Державний університет «Житомирська політехніка»

ЛЕКЦІЯ 3

ВИДИ КРИПТОВАЛЮТ та МЕХАНІЗМИ КОНСЕНСУСУ

2024

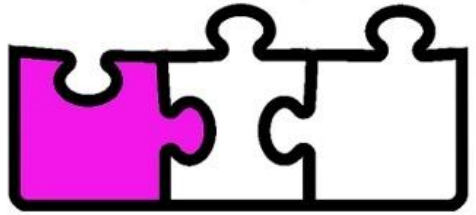
к.т.н., доц. Лобанчикова Надія

1. Надходження інформації

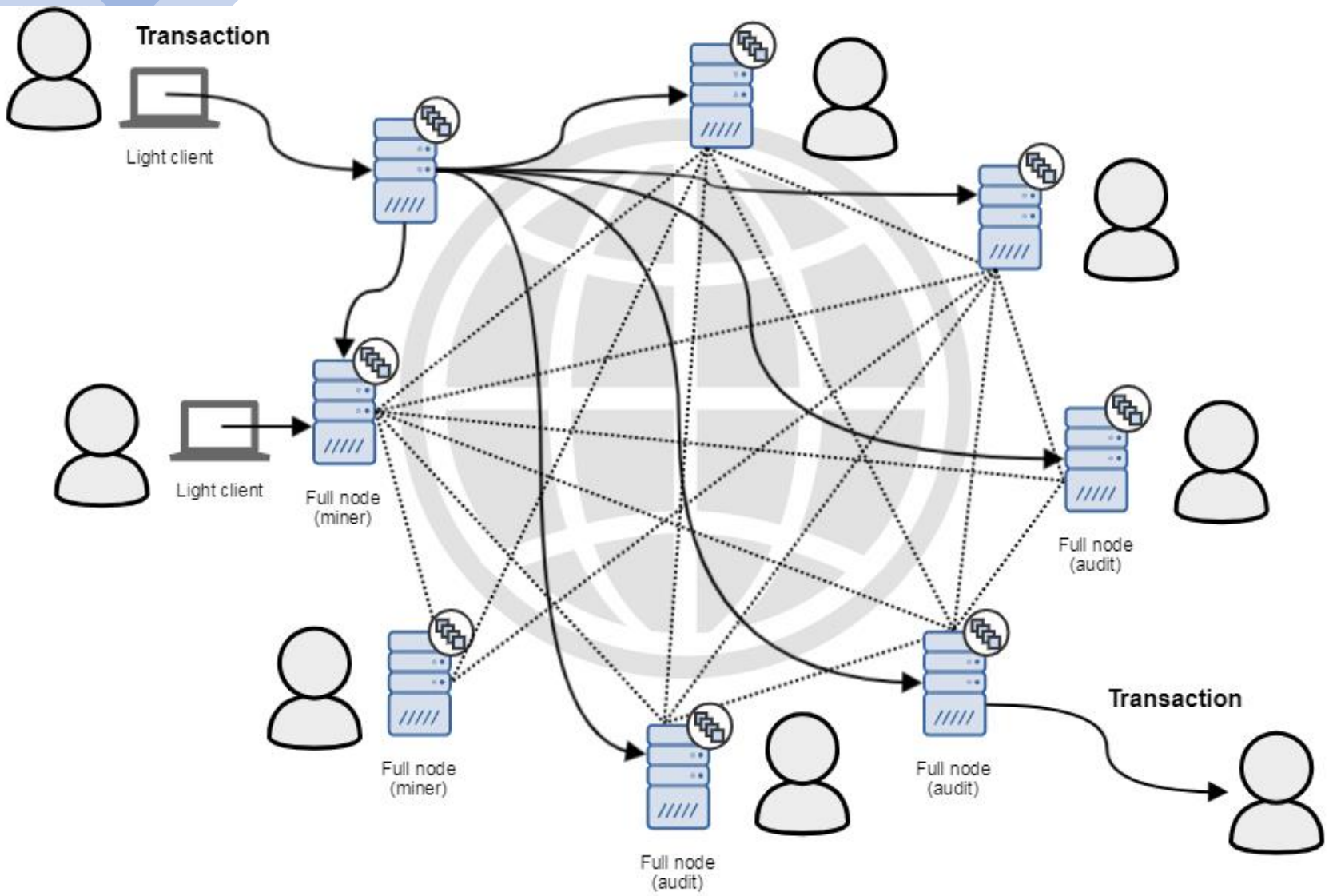
2. Перевірка та підтвердження інформації

