# 7.8. Електронні гроші і криптовалюти

Поки що криптовалюти залишаються новою і відносно маловивченою технологією, яка не має усталеної термінології та систематизації. Нові користувачі індустрії і навіть засоби інформації часом плутають терміни «електронні гроші» і «криптовалюта», використовуючи їх як синонімів.

Електронні гроші – це фіатні валюти у цифровому вигляді, які контролюються через банківську систему чи іншого посередника – оператора електронних платежів. Фіатна валюта - це валюта, вартість якої забезпечена державою, що її випускає. До фіатных належать всі сучасні державні валюти - долари США, євро, гривні тощо.

Емітентом електронних грошей може бути державний або комерційний банк, що має ліцензію Національного банку на випуск електронних грошей держава чи приватна організація. Емітент електронних грошей здійснює випуск електронних грошей і приймає на себе безумовне та безвідкличне зобов'язання щодо погашення електронних грошей власникам, які пред'являють електронні гроші до переведення в готівку. Під поняття електронних грошей потрапляють практично всі популярні платіжні системи PayPal, Qiwi, WebMoney та інші.

Гроші на електронних гаманцях не підлягають державному страхуванню. Доступ до електронного гаманця надається за логіном та паролем. Деякі платіжні системи додатково використовують файли із закритими ключами та двофакторну автентифікацію.

### Різниця між криптовалютою та електронними грішми

Лінія поділу між криптоактивами та електронними грошима проходить за технічними та частково економічними характеристиками:

* **Децентралізація**. Криптовалюти функціонують у розподіленій мережі та не мають єдиного центру зберігання та обробки інформації, як, наприклад, WebMoney. Децентралізація також передбачає спеціальні способи підтвердження справжності транзакцій - PoW, PoS та інші різновиди протоколів доказу.
* **Анонімність**. При використанні криптовалют користувачі не зобов'язані підтверджувати свою особу – немає бази даних з персональною інформацією учасників транзакції, крім їх IP та адреси гаманця. Хоча дедалі більше бірж криптовалют зобов'язують користувачів проходити перевірки KYC, власники криптоактивів знаходять способи мінімізувати розкривання персональної інформації. У централізованих платіжних системах відправляти чи отримувати гроші не верифікованому користувачеві якщо й можна, то лише з низкою обмежень.
* **Прозорість**. У традиційних електронних платіжних системах дані про рахунок користувача є тільки у центрального оператора і не розкриваються іншим учасникам для збереження банківської таємниці. Блокчейн відкритий для будь-кого, тому, всі можуть подивитися з якого гаманця були надіслані гроші, розмір переказу та адресу одержувача. Однак, є конфіденційні криптовалюти, наприклад, Zcash, розробники яких використовують механізми криптографії для приховування інформації про суму транзакції, її одержувача та відправника.
* **Нерегульована вартість та емісія.** Вартість та порядок випуску електронних грошей встановлює їхній емітент (держава, розробники гри тощо). Криптовалюта випускається за заздалегідь встановленими правилами, та її вартість у фіаті залежить від попиту, відкритий ринок визначає справедливу вартість активу.

Досить довго характерною ознакою криптовалют була відсутність законодавчого регулювання обігу та офіційного визнання платіжним засобом. Станом на 2021 рік багато країн так чи інакше впровадили криптовалюту у свої правові системи, а в Японії та Сальвадорі вона навіть вважається платіжним засобом.

### Плюси та мінуси електронних грошей

Незважаючи на те, що криптовалюти користуються все більшою популярністю як прогресивний спосіб оплати, традиційні електронні гроші також мають сильні сторони:

* **Ліквідність**. Електронними грошима можна розрахуватися практично за будь-який товар чи послугу – їхня ліквідність забезпечена державою чи емітентом.
* **Швидкість переказів**. Централізовані електронні платіжні системи обробляють кілька тисяч операцій на секунду. При цьому блокчейн Біткоїна обробляє приблизно 5-7 транзакцій на секунду, а Ефіріуму - 15-20 транзакцій.
* **Доступність**. Звичайному користувачеві створити електронний гаманець простіше, ніж криптовалютний гаманець. Електронний гаманець легко поповнити і не потрібно думати про зберігання закритих ключів. Ціна валюти в електронному гаманці дорівнює вартості відповідної фіатної валюти.

