радіозв'язку застосовується рідко в зв'язку зі складнощами технічної реалізації. Крім цього, скремблери з ШПФ вносять в канал зв'язку тимчасову затримку.

Найпростішим видом часового перетворення є часова інверсія, при якій вихідний сигнал ділиться на послідовність часових сегментів і кожен з них передається інверсно в часі – з кінця до початку.

У скремблері з часовими перестановками мовний сигнал ділиться на часові кадри, кожен з яких в свою чергу поділяється на сегменти, а потім сегменти мовного сигналу піддаються перестановці.

Для подальшого підвищення ступеня закриття мовлення використовується комбінація часового і частотного скремблювання. В такому скремблері після аналого-цифрового перетворення спектр цифрованого мовного сигналу розбивається на частотно-часові елементи, які потім перемішуються на частотно-часовій площині відповідно до одного з криптографічних елементів і підсумовуються, не виходячи за межі частотного діапазону вихідного сигналу.

Отже, скремблювання підвищує надійність синхронізації пристроїв, підключених до лінії зв'язку (забезпечує надійне виділення тактової частоти безпосередньо з прийнятого сигналу), зменшує рівень перешкод, випромінюваних на сусідні лінії багатожильного кабелю, та захищає інформацію, що передається, від несанкціонованого доступу.

Література

1. Журнал «Схемотехника». 2004, N12. С. 25–27.
2. Конахович Г. Ф., Климчук В. П., Паук С. М. Защита информации в телекоммуникационных системах. К.: «МК-Пресс», 2005. 288 с.
3. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток. М.: Радио и связь, 1985.

УДК 004.01

ЧОМУ БЛОКЧЕЙН – ЦЕ ЦІННО

А. І. Катаєва, К. В. Захарова

Застереження: Стаття несе ознайомчу мету, а не фінансову пораду.

03 січня 2009 року в 20:15 (GMT +2) невідомий створив перший (нульовий) блок першої в світі криптовалюти у розмірі 50 монет, вартістю $0.00 [1]. Станом на 18 квітня 2021 року 17:50 (GMT +3) цей блок коштував би $2,782,134.50. Через 12 років після запуску до обігу блокчейну, сьогодні вже створено більше 9 тис. різноманітних криптовалют, з загальною капіталізацією у розмірі більше 2-ох трильйонів доларів [2].

Як випадковий набір чисел може бути переведений на реальні, чималі, кошти? Відповідь полягає в унікальності проекту.

Що таке «блокчейн»?

Все, що потрапляє в блокчейн, навіки там і залишається.

«Блок-Чейн» (з англ. «Block» – блок, «Chain» – ланцюг) – збірна назва впорядкованих транзакцій (блоків), що зв'язані хешами (ланцюгами). Оскільки кількість платежів та переводів невпинно збільшується, збільшується і кількість блоків, так зародилася інтернет-система у вигляді хеш-дерева.

Кожен блок є цілком захищеним від підробки та будь-яких змін. Блок містить у собі наступну інформацію:

1. Хеш – унікальний ідентифікатор блока;

2. Підтвердження – скільки разів «проходили» через даний блок – чим більше підтверджень, тим «старіший» блок;

3. Час створення блоку;

4. Ріст – кількість блоків підключених до блокчейну;

5. «Шахтар» – хто підтвердив транзакції в блоці;

6. Кількість транзакцій, що включені в даний блок;

7. Складність – математичне значення, наскільки важко знайти дійсний хеш для цього блоку;

8. Корінь меркла – кореневий вузол, нащадок усіх хешованих пар у дереві;

9. Версія –версія блоку, що відноситься до пропозицій протоколів, які тривають;

10. Біти – суб-одиниця валюти, що дорівнює 10^{-6} однієї монети;

11. Вага – вимір для порівняння розміру різних транзакцій між собою пропорційно обмеженню розміру блоку;

12. Розмір блоку;

13. Nonce – випадкове значення, яке регулюється, щоб отримати доказ роботи;

14. Об'єм транзакцій – орієнтовно загальна сума транзакцій у даному блоці;

15. Нагорода за блок – статична винагорода «шахтарю», який розрахував хеш для цього блоку;

16. Комісія за нагороду – сума комісій за транзакції, що повертається «шахтарю» за обчислення хешу для цього блоку.

Як можна побачити, усе цілком прозоро, можна дізнатися звідки, куди та скільки монет було переправлено. Відкритий блокчейн надає рівні права усім користувачам. Електронні платежі не проходять через посередників та не покладаються на довіру між покупцем та продавцем. Запропонована однорангова (peer-to-peer) мережа з використанням підтвердження роботи (proof-of-work) для запису публічної історії транзакцій, стає обчислювально непрактичним для зловмисника [3]. Така система цілковитого захисту і приваблює нових інвесторів.