3. Створення блоку

4. Приєднання нового блоку до ланцюга

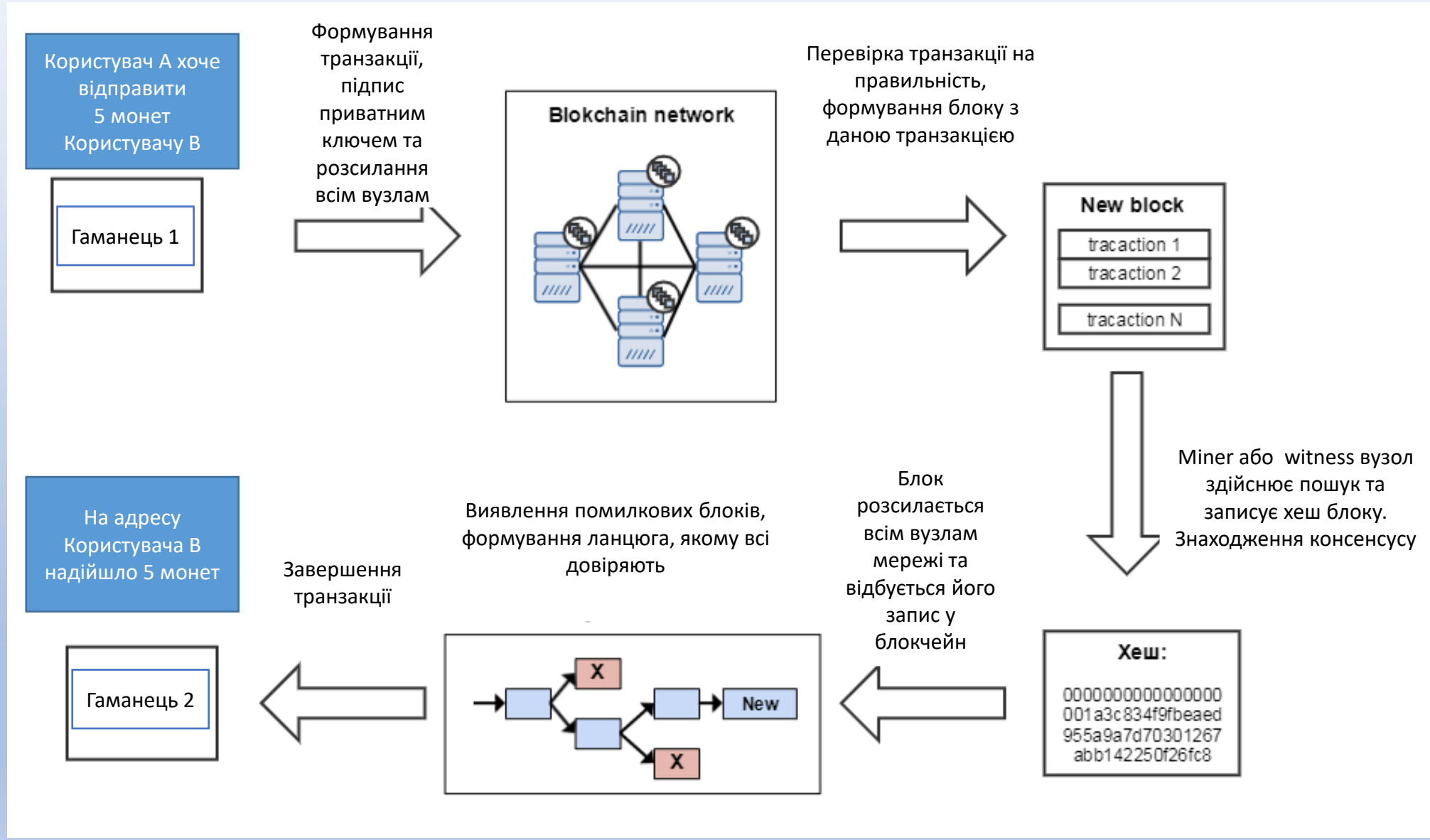


Архітектура мережі:



Кожен учасник може запустити свою ноду з повною копією блокчейну (full node).
Повні ноди, які можуть записувати транзакції в блокчейн, називаються **вузлами консенсусу** (witness) або майнерами (miner).
Повні ноди, які лише перевіряють правильність транзакцій, називаються **вузлами аудиту** (audit).
Легкі клієнти (light clients) не зберігають повних копій блокчейна, а взаємодіють із мережею, використовуючи повні ноди.
Більшість користувачів для транзакцій використовують саме легких клієнтів або web гаманці. Усі ноди пов'язані друг з одним. При такому наборі елементів архітектура мережі стає більш стійкою.

Життєвий цикл транзакції



```
Private key: 0a78194a8a893b8baac7c09b6a4a4b4b161b2f80a126cbb79bde231a4567420f
Public key: 0579b478952214d7cddac32ac9dc522c821a4489bc10aac3a81b9d1cd7a92e57ba
Address: 0x3814JnJpGnt5tB2GD1qfKP709W3KbRdfb27V
```

```
From: 0x48C89c341C5960Ca2Bf3732D6D8a0F4f89Cc4368
To: 0x367adb7894334678b90afe7882a5b06f7fbc783a -
```

