Тема 1. Технології блокчейн

[1 Історія цифрових фінансових систем та еволюція технології Блокчейн 2](#_Toc49857439)

[1.1 Цифрові фінансові системи 2](#_Toc49857440)

[1.2 Історія Блокчейн систем 2](#_Toc49857441)

[2.1 Поняття розподіленої системи 4](#_Toc49857442)

[2.2 Поняття блокчейн системи 4](#_Toc49857443)

[2.2.1 Цілісність даних в блокчейн системах (геш-функції) 6](#_Toc49857444)

[2.2.2 Підписання даних (асиметрична криптографія) 8](#_Toc49857445)

[2.3 Класифікація блокчейн систем 10](#_Toc49857446)

[2.3.1 Інклюзивний (permissionless) блокчейн 10](#_Toc49857447)

[2.3.2 Ексклюзивний (permissioned) блокчейн 11](#_Toc49857448)

[2.3.3 Публічний (public blockchain) блокчейн 12](#_Toc49857449)

[2.3.4 Блокчейн, що належить консорціуму (consortium blockchains) 13](#_Toc49857450)

[2.3.5 Приватний блокчейн (fully private blockchains) 13](#_Toc49857451)

[2.4 Питання конфіденційності даних і безпеки транзакцій 13](#_Toc49857452)

1 Історія цифрових фінансових систем та еволюція технології Блокчейн

* 1. Цифрові фінансові системи

*Слайд 5.*

Дослідження цифрових грошей відносяться до початку 1980-х років [D. Chaum, “Blind signatures for untraceable payments,” in Advances in cryptology, pp. 199–203, Springer, 1983.]. У 1990 році електронна готівкова корпорація DigiCash Inc. зробила первинну спробу створення криптовалютної системи [D. Chaum, A. Fiat, and M. Naor, “Untraceable electronic cash,” in Proceedings on Advances in cryptology, pp. 319–327, Springer-Verlag New York, Inc., 1990.]. У транзакціях DigiCash були задіяні криптографічні протоколи та спрямовані на забезпечення його користувачів анонімністю. Однак у 2000 році проект потерпів невдачу, незважаючи на те, що спочатку був привабливим. Девід Чаум, його засновник, вважав, що нездатність DigiCash досягти успіху була пов'язана з його технологією, яка передувала дозріванню електронної комерції в Інтернеті. Іншими причинами, які призвели до його невдачі, були співпраця банків з обробкою транзакції, завдяки чому DigiCash була централізованою системою.

У 1998 році Вей Дай запропонував децентралізовану цифрову систему готівкових грошей, b-money [W. Dai, “b-money.” http://www.weidai.com/bmoney.txt, 1998.]. B-money – це анонімна та розподілена система цифрових коштів, яка спрямована на забезпечення транзакцій, що неможливо відстежити. Однією з головних переваг цієї системи було те, що вона виключала потребу в центральній владі. Однак, b-money були лише початковою та неповною ідеєю. B-money не вирішувала належним чином деякі ключові питання, включаючи можливості подвійних витрат.

На початку 2000 року Digital Gold Currency (DGC), валюта, підкріплена золотом, набула деякої популярності. DGC вважається цифровою валютою другого покоління. Її випускають деякі компанії, які дозволяють користувачам платити один одному в одиницях, подібних до золотих злитків. Приклади включають iGolder, gbullion та e-Gold. Хоча, здавалося, у DGC світле майбутнє, він втратив популярність завдяки своїй централізованій структурі. Політика також могла зіграти певну роль у зменшенні її популярності. Компанії, які надавали DGC, були змушені закрити федеральний уряд через їх нездатність виконувати урядові постанови [M.-C. Frunza, “Solving modern crime in ﬁnancial markets: Analytics and case studies,” ch. Cryptocurrencies: A New Monetary Vehicle, pp. 39–75, Academic Press, 2016.].

У 2003 році Second Life [“Second life - virtual worlds, virtual reality, vr, avatars, free 3d chat.” http://secondlife.com/, 2017.], онлайн віртуальний світ, ввів цифрову валюту, яку називають Linden доларом. Долар Linden обмінюється на фіатні валюти. Користувачі Second Life використовували цю валюту для прямих транзакцій. Однак, подібно до своїх попередніх цифрових валют, долар Linden є централізованою цифровою валютою, яку контролює його творець Linden Labs [“Create virtual experiences — linden lab.” https://www.lindenlab.com/, 2017.]. Більше того, його ціна є нестабільною та нестабільною, що робить її ризикованою валютою.