Проте, електронні гроші мають низку недоліків, які й сприяли появі платіжних мереж нового покоління:

* **Централізація.** Електронні платіжні системи мають один центр обробки та зберігання інформації, який відносно легко атакувати. Центральний сервер стає так званою "точкою відмови".
* **Дорожнеча.** Комісії при традиційних переказах вищі через необхідність утримання штату співробітників та обладнання.
* **Залежність регулятора.** Єдиний організаційний центр – це також «точка відмови». Якщо влада вирішить, що цю платіжну систему потрібно закрити — її роботу відразу зупиняють, не питаючи думки користувачів.

Електронні гроші з усіма їхніми перевагами та недоліками залишаються важливою частиною нашого життя і використовуються повсюдно - від покупки в магазинах до транскордонних переказів між компаніями. Подібне становище електронних грошей зберігатиметься, поки криптовалюти не отримають масового визнання та поширення.

### Плюси та мінуси криптовалют

Оскільки криптовалюти з'явилися як відповідь на слабкі сторони традиційних електронних платіжних систем, їх плюси дзеркально відображають мінуси електронних грошей:

* **Стійкість до злому системи загалом**. Для внесення змін до блокчейну зловмисник повинен зламати не один центр обробки даних, а взяти під контроль понад 51% майнінгових потужностей або монет у мережі. Для великих криптовалют це завдання практично нездійсненне. Проте, непопулярні альткоїни час від часу стають жертвами таких атак.
* **Низька вартість переказів.** Децентралізація передбачає, що немає єдиного центру, який оплачує роботу співробітників та утримання обладнання. Оператор кожного вузла сам несе всі витрати, що здешевлює транзакції порівняно з електронними платіжними системами. Хоча через зростання популярності криптовалют у 2021 році комісії в мережах Біткоїна та Ефіріуму багаторазово виросли та досягли історичних максимумів, розробники постійно працюють над їх зменшенням через розробку оновлень.
* **Саморегульованість.** Роботу Біткоїна або Ефіріуму неможливо зупинити лише за бажанням регулятора. Для цього доведеться вимкнути всі вузли мережі.
* **Конфіденційність.** У блокчейні не зберігається особиста інформація про користувачів, тому і вкрасти ці дані ніхто не може.

У криптовалют є і серйозні мінуси, які поки що не дозволяють їм набути масового поширення.

* **Волатильність**. Стрибки курсу не дозволяють зафіксувати цінність криптовалюти, що ускладнює її використання у повсякденному житті. Виняток — стейблкоїни, зазвичай їхня ціна прив'язана до долара США або євро.
* **Відносно низька ліквідність.** Ніхто не зобов'язаний купувати у користувача криптовалюту або обмінювати її на інший актив. За скільки власник продасть монети і чи продасть їх взагалі, вирішує лише ринок.
* **Масштабування.** Низька пропускна здатність ранніх блокчейнів обмежує кількість користувачів та збільшує час переказів, що відштовхує багатьох людей. Проте, прогрес відбувається. Наприклад, розробники Ефіріуму активно працюють над запуском другої ітерації мережі, яка має значно збільшити пропускну здатність блокчейну. Рішення другого рівня Ефіріуму типу Hermez можуть забезпечити стократне збільшення пропускної спроможності. А деякі проекти, наприклад Solana та Kadena, здатні обробляти сотні тисяч транзакцій за секунду і можуть зрівнятися за швидкістю з Visa. Проте, висока швидкість, зазвичай, забезпечується з допомогою часткової централізації.
* **Необоротність транзакцій.** Якщо при зломі електронної платіжної системи сервер може просто зробити резервну копію всіх даних або скасувати переказ відправлених шахраям грошей, то криптовалюти такої можливості не надають. Якщо у користувача були вкрадені закриті ключі та монети переведені на іншу адресу, повернути їх неможливо.