Цифрова адреса відправника

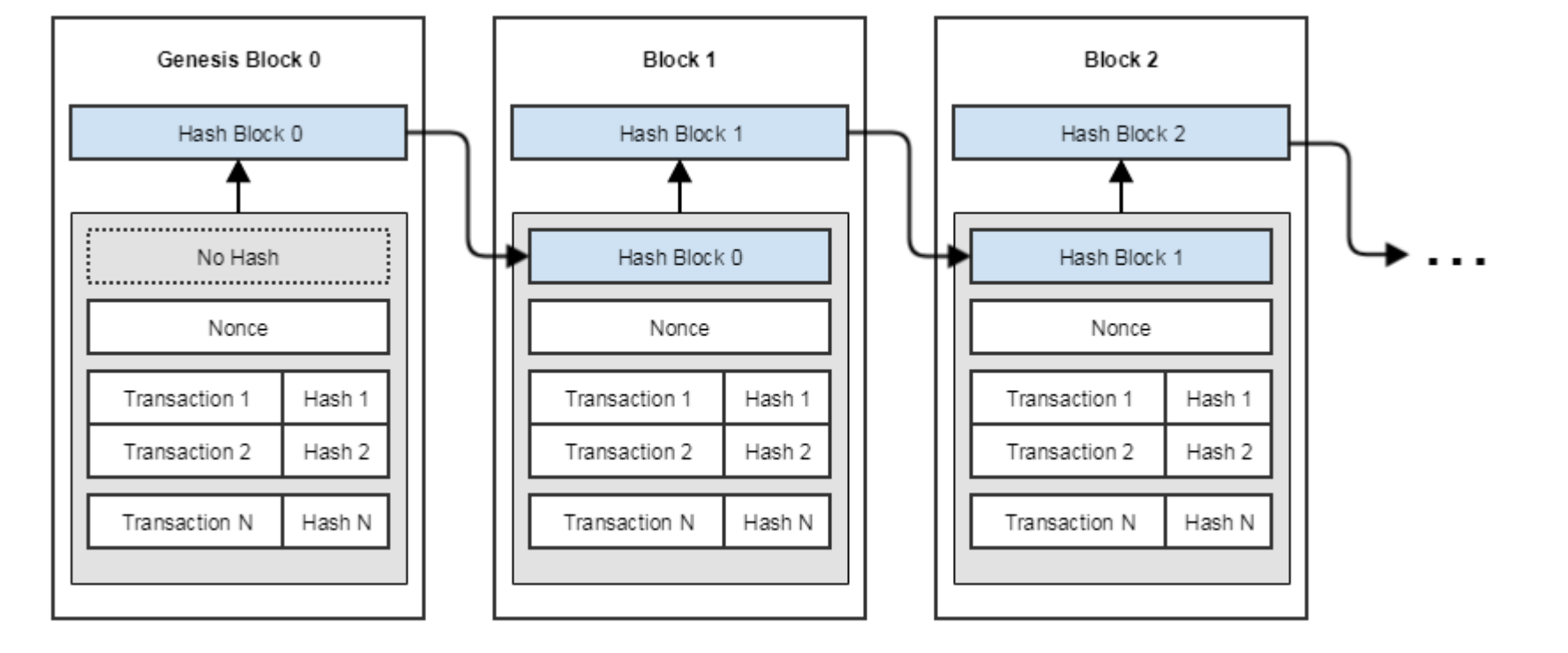
Цифрова адреса отримувача

```
Value: 0.0001
```

Сума транзакції

```
Transaction Hash: 0x617ede331e8a99f46a363b32b239542bb4006e4fa9a2727a6636ffe3eb095cef
```

Хеш транзакції


Genesis Block 0
Hash Block 0
No Hash
Nonce
Transaction 1
Hash 1
Transaction 2
Hash 2
Transaction N
Hash N
Block 1
Hash Block 1
Hash Block 0
Nonce
Transaction 1
Hash 1
Transaction 2
Hash 2
Transaction N
Hash N
Block 2
Hash Block 2
Hash Block 1
Nonce
Transaction 1
Hash 1
Transaction 2
Hash 2
Transaction N
Hash N
...

1.ТИПИ КОНСЕНСУС-МЕХАНІЗМІВ БЛОКЧЕЙНУ

Консенсус блокчейна - це процедура, в ході якої учасники мережі досягають згоди про поточний стан даних у мережі. Завдяки цьому алгоритми консенсусу встановлюють надійність і довіру до мережі.

Основні висновки:

Механізми консенсусу (також відомі як протоколи консенсусу або алгоритми консенсусу) використовуються для перевірки транзакцій та підтримки безпеки блокчейн.

Існує безліч різних типів механізмів консенсусу, кожен з яких має свої переваги та недоліки

Механізми Proof-of-Work (PoW) і Proof-of-Stake (PoS) - два механізми консенсусу, що найбільш широко використовуються.

