	width:<ширина>	Знайти зображення з вказаною шириною (в пікселях)

СИНТАКСИС ФУНКЦІЙ:

	функція:значення	Равно значенню
	функція:<=значення	Менше или равно значенню
	функція:<значення	Менше значення
	функція:=значення	Равно значенню
	функція:>значення	Больше значення
	функція:>=значення	Больше или равно значенню
	функція:поч-кін	Знаходиться в діапазоні значень з початку до кінця
	функція:поч-кін	Знаходиться в діапазоні значень з початку до кінця

СИНТАКСИС РОЗМІР:

	розмір[kb mb gb]	
--	----------------------	--

КОНСТАНТИ РОЗМІР:

	empty	
	tiny	0 КБ < розмір <= 10 КБ
	small	10 КБ < розмір <= 100 КБ
	medium	100 КБ < розмір <= 1 МБ
	large	1 МБ < розмір <= 16 МБ
	huge	16 МБ < розмір <= 128 МБ
	gigantic	розмір > 128 МБ
	unknown	

СИНТАКСИС ДАТ:

	рік	
	місяць/рік або рік/місяць - в залежності від регіональних налаштувань	
	день/місяць/рік, місяць/день/рік або рік/місяць/день - в	

	залежності від регіональних наалаштувань	
КОНСТАНТИ ДАТ:		
	today	
	yesterday	
	tomorrow	
	<last past prev current this coming next><year month week>	
	<last past prev coming next><x><years months weeks hours minutes mins seconds secs>	
	january february march april may june july august september october november december	
	jan feb mar apr may jun jul aug sep oct nov dec	
	sunday monday tuesday wednesday thursday friday saturday	
	sun mon tue wed thu fri sat	
	unknown	
КОНСТАНТИ АТРИБУТІВ:		
	A	Готовий до архівування
	C	Стиснутий
	D	Папка
	E	Зашифрований
	H	Прихований
	I	Вміст не проіндексовано
	L	Точка монтування
	N	Обичний
	O	На відключеному носії
	P	Розріджений файл
	R	Тільки для читання
	S	Системний
	T	Тимчасовий
	V	Пристрій
ОПЕРАТОРИ:		

	пробіл	AND ('i')
		OR ('або')
	!	NOT ('ні')
	< >	Дужки
	" "	Знайти точну фразу
СИМВОЛИ ПІДСТАНОВКИ (ШАБЛОНИ):		
	*	Нуль чи більше символів
	?	Один символ
МАКРОСИ:		
	quot:	Символ подвійні лапки(")
	apos:	Символ апострофа (')
	amp:	Символ амперсанда (&)
	lt:	Знак 'менше' (<)
	gt:	Знак 'більше' (>)
	#<n>:	Буквений юнікодний символ з кодом<n> в десятковому вигляді
	#x<n>:	Буквений юнікодний символ з кодом <n> в 16-ковому вигляді
	audio:	Пошук аудіофайлів
	zip:	Пошук архивів
	doc:	Пошук документів
	exe:	Пошук виконуючих файлів
	pic:	Пошук графічні файли
	video:	Пошук відеофайлів
МОДИФИКАТОРИ:		
	ascii:	Дозволити швидке ASCII-порівняння регістрів букв
	case:	Розрізняти регістри букв
	diacritics:	Розрізняти діакритичні знаки
	file:	Тільки файли
	folder:	Тільки папки
	noascii:	Заборонити швидке ASCII-порівняння регістрів букв
	nocase:	Не розрізняють регістри букв
	nodiacritics:	Не розрізняють діакритичні знаки
	nofileonly:	Не дозволяють тільки файли
	nofolderonly:	Не дозволяють тільки папки
	nopath:	Не враховують шлях

	noregex:	Забороняють регулярні вирази
	nowfn:	Відключити зіставлення тільки цілих імен файлів
	nowholefilename:	Відключити зіставлення тільки цілих імен файлів
	nowholeword:	Відключити зіставлення тільки цілих слів
	nowildcards:	Заборонити символи підстановки(шаблони)
	noww:	Відключити зіставлення тільки цілих слів
	path:	Зіставляти шлях і ім'я файла
	regex:	Дозволити регулярні вирази
	utf8:	Заборонити швидке ASCII-порівняння регістрів букв
	wfn:	Зіставляти тільки цілі імена файлів
	wholefilename:	Зіставляти тільки цілі імена файлів
	wholeword:	Зіставляти тільки цілі слова
	wildcards:	Дозволити символи підстановки(шаблони)
	ww:	Зіставляти тільки цілі слова