З кожним роком розробники вирішують ці проблеми дедалі ефективніше, тому, можливість розрахуватися криптовалютами за покупку в супермаркеті — лише питання часу. Однак електронні гроші також залишатимуться важливою частиною фінансової системи ще довгий час завдяки налагодженій роботі таких систем та їх зручності.

## Криптовалюта Біткоїн

Блокчейн-гаманець для зберігання Біткоїнів засновано в 2011 році. Він пропонує не просто зберігати кошти, але і є оглядачем блоків, тобто, саме тут можна переглянути яка транзакція, куди була відправлена, а також простежити ланцюжок передачі коштів від моменту їх виникнення. Якщо необережно купити криптовалюту або продати, то можна видати дані про себе, які будуть доступні для кожного.

Гаманець давно користується хорошою репутацією як надійний і зручний сервіс, хоча і стягує високі комісії за перекази. При невеликому розмірі комісії (встановлює сам користувач) транзакція може тривати довго, а потім повернутися до свого власника непідтвердженою. Незважаючи на це, багато користувачів користуються цим сервісом, завести на ньому акаунт може любий.

### Реєстрація Блокчейн гаманця

Нижче наведено короткий перелік дій користувача, що в кілька кроків зробить його власником акаунту на [Blockchain](https://blockchain.info/#_blank)[.info](https://blockchain.info/)

1. Перейти на офіційний сайт онлайн гаманця і вибрати розділ «Гаманець».
2. Вибрати одну з кнопок створення гаманця - в верхній частині екрану або по центру кнопка «Sign Up».



1. Ввести мінімум даних про особу: пошту, пароль і підтвердити згоду з умовами використання сервісу.
2. Реєстрація завершена, верифікувати пошту, оскільки це дозволить отримати доступ до гаманця при різних несприятливих моментах.

Для входу в систему вибрати в розділі «Гаманець» функцію «Login in», а потім вказати дані, які були задані при реєстрації. Вже з особистого кабінету можна налаштувати рівень безпеки облікового запису, який буде найбільш зручним.

Важливо зберігати пароль доступу до гаманця, адже його втрата загрожує втратою грошей. Для того, щоб мати шанс відновлення доступу або у разі втрати закритого ключа слід відразу запросити мнемонічний код і зберігати його в надійному місці.

### Алгоритм переказу грошей в блокчейні

1. Користувач А хоче переказати певну суму до користувача В. Вони відкривають біткоїн-гаманці і 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 (розмір 1 Мб).
4. Блоку привласнюється номер і майнери обчислюють для нього хеш - спеціальний код, що містить відомості про цей та попередній блоки.
5. Блок розсилається до всіх майнерів блокчейн-мережі і вони перевіряють правильність даних.
6. Якщо помилки не знайдено, то кожен майнер 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 блока 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.

Технологія блокчейн побудована так, що до моменту внесення запису в блок він вважається непідтвердженим (недійсним). Користувач мережі може використовувати запис, але немає гарантій достовірності здійсненої операції. Виникають ситуації, коли непідтверджений запис згодом скасовують. Як тільки запис зберігся в сформованому, прохешованому блоці і цей факт підтверджено, то його скасування вже неможливе.

Шифрування блоків гарантує, що користувачі можуть користуватися лише тими частинами ланцюжка блоків, до яких вони мають закриті ключі, без яких зчитування запису є неможливою. Шифрування гарантує синхронізацію копій розподіленого ланцюжка блоків у всіх майнерів.

Замість того, щоб звертатися до третіх осіб, наприклад, фінансово-кредитних організацій, в якості посередників при проведенні транзакцій, вузли блокчейн-мережі використовують спеціальний протокол консенсусу для узгодження вмісту реєстру, а також криптографічні алгоритми хешування і електронно-цифрового підпису для забезпечення цілісності транзакції і передачі її параметрів.