1.2 Історія Блокчейн систем

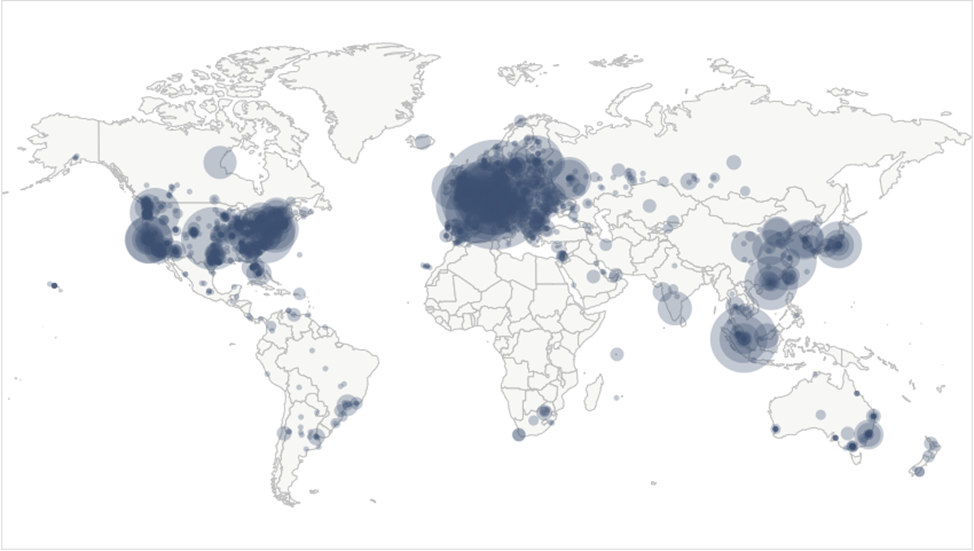
У 1991 році перший безпечний блокчейн запропонували Стюарт Хабер (Stuart Haber) та В. Скотт Сторнетта (W. Scott Stornett) [S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” in Conference on the Theory and Application of Cryptography, pp. 437–455, Springer, 1990.]. Їх блокчейн був спрямований на засвідчення створення або модифікації цифрового запису шляхом цифрової фіксації мітки часу. Однак цей блокчейн не був ефективним, оскільки кожен запис незалежно відмічався міткою часу. Для підвищення ефективності у 1992 році [D. Bayer, S. Haber, and W. S. Stornetta, “Improving the efﬁciency and reliability of digital time-stamping,” in Sequences II, pp. 329–334, Springer, 1993.] були включені до блокчейнів дерева Меркле [R. C. Merkle, “A digital signature based on a conventional encryption function,” in Conference on the Theory and Application of Cryptographic Techniques, pp. 369–378, Springer, 1987]. Вони покращили ефективність, обробляючи кілька цифрових записів в один блок.

31.10.2008 році Сатоші Накамото оприлюднив білу книгу (white paper), в якій запропонував Биткойн [S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” https://bitcoin.org/bitcoin.pdf, 2008]. Біткойн – це онлайн-система цифрових грошових коштів Peer-to-Peer (P2P), яка не потребує довіреної третьої сторони. У Bitcoin користувачі володіють правами власності на віртуальні криптовалюти, які позначаються як біткойни (BTC). Користувачі генерують транзакції для передачі BTC та зберігають їх у загальнодоступному блокчейн реєстрі. Найменша доля цінності BTC, відома як сатоші, еквівалентна 0,00000001 BTC.

Нарешті, 03.01.2009 було створено генезис блок реєстру криптовалюти Біткойн, де було реалізовано перший ланцюг блоків який надалі використано в якості основи для блокчейн технології.

*Слайд 6.*

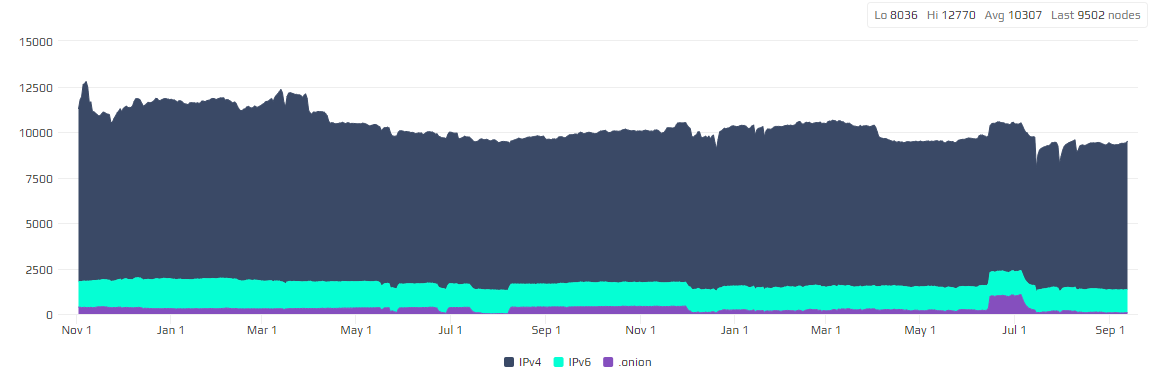
На теперішний час (станом на 01.11.2019) мережа Біткойн нараховує 9522 вузлів, яких можливо досягнути. Онлайн карту концентрації вузлів Біткойн можливо переглянути на ресурсі Bitnodes [Bitnodes https://bitnodes.earn.com/], скріншот наведено на рис. \_\_



**Рис. \_\_.** – Карта концентрації доступних біткойн-вузлів, знайдених в країнах по всьому світі. Скріншот з Bitnodes (https://bitnodes.earn.com/) станом на 01.11.2019

*Слайд 7,8,9.*

«Живу» карту вузлів Біткойн мережі можливо переглянути також на ресурсі Bitnodes за посиланням <https://bitnodes.earn.com/nodes/live-map/>, а також динаміку зміни доступних вузлів за останні два роки (рис. \_\_).