ФУНКЦІЇ:

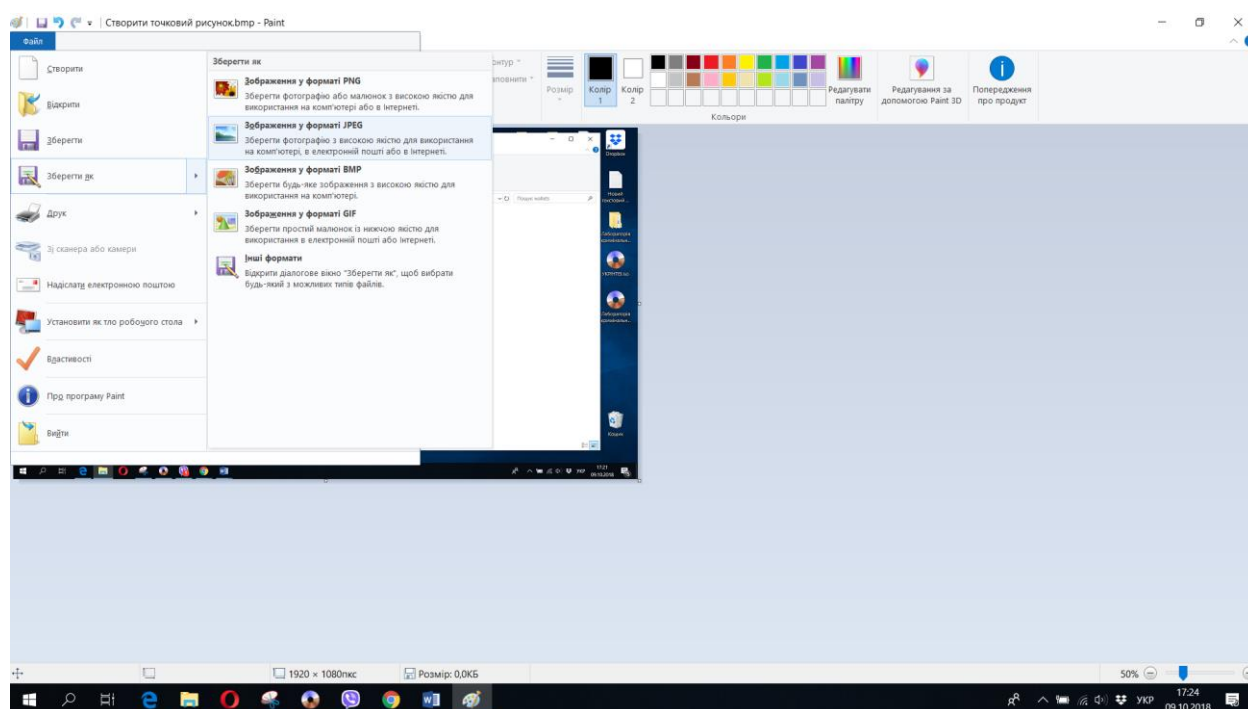
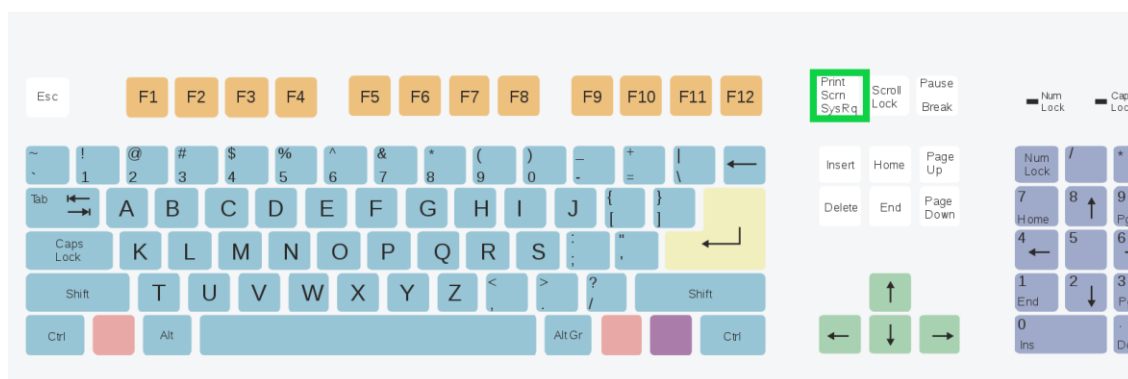
	album:<текст>	Знайти носій по альбому в метаданих.
	ansicontent:<текст>	Знайти ANSI-файл, що містить вказаний текст
	artist:<текст>	Знайти носій по виконавцю в метаданих
	attrib:<атрибути>	Знайти файли і папки з зазначеними файловими атрибутами
	attribdupe:	Знайти файли і папки з однаковими атрибутами