Децентралізація та централізація

Категорична заява: «істинної» децентралізації мереж криптовалют, сьогодні, або вже не існує, або її дуже важко зустріти.

Блокчейни поділяються на децентралізовані, частково централізовані та повністю централізовані.

Повна централізація часто зустрічається у валютах бірж, тобто керівництво та сама мережа належить розробникам валюти. Це не відповідає повному захисту вкладень, оскільки вкладники покладаються на довіру, тобто є високий рівень можливого шахрайства з боку керівництва, але це може зменшувати комісію за транзакцію, бо передача відбувається без стороннього підтвердження.

Часткова централізація – коли керівництво централізоване, а мережа децентралізована. Тобто розробники мають право змінювати умови нагород «шахтарям», випускати оновлення мережі, змінювати кількість доступних монет, тощо, але не мають безпосереднього доступу до самих блоків. Захист вкладень настільки ж потужний, наскільки і в повністю децентралізованому блокчейні, але існує опосередкований вплив на курс зі сторони розробників.

Децентралізація – коли блокчейн належить усім одночасно, але ніхто не може його змінити. Для користування децентралізованою мережею потрібно встановити на свій пристрій інформацію про всі минулі блоки та мати простір для збереження наступних блоків. На даний час, для найбільшої криптовалюти, загальна вага мережі перевищує 350ГБ [4].

Чому ж спочатку було сказано, що «істинної» децентралізації не існує? Вище було багато разів згадано «шахтарів», хто ж вони? «Шахтарі» або «майнери» – це ті, хто підтверджує транзакції, та отримують плату за це. Зазвичай, для цього використовують технічні потужності, тому, чим більша потужність, тим більше транзакцій

підтверджується, та тим більше отримує «шахтар». Звідси й випливає інша сторона – якщо хтось отримає 50 % потужностей мережі, це буде пряма загроза захисту мережі. Є поняття – «Атака 51 %» – коли власник найбільшої частки загальної потужності може змінювати ланцюги транзакцій, для відправлення одних і тих самих монет різним отримувачам. Але найближчим часом це не передбачається, оскільки більша потужність мережі рівномірно розподілена між п'ятьма пулами [5] (веб-платформа, що групує «шахтарів-учасників», для більш-менш рівномірного розподілення нагород).

Висновки. Створюється все більше цікавих проектів, що використовують за основу технологію блокчейнів. І це не лише криптовалюти, а й державні проекти, чи фінансове забезпечення компаній. При над швидкому збільшені різноманіття блокчейнів потрібно швидко орієнтуватися в їх характеристиках.

Блокчейн – це технологія створення захищеної бази даних для забезпечення прозорості будь-яких операцій з фінансами. Тому, тримаймо серце відкритим до нового, але не забуваймо аналізувати головою!

Література

1. Bitcoin Explorer. Блок 0. URL: https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f (дата звернення: 18.04.2021)
2. Today's Cryptocurrency Prices by Market Cap. URL: https://coinmarketcap.com/ (дата звернення: 18.04.2021)
3. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System. Whitepaper. URL: https://bitcoin.org/bitcoin.pdf
4. Завантажити Bitcoin Core. Остання версія: 0.21.0. URL: https://bitcoin.org/uk/download (дата звернення: 18.04.2021)
5. Пулы для майнинга криптовалют: рейтинг крупнейших и лучших, принцип работы, критерии выбора, рекомендации. URL: https://profinvestment.com/mining-pools/ (дата звернення: 18.04.2021)

УДК 004.832.25:004.855.5

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ В СФЕРІ ОХОРОНИ ЗДОРОВ'Я

П. К. Ніколюк, К. В. Захарова

Смартфони вже давно не використовують лише для швидкого голосового-, відеозв'язку з родичами чи друзями. Замовлення їжі чи захищеного таксі через мобільний додаток – неєдині допоміжні зручності, які ми відчули саме в період пандемії аби зайвий раз не контактувати з людьми та не наражати себе й близьких на небезпеку. Але що ми робимо, коли запідозрюємо в себе якусь хворобу чи, актуальний сьогодні, коронавірус? Тут є декілька варіантів дій:

1. Іти напряму до сімейного лікаря, в лікарню, де в достатній кількості присутні:
    a. Здорові люди, яких Ви можете заразити вірусною хворобою, якщо Ви все ж таки хворі.
    b. Хворі люди, які можуть заразити Вас, новою, чи ще гірше, додатковою вірусною хворобою.
2. Дзвонити в швидку, в яких постійне завантаження, особливо в сьогодення, дочекатися її та контактувати з лікарями, які непідраховану кількість разів контактували з іншими хворими і потенційно можуть переносити в/на собі вірус.