**Рис. \_\_.** – Динаміка зміни доступних Bitcoin-вузлів за останні два роки. Скріншот з Bitnodes (<https://bitnodes.earn.com/dashboard/?days=730>) станом на 02.11.2019

2. Огляд технології блокчейн

У даному розділі будемо дотримуватися визначення, понять та термінів наведених у NIST.IR 8202[NISTIR 8202 Blockchain Technology Overview https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf] (та його проекти від січня 2018 [Draft NISTIR 8202 Blockchain Technology Overview https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf]), ANSI X9 [ASC X9 Study Group Report Distributed Ledger and Blockchain Technology Study Group <https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf>] (з вказаними рекомендаціями з безпеки в галузі стандартизації), стандарті Німеччини «Валідація даних з використанням блокчейна» [DIN SPEC 3104:2019-04 Blockchain-basierte Datenvalidierung <https://dx.doi.org/10.31030/3042007>] та інших тематичних джерел наведених за текстом.

*Слайд 10.*

2.1 Поняття розподіленої системи

Зараз використовуються різні поняття і визначення розподіленої системи. Узагальнюючи, їх можна звести до наступних визначень[Распределенные системы: учебное пособие для студентов, обучающихся по направлению подготовки 38.03.05 Бизнесинформатика / [авт.-сост. А.В. Демина, О.Н. Алексенцева]. – Саратов: Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2018. – 108 с <http://www.seun.ru/content/learning/4/science/1/doc/Demina_Aleksenzeva.pdf>]:

* розподіленою системою називається набір незалежних комп’ютерів, що представляється їх користувачам єдиною системою;
* розподіленої інформаційної системою називається сукупність взаємодіючих між собою програмних компонент. Кожна з них може розглядатися як програмний модуль (застосунок), що виконується в рамках окремого процесу.

Користувачі і застосунки одноманітно працюють в розподілених системах незалежно від того, коли і де відбувається ця взаємодія.

Ще однією важливою характеристикою розподілених систем є здатність забезпечення однакової роботи користувачів і застосунків в розподілених системах.

Розподілені системи повинні порівняно легко піддаватися розширенню і масштабуванню. Вихід з ладу однієї з частин розподіленої системи не повинен призводити до збою всієї розподіленої системи.

*Слайд 11.*

2.2 Поняття блокчейн системи

Блокчейн (blockchain або block chain – «ланцюжок блоків») системи є захищеними від несанкціонованого доступу цифровими реєстрами, реалізованими в розподіленому вигляді (тобто без центрального сховища) і, як правило, без центрального органу (тобто банку, компанії або уряду). Цифровий реєстр блокчейн систем складається з криптографично підписаних транзакцій, які згруповані в блоки. Кожен блок криптографично пов’язаний з попереднім (що робить його фальсифікацію очевидним) після перевірки і прийняття консенсусного рішення. Нові блоки реплікуються по копіям реєстру в мережі, і будь-які конфлікти дозволяється автоматично з використанням встановлених правил.

На базовому рівні блокчейн система дозволяє спільноті користувачів записувати транзакції в загальному реєстрі в межах цієї спільноти, так що при нормальній роботі блокчейн мережі жодна транзакція не може бути змінена після публікації, що в значній мірі відрізняє їх від традиційних баз даних.

Теоретично технологія блокчейн може бути застосована для організації даних в будь-який СУБД [Книга Блокчейн, раздел 7.1]. Ланцюжок блоків може бути організований на абстрактному рівні, програмному забезпеченню не обов’язково буде зберігати дані транзакцій в організованих блоках, достатньо, щоб заголовок блоку задовольняв відповідного формату. Отже, вузол мережі може організувати зберігання і обробку транзакцій будь-яким зручним йому чином, а для виконання синхронізації з іншими вузлами дані формуються в блоки певного формату і передаються по мережі.

Кожен користувач блокчейн мережі має можливість дізнатися, яка транзакція була в певний відрізок часу. Існування розподіленого реєстру підтримується за допомогою розподілених зусиль безлічі користувачів. Власник повного вузла може переконатися в коректності стану історії всіх транзакцій, що робить роботу в реєстрі прозорою для аудитора. Якщо хтось із користувачів навмисне складе некоректну транзакцію і відправить її в мережу, чесні учасники відразу це помітять і не підтвердять її.

У користувача є можливість використовувати легку клієнтську програму, де буде відображатися поточний стан бази даних, що не запускаючи при цьому повний вузол. Звичайно, такий підхід можна застосувати, якщо користувач довіряє, що облікова система працює надійно.