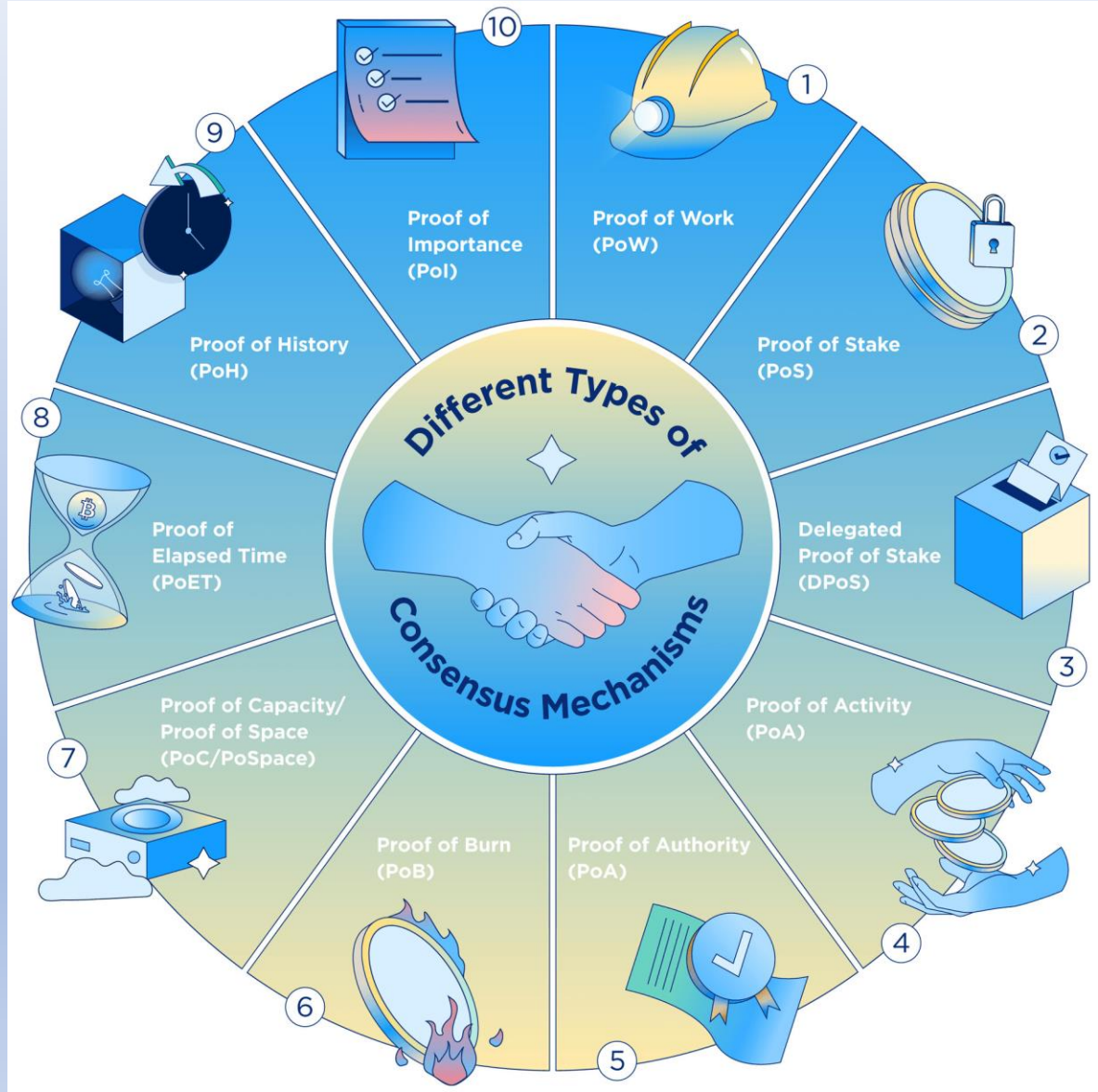
Механізми консенсусу становлять основу всіх криптовалютних блокчейнів та забезпечують їхню безпеку.

- Блокчейн - це децентралізована, розподілена і найчастіше публічна цифрова база даних, яка використовується для запису транзакцій. Кожна така транзакція записується у вигляді блоку даних, який повинен бути незалежно перевірений одноранговими комп'ютерними мережами, перш ніж його можна буде додати в ланцюжок. Ця система допомагає захистити блокчейн від шахрайських дій та вирішує проблему "подвійних витрат".

Для того щоб гарантувати, що всі учасники мережі блокчейн згодні з однією версією історії, мережі блокчейн, такі як Bitcoin і Ethereum, реалізують так звані механізми консенсусу (також відомі як протоколи консенсусу або алгоритми консенсусу). Ці механізми спрямовані на те, щоб зробити систему стійкою до відмови.

Консенсус - це процес, під час якого група рівних нод (вузлів) у мережі визначає, які транзакції в блокчейні дійсні, а які ні. Механізми консенсусу – це методики, що використовуються для досягнення цієї згоди. Саме ці набори правил допомагають захистити мережу від зловмисної поведінки та атак хакерів.

Існує безліч різних типів механізмів консенсусу, залежно від блокчейну та його застосування. Хоча вони відрізняються за енергоспоживанням, безпекою та масштабованістю, всі вони мають одну мету: забезпечити достовірність і чесність записів.



Proof-of-Work (PoW)

Використовується в Bitcoin, EthereumPoW та багатьох інших публічних блокчейнах. Доказ роботи (PoW) був першим створеним механізмом консенсусу. Він вважається найнадійнішим і найбезпечнішим з усіх механізмів консенсусу, незважаючи на існуючі побоювання з приводу масштабованості. Хоча термін "Proof-of-Work" був уперше введений на початку 1990-х років, саме засновник Біткойна Сатоші Накамото вперше застосував цю технологію у контексті цифрових валют.