	attributes:<атрибути>	Знайти файли і папки з зазначеними файловими атрибутами
	bitdepth:<цветность>	Знайти зображення тільки з роздільним числом біт на піксель.
	child:<імя_файла>	Знайти папки, що містять файли з відповідним ім'ям.
	childcount:<кількість >	Знайти папки, що містять зазначену кількість підпапок і файлів

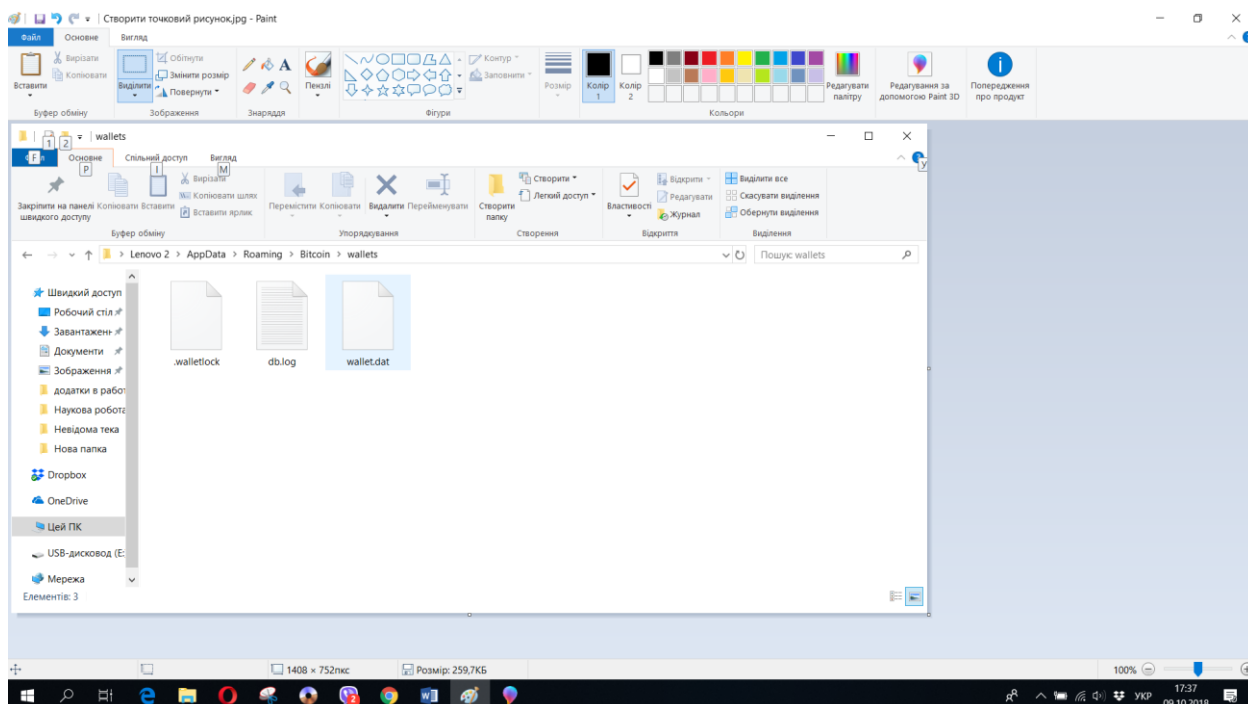
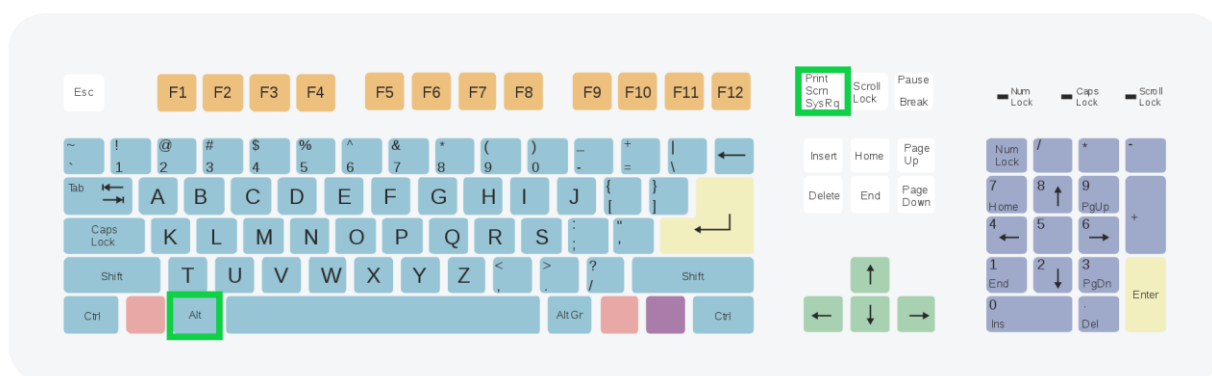
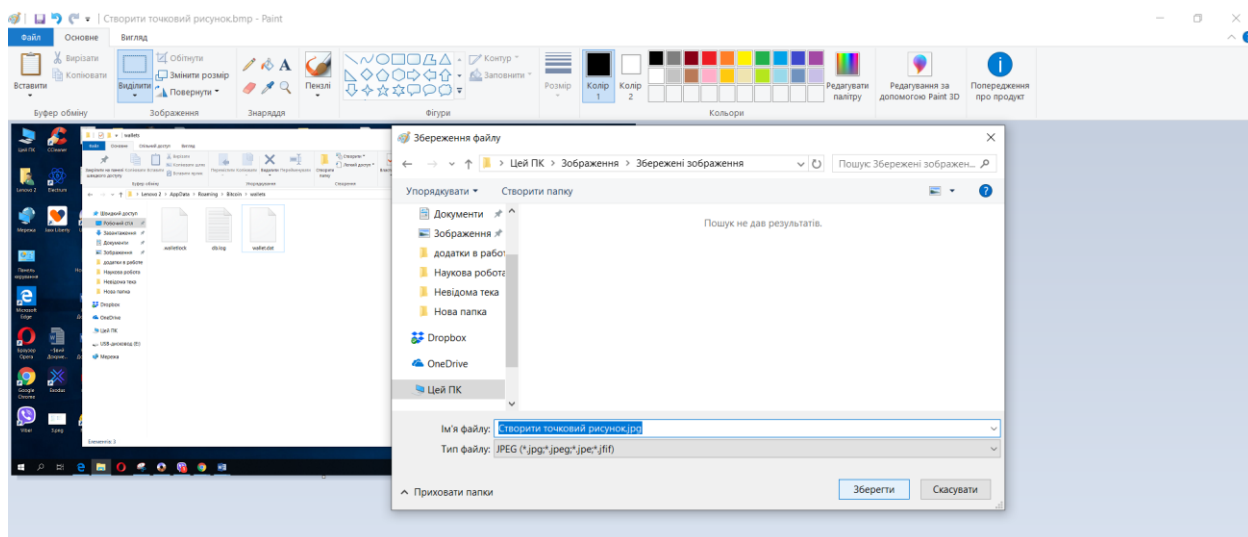
Таблиця : Оператори пошуку файлової системи Windows