Якщо мова йде про систему обліку, яка контролюється однією організацією, і з якихось причин ланцюжок блоків був переписан, то у користувача блокчейн системи в цифровому гаманці залишаються докази у вигляді транзакцій, завірених цифровим підписом організації. Тому питання довіри між партнерами в обліковій системі із застосуванням блокчейн технологій не так актуальне. У таких випадках надійність роботи можуть забезпечити правила роботи протоколу.

Кожен створений блок містить геш попереднього. Таким чином створюється ланцюжок блоків, який бере початок від так званого генезис блоку (перший блок в блокчейн системі) до останнього знайденого системою блоку. Для зв’язку блоків повинна використовуватися стійка геш-функція.

Чесні користувачі блокчейн системи завжди будують свій блок на останньому існуючому блоці, посилаючись на нього. Продовження ланцюга вважається дійсним тільки якщо в ньому є інформація про всі попередні ланки ланцюга і починається він з генезис блоку.

За допомогою впровадження блокчейн технології між користувачами мережі встановлюються довірчі відносини, адже не маючи відповідного ключа ніхто не зможе ввести зміни в ланцюжок з блоків. Будь-які непідтверджені закритими ключами зміни відхиляються системою.

*Слайд 12.*

Основні характеристики технології блокчейн можна описати як:

*Безпека* – блокчейн системи безпечні з криптографічної точки зору, гарантуючи, що дані які містяться у реєстрі не були підроблені, і що дані в реєстрі ідентичні.

*Загальнодоступність* – реєстри розподіляється між кількома учасниками. Це забезпечує прозорість через учасників вузла в мережі блокчейн.

*Розподіленість* – блокчейн може бути розподілений. Це дозволяє масштабувати кількість вузли мережі блокчейн, щоб зробити її більш стійкою до атак зловмисників. Зі збільшенням кількості вузлів зменшується здатність нечесного учасника системи впливати на консенсус протокол, який використовується в блокчейн системах.

*Слайд 13.*

2.2.1 Цілісність даних в блокчейн системах (геш-функції)

Важливим компонентом блокчейн технології є використання криптографічних геш-функцій для багатьох операцій. Гешування – це метод застосування криптографічної геш-функції до даних, який обчислює унікальний вихід (так званий геш-значення або просто геш) для введення майже будь-якого розміру (наприклад, файлу, тексту або зображення). Це дозволяє окремим суб’єктам незалежно приймати вхідні дані, гешувати ці дані і отримувати один і той ж самий результат, доводячи, що в даних не було ніяких змін. Навіть самі незначні зміни на вході (наприклад, зміна одного біта) призведе до зовсім іншого вихідного значення геш-функції.

Блокчейн система гарантує цілісність, надаючи обіцянку «незмінності», що в цьому контексті означає гарантію відсутності видалення, постійного запису будь-якого елементу, доданого до блокчейну. Однак в дійсності базова функціональність блокчейна не забезпечує незмінність як таку і лише існує можливість виявлення змін після запису транзакції в реєстр.

Будь-яка задана копія реєстру, як і будь-які цифрові дані, може бути змінені в будь-який час. Процес консенсусу вимагає, щоб ці зміни були узгоджені з розподіленими копіями блокчейна.

Таким чином, цілісність будь-яких даних в блокчейн системі залежить від сильних криптографічних функції гешування і сталого функціонування узгоджувальних процесів.

Криптографічні геш-функції мають такі важливі захисні властивості:

1. *Незворотність або стійкість до відновлення прообразу*. Це означає, що вони є односторонніми функціями; для заданого значення геш-функції  повинно бути обчислювально неможливо знайти блок даних , для якого .

2. *Стійкість до колізій першого роду або до відновлення другого прообразу*. Це означає, що не можна знайти вхідні дані, які гешують до певного значення. Більш конкретно, криптографічні геш-функції спроектовані таким чином, щоб для заданого повідомлення  має бути обчислювально неможливо підібрати інше повідомлення , для якого . Єдиний доступний підхід – це вичерпний пошук вхідного простору, що неможливо з обчислювальної точки зору.

3. *Стійкість до колізій другого роду*. Це означає, що не можна знайти два входи, які гешуют до одного і того ж виходу. Більш конкретно, в обчислювальному відношенні неможливо знайти будь-які два входи, які виробляють один і той же геш-значення (наприклад, знайти , при яких ).

Конкретної криптографічної геш-функцією, що використовується в багатьох реалізаціях блокчейна, є алгоритм безпечного гешування (SHA - Secure Hash Algorithm) з вихідним розміром 256 біт (SHA-256). Багато комп’ютерів підтримують цей алгоритм апаратно, що робить його швидким для обчислень. Вихід SHA-256 становить 32 байта (32 байта = 256 біт), як правило, відображається у вигляді шістнадцятирічного рядка з 64 символів.