Механізм консенсусу гарантує, що розподілені реєстри є точними копіями, що зменшує ризик появи шахрайських транзакцій, оскільки стороннє втручання може виникнути в багатьох місцях одночасно. Криптографічні алгоритми хешування, такі як алгоритм обчислень SHA256, гарантують, що будь-яка зміна вхідних даних транзакції, навіть сама незначна, призведе до появи іншого значення хешу в результатах розрахунків, що вказує на ймовірність компрометації вхідних даних транзакції. Електронно-цифрові підписи гарантують, що транзакції здійснюються легітимними відправниками (підписані закритими ключами), а не зловмисниками.

Децентралізована однорангова блокчейн-мережа позбавляє окремих учасників або груп учасників можливості контролювати базову інфраструктуру або дестабілізувати всю систему. Всі учасники мережі є рівними і під’єднуються до неї за одними протоколами. Учасниками можуть бути фізичні особи, державні структури, організації або об'єднання всіх перелічених типів учасників.

Отже, система записує хронологічний порядок проведення транзакцій зі всіма вузлами мережі, що визнали дійсність транзакцій за допомогою обраної моделі консенсусу. Результатом є транзакції, які не підлягають скасуванню і узгоджені всіма учасниками мережі децентралізовано.

### Транзакція

Криптовалюта, наприклад біткоїн є послідовністю цифрових підписів. Структуру транзакції в криптовалюті наведено на рис.1:



Рис.1. Структура транзакцій в мережі біткоїн

Публічний ключ учасника (1,2,3) - це власне адреса, куди слід перевести певну суму коштів.

Хеш транзакції - сама інструкція, вона містить інформацію про суму переказу і адресу призначення. А головне, звідки взялися ці гроші, які потрібно перевести, тому, на рисунку зображено стрілки, що йдуть від попередньої транзакції.

Підпис учасника (1,2,3) – подібно до автографу на чеку, який за допомогою приватного ключа підтверджує ваші повноваження, як власника коштів. Якщо публічний ключ можна роздавати всім, то приватний ключ слід тримати при собі. Цей ключ надає повний доступ до операцій за рахунком. Це схоже на пластикову картку, її можна показувати, навіть дати вставити в банкомат, а для зняття грошей потрібен буде пін-код.

Транзакція готова і далі вона потрапляє в блок. Все свіжі транзакції запускаються у мережу, де вони очікують, коли їх причеплять до ланцюжка. Мережа в свою чергу містить велику кількість вузлів, які займаються формуванням нового блоку і перевіркою достовірності транзакції.

Вузли шляхом обчислень підбирають хеш для блоку просто перебираючи різні значення. Коли це значення знайдено і відповідає всім вимогам, блок вважається сформованим.

### Відомості про блок

* Сьогодні Майнери формують (добувають) в середньому один блок кожні 10 хвилин.
* В кожному блоці може зберігатися максимум 1 Мб даних.
* Таке обмеження закладено в код біткоїнів, але пропускна здатність мережі цим не обмежується.

У блок розміром 1 Мб можна вмістити дані приблизно про 3-5 тисячі простих транзакцій (між двома гаманцями з невеликою кількістю входів і виходів), тобто мережа пропускає в середньому 7 транзакцій в секунду. Для сьогоднішньої кількості користувачів це не критично, але для майбутнього масового використання дуже мало.

Кількість транзакцій, які вміщуються в один блок, скорочується, по-перше, за рахунок багатоадресних транзакцій - наприклад, розсилка пулами винагороди майнерам. А по-друге, за рахунок того, що деякі компанії використовують ланцюжок блоків Біткоїнів для нефінансового застосування, передачі даних або підтримки реєстру (компанія Factom, проект Counterparty, біржа Nasdaq).

До недавнього моменту блоки досить рідко заповнювалися даними цілком, на існування обмеження розміру не звертали уваги. Однак, разом з тим, як визнання біткоїна зростає і ним починає користуватися все більше людей, збільшується і кількість транзакцій, в результаті чого кожен блок в ланцюжку все більше заповнюється даними.

