

УДК 336 (477)

Коваль О.А.¹, Цимбал Є.С.²

¹ канд. екон. наук, доц. НУ «Запорізька політехніка»

² студ.гр. ФЕУ-112 НУ «Запорізька політехніка»

КРИПТОВАЛЮТА

Криптовалюта – різновид цифрової валюти, облік внутрішніх розрахункових одиниць якої забезпечує децентралізована платіжна система (немає внутрішнього чи зовнішнього адміністратора або будь-якого його аналога), що працює в повністю автоматичному режимі.

Залежно від функцій і сфери застосування розрізняють різні типи криптовалют, зокрема стейблкоїни, NFT, токени управління і обгорнуті активи. Біткоїн – це золотий стандарт і перша криптовалюта ринку криптовалют.

Ще в 60-х роках минулого століття професійні криптографи обговорювали можливість створення глобальної інформаційної мережі. Перші практичні кроки в цьому напрямку було зроблено у 80-ті. За допомогою інфомережі почали здійснювати обмін брокерськими даними, які були потрібні для торгівлі на біржах. У цей же час з'явилася ідея цифрових грошей. Одним із проєктів, близьким до сучасних криптовалют, є b-money. Проєкт заснував програміст Вей Дай. Чималий внесок у становлення криптовалюти зробив Адам Бакер. Саме він 1997 року застосував HashCash – технологію, стійку до спаму і DoS-атак. Біткоїн, створений анонімним користувачем під ніком Сатоші Накамото, став першою успішною криптовалютою, що набула широкого поширення.

Більшість криптовалют застосовують технологію під назвою блокчейн. Останній є послідовністю ієрархічно пов'язаних блоків. Він вміщує в себе базу даних про всі проведені транзакції. Нові транзакції записуються в блоки, які створюють оператори нод. Кожен з комп'ютерних вузлів зберігає свою копію блокчейна і в ході досягнення

консенсусу підтверджує нові блоки, передаючи результат іншим нодам. На основі цієї інформації змінюються баланси користувачів.

У криптовалютах широко застосовуються хеш-функції. Остання дає змогу «згорнути» довільний масив даних в один рядок – хеш. Блокчейн є єдиним цілим, оскільки кожен наступний блок включає хеш попереднього. Використання інших даних призводить до суттєвої зміни цього рядка. Алгоритм виключає можливість скасування транзакції без зміни всіх наступних блоків.

За підтвердження транзакцій і перевірку всіх даних блокчейна відповідає алгоритм консенсусу, у якому беруть участь члени мережі – ноди. Найпопулярнішими алгоритмами консенсусу є вже згаданий Proof-of-Work (використовується в біткоїні) і Proof-of-Stake.

Щоб підтвердити транзакції, вузли витрачають обчислювальну потужність або блокують власні кошти, які виступають гарантією достовірності даних. Після додавання нового блоку вже неможливо повторно витратити кошти, витрачені на поточному етапі. У процесі досягнення алгоритму його учасники отримують нові криптовалюти (як у PoW, так і в PoS). Таким чином, ці механізми слугують способом емісії нової криптовалюти.

Блокчейн-адреси, де зберігаються криптовалюти, побудовані на базі двох ключів – публічного і приватного. Перший використовується для «відкритої» частини адреси, другий – для підпису транзакцій і доступу до адреси. Закритий ключ призначений тільки для власника адреси. Наявні комп'ютерні потужності не дають змоги зламати блокчейн-адресу, зокрема «вгадати» приватний ключ методом підбору. Створювати блокчейн-адреси та керувати ними можна в спеціальному додатку – гаманці.

Щоб перевести криптовалюту, користувач відправляє в мережу «доручення», яке містить інформацію про суму переказу та адресата. Дані переказу автоматично верифікуються електронним підписом за допомогою приватного ключа. Після потрапляння повідомлення в мережу воно включається в один із наступних блоків, який «добувають» ноди блокчейна. Будь-яка нода може перевірити підпис кожного переказу, використовуючи публічний ключ. Такий алгоритм гарантує збереження коштів і неможливість здійснення транзакцій третіми особами.

Після додавання блоку в ланцюжок усі його транзакції вважаються підтвердженими і незворотними. Верифікація всіх транзакцій, зокрема минулих, відбувається кожен цикл досягнення консенсусу мережі. Недостовірні дані можуть потрапити в блокчейн, тільки якщо зловмисник зможе розшифрувати хеш блоків або контролюватиме істотну частку всіх нод мережі.

Залежно від особливостей і характеристик альткоїнів, їх можна розділити на безліч різних груп. Але існує три напрямки, які мають сильні відмінності в самій базовій концепції:

- інноваційні технології;
- стабільні активи;
- анонімні монети.

Такі монети володіють технологіями, яких немає у біткоїна.