Оператор	Значення	Приклад
При умові що точна назва невідома		
*	Знак що замінює	wall*
?	Дозволяє шукати тільки один пропущений символ	W?
#	Використовується для пошуку будь-якого числа	9#8
Пошук файла по його властивості		
king	Тип файла	king: document
tags	Теги, якими змінили файл	tags:пароль
author	ім'я користувача, який створив файл	author: User
Вираз «і», «або», «ні»		
AND(і)	Шукає декілька слів або виразів, чкі присутні в одному файлі.	Bitcoin AND Letecoin
OR(або)	Шукає файли, в яких присутні хоча б деякі слова і вирази.	Bitcoin OR Letecoin OR <u>Ethereum</u>
NOT(ні)	Шукає файли, немає згаданого виразу	Bitcoin NOT Letecoin
«»	Шукають файли, які містить точну фразу.	«Bitcoin і Letecoin»
()	Шукають файли, які можуть розміщуватись в будь якій послідовності.	(letecoin bitcoin)
> і <	Шукають файли, з не точно вказаними величинами.	date:>01/01/2018

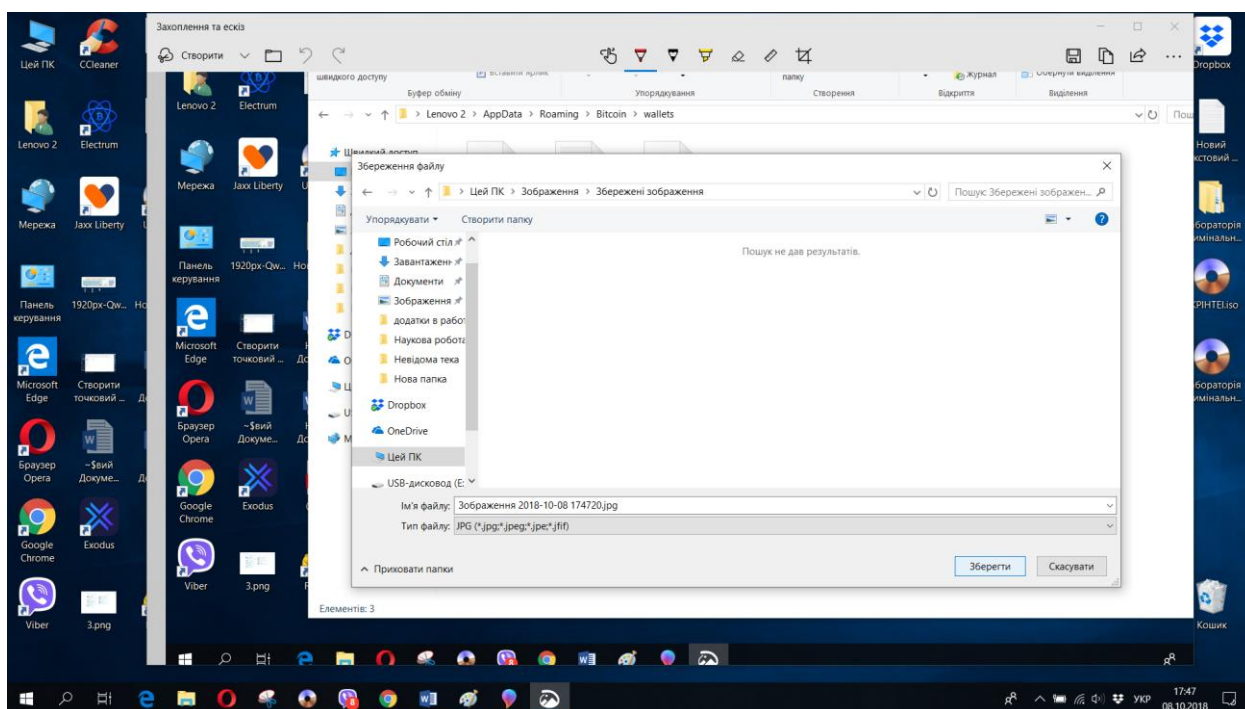
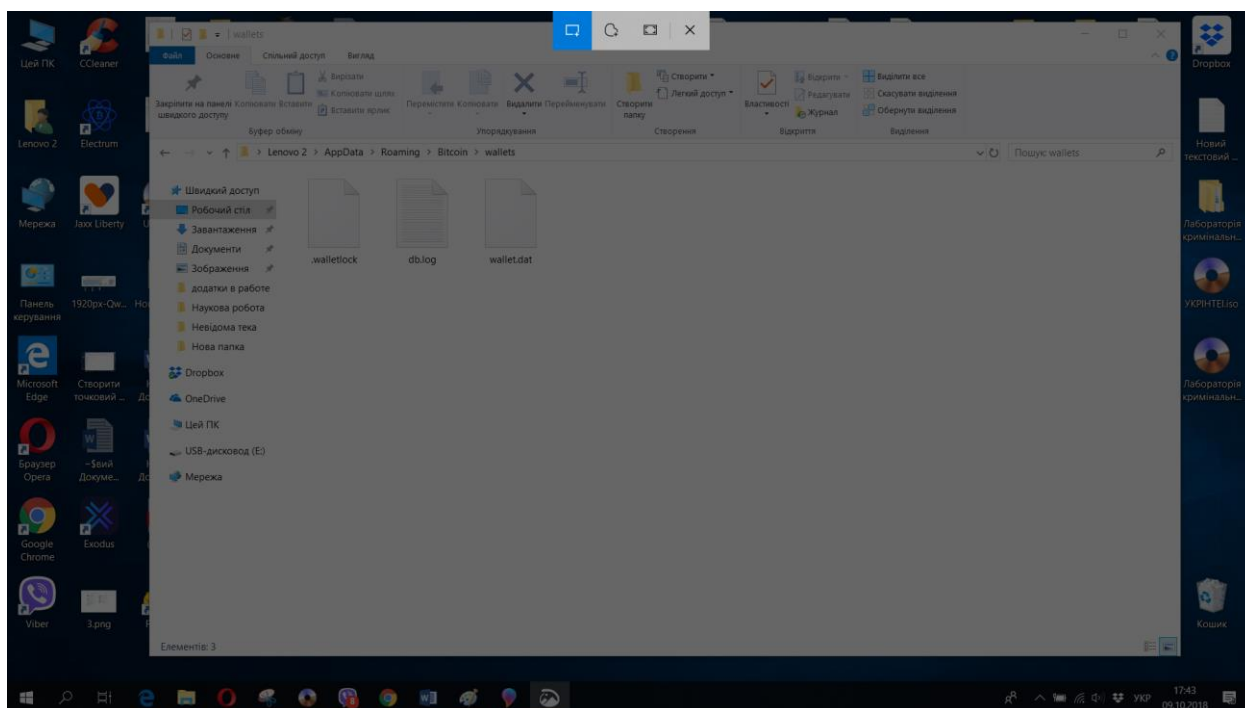
ФІКСАЦІЯ ЗА ДОПОМОГОЮ СТАНДАРТНИХ КОМПОНЕНТІВ ОПЕРАЦІЙНОЇ СИСТЕМИ ЗА ДОПОМОГОЮ КЛАВІШІ PRINTSCREEN