У PoW майнери по суті змагаються один з одним у вирішенні надзвичайно складних обчислювальних головоломок за допомогою потужних комп'ютерів. Той, хто першим вигадає 64-значне шістнадцяткове число ("хеш"), отримує право на формування нового блоку та підтвердження транзакцій. Успішний майнер також отримує винагороду у вигляді наперед визначеної суми криптовалюти, відомої як "винагорода за блок".

Оскільки для генерації нових блоків потрібна велика кількість обчислювальних ресурсів та енергії, операційні витрати PoW, як відомо, високі. Це є бар'єром на шляху нових майнерів, що призводить до побоювань щодо централізації та обмежень масштабованості.

Найбільш поширеною критикою PoW є вплив споживання електроенергії на довкілля. Це змусило багатьох шукати стійкіші, енергоефективні протоколи консенсусу.

Proof of Stake (PoS)

Доказ ставки, як випливає з назви, цей популярний метод консенсусу ґрунтується на процесі, відомому як "стейкінг". У системі доказу ставки (PoS) майнери повинні внести свою "ставку" цифрової валюти, щоб отримати шанс бути випадково обраним як валідатор. Процес не схожий на лотерею, де чим більше монет ви ставите, тим вищі ваші шанси.

На відміну від PoW, де майнери стимулюються винагородою за блок (ново створені монети), ті, хто робить свій внесок у систему PoS, просто отримують комісію за транзакцію.

PoS розглядається як більш стійка та екологічна альтернатива PoW, а також як більш захищена від 51% атак. Однак оскільки система віддає перевагу організаціям з великою кількістю токенів, PoS викликала критику за те, що вона може призвести до централізації. До відомих платформ PoS відносяться Ethereum (після оновлення Merge), Cardano (ADA), Solana (SOL) та Tezos (XTC).

Delegated Proof-of-Stake (DPoS)

Модифікація механізму консенсусу PoS, делегований доказ частки (DPoS) спирається на систему голосування на основі репутації для досягнення консенсусу. Користувачі мережі "голосують" за вибір "свідків" (також відомих як "виробники блоків") для забезпечення безпеки мережі від їхнього імені. Тільки свідки вищого рівня (набрали найбільшу кількість голосів) отримують право підтверджувати транзакції у блокчейні.

Щоб проголосувати, користувачі додають свої токени в стейкінг пул. Потім голоси зважуються залежно від розміру частки кожного учасника голосування - що більше в нього монет у стейкінгу, то більше вписувалося право голосу. Вибрані свідки, які успішно підтвердили транзакції в блоці, одержують винагороду, яка зазвичай ділиться з тими, хто за них голосував.

Свідки вищого рівня завжди мають ризик бути заміненими тими, хто вважається більш надійним і, отже, отримує більше голосів. Вони навіть можуть бути виключені зі списку, якщо не справляються зі своїми обов'язками або намагаються підтвердити шахрайські транзакції. Це стимулює свідків завжди залишатися чесними, забезпечуючи цілісність блокчейну.

Хоча DPoS менш поширений, ніж PoS, багато хто вважає його більш ефективним, демократичним та фінансово всеосяжним, ніж його попередник. Її використовують Lisk (LSK), EOS.IO (EOS), Steem (STEEM), BitShares (BTS) та Ark (ARK).

Proof-of-Action (PoA)

Доказ активності (PoA) – це гібрид механізмів консенсусу PoW та PoS. Він використовується в блокчейн-проектах Decred (DCR) та Espers (ESP).

У системах PoA процес майнінгу починається, як і в PoW, коли майнери змагаються у вирішенні складного математичного завдання, використовуючи величезні обчислювальні потужності. Однак після того, як блок видобуто, система перемикається на PoS, при цьому успішно згенерований заголовок блоку транслюється в мережу PoA. Потім випадково вибирається група валідаторів, які підписують хеш, підтверджуючи новий блок. Як і в PoS, що більше монет у валідатора, то вищі його шанси бути обраним. Після того, як кожен обраний валідатор підписав блок, він додається до мережі та готовий до реєстрації транзакцій. Винагорода за блок ділиться між майнером та валідаторами.

Хоча система PoA була розроблена з наміром об'єднати найкращі риси PoW і PoS, уникаючи при цьому їхніх недоліків, вона викликала критику за енергоємний етап майнінгу та притаманну їй упередженість до валідаторів, які мають велику кількість монет.

Proof-of-Authority (PoA)

Не плутати з доказом активності (також "PoA"), доказ репутації (PoA) працює шляхом вибору своїх валідаторів на основі репутації. Модифікована версія PoS була запропонована співзасновником Ethereum та колишнім технічним директором Гевіном Вудом у 2017 році.

У PoA валідатори не роблять блокування своїх монет у стейкінгу. Натомість вони мають поставити на кон свою репутацію за право підтверджувати блоки. Це дуже відрізняється від більшості протоколів блокчейну, які зазвичай не вимагають розкриття особистості для участі.