Яскравий приклад – проєкт Ethereum (ETH), у якого є власний блокчейн, що має ширші функції. Він забезпечує можливість створення токенів (нових криптоактивів на базі блокчейну Ethereum), а також дає змогу використовувати смарт-контракти.

Стейблкоїни – це стабільні криптомонети. Їх активно використовують трейдери для хеджування ризиків. Такі активи називають «цифровими притулками», оскільки вони захищають капітал від сильної зміни ціни. Наприклад, у біткоїна проблема високої волатильності залишається невирішеною.

Анонімні – це конфіденційні альткоїни, що добре підходять користувачам, які бажають приховати інформацію про свої активи і транзакції. Під час операцій з анонімними криптовалютами буде складно отримати дані про рух коштів між різними гаманцями. Приклади – Monero, ZCash, Dash, Grin.

Створення Ethereum: крім того, що блокчейн Ethereum уможливив використання смарт-контрактів, він виділяється і за рахунок інших переваг:

- підвищена швидкість операцій;
- більш стабільна робота (ніж у BTC);
- програмні рішення, що дають змогу створювати різні децентралізовані додатки.

Під час створення блокчейна розробники ухвалюють рішення про те, якою буде токеноміка проєкту. Розподіл початкового випуску монет між користувачами визначається розробникам. Зазвичай частина активів залишається команді проєкту. Кошти резервуються на рекламу розробку і розвиток проєкту. Частина монет використовуються для залучення інвестицій. Їх можуть купити великі інвестори в рамках одного або декількох раундів. Багато проєктів використовують публічний токенсейл для продажу віртуальних активів усім охочим. В інших випадках практикують розподіл монет між активними користувачами – аїдроп. На вартість криптовалюти впливає халвінг. Механізм використовується в криптовалютах, які виплачують фіксовану винагороду за блок. На ціну криптовалюти впливає спалювання монет. Останнє передбачає виведення з обігу деякого обсягу активів. Основним

показником затребуваності віртуального активу є ринкова капіталізація. Остання дорівнює добутку обсягу монет, що перебувають в обігу, на вартість одиниці.

Що більше уваги привертається до технології блокчейн, то досконалішою вона стає. Розробники ставлять перед собою нові завдання і знаходять способи вирішити їх. Підсумок – збагачення криптосегмента новими проектами зі стабільнішими, зручнішими та гнучкішими функціями. Популяризація цифрових грошей призводить до їх активного використання в усьому світі як платіжного засобу, способу заробітку або інструменту збереження капіталу. Популярність криптогрошей мотивує держави створювати власні цифрові національні валюти. З їхньою допомогою все, що стосується платежів і переказів, буде максимально спрощено і прискорено.

Криптовалюта – це цифрові гроші, засновані на технології блокчейн. Немає єдиного органу, як-от центральний банк, що контролює її випуск і вартість. Натомість це лягає на плечі користувачів блокчейну.

Першою криптовалютою став біткоїн. Його створила людина чи група людей під псевдонімом Сатоші Накамото. Досі невідомо, хто ховається за цим ім'ям.

Криптовалюта має як переваги, так і недоліки. Плюсами криптовалюти є швидкі транзакції, відсутність посередників і можливість пересилати гроші через кордони. Мінусами вважається те, що крипту часто використовують для відмивання грошей тощо.

У світі багато компаній, що приймають криптовалюту. Наприклад, Shopify, Microsoft, WordPress та інші. В Україні використати цифрові монети можна, щоб оплатити покупки у «Фокстроті» та послуги компанії Civilly або зробити пожертву в офіційний криптовалютний фонд Aid For Ukraine. В останньому випадку кошти підуть на боротьбу з російськими загарбниками.

Якщо ви володієте криптою, то відповідаєте за її зберігання. Якщо ви новачок, найпростіше зберігати її на біржі. Але в такому випадку ви можете втратити свої інвестиції, якщо з біржею щось трапиться. Найбезпечніший спосіб – зберігати крипту на «холодному» гаманці.

Ні в якому разі не можна передавати свої ключі від гаманця іншим особам. Ще не варто висилати крипту людям, які обіцяють великі заробітки. Так ви вбережете себе від шахраїв.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Головна сторінка багатомовного порталу Вікіпедії [Електронний ресурс]. – Режим доступу: <https://ru.wikipedia.org/wiki/>

2. Когут Ю.І. Технології блокчейн та криптовалюта: ризики та кібербезпека. – К. : Сідкойн. 2022. – 316 с.
3. Антонопулос А. The Internet of Money [Електроний ресурс]. – Режим доступу: <https://nashformat.ua/products/>
4. Головна сторінка Forklog [Електроний ресурс]. – Режим доступу: <https://forklog.com/cryptorium/chto-takoe-kriptoalyuta-prostymi-slovami>