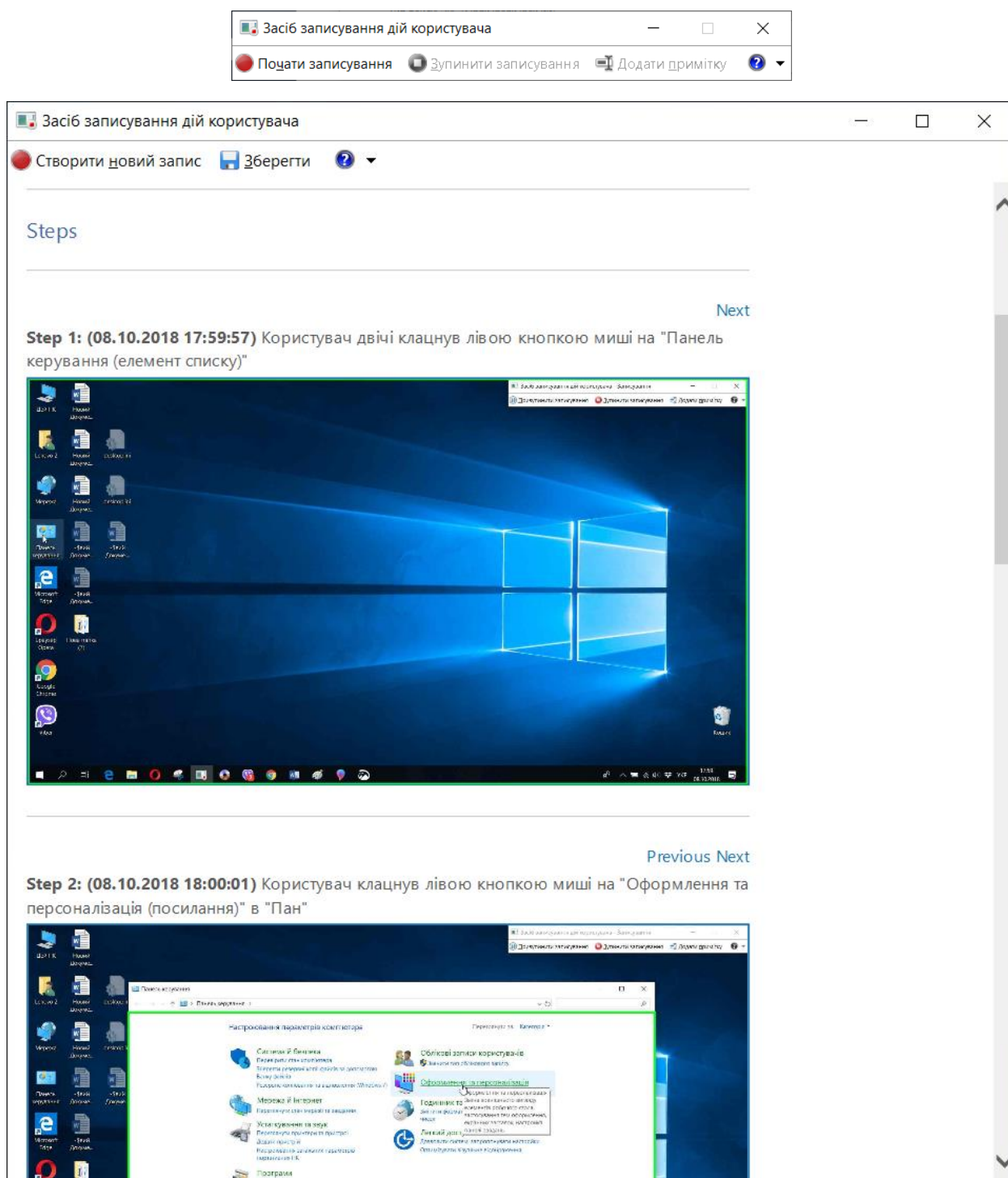
Додаток 14 продовження



СТВОРЕННЯ ЗНІМКУ ЗА ДОПОМОГОЮ СИСТЕМНОГО ІНСТРУМЕНТУ «ЗАХОПЛЕННЯ ТА ЕСКІЗ»



ФІКСАЦІЯ ЗА ДОПОМОГОЮ «ЗАСОБУ ЗАПИСУВАННЯ ДІЙ КОРИСТУВАЧА»



Додаток 16 продовження

Засіб записування дій користувача
— □ ×

Створити новий запис
Зберегти
?

Additional Details

The following section contains the additional details that were recorded.
 These details help accurately identify the programs and UI you used in this recording.
 This section may contain text that is internal to programs that only very advanced users or programmers may understand.
 Please review these details to ensure that they do not contain any information that you would not like others to see.

Сеанс записування: 08.10.2018 17:59:50 - 18:00:10

Записані кроки: 3, Пропущені кроки: 0, Інші помилки: 0

Операційна система: 17763.1.amd64fre.rs5_release.180914-1434 10.0.0.0.2.48

Крок 1: Користувач двічі клацнув лівою кнопкою миші на "Панель керування (елемент списку)"
 Програма: Провідник Windows, 10.0.17763.107 (WinBuild.160101.0800), Microsoft Corporation, EXPLORER.EXE /LOADSAVEDWINDOWS, EXPLORER.EXE
 Елементи інтерфейсу користувача: Панель керування, SysListView32, SHELLDLL_DefView, WorkerW

Крок 2: Користувач клацнув лівою кнопкою миші на "Оформлення та персоналізація (посилання)" в "Пан"

Програма: Провідник Windows, 10.0.17763.107 (WinBuild.160101.0800), Microsoft Corporation, EXPLORER.EXE /LOADSAVEDWINDOWS, EXPLORER.EXE
 Елементи інтерфейсу користувача: Оформлення та персоналізація, ControlPanellink, CPCategoryPanel, Element, Область подання папок, Element, Область Провідника, HwndView, DuiViewWndClassName, Панель керування, ShellTabWindowClass, Панель керування, CabinetWClass

Крок 3: Користувач клацнув лівою кнопкою миші на "Відобразити приховані файли та папки (посилання)" в "Офо"

Програма: Провідник Windows, 10.0.17763.107 (WinBuild.160101.0800), Microsoft Corporation, EXPLORER.EXE /LOADSAVEDWINDOWS, EXPLORER.EXE
 Елементи інтерфейсу користувача: Відобразити приховані файли та папки, ControlPanellink, Button, CPCategoryPanel, Element, Область подання папок, Element, Область Провідника, HwndView, DuiViewWndClassName, Оформлення та персоналізація, ShellTabWindowClass, Оформлення та персоналізація, CabinetWClass

