DOI 10.34185/1562-9945-6-137-2021-02
УДК 004.056.5

О.С. Волковський, М.В. Пачевський, Є.О. Обидєнний

КОНЦЕПЦІЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Анотація. У сучасному демократичному цифровому суспільстві зростає актуальність проведення відкритих та об'єктивних голосувань з використанням нових інформаційних технологій. Існуючі рішення для подібних систем голосування зосереджені на технічних та юридичних проблемах, а не на застосуванні нових інформаційних технологій у стадії голосування. Було проведено аналіз проблем сучасних виборчих систем, і, на підставі аналізу їх недоліків запропоновано алгоритми, та практичну реалізацію системи голосування на основі застосувань технології блокчейн зі спеціальною реалізацією смарт-контрактів, у якій недоліки існуючих систем усунуті.
Ключові слова: блокчейн, смарт-контракт, система голосування.

Вступ та постановка проблеми. Нині демократичне голосування є одним із найпопулярніших методів вирішення суспільно важливих питань у розвинутих країнах. Найбільш поширеним методом голосування є паперова система. Даний метод має певні недоліки, серед яких технічні (фальсифікації, помилки в підрахунках, відсутність прозорості проведення), соціальні та економічні (висока вартість для бюджету). Електронні системи голосування не набули свого поширення через проблеми з безпекою, верифікацією результатів або некоректною роботою програмного забезпечення [1, 2].

Технологія блокчейн (від англ. blockchain ланцюжок блоків даних) пропонує нові можливості для розробки абсолютно інших видів цифрових послуг завдяки ключовим особливостям цієї технології, таким як прозорість і захищеність процесу передачі даних. Розробники мають можливість вивести систему голосування на новий інформаційно-технологічний рівень, який відповідає сучасним вимогам. Застосування смарт контрактів у поєднанні з технологією блокчейн допоможе вирішити більшість існуючих проблем сучасних систем голосування.

© Волковський О.С., Пачевський М.В., Обидєнний Є.О., 2021

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Аналіз останніх досліджень.Блокчейн-технологія у системах цифрового голосування викликає великий інтерес, що призводить до появи значної кількості досліджень. У роботах [3-5] досліджуються проблеми традиційних виборчих систем. Автори сходяться на думці, що існуючі методи, зокрема електронні системи, не можуть забезпечити достатній рівень прозорості та надійності, що не позначається на довірі виборців. У цих дослідженнях розбирається принцип роботи технології блокчейн, а також переваги її використання в системі виборів.

У табл. 1 представлено огляд та аналіз робіт про системи голосування на основі технології блокчейн.

Необхідно наголосити, що безпека голосування завжди є найбільшою проблемою при розгляді питання про впровадження цифрової системи голосування. Всі автори сходяться на тому, що з урахуванням особливостей технології блокчейн не може бути жодних сумнівів у здатності системи захистити дані від потенційних атак та фальсифікацій. Система голосування є складним механізмом, і при її розробці потрібно враховувати як людський фактор, так і особливості проведення голосувань у конкретній країні.

Таблиця 1

Зміст	Barnes A., Brake C,Perry T. (2018)[3]	Ben Ayed A. (2017)[4]	Boucher P. (2016)[5]
Аналіз існуючих виборчих систем	+	+	+
Огляд технології блокчейн	-	+	-
Перспективи використання технології блокчейн у виборчих системах	+	+	+
Практична реалізація системи голосування на основі технології блокчейн	-	-	-

Незважаючи на те, що автори пояснюють теоретичну основу технології, описують перспективи та переваги подібної системи, жодне з розглянутих вище досліджень не визначає структуру роботи системи голосування на практиці, і в них відсутні конкретні методи, алгоритми та концепти для практичної реалізації системи.

З урахуванням аналізу недоліків зазначених досліджень було поставлено завдання розробки системи голосування на основі технології блокчейн, структури її роботи, а також конкретних алгоритмів і моделей для її практичної реалізації.

Формулювання цілей статті. Метою дослідження є розробка інформаційної системи елекронного голосування на базі технології блокчейн Необхідно розробити алгоритм роботи електронного голосування , з достатнім рівнем безпеки та аналізом всіх можливих обмежень системи, розробити практичну реалізацію системи, привести модель роботи електронного голосування.

Основна частина. Розглянемо алгоритм роботи технології блокчейн на конкретному прикладі голосування:

Виборець хоче вибрати певного кандидата, тобто перевести свій токен (голос) на адресу обраного кандидата.

Ця транзакція пересилається в мережу, що складається з комп'ютерів, рівноправних вузлів, званих "нодами" (від англ. Node - вузол). Ця мережа з нод необхідна щоб обробити (підтвердити) цю транзакцію. Перевагою є те, що дана мережа може бути децентралізована, що знизить ймовірність спеціального втручання в роботу системи та підвищить довіру виборців.

Мережа з нод підтверджує транзакцію та статус користувача, використовуючи спеціальні алгоритми. В інших системах підтверджена транзакція може бути не лише "голосом", а також передачею грошей або даних.

Після підтвердження, транзакція поєднується з іншими підтвердженими транзакціями, формуючи новий блок цифрового реєстру.

Даний блок додається в блокчейн з використанням хеша попереднього блоку, тим самим місце кожного блоку в ланцюжку стає унікальним і не підлягає зміні, так як у разі спроби змінити конкретний блок всі наступні блоки стають не валідними.

У результаті транзакція завершена і записана до блокчейну, що гарантує її достовірність і захищеність, а обраний кандидат отримує "голос", що автоматично відображається для всіх спостерігачів.

Практична реалізація системи голосування. Вимоги до системи голосування:

- Аутентифікація. Можливість голосувати має певна кількість людей, які отримали на це право. Система не повинна підтримувати процес самостійної реєстрації, список виборців має бути підготовлений і завантажений заздалегідь. Безпосередньо перед голосуванням