Група дослідників влаштувала «тест на стресостійкість» мережі шляхом «спаму» ланцюжка блоків множиною транзакцій на крихітні суми, в результаті якого протягом 8 годин кожен блок в мережі був заповнений повністю, і велика кількість транзакцій, що не вмістилися в блоки, залишилися непідтвердженими.

Серед головних переваг біткоїна виділяють швидкі і дешеві перекази коштів (комісія для майнерів). Деякі користувачі при переказі Біткоїнів навмисне збільшують розмір комісії, щоб їх транзакція була пріоритетною для підтвердження, тобто підтвердження звичайних транзакцій може відбуватися вже в другому, третьому і так далі блоках, а значить займати за часом 20, 30 і навіть більше хвилин (а іноді і пару годин). Звичайно, розробляються різні програмні рішення, щоб при оплаті біткоїнів не доводилося стояти по півгодини на касі в очікуванні підтвердження, але технічно з ростом масштабів використання біткоїнів такі затримки будуть траплятися все частіше і частіше.

У 2010 році на технологію Біткоїнів звернуло увагу багато користувачів, серед яких виявилися не самі добропорядні, і мережа Біткоїн почала піддаватися численним атакам. Автори біткоїна швидко на це зреагували і внесли кілька поправок до протоколу, щоб зробити його більш стійким. Однією з цих поправок стало рішення встановити межу розміру блоку в 1 Мб.

До того моменту у біткоїна не було обмеження на розмір блоку, обсяг транзакцій був дуже малий і вважалося, що 1 Мб вистачить як для захисту мережі, так і для резервного простору для майбутнього зростання обсягів транзакцій, перш ніж масштаби мережі будуть збільшені. Обмеження було введено як міра проти зловмисників, які могли навмисно створювати великі блоки з метою обвалити ще зовсім молоду на той момент мережу. Такі атаки в принципі можливі і сьогодні, саме тому і необхідне обмеження розміру, але зараз такі атаки значно більш затратні і, по суті, стали неефективними.

### Ключі

Інформація Блокчейн (блоки і інформація в них) доступна для кожного бажаючого, будь-який блок відкривається для вивчення ([приклад](https://blockchain.info/tx/8088eeadbb0c6cbc6cc87ffacc05045f50195bd3837ec392a894465693578b57#_blank)). Ланцюжок блоків за необхідності дозволяє відстежити, а також оцінити шлях зміни інформації, перевірити коректність даних. Блокчейн - це система, що дозволяє перевіряти інших учасників і не довіряти нікому. За наявності будь-яких сумнівів проводиться перевірка, після чого приймається рішення.

Всі дані в системі захищені. Ланцюжок Блокчейну надійно зашифрований і це відкриває шляхи для отримання достовірної і відкритої інформації. Через інформацію в блоці можна побачити всіх мільйонерів, але ось дізнатися, кому мільйони належать, нереально. Для того щоб переглянути дані потрібно підтвердження права власності на цю транзакцію.

Для ідентифікації користувача застосовується спеціальний ключ. Захист і надійність блокчейну будується на цих ключах, за допомогою яких спрощується процес перевірки коректності та правдивості інформації. Сам криптографічний ключ - група букв і цифр, розрахунок яких проводиться із застосуванням спеціально створеного алгоритму, що називається функцією хеш. При цьому у користувача є лише один ключ, якому притаманні дві різні властивості:

1. Маючи ключ на руках, не вийде дізнатися первинну (вхідну) інформацію.
2. Підібрати інший пакет даних, що дозволяють створити такий же ключ, неможливо.

Наявність на руках ключа ще нічого не означає. Людина, яка має ключ, не зможе завдати шкоди системі або іншому користувачеві. З іншого боку, вивчення наявної інформації дозволяє перевірити відповідність даних до певного ключа. Навіть за невеликої корекції даних ключ буде змінено.