Оскільки цей механізм практично не потребує обчислювальної потужності, він набагато менш ресурсомісткий, ніж деякі його попередники, зокрема PoW. Він також є одним з менш витратних варіантів, що робить його найкращим рішенням для приватних мереж, таких як JP Morgan (JPMCoin). Інші проекти на основі PoA включають VeChain (VET) та тестову мережу Ethereum Kovan.

Незважаючи на високу масштабованість, слабке місце в цьому проекті знаходиться в області децентралізації, оскільки в мережі можуть брати участь лише обрані. Крім того, вимога до валідаторів бути ідентифікованими також підвищує ризик корупції та маніпуляцій з боку третіх осіб.

Proof of Burn (PoB)

Іншою більш стійкою альтернативою алгоритму PoW Біткойна є доказ спалювання (PoB). У PoB майнери отримують право видобувати блок, "спалюючи" (знищуючи) заздалегідь певну кількість токенів у спосіб, що перевіряється - а саме, відправляючи їх на "адресу спалювача", де їх не можна відновити або витратити. Чим більше монет спалено, тим більше шансів бути обраним випадковим чином.

На відміну від PoS, де майнери можуть отримати або продати свої заблоковані монети, якщо вони колись покинуть мережу, спалені монети втрачаються безповоротно. Цей метод, який вимагає від майнерів жертвувати короткостроковим багатством, щоб отримати довічний привілей на створення нових блоків, допомагає стимулювати довгострокову відданість майнерів. Акт спалювання монет також призводить до їхнього дефіциту, обмежуючи інфляцію та підвищуючи попит.

Криптовалюти, що використовують протокол доказу спалювання, включають Slimcoin (SLM), Counterparty (XCP) та Factom (FCT).

Proof of Capacity / Proof of Space (PoC / PoSpace)

На відміну від більшості своїх попередників, які надають права на майнінг на основі обчислювальної потужності або кількості монет, доказ потужності (PoC) – також відомий як доказ простору (PoSpace) – засновує свій алгоритм майнінгу на кількості вільного місця на жорсткому диску майнера.

У PoC майнери заздалегідь генерують список всіх можливих хешів у процесі, що називається "плануванням". Потім ці схеми зберігаються на твердому диску. Чим більший обсяг пам'яті у майнера, тим більше можливих рішень. Чим більше рішень, тим вищі шанси отримати правильну комбінацію хешів та виграти винагороду.

Оскільки PoC не вимагає дорогого чи спеціалізованого обладнання, він відкриває можливості для участі у мережі звичайній людині. Таким чином, він є менш енергоємним і більш децентралізованою альтернативою деяким більш поширеним механізмам консенсусу, що розглядаються в цьому посібнику. Однак поки не так багато розробників вирішили використовувати цю систему, і є побоювання, що вона піддається атакам шкідливих програм. В даний час цей механізм використовується в Signum (SIGNA) – раніше Burstcoin (BURST), Storj (STORJ) та Chia (XCH).

Proof-of-Elapsed Time (PoET)

Доказ часу, що минув, використовується в блокчейн-мережах з допуском (тих, які вимагають від учасників ідентифікувати себе). PoET використовує довірені обчислення для забезпечення випадкового часу очікування під час створення блоку. Вона була розроблена компанією Intel на початку 2016 року і заснована на спеціальному наборі інструкцій процесора, що називається Intel Software Guard Extensions (SGX).

Алгоритм консенсусу на основі лотереї часу PoET працює шляхом випадкового призначення різного часу очікування для кожного вузла в мережі. Під час періоду очікування кожен із цих вузлів переходить у "сплячий режим" на певний час. Перший, хто прокинувся (тобто той, у кого найменший час очікування) отримує право на видобуток. Така рандомізація гарантує, що кожен учасник має рівні шанси стати переможцем, забезпечуючи справедливість у мережі.

Механізм консенсусу PoET є високоефективним, менш ресурсомістким та масштабованим. Він був реалізований у системі Sawtooth компанії Hyperledger.

Proof-of-History (PoH)

Як випливає із назви, доказ історії (PoH) забезпечує доказ історичних подій. Розроблений компанією Solana Labs (SOL), PoH дозволяє вбудовувати "тимчасові мітки" в блокчейн, перевіряючи проходження часу між транзакціями без необхідності покладатися на інші вузли.

Цей метод тимчасових міток забезпечується так званою функцією затримки, що верифікується (verifiable delay function, VDF) SHA-256 з послідовним хешуванням. Вона працює, приймаючи результат транзакції і використовуючи його як вхідні дані для наступного хеша, що дозволяє всім чітко бачити, яка подія сталася в певній послідовності. Оскільки VDF можуть бути вирішені лише одним процесорним рахунком, PoH значно знижує обчислювальну вагу блокчейна, роблячи його швидшим та енергоефективнішим, ніж багато його сучасників.

Оскільки PoH використовується тільки в Solana, його ще доведеться протестувати у великих масштабах.