Це означає, що існує  або 115 792 089 237 316 195 423 570 985 008 687 907 853 269 984 665 640 564 039 457 584 007 913 121 299 399 936 можливих геш-значень. Алгоритм для SHA-256, як і для багатьох інших, стандартизований і вказано в Федеральному стандарті обробки інформації (FIPS - Federal Information Processing Standard) 180-4 [National Institute of Standards and Technology, Secure Hash Standard (SHS), Federal Information Processing Standards (FIPS) Publication 180-4, August 2015. <https://doi.org/10.6028/NIST.FIPS.180-4>]. Веб-сайт NIST Secure Hashing [National Institute of Standards and Technology (NIST), Secure Hashing website, <https://csrc.nist.gov/projects/hash-functions>] містить специфікації FIPS для всіх затверджених NIST алгоритмів гешування.

Оскільки існує нескінченна кількість можливих вхідних значень і кінцеве кількість можливих вихідних геш-значень, можливо, але дуже малоймовірно, щоб виникне колізія, коли  (тобто геш-функція від двох різних входів дає один і той же вихід). Кажуть, що SHA-256 стійкий до колізій, оскільки для знаходження колізії в SHA-256 необхідно виконати алгоритм в середньому приблизно  раз (що становить 340 282 366 920 938 463 463 374 607 431 768 211 456; приблизно ).

Щоб уявити це в перспективі, швидкість гешування (геш-кодування в секунду) всієї мережі біткойна в 2015 році становила 300 квадрильйонів гешів в секунду (300 000 000 000 000 000/с) [“Hash per Second.” Bitcoin Wiki, <http://en.bitcoin.it/wiki/Hash_per_second>]. Таким чином, всієї біткоін мережі знадобиться приблизно 35 942 991 748 521 () років для створення колізії (зверніть увагу, що вік Всесвіту складає  років [As estimated by measurements made by the Wilkinson Microwave Anisotropy Probe <https://map.gsfc.nasa.gov/universe/uni_age.html>]). Навіть якщо знайдуться будь-які вхідні дані  та , які виробляють одинакові геш-значення, малоймовірно, щоб обидва входи були дійсними в контексті блокчейн мережі (тобто  та  є дійсними транзакціями).

*Слайд 14.*

У блокчейн мережі криптографічні геш-функції використовують для цілого ряду завдання, таких як:

* Створення адреси користувача.
* Створення унікальних ідентифікаторів.
* Захист цілісності даних блоку – мається на увазі гарантія того, що інформація може бути оброблена, і буде як і раніше, представляти узгоджений стан записів з плином часу. Основою блокчейн технології є впевненість, що дані всередині структури не можуть бути змінені після запису без виявлення факту зміни. Це досягається за рахунок забезпечення цілісності даних за допомогою геш-кодування (зазвичай з використанням дерева Меркла).
* Захист заголовка блоку – вузол публікації геширует заголовок блоку. Якщо блокчейн мережа використовує модель консенсусу заснованого на доказі виконаної роботи, вузлу публікації потрібно гешировать заголовок блоку з різними значеннями nonce, поки не будуть виконані вимоги складності. Геш-значення поточного заголовка блоку буде включений в заголовок наступного блоку, де він буде захищати дані заголовка поточного блоку. Оскільки заголовок блоку включає в себе геш-представлення даних блоку, самі дані блоку також захищені, коли геш заголовок блоку зберігається в наступному блоці.

Існує безліч сімейств криптографічних геш-функцій, які використовуються в технології блокчейна (SHA-256 – не єдина), наприклад, Keccak (який був обраний NIST в якості переможця конкурсу на створення стандарту гешування SHA-3), а також RIPEMD160 [National Institute of Standards and Technology, SHA-3 Standard: PermutationBased Hash and Extendable-Output Functions, Federal Information Processing Standards (FIPS) Publication 202, August 2015. <https://doi.org/10.6028/NIST.FIPS.202>]. На сьогоднішній день, в різних блокчейн системах використовується більш 40 різних геш-функцій, наведемо деякі з них: ГОСТ 34.311; GROESTL 256; GROESTL 512; KECCАK 256; KECCАK 512; КУПИНА 256; КУПИНА 512; SHA2 256; SHA2 512; СТРИБОГ256; СТРИБОГ512; BMW; J-H; SKEIN; LUFFA; CUBEHASH; SHAVITE; SIMD; ECHO; HAMSI; FUGUE; SHABAL; WHIRLPOOL; LOSELOSE; DJB-2; RIPEMD160; DAGGER-HASHIMOTO; ETHASH; SCRYPT; BLAKE256; BLAKE512; EQUIHASH; LYRA2RE; LYRA2REV2; BALLOON; ARGON2I; ARGON2D; MTP-ARGON2; RANDOMX; PROGPOW; X11; X12; X13; X14; X15; X17. Більш докладно геш-функцій і питання їх застосування розглянуті в наступних розділах.

