Щербаков Сергій Сергійович

аспірант

Класичний приватний університет, м. Запоріжжя

ORCID 0009-0002-8056-7578

Науковий керівник

Хрипко Сергій Леонідович

професор, доктор технічних наук

завідувач кафедри інформаційних технологій та дизайну

**ДОСЛІДЖЕННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЇ ДЛЯ ПІДТВЕРДЖЕННЯ ЦІЛІСНОСТІ ДАНИХ**

Інтернет змінив багато аспектів життя, суспільства та бізнесу. Однак спосіб, у який люди та організації здійснюють транзакції один з одним, коли не перебувають поруч, за останні кілька десятиліть не сильно змінився. Для здійснення такої транзакції потрібна третя сторона, якій можна було б довіряти. Вважається, що блокчейн і є тим компонентом, який завершує головоломку Інтернету та робить його більш відкритим, доступнішим і надійнішим [1-3].

Блокчейн з точки зору бізнесу – це система записів для однорангової транзакції вартості. Це означає, що немає потреби в надійному посереднику, такому як банки, брокери чи інші служби умовного депонування, щоб служити надійною третьою стороною. Наприклад, якщо один користувач платить іншому користувачеві 10 доларів, чому це повинне проходити через банк. (мал. 1.1) [4]. Децентралізовані фінанси виділяються як альтернатива традиційним, оскільки вони можуть позбутися фінансової бюрократії, яка є тягарем сучасної фінансової системи. Децентралізовані фінанси дозволяють робити транзакції з мінімальними комісіями та майже миттєво у будь-які куточки світу.



Рисунок 1.1 – Транзакція з посередником та P2P транзакція

Блокчейн – це тип зберігання даних, який дозволяє цифровим чином ідентифікувати та відслідкувати транзакції. Передаючи цю інформацію по розподіленій комп’ютерній мережі, створювати розподілену мережу довіри в якомусь сенсі [7].

З прикладної точки зору блокчейн – це інновація, що базується на трьох концепціях: мережі P2P, асиметричній криптографії та розподіленому консенсусі на основі вирішення математичних задач. Ці ідеї не є новими і розвиваються далі.

Блокчейн може розглядатися як синхронізована БД з такою кількістю копій, як і вузлів в мережі; як суперкомп’ютер, сформований складовими з усіх центральних та графічних процесорів, що належать до нього. Він використовується для збереження і обробки інформації, або як API. Різниця в тому, що не потрібно розробляти бекенд, і можно бути впевненими, що всі дані добре захищені та правильно оброблені в мережі (мал. 1.2). Можна припустити, що блокчейн – це журнал, в якому факти об’єднуються в ланцюг однотипних вузлів [8, 9].



Малюнок 1.2 – Централізована та децентралізована архітектури

Мережі P2P та інші розподілені системи повинні розв’язувати непросту проблему: вирішення конфліктів або їх аналіз та узгодження. Реляційні БД забезпечують цілісність через посилання, але така функціональність не існує в розподілених системах. За умови, що 2 несумісні факти надходять одночасно, система повинна мати інструкцію, щоб визначити, який факт є правильним.

Сатоші Накамото запропонував в 2008 році концепцію – надання єдиної точки доступу, до великої кількості даних для всіх учасників. У 2009 році була перша реалізація на практиці – біткойн – цифрова валюта [2].

Дані в блокчейн збираються та поступово накопичуються, створюючи певний журнал з даними, що постійно доповнюється (мал. 1.3). В даний журнал не можна вносити які-небудь зміни або видаляти хоч якусь інформацію. Туди можна записати скільки завгодно транзакцій, що робить таку технологію унікальною.



Малюнок 1.3 – Візуалізація децентралізованого Блокчейн

Технологія блокчейн є гибрид, тобто поєднання централізованого та децентралізованого способів, але все одно основним буде скоріш за все один із типів. Наприклад, найважливіші вразливі дані будуть зберігатися децентралізовано (у блокчейні), а якісь складні розрахунки чи якийсь невеликий обсяг даних, який дуже дорого записувати у блокчейн, може зберігатися десь на централізованому сервісі. Щоб затвердити транзакцію, її формат та підписи повинно бути перевірено, а потім записано в блок. Факти згруповуються в блоки, і в мережі залишається лише один блоковий ланцюжок. Кожен новий блок має посилання до попереднього блоку (мал. 1.4). Перш ніж додавати до блоку, факти розглядаються як неузгоджені.