Proof-of-Importance (PoI)

Вперше з'явилася в NEM (XEM), доказ важливості (PoI) вибирає своїх майнерів на основі певних критеріїв у процесі, який називається "збирання врожаю". Загальні вимоги включають кількість та розмір транзакцій за останні 30 днів, кількість заблокованих монет та активність мережі. На основі цих факторів вузлам надається бал важливості. Чим вищий цей показник, тим вища ймовірність того, що його оберуть для створення блоку та отримання супутньої комісії за транзакцію.

Незважаючи на схожість з PoS, використання додаткових показників у PoI дозволяє відмовитися від притаманної першому варіанту тенденції винагороджувати багатих, зважаючи на загальну підтримку мережі учасниками. Таким чином, висока ставка в POI не обов'язково гарантує виграш блоку.

Внутрішня валюта додатків

Щоб централізований додаток зберігав працездатність протягом тривалого часу, його власнику потрібно якось отримувати прибуток. ДД не мають власника, але все одно вузли ДД потребують обладнання та мережевих ресурсів для підтримки роботи. Тобто вузли ДД мають приносити якусь вигоду в обмін на зусилля щодо підтримки їхньої працездатності. Саме тут входить у гру внутрішня валюта. Більшість ДД мають вбудовану внутрішню валюту. Точніше, більшість успішних ДД мають вбудовану внутрішню валюту.

Внутрішня валюта додатків

- Протокол консенсусу визначає, скільки валюти отримує вузол.
- Ті вузли, які сприяють підтримці та управлінню ДД, заробляють валюту.
- Вузли, які лише зчитують дані, нічого не отримують.

все, що має достатній попит та недостатню кількість, має цінність.

Чим більше користувачів використовують ДД, тим більше попит на валюту і тим вищою вона цінується.

Встановлення фіксованого обсягу валюти , що випускається , призводить до її нестачі і підвищує вартість. Зазвичай валюта вводиться в обіг поступово, щоб вузли, що знову підключилися, теж мали можливість заробити.

Недоліки внутрішньої валюти

- ДД не може бути безкоштовним для всіх.

ДД з контрольованм доступом(КДП) потрібно отримати дозвіл на підключення до мережі, який залежить від додатку.

Оскільки вам потрібний дозвіл, протокол консенсусу відкритої програми може погано працювати у разі ДД з контрольованим доступом. Тому ДД з контрольованим доступом використовують інші протоколи консенсусу. Крім того, ці додатки не мають внутрішньої валюти.

Види популярних криптовалют

>>7000

Популярні криптовалюти

Bitcoin

Біткойн – це децентралізована валюта та децентралізований додаток. Регістр – список транзакцій. В регистр ми можемо тільки додавати нову транзакцію (в БД ми можемо додавати записи, модифікувати дані та видаляти записи). БД може виконувати роль регістра.

Ось кілька причин, з яких люди використовують мережу Bitcoin :

- ✓ основна вигода від використання біткойну - це простий і швидкий спосіб виконувати платежі по всьому світу;
- ✓ вартість звичайного банківського переказу вища порівняно з транзакцією в мережі Bitcoin ;
- ✓ хакери можуть вкрасти вашу платіжну інформацію у оператора звичайної платіжної системи, але розкрадання платіжних адрес Bitcoin абсолютно марно, тому що транзакція стає дійсною тільки в тому випадку, якщо підписано вашим закритим ключем, який немає необхідності кудись передавати, щоб зробити платіж.

Популярні криптовалюти

Bitcoin

Найпопулярніша криптовалюта була створена наприкінці 2008-го – на початку 2009-го років. Наразі капіталізація біткоїну перевищила $441 млрд., що набагато більше, ніж інші види віртуальних грошей. Ціна 1 btc подолала планку $24-25 тис. (був і по 35 тис.), що стало черговим досягненням цифрової валюти. Природно, саме біткоїн виступає як основний об'єкт інтересу з боку потенційних інвесторів та предметом торгів на різних криптовалютних біржах.
При цьому дуже важливо розуміти, що фінансові аналітики щодо прогнозів та перспектив подальшого зростання курсу біткоїну далеко не одностайні. Частина експертів прогнозує збереження вражаючої динаміки цього виду криптовалюти. Однак деякі фахівці передбачають повну протилежність такому розвитку подій, пророкуючи швидке падіння біткоїну.

Ethereum

Друга за популярністю та розміром капіталізації криптовалюта світу. Незважаючи на порівняно невеликий вік, обсяг торгів ефіріумом або ефіром, як часто називають цей вид цифрових грошей російською мовою, досяг на даний момент $206 млрд., набагато перевершуючи решту криптовалют, за винятком біткоїну. Платіжну систему Ethereum було запущено в середині 2015 року. За два з невеликим роки криптовалюта змогла впевнено вийти на друге місце, у деяких сегментах складаючи впевнену конкуренцію ще биткоіну, який нещодавно здавався недосяжним. Деякі фахівці саме ефір вважають найперспективнішим видом віртуальних грошей.