*Слайд 15.*

2.2.2 Підписання даних (асиметрична криптографія)

Технологія блокчейна використовує криптографію з асиметричним ключем (публікація FIPS 186-4 Стандарт цифрового підпису, визначає загальний алгоритм цифрового підпису, який може використовуватися в блокчейн технології: алгоритм цифрового підпису на еліптичних кривих [National Institute of Standards and Technology (NIST), Digital Signature Standard, Federal Information Processing Standards (FIPS) Publication 186-4, July 2013. <https://doi.org/10.6028/NIST.FIPS.186-4>], тобто криптографію з відкритим ключем). Криптографія з асиметричним ключем використовує пару ключів: відкритий ключ і закритий ключ які математично пов’язані один з одним. Відкритий ключ є загальнодоступним без зниження безпеку процесу, але закритий ключ повинен залишатися в секреті, якщо дані повинні зберігатися захищеними за допомогою криптографії. Незважаючи на наявність зв’язку між двома ключами, секретний ключ не може бути ефективно визначено на основі знання відкритого ключа. Можна зашифрувати секретним ключем, а потім розшифрувати за допомогою відкритого ключа. Крім того, можна зашифрувати відкритим ключем, а потім розшифрувати за допомогою закритого ключа.

Асиметрична криптографія дозволяє встановити довірчі відносини між користувачами, які не знають або не довіряють один одному, надаючи механізм для перевірки цілісності та автентичності транзакції, дозволяючи самим транзакціях залишатися відкритими. Для цього транзакції мають цифровий підпис. Це означає, що закритий ключ використовується для шифрування транзакції так що будь-який користувач отримав відкритий ключ може його розшифрувати. Оскільки відкритий ключ знаходиться у вільному доступі, шифрування транзакції за допомогою секретного ключа доводить, що підписант транзакції володіє секретним ключем. Крім того, можна зашифрувати дані за допомогою відкритого ключа користувача, так що тільки користувач, який має доступ до секретного ключа, зможе розшифрувати ці данні.

Недоліком є те, що криптографія з асиметричним ключем порівняно повільно обчислюється. Це відрізняється її від криптографії з симетричним ключем, в якій один секретний ключ використовується для зашифрувати і розшифрувати. При використанні криптографії з симетричним ключем користувачі вже повинні мати встановлені довірчі відносини один з одним для обміну попередніми загальним ключем. У симетричній системі будь-які зашифровані дані, які можуть бути розшифровані за допомогою попереднього загального ключа, підтверджують, що вони були відправлені іншим користувач з доступом до загальнодоступного ключа; жоден користувач без доступу до загальнодоступного ключа не зможе отримати доступ до розшифрування даними. У порівнянні з криптографією з асиметричним ключем криптографічні алгоритми з симетричний ключ дуже швидко обчислюється. Через це, коли хтось стверджує, що шифрує щось з використанням криптографії з асиметричним ключем, частіше дані шифруються за допомогою симетричних криптографічних алгоритмів, а сам симетричний ключ шифрується з використанням криптографії з асиметричним ключем. Цей спосіб значно прискорює криптографію з асиметричним ключем.

Нижче наведено короткий опис використання криптографії з асиметричним ключем у багатьох блокчейн мережах:

* Закриті ключі використовуються для цифрового підпису транзакцій.
* Відкриті ключі використовуються для отримання адрес.
* Відкриті ключі використовуються для перевірки підписів, створених за допомогою закритих ключів.
* Асиметрична криптографія надає можливість перевірити, що користувач, який передає значення іншому користувачеві, має закритий ключ та здатний підписати транзакцію.

Деякі ексклюзивні блокчейн мережі можуть використовувати існуючу в бізнесі інфраструктуру відкритих ключів для криптографії з асиметричним ключем для надання облікових даних користувача, замість того щоб кожен користувач блокчейн мережі міг керувати своїми власними асиметричними ключами. Це робиться шляхом використання існуючих служб каталогів і використання цієї інформації в блокчейн мережах. Блокчейн мережі, які використовують існуючу службу каталогів, можуть отримувати до неї доступ через існуючі протоколи, такі як спрощений протокол доступу до каталогів (LDAP - Lightweight Directory Access Protocol [LDAP.com, <https://www.ldap.com>]), і використовувати інформацію з каталогу безпосередньо або імпортувати її у внутрішній центр сертифікації в блокчейн мережі.

*Слайд 16.*

2.3 Класифікація блокчейн систем

Блокчейн мережі можуть бути класифіковані на основі моделі дозволів, яка визначає, хто може підтримувати мережу (наприклад, публікувати блоки). Існує два високорівневих підходу до класифікації блокчейн системи: *інклюзивний* (загальнодоступний, від англ. permissionless – без дозволу) і *ексклюзивний* (що вимагає дозволу, від англ. permissioned – дозволено).

У інклюзивній блокчейн мережі кожен може читати і писати без авторизації. В ексклюзивних блокчейн мережах беруть участь конкретні люди або організації і забезпечується більш детальний контроль. Ексклюзивні блокчейн мережі часто розгортаються для групи організацій і окремих осіб, таких як, наприклад, консорціуми. Знання відмінностей між цими двома категоріями дозволяють зрозуміти, яке підмноження блокчейн технологій може бути застосовне до конкретних потреб.