Recording_20181008_1804.mht

Документ MHTML

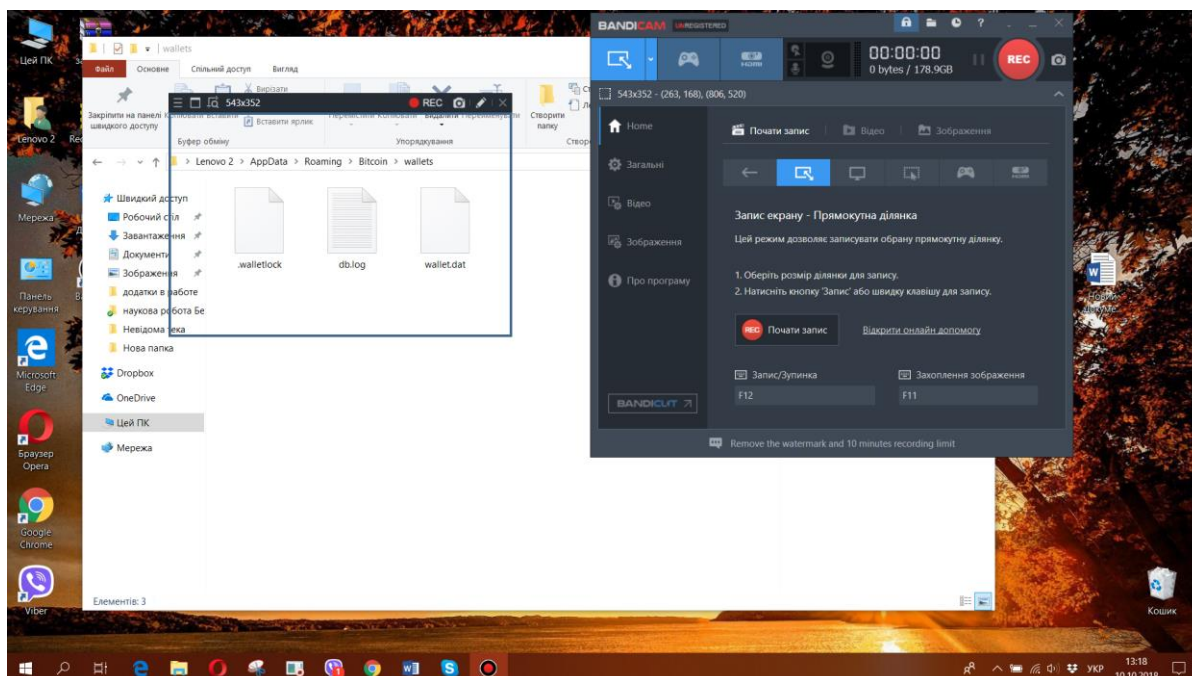
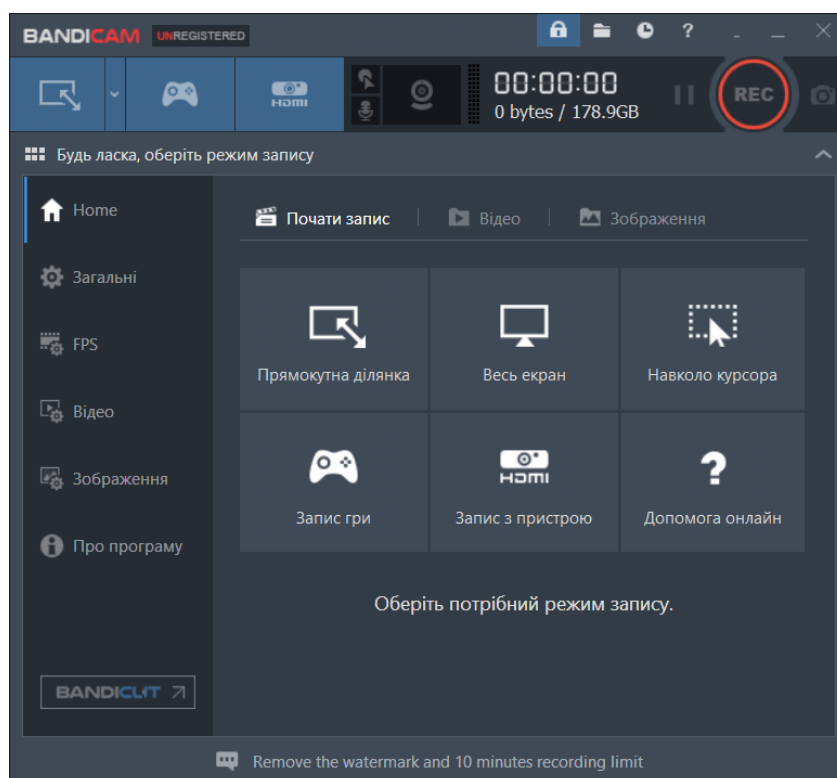


Дата змінення: 08.10.2018 18:00

Розмір: 429 КБ

Дата створення: 08.10.2018 18:05

ФІКСУВАННЯ ЗА ДОПОМОГОЮ ДОДАТКОВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ «BANDICAM SCREEN RECORDER»



Додаток 17 продовження