### Як знайти біткоїн-транзакцію в блокчейні?

Block Explorer - це веб-сайт або сервіс, де можна переглядати блоки, адреси гаманців, мережний хешрейт (одиниця, що відображає обчислювальну потужність обладнання для видобутку криптовалюти (майнінгу), дані транзакцій та іншу ключову інформацію в блокчейні) забезпечує візуально привабливий і зручний спосіб навігації біткоїнів в блокчейн-ланцюжку. Він надає можливість вивчати біткоїн-транзакції, створює інформативні графіки і таблиці, що відображають активність в мережі.

Щоб знайти біткоїн-транзакцію, користувачі можуть піти на сайт https://blockchain.info і скористатися панеллю пошуку, що розташована нагорі справа. За допомогою цієї функції можна отримати інформацію про конкретну біткоїн-адресу, хеш транзакції, або номер блоку, якщо ввести їх в пошукове вікно.

Для прикладу можна подивитися на [цю транзакцію](https://blockchain.info/tx/8088eeadbb0c6cbc6cc87ffacc05045f50195bd3837ec392a894465693578b57#_blank).

### Підтвердження мережі Біткоїн

Підтвердження транзакції потрібно для того, щоб запобігти повторній витраті одних і тих же грошових коштів. Як тільки відправник переказує кошти, транзакція потрапляє в мережу Bitcoin для виконання і додавання до блоку.

Саме процес додавання транзакції до складу знайденого блоку, називається підтвердженням транзакції, один блок містить одне підтвердження. Як тільки транзакція отримує підтвердження, монети біткоїн стають доступними для подальшого їх використання.

Швидкість підтвердження залежить від багатьох факторів, таких як: завантаженість самої мережі Біткоїн, розмір комісії зазначеної при переказі, швидкість Інтернет з'єднання, технічна справність ресурсу, де знаходитися гаманець і т. д. В середньому підтвердження транзакції тривати від 30 хвилин до декількох годин. Але іноді підтвердження можна чекати 2-6 днів, якщо мережа Біткоїн перевантажена.

Підтвердження операцій в мережі Біткоїн залежить від роботи майнерів. Саме ці люди виконують обчислення і діють виключно в своїх фінансових інтересах. Обмінник не займається майнінгом біткоїнів і не може жодним чином вплинути на роботу Майнерів. Це не залежний від обмінника процес, який відбувається після виконання переказу Біткоїнів з адреси обмінника на адресу вказану користувачем в транзакції.

Підтвердження від мережі слід чекати доки майнер не виконає певні дії з видобутку блоків. Це фундаментальні властивості мережі Біткоїн.

Зобов'язання обмінника вважаються виконаними після переказу монет Біткоїн на вказану клієнтом адресу, що підтверджується записом в загальнодоступному реєстрі.

Будь-які претензії до обмінника щодо підтверджень в мережі Біткоїн є безпідставними, оскільки підтвердження в мережі Біткоїн це неконтрольований обмінником процес, процес, який залежить від дій третіх осіб. Цей процес відбувається після успішного завершення обміну в гаманці користувача.

Досить часто мережа Біткоїн буває завантаженою. Це може бути викликано різними обставинами: велика кількість необроблених транзакцій, атаки на мережу хакерами і т.д. У такі періоди час очікування підтверджень може збільшитися від декількох годин і до декількох діб.

## Контрольні питання

1. Провести коротке порівняння електронної та криптовалюти.
2. Навести сильні та слабкі сторони електронних грошей.
3. Навести сильні та слабкі сторони криптовалют.
4. Яким чином можна отримати чи переказати криптовалюту?
5. Як знайти біткоїн-транзакцію в блокчейні?

## Використані матеріали

* Електронні гроші та криптовалюти <https://bits.media/pr/elektronnye-dengi-i-kriptovalyuty-v-chem-raznitsa/>
* How Bitcoin Works Under the Hood <https://youtu.be/Lx9zgZCMqXE>
* Біткоїн - інноваційна платіжна система та новий вид грошей <https://bitcoin.org/uk/>
* Bitcoin Wiki <https://en.bitcoin.it/wiki/Main_Page>
* Глобальна платформа Ethereum <https://ethereum.org/ru/>