Крім того блокчейн технологія може бути класифікована за доступністю. Так, спочатку блокчейн технологія передбачає повну свободу і незалежність системи, в якій немає єдиного адміністратора. Однак інтерес до нової технології з боку великих компаній і фінансових інститутів призвів до появи більш централізованих форм блокчейна, коли при збереженні розподілених даних присутній централізована система контролю.

Такі трансформації дозволяють говорити про різні види доступності блокчейн систем [14BitcoinWiki https://ru.bitcoinwiki.org/wiki/Блокчейн]:

* публічна блокчейн система;
* блокчейн система, яка належить консорціуму або групі людей;
* повністю приватна блокчейн система.

Вони відрізняються рівнем доступу до інформації учасників блокчейн системи, а також їх можливістю впливати на її розвиток.

2.3.1 Інклюзивний (permissionless) блокчейн

Інклюзивні блокчейн мережі – це відкриті для всіх децентралізовані платформи. Публікація блоків проводиться без дозволу будь-якого органу. Інклюзивні блокчейн платформи часто є програмним забезпеченням з відкритим вихідним кодом, вільно доступним для всіх, хто хоче завантажити їх. Оскільки кожен має право публікувати блоки, це призводить до того, що кожен може читати блокчейн, а також випускати транзакції в блокчейн систему. Будь-який користувач блокчейн мережу може читати і записувати реєстр блокчейн системи.

Інклюзивні блокчейн мережі відкриті для участі всіх, включаючи зловмисників, які можуть намагатися публікувати блоки таким чином, щоб скомпрометувати систему. Щоб запобігти такій поведінці користувачів, інклюзивні блокчейн мережі часто використовують багатопартійну угоду або систему «консенсусу», яка вимагає від користувача витрачати або підтримувати ресурси при спробі опублікувати блоки. Це заважає зловмисникам легко скомпрометувати систему. Приклади таких моделей консенсусу включають доказ роботи і доказ частки володіння.

Консенсус системи, в інклюзивних мережах, зазвичай заохочують чесну (тобто таку, яка відповідає протоколу) поведінку користувачів, за допомогою винагороди за проведену публікацію блоків. Винагорода, як правило, проводиться у вигляді видачі користувачеві власної криптовалюти, що призводить до матеріальної зацікавленості користувачів і тим самим стимулює функціонування блокчейн мережі.

2.3.2 Ексклюзивний (permissioned) блокчейн

Ексклюзивні блокчейн мережі - це мережі, в яких користувачі, наприклад ті, що публікують блоки, повинні бути авторизовані деякою уповноваженою структурою (будь то централізована або децентралізована). Оскільки тільки авторизовані користувачі підтримують блокчейн, можна обмежити доступ для читання і обмежити, хто може здійснювати транзакції. Таким чином, ексклюзивні блокчейн мережі можуть дозволити будь-кому читати блокчейн, або можуть обмежити доступ для читання тільки уповноваженим особам. Вони також можуть дозволити будь-кому відправляти транзакції бути включеним в блокчейн або, знову ж таки, вони можуть обмежити цей доступ тільки авторизованим фізичним особам. Ексклюзивні блокчейн мережі можуть створюватися і підтримуватися з використанням відкритого або закритого вихідного програмного забезпечення.

Ексклюзивні блокчейн мережі можуть мати таку ж прозорість цифрових активів, децентралізацію, відмовостійкість і надмірність зберігання даних як інклюзивні блокчейн мережі. Ексклюзивні блокчейн мережі також використовують консенсусні моделі для публікації блоків, але ці методи часто не вимагають витрат або забезпечення ресурсами (на відміну від поточних інклюзивних блокчейн мереж). Це пов’язано з тим, що для участі в ексклюзивній блокчейн мережі необхідно встановлення особи учасника; і учасники блокчейн мережі користуються певним рівнем довіри один до одного, оскільки їм всім було дозволено публікувати блоки, і якщо вони будуть порушувати правила мережі їх авторизація може бути відкликана. Консенсусні моделі в ексклюзивних блокчейн мережах зазвичай швидше і дешевше в обчислювальному відношенні.

Ексклюзивні блокчейн мережі також можуть використовуватися організаціями, яким необхідно більш жорстко контролювати і захищати свої блокчейни. Однак, якщо один об’єкт управляє тим, хто може публікувати блоки, користувачі ланцюжка блоків повинні будуть довіряти цьому об’єкту. Ексклюзивні блокчейн мережі також можуть використовуватися організаціями, які хочуть працювати разом, але можуть не повністю довіряти один одному. Вони можуть створювати ексклюзивну блокчейн мережу і запрошувати ділових партнерів записувати свої транзакції в загальний розподілений реєстр. Ці організації можуть визначити модель консенсусу, яка буде використовуватися з міркувань на то, наскільки вони довіряють один одному.

Крім довіри, ексклюзивні блокчейн мережі забезпечують прозорість і розуміння, які можуть допомогти краще інформувати бізнес-рішення і притягати до відповідальності сторони, які «погано» себе ведуть. Тому такі мережі можуть явно включати об’єкти аудиту і нагляду, які мають можливість перевірки в режимі реального часу, а не тільки періодичним чином. Деякі ексклюзивні блокчейн мережі підтримують можливість вибіркового розкриття інформації про транзакції на основі ідентифікаційних даних або облікових даних користувачів блокчейн мережі. З цією функцією може бути досягнута деяка ступінь конфіденційності в транзакціях. Наприклад, може статися так, що блокчейн записує транзакцію між двома користувачами блокчейн мережі, але фактичний зміст транзакцій є відомим тільки для залучених сторін.

Деякі ексклюзивні блокчейн мережі вимагають, щоб всі користувачі були авторизовані для відправки та отримання транзакцій (тобто забороняють бути анонімними або навіть псевдоанонімними). У таких системах сторони працюють разом для досягнення загального бізнес-процесу з природними перешкодами для здійснення шахрайства чи іншої поведінки в якості недобросовісного учасника (так як їх можна ідентифікувати). Якщо станеться недобросовісна поведінка, добре відомо, які організації включені, які засоби правового захисту доступні і як використовувати ці засоби у відповідній судовій системі.

2.3.3 Публічний (public blockchain) блокчейн

До публічних блокчейн мереж (public blockchain) може отримати доступ будь-яка людина. Це означає, що він може відправляти транзакції і чекати їх включення, якщо вони дійсні, а також брати участь в процесі консенсусу, тобто визначення того, які блоки додаються в ланцюжок.

Такі системи зазвичай вважаються «повністю децентралізованими».

2.3.4 Блокчейн, що належить консорціуму (consortium blockchains)

Блокчейн мережі, якими володіють консорціуми (consortium blockchains) контролюються заздалегідь обраним набором вузлів. В якості прикладу, можливо навести систему з 15 фінансових установ, кожне з яких управляє вузлом, і 10 з яких повинні підтвердити кожен блок, щоб його визнали дійсним і додали в ланцюг.

Право читати блок-ланцюжок може бути загальнодоступним, або обмежена учасниками. Можливі «гібридні» системи, коли кореневі геш блоки є загальнодоступними, але всі члени блокчейна можуть здійснювати лише обмежене число запитів і підтверджень транзакцій деяких частин блокчейна.

Такі ланцюга можна назвати «частково децентралізованими».

2.3.5 Приватний блокчейн (fully private blockchains)

Повністю приватний блокчейн (fully private blockchains) – це ланцюжок блоків, в якій запис нових блоків закріплено тільки за однією організацією. Дозвіл на читання може бути загальнодоступним або обмежений в тій чи іншій мірі.

Можливі додаткові опції (управління базами даних, аудит тощо) всередині однієї компанії, коли в багатьох випадках загальнодоступність не є потрібною. Хоча без неї не обійтися, коли потрібно публічний звіт про діяльність.

*Слайд 17.*

2.4 Питання конфіденційності даних і безпеки транзакцій

Блокчейн системи, як правило, не шифрують дані в ланцюжку блоків, тому не забезпечують конфіденційність, що означає, що конфіденційні дані, що зберігаються в ланцюжку, можуть бути переглянуті і вкрадені. Це означає, що для забезпечення безпеки даних необхідно застосовувати стандартні методи захисту системи і даних до блокчейн системам.

Фінансові послуги зазвичай мають справу з ексклюзивними типами даних різної чутливості, від захищеної законом інформації до публічних записів. Відповідно до вимог до ризику ці елементи даних отримують різний захист у відповідних інформаційних системах і часто зберігаються у різноманітних системах. Архітектури блокчейна можуть збирати різні дані і об’єкти в рамках спільного рішення. Інформація в ланцюжках блоків може включати в себе затвердження ідентичності, контент декількох типів, інформацію про підтримку, дії / директиви смарт-контрактів, позначки часу, перевірки і правила тощо. Таким чином, структура всієї системи повинна бути здатна охопити всі об’єкти, а також забезпечити безпечний, конфіденційний, розмежований доступ до всіх без винятку об’єктів в рамках даної транзакції.

Оцінюючи потребу в заходах, пов’язаних з конфіденційністю, враховується ступінь, в якій блокчейн технологія за своєю природою забезпечує або не забезпечує захист конфіденційності або конфіденційних даних, які можуть завдати шкоди, якщо піддаються впливу сторонніх осіб. Незалежно від того, чи використовується ексклюзивний або інклюзивний блокчейн, цілісність даних забезпечується за допомогою гешування, але в блокчейн системах немає стандартного механізму, що забезпечує конфіденційність.

В доповнення до процесів, які захищають дані, що зберігаються, застосунок повинен також розробити політики відповідності, сертифікації та аудиту, які гарантують, що всі користувачі будуть працювати так, щоб підтримувати цілісність системи.

Учасники фінансових послуг не повинні мати побоювання з приводу умов, в яких працює їх блокчейн. Певний рівень довіри потрібний для роботи в блокчейн середовищі з дотриманням нормативних вимогах, конфіденційності тощо (особливо тому, що блокчейн застосунка можуть використовуватися на міжнародному рівні).