Ethereum - це децентралізована платформа, на якій можна запускати програми у вигляді смарт-контрактів (smart contract , розумний контракт). Програма може складатися з одного або кількох смарт-контрактів. Смарт-контракт Ethereum - це програма, яка виконується в мережі Ethereum і працює виключно так, як запрограмовано, без ризику простою, цензури, шахрайства та втручання третьої сторони. Головна перевага Ethereum для виконання смарт-контрактів полягає в тому, що контракти можуть легко взаємодіяти один з одним. Більше того, вам не треба турбуватися про інтеграцію протоколу консенсусу та інші речі — навпаки, вам лише потрібно написати логіку прикладу

Litecoin

Лайткоїн є похідною (фахівці з криптовалют використовують спеціальний термін - форк) біткоїну. Найпопулярнішу цифрову валюту часто називають віртуальним золотом, а лайткоїн за аналогією називають віртуальним сріблом. Він з'явився у 2011-му році, швидко набираючи популярності та капіталізації. Однак, сьогодні лайткоїн з обігу торгів займає лише 14-е місце, що не заважає експертам відносити його до перспективних криптовалют.

Bitcoin Cash

Цей вид віртуальних грошей з'явився – 1 серпня 2018 року. Фактично він є форком биткоина, отриманий в результаті введення нових правил блокчейна останнього. Bitcoin Cash (прийняті сьогодні скорочення - BCash , BCC і BCH) має спільну з біткоіном історію, але в даний час торгується самостійно. За чотири неповні місяці капіталізація нової цифрової валюти склала майже $27 млрд., що є одним із найістотніших приростів за такий короткий проміжок часу. В даний час за обсягом капіталізації BCash утримує 28 місце серед усіх криптовалют і капіталізація складає трохи більше $2,5 млрд

Monero

Головною особливістю криптовалюти є найбільший із існуючих сьогодні рівень анонімності платіжної системи. Монеро було створено на основі оригінального протоколу CryptoNote навесні 2014 року. В даний час цей вид віртуальних грошей не входить до топ-10 з капіталізації. Проте відсутність криптовалюти в основних рейтингах знижує інтерес до неї, що дозволяє заробити на майнінгу навіть за допомогою звичайного комп'ютера, що давно неможливо зробити, видобуваючи популярніші види цифрових валют.

Dash

Криптовалюта була випущена на початку 2014 року під назво
Xcoin . Весною 2015-го року вона стала називатися Dash . Майже відразу після появи цей вид віртуальних грошей став мати серйозний попит. Багато в чому він обумовлений наявністю деяких характерних особливостей, головною з яких є прийняття рішень щодо подальшого розвитку системи шляхом волевиявлення всіх членів мережі. Такого рівня децентралізації до появи Dash ще не було. Величина капіталізації становить майже $804 млн., що ставить криптовалюту на 66-те місце за цим показником.

Zcash

Цей вид цифрової валюти з'явився приблизно рік тому – восени 2016 року. Практично відразу ж Zcash (коротка назва - ZEC) став мати ажіотажний попит, що дозволило йому на короткий час навіть увійти в топ-5 криптовалют з капіталізації. Однак, через якийсь час ціна цілком передбачувано дещо впала. Принцип роботи платіжної системи робить практично неможливим відстеження та контроль фінансових операцій, що здійснюються з використанням ZCash .

Рівень капіталізації $817 млн., 67 місце у рейтингу.

BitShares

MaidSafeCoin

VertCoin

Factom

DigiByte

NEM (XEM)

Dogecoin

Nautiluscoin

Clams

Список Спостереження | Портфель | Криптовалюти | Категорії | DeFi | NFT | Metaverse | Polkadot | BNB Chain | Solana | Avalanche | Показати рядки 100 | Фільтри | Налаштува

#	Ім'я	Ціна	1h %	24h %	7d %	Ринкова Капіталізація	Обсяг(24г)	Циркуляційний Запас	Останні 7 днів
1	Bitcoin BTC	€22,868.90	0.14%	1.72%	10.23%	€441,286,665,917	€26,784,992,173 1,174,323 BTC	19,296,368 BTC	
2	Ethereum ETH	€1,576.96	0.14%	1.31%	9.29%	€192,979,185,723	€7,215,974,884 4,588,979 ETH	122,373,866 ETH	
3	Tether USDT	€0.9364	0.16%	0.71%	1.57%	€65,925,039,881	€40,653,224,560 43,414,648,465 USDT	70,403,206,011 USDT	
4	BNB BNB	€296.31	0.11%	0.31%	0.12%	€46,786,762,232	€507,844,550 1,717,538 BNB	157,897,342 BNB	
5	USD Coin USDC Купити	€0.9363	0.16%	0.70%	1.56%	€39,201,696,235	€3,161,523,978 3,377,000,133 USDC	41,869,724,943 USDC	
6	XRP XRP Купити	€0.3632	0.07%	1.59%	2.59%	€18,451,771,922	€802,902,558 2,212,360,574 XRP	50,799,084,881 XRP	
7	Cardano ADA	€0.376	0.46%	0.95%	9.11%	€13,026,308,732	€350,142,196 936,947,492 ADA	34,646,666,662 ADA	

8°C Bewolkt

Поиск

УКР

05:02
20/02/2023