обґрунтовано необхідність подальшого вдосконалення наявних і розробки нових напрямків з використанням сучасних інформаційних технологій.

1 *Боюн В. П.* Динамическая теория информации. Основы и приложения / В.П. Боюн. - К: Институт кибернетики им. В.М. Глушкова НАН Украины, 2001.- 326 с.
2 *Жураковський Ю.П.* Теорія інформації та кодування: підручник. / Ю.П. Жураковський, В.П. Полторак. - К.: ВШ, 2001. - 255с.
3 *Цапенко М.П.* Измерительные информацыонные системи: Структуры и алгоритмы, системотехническое проектирование: уч. пособие для вузов / М.П. Цапенко. - 2-е изд., перераб. и доп. - М.: Энергоатомидат, 1985. - 438с.
4 *Арутюнов П.А.* Теорія и применение алгоритмических измерений / П.А. Арутюнов. - М.: Энергоатомиздат, 1990. - 256с.
5 *Малла С.* Вэйвлеты в обработке сигналов: Пер. с англ. / С. Малла. - М.: Мир, 2005. - 671 с.
6 *Шеннон К.Э.* Работы по теории информации и кибернетика. / К.Э. Шеннон. - М.: Изд-во иностр. лит., 1963. - 829 с.
7 *Николайчук Я.М.* Теорія джерел інформації. / Видання друге, виправлене/, - Тернопіль: ТзОВ «Тернограф», 2010. - 536 с.
8 *Храмов А.В.* Первинні вимірювальні перетворювачі вимірювальних приладів і автоматичних систем: навч. посіб. - К.: Вища школа, 1998. - 527 с.

http://doi.org/10.5281/zenodo.3612254

Поступила 3.10.2019р.

УДК 004.6; 550.8.05

В. Кучковський, Львів
Н. Шаховська, Львів

БЛОКЧЕЙН ЯК БАЗА-ДАНИХ, ЙОГО ВИКОРИСТАННЯ, ОПИС РОЗУМНИХ КОНТРАКТІВ І МАЙБУТНІЙ ПОТЕНЦІАЛ

Abstract. The article deals with information technology blockchain. The possibility of databases creating using blockchain is described. The simple writing data procedure to the blockchain is realized. The main domains for the technology applying are given. The smart contract in blockchain are shown. The potential of this technology is described

Keywords — blockchain, cryptocurrencies, smart contracts, potential.

Вступ

Блокчейн (Blockchain) – це не зовсім нова технологія. Усі елементи, які використовує блокчейн, такі як: Інтернет, криптографія та протокол передачі, відомі людям вже кілька десятиліть.Тому технології як такі, а точніше способи, якими ці давно існуючі технології пов'язані і використовуються, не

можна вважати революційними в блокчейні.

Кожен, хто цікавиться цією технологією (і вкладає в неї гроші), сприймає блокчейн як інструмент, з допомогою якого можна досягти не тільки більшої ефективності та безпеки, але й абсолютно нового технологічного напряму.

Основна частина

II.1. Види баз даних

Однією з основних частин блокчейн є бази даних – централізовані, децентралізовані і розподілені [1, 2]. Наведемо відмінності між основними типами баз даних.

- Централізована база даних.

Приклади цієї БД: «збережені» фотографії, відео в instagram, товари в інтернет-магазині. Ці дані можна знайти в великому фізичному центрі обробки даних з великою кількістю серверів і жорстких дисків. Проблема централізованої бази даних полягає саме в її центральності - вона легко знищується разом з усіма цінними даними.

- Децентралізовані бази даних.

Децентралізація дуже тісно пов'язана з розподілом бази даних (працює на декількох пристроях). Децентралізована база даних означає, що немає одного головного центру, тому дані не тільки поширюються з одного місця, але і мають кілька основних вузлів. Перевага полягає саме в децентралізованому характері – відмова одного користувача не впливає на подальше функціонування мережі.

- Розподілені бази даних.

Для роботи не потрібні величезні центри обробки даних. Технологія надається всіма її користувачами. Користувачі на своїх комп'ютерах можуть тримати ноди для підтримки бази даних. Усі дані в цій базі даних кодуються хешованим алгоритмом.

На рис. 1 показано, який вплив матиме потенційна атака на централізовану базу даних. Досить знищити основний вузол, і дані безповоротно будуть втрачені, або відновленні з втратами.

Рис. 1. Приклади типів баз даних

Управління децентралізованою базою даних і аналіз даних заздалегідь поділяються всіма її користувачами. Таким чином, блокчейн являє собою децентралізовану базу даних, яка в цілому поширюється мережею незалежних (розподілених) комп'ютерів.

Існує можливість запису даних в Blockchain будь-якої інформації – від тексту до файлів.

Для демонстрації беремо криптовалюту Mooncoin. Створимо транзакцію на 8.78711729 MOON.


```
[
  {
    "txid":
"e441450043c54f1d6e358f63cfbe618215f485ecb5feb851dfe2fbae902a4150",
    "vout": 1,
    "address": "2Ng9J6jh95ZR8t9d6wqUE2sfWtwJo7TAcN",
    "account": "",
    "scriptPubKey": "76a91469f91565dfabe1009d480611f2ea55cc1889ddde88ac",
    "amount": 8.78711729,
    "confirmations": 10,
    "spendable": true,
    "solvable": true
  }
]
```


Для відправлення та запису слова обрано: DEFAULT.ABCD.BZ. При переведенні у HEX формат отримаємо: 44454641554c542e414243442e425a.

```
function strToHex($string) {
    $hex='';
    for ($i=0; $i < strlen($string); $i++) {
        $hex .= dechex(ord($string[$i]));    }
    return $hex; }
```

Створюємо raw формат виходу транзакції:

createrawtransaction
'[{"txid":"e441450043c54f1d6e358f63cfbe618215f485ecb5feb851dfe2fbae902a4150","vout":1}]'
'{"2DBLfPEDC88QxV4bnMzaVmXEd78YE5bSVX":1,"data":"44454641554c542e414243442e425a"}'

Після перетворення отримуємо стрічку:

010000000150412a90aefbe2df51b8feb5ec85f4158261becf638f356e1d4fc543004541e40100000000ffffffff0200e1f505000000001976a91401cd60975e1ca2d3a0583fc1c6d6b2a764ef408988ac0000000000000000116a0f44454641554c542e414243442e425a00000000

Ця стрічка являє собою транзакцію, в якій зашифроване задане слово. За допомогою функції signrawtransaction підписуємо транзакцію:

{
"hex":
"010000000150412a90aefbe2df51b8feb5ec85f4158261becf638f356e1d4fc543004
541e4010000006a47304402203a889974c7f27c1a4faf1168509887a614e60327ed81
623d5bb040bd079cb1ff022018e657b87a227bc27b2655750297f57222dac5683ff3a
3cc0f1b451c93a20cea012102aef7fed90d530e790da2c7cf9638a0263aa7a1c72be5f
786357bdee1c8e008a7ffffffff0200e1f505000000001976a91401cd60975e1ca2d3a0
583fc1c6d6b2a764ef408988ac0000000000000000116a0f44454641554c542e4142
43442e425a00000000",
"complete": true
}

і відправляємо в мережу:

sendrawtransaction
010000000150412a90aefbe2df51b8feb5ec85f4158261becf638f356e1d4fc5430045
41e4010000006a47304402203a889974c7f27c1a4faf1168509887a614e60327ed816
23d5bb040bd079cb1ff022018e657b87a227bc27b2655750297f57222dac5683ff3a3
cc0f1b451c93a20cea012102aef7fed90d530e790da2c7cf9638a0263aa7a1c72be5f7
86357bdee1c8e008a7ffffffff0200e1f505000000001976a91401cd60975e1ca2d3a05
83fc1c6d6b2a764ef408988ac0000000000000000116a0f44454641554c542e41424
3442e425a00000000 true

Вказана фраза назавжди записалась у блокчейн криптовалюти Mooncoin.

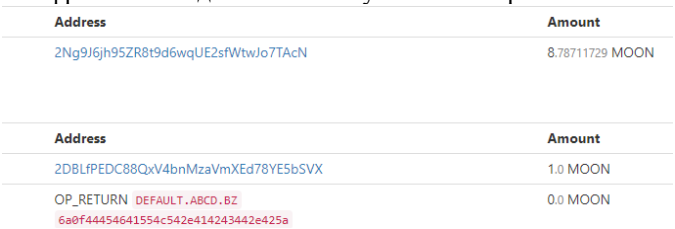

Рис. 2. Запис, доступний для перегляду на Blockexplorer

Чим більший розмір кодованих даних, тим більше потрібно монет на оплату комісії, так як оплачується розмір транзакції. Максимальний розмір транзакції не може бути більшим, ніж максимальний розмір блоку. Звідси виходить що, якщо зробити форк безкінечну емісію на адресах та розширити розмір блоку, то можна використовувати його для організації розподіленої бази даних для внутрішнього використання [3, 4].

II.2. Модель блокчейн

Блокчейн приймає два нових типи транзакцій: *Taccess*, що використовується для управління доступом, і *Tdata*, для зберігання і пошуку даних. Ці операції в мережі можуть бути легко інтегровані в комплект для розробки програмного забезпечення для мобільних пристроїв (SDK), чиї служби можуть використовувати в процесі розробки.

Для ілюстрації розглянемо наступний приклад: користувач встановлює програму, яка використовує нашу платформу для збереження її конфіденційності. Коли користувач підписується вперше, генерується новий спільний (користувач, сервіс) ідентифікатор і надсилається, разом з відповідними дозволами, блокчейн в транзакції *Taccess*. Дані, зібрані на телефоні (наприклад, дані датчиків розташування), шифруються за допомогою спільного ключа шифрування і надсилаються блокові в транзакції *Tdata*, який згодом направляє її до сховища ключ-значення без блоку, зберігаючи лише вказівник до даних у загальній книзі (покажчик - хеш даних SHA-256).

Тепер і служба, і користувач можуть запитувати дані за допомогою транзакції *Tdata* з вказівником (ключем), пов'язаним з нею. Потім блокчейн перевіряє, що цифровий підпис належить або користувачеві, або службі. Для служби також перевіряються її дозволи на доступ до даних. Нарешті, користувач може змінити дозволи, надані сервісу, у будь-який час, видавши транзакцію *Taccess* з новим набором дозволів, включаючи відкликання доступу до раніше збережених даних. Розробка веб-панелі (або мобільної панелі), яка дозволяє переглядати та редагувати дані, досить тривіальна і схожа на розробку централізованих гаманців, таких як Coinbase для Bitcoin1.

II.3. Приклади використання блокчейн

Наведемо приклади використання технології блокчейн: виборча система, реєстрація в земельному кадастрі, авторські і художні права, фінансовий сектор, логістика.

Децентралізовані вибори. Завдяки технології блокчейн демократичний вибір може бути, нарешті, справді демократичним. Громадяни голосують анонімно, відправляючи свою “монету” в гаманець вибраного ними кандидата. Блокчейн фіксує і підтверджує транзакцію. Переможець визначається за кількістю жетонів у гаманці. Оскільки блокчейн є публічною технологією, кожен виборець може відстежити частку свого голосу.

Земельний кадастр. Запис в земельній книзі через блокчейн не зникне і буде записаний там назавжди. Це ефективно запобігає несанкціонованому поводженню з нерухомістю, незаконному привласненню фінансових авансів і так далі. Впровадження цієї технології в області реєстрації нерухомості вже розглядалося декількома проектами. Система блокчейна не тільки буде ефективна проти шахрайства, але і допоможе знизити загальну вартість реєстрації та роботи бази даних.

Авторські права та права на художній твір. До появи Інтернету цієї проблеми не існувало. Звичайно, можна було скопіювати музику, книгу і фільми, але це робилося в дуже невеликому масштабі. Але потім, коли ера Інтернету набрала силу, ці галузі стали дуже сильно страждати. Блокчейн може вирішити цю проблему дуже ефективно. RIAA може створити невідновну копію пісні для одного покупця через блокчейн. Але таке теж можна обійти, за допомогою перезапису пісні під час її програвання.

Фінансовий сектор. У фінансовій сфері блокчейн можна використовувати для торгівлі, міжнародних переказів, нормативної звітності, бухгалтерського обліку та аудита. Також буде простіше розслідувати випадки махінацій, через ланцюжкову схему.

Логістика. Для логістики блокчейн підходить через свою структуру, так як він працює по принципу ланцюга. Якщо взяти приклад пересилання товару, то сам товар можна позначити як транзакцію, яку пересилають з адреси на інший адрес, якщо вона прийшла на пункт доставки. При неуспішній доставці товару, транзакцію можна відправити на неіснуючу адресу і тим самим позначити, що товар загублений. Для перегляду статусу доставки можна використовувати block explorer.

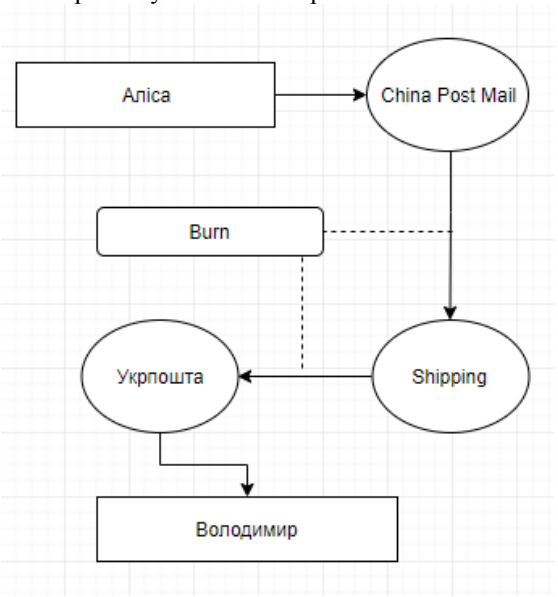

Рис. 3. Приклад передачі товару

На рис. 3. позначено приклад логістики за допомогою блокчейну.

II.4. Розумні контракти

Розумні контакти (з англ. «smart conctracts») дуже популярні останнім часом, тому про них досить багато говорять, як і про Blockchain.

Смарт-контракти такі самі, як і звичайні контракти, але вони повністю цифрові. Розумний контракт можна представити як програму, яка зберігається в блокчейні [5].

Принцип смарт контрактів, можна продемонструвати як машину зі звичайною питною водною. Після отримання монет він видасть напій або поверне кошти власнику, якщо виявить, що отримані гроші не відповідають

ціні. Він також може повернути переплату і скасувати транзакцію. Будь-хто, хто має достатньо монет, може закрити цей звичайний контракт.

Тим не менше, це порівняння повністю відображає поняття розумних контрактів. Немає можливості заздалегідь вивчити умови контракту і необхідно покладатися на презентацію виробника. Розумний контракт між двома сторонами можна укласти, завантаживши контракт у віртуальну мережу Ethereum (ця криптовалюта була створена для підтримки розумних контрактів). Мережа гарантує обом сторонам, що контракт буде виконаний відповідно до правил його вихідного коду, який може прочитати кожен, а хід контракту може відстежуватися обома сторонами завдяки блокчейну.

III.5. Подальше використання блокчейн

Технологія, яка успішно використовується в криптовалюті Bitcoin, що забезпечує найвищий рівень безпеки проведених в ній транзакцій, буде використовуватися не тільки у фінансовій галузі або державній інфраструктурі, але і в промисловій галузі. Блокчейн може повністю змінити функціонування виробничих компаній. В даний час галузь страждає від нестачі прозорості в ланцюжку поставок. Коли він розширюється, отримання повного уявлення про всі транзакції, здійснені постачальниками, субпідрядниками або клієнтами, стає незрозумілим. В результаті кінцевий користувач не може простежити шлях, по якому пройшли всі елементи, складові в кінцевий продукт. Проте, він має залишкову інформацію, наприклад, про країну, в якій проходив заключний етап виробництва або про тип матеріалів, використовуваних у ньому.

Технологія Blockchain може покращити прозорість та ідентифікацію в ланцюжку виробничих поставок, використовуючи захищену від шахрайства розподілену базу даних і контрольований доступ. Це дозволить збирати ключову інформацію про походження кожного окремого інгредієнта, використовуваного в процесі виробництва. Це означає новий рівень прозорості та безпеки.

Усе більше і більше компаній планують впровадити базу даних, яка поширюється по мережі і містить захищені блоки інформації про всі транзакції, пов'язані з обраним продуктом.

Безпека інформаційних потоків контролюється, серед іншого розширена криптографія, яка є невід'ємною частиною Blockchain. На практиці це означає, що немає можливості що хтось буде маніпулювати системою, вносячи зміни в колись збережені дані. Децентралізація має ще одну важливу перевагу: навіть якщо хакери можуть успішно провести атаку, яка виключить деякі з ключових комп'ютерів з обігу, вона все одно не паралізує роботу системи.

Висновки

Описана база даних, що використовується в blockchain. Аналізуються приклади реальних областей для блокчейн. Визначено поняття

інтелектуальних контракти\ів та їх потенціал для blockchain. Аналіз блокованих даних корисний для досліджень і комерційних додатків. Значне місце в аналізі займає BlockSci. Це програмне забезпечення з відкритим вихідним кодом для аналізу діапазону блоків.

1. Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

2. *Plotnikov, V., & Kuznetsova,* V. (2018). The Prospects for the Use of Digital Technology "Blockchain" in the Pharmaceutical Market. In *MATEC Web of Conferences* (Vol. 193, p. 02029). EDP Sciences.

3. *Pastor, I. G., Olaso, J. R. O., & Fuente, F. S.* Unveiling the Opportunities of Using Blockchain in Project Management. *Research and Education in Project Management (Bilbao, 2018)*, 22.

4. *Kushch, S., & Prieto Castrillo, F*. (2017). A review of the applications of the Block-chain technology in smart devices and dis-tributed renewable energy grids.

5. Lytvyn, V., Kuchkovskiy, V., Vysotska, V., Markiv, O., & Pabyrivskyy, V. (2018, September). Architecture of System for Content Integration and Formation Based on Cryptographic Consumer Needs. In 2018 IEEE 13th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT) (Vol. 1, pp. 391-395). IEEE.

http://doi.org/10.5281/zenodo.3612256

Поступила 19.09.2019р.

УДК 004.032.26

І.Є. Ваврук, Львів
Д.В. Воловик, Львів

ВИДІЛЕННЯ ГРАНИЦЬ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Abstract. The method of extracting edges of image using a convolutional artificial neural network is developed.

Keywords. Artificial Neural Network, Convolutional Neural Network, Smoothing, Activation Function, image edges.

Постановка проблеми

Комп'ютерний зір широко використовується для імітації ефекту людського зору шляхом електронного «сприйняття» та «розуміння» зображення. Надання комп'ютерам можливості «бачити» є нелегким завданням. Для забезпечення комп'ютерного зору важливим етапом є