Малюнок 1.4 – Блоки в технології блокчейн

Основна концепція, яку розв’язує блокчейн, насамперед зосереджена на забезпеченні приватного та безпечного спілкування між двома сторонами. Насамперед це було зумовлено першим впровадженням технології блокчейн для цифрової валюти, і це не випадково, оскільки гроші все-таки є комунікаційною технологією, оскільки обмін грошима залежить від комунікації.

Таким чином, блокчейн можна подати так:

* однорангова система транзакцій цінностей без довірених третіх сторін між ними (немає потреби в довірених третіх сторонах, які виступають посередниками для перевірки, захисту та розрахунків за транзакціями);
* спільна, децентралізована та відкрита книга транзакцій. Ця база

даних реєстру відтворюється на великій кількості вузлів;

* база даних реєстру є базою даних лише для додавання і не може бути змінена чи змінена. Це означає, що кожен запис є постійним. Будь-який новий запис у ньому відображається на всіх копіях баз даних, розміщених на різних вузлах.

Так само, як TCP/IP був розроблений для досягнення відкритої системи, технологія блокчейн була розроблена для справжньої децентралізації. Щоб це зробити, творці біткойна зробили його відкритим, щоб він міг надихнути багато децентралізованих програм.

Технологію блокчейн можна розглядати як шарову структуру.

Мета полягає не в тому, щоб стандартизувати технологію блокчейн, а в тому, щоб краще розуміти. Всі шари присутні на всіх вузлах (мал. 1.5).



Рисунок 1.5 – Шари блокчейну

Application Layer. Це включає традиційний стек технологій для розробки програмного забезпечення, як-от конструкції програмування на стороні клієнта, сценарії, API, фреймворки розробки тощо. Для програм, які розглядають блокчейн як серверну частину, ці програми, можливо, потрібно буде розмістити на деяких вебсерверах, і для цього може знадобитися веброзробка застосунків, серверне програмування та API тощо. В ідеалі хороші блокчейн-програми не мають моделі клієнт-сервер, і немає централізованих серверів, до яких клієнти мають доступ, саме так і працює біткойн.

Execution Layer. Рівень виконання – це місце, де виконання інструкцій, замовлених прикладним рівнем (Application Layer), відбувається на всіх вузлах у мережі блокчейн. Інструкції можуть бути простими інструкціями або набором кількох інструкцій у формі смарт-контракту. Усі вузли в мережі блокчейн повинні виконувати програми/скрипти незалежно. Детерміноване виконання програм/скриптів на одному наборі вхідних даних і умов завжди дає однаковий вихід на всіх вузлах, що допомагає уникнути невідповідностей.

Semantic Layer. Також називається логічним рівнем, займається перевіркою транзакцій, що виконуються, перевіркою блоків, що генеруються в мережі, відповідає за зв’язування блоків, створених у мережі.

Propagation Layer. На цьому рівні вузли синхронізуються один з одним відносно поточного стану мережі. Коли транзакція здійснюється, вона транслюється на всю мережу. Так саме, коли вузол хоче запропонувати блок, він поширюється на всю мережу, щоб інші вузли могли будувати його, вважаючи його останнім блоком.

Consensus Layer. На цьому базовому рівні забезпечується безпека та захист блокчейну. Мета цього рівня – узгодити стану реєстру між усіма вузлами. У Bitcoin або Ethereum консенсус досягається за допомогою методів стимулювання, які називаються «майнінг». Біткойн і Ethereum використовують механізм консенсусу Proof of Work (PoW). Після створення нового блоку блок поширюється на всі інші вузли, щоб перевірити, чи дійсний новий блок із транзакціями в ньому, і на основі консенсусу з усіх інших вузлів новий блок додається до блокчейну. Існує багато різних варіантів консенсусних алгоритмів, таких як Proof of Stake (PoS), delegated PoS (dPoS), Practical Byzantine Fault Tolerance (PBFT).

Основні властивості блокчейну, що викликали його широке застосування, полягають у наступному.

Незмінність. Запис транзакції неможливо змінити. Коли транзакція додається в мережу, то кожен вузол має її копію. Незмінність зростає із кількістю блоків записаних поверх блоку, і через певний час стає повністю незмінним., оскільки вони криптографічно захищені. Зареєстрована транзакція назавжди залишається в блокчейні.

Стійкість до підробок. У блокчейні транзакції є відкритими. Криптографічний хеш і цифрові підписи використовуються для забезпечення стійкості системи до підробок. Обчислювально неможливо підробити чийсь підпис. Якщо користувач робить транзакцію та підписуєте її хеш, ніхто не зможе пізніше змінити транзакцію та сказати, що була підписана інша транзакція. Крім того, користувач не можете пізніше стверджувати, що ніколи не здійснювали транзакцію, оскільки він її підписав.

Захист від подвійних витрат. Такі атаки можуть здійснюватися як у грошових, так і в негрошових транзакціях. Подвійні витрати – це спроба витратити ту саму суму кільком людям. Приклад: у користувача в обліковому записі є 100 доларів США, а він платить 90 доларів двом чи більше сторонам. Або якщо хтось володіє землею і продає ту саму ділянку землі двом людям.

У централізованій системі легко запобігти подвійним витратам, оскільки центральний орган знає про всі транзакції. Блокчейн-рішення також має бути захищеним від таких атак. Єдиний можливий спосіб запобігти подвійним витратам у блокчейні – це бути в курсі всіх транзакцій. Якщо знати про всі транзакції в минулому, то можно визначити, чи є транзакція спробою подвоїти витрати. Таким чином, вузли, які перевірятимуть транзакції, обов’язково повинні бути доступні для всіх даних блокчейну, починаючи з блоку генезису.

Стійкість. Мережа має бути достатньо стійкою, щоб витримувати тимчасові збої вузлів, недоступність деяких обчислювальних вузлів час від часу, затримку у мережі, падіння пакетів тощо.

Можливість проведення аудиту. Блокчейн – це ланцюжок блоків, які з’єднані між собою хешами. Можливість перевірки існує завдяки тому, що блоки пов’язані у зворотному напрямку до блоку генезису, і вона не повинна порушиться будь-якою ціною. Крім того потрібна можливість швидкої перевірки транзакція, яка мала місце у минулому.

# Таким чином, ми проаналізували основні принципи та характеристики технології блокчейн. Блокчейн є децентралізованою технологією, яка забезпечує незмінність, стійкість до підробок та захист від подвійних витрат у транзакціях, роблячи їх більш відкритими, доступними та надійними.

# **СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ**

1. Untung Rahardja, S. K., & EkaPurnamaHarahap, Q. (2020).

Authenticity of a diploma using the blockchain approach. Int. J., 9(1. 2).

1. Bellucci, M., Bianchi, D. C., & Manetti, G. (2022). Blockchain in accounting practice and research: systematic literature review. Meditari Accountancy Research, 30(7), 121-146.
2. Trivedi, U. B., & Sharma, S. (2023). Digitally Signed Document Chain (DSDC) Blockchain. In Proceedings of Third International Conference on Computing, Communications, and Cyber-Security (pp. 715-727). Springer, Singapore.
3. Vatsaraj, V., Shah, J., Verma, S., & Dholay, S. (2021, July). Decentralized Document Holder Using Blockchain. In 2021 12th International Conference on Computing Communication and Networking Technologies

(ICCCNT) (pp. 1-5). IEEE.

1. Яресько, К. (2022). Блокчейн для підтвердження оригінальності документів. TRENDS IN THE DEVELOPMENT OF SCIENCE IN THE

MODERN WORLD, 33, 420.

1. Кравченко, П. О., Скрябін, Б. Б., & Дубініна, О. М. (2019).

Блокчейн і децентралізовані системи. Частина 1. ПРОМАРТ.

1. Swan, M. (2015). Blockchain: Blueprint for a new economy. "

O'Reilly Media, Inc.".

1. Tariq, A., Haq, H. B., & Ali, S. T. (2022). Cerberus: A blockchain-based accreditation and degree verification system. IEEE Transactions on Computational Social Systems.
2. Treiblmaier, H., & Clohessy, T. (2020). Blockchain and distributed ledger technology use cases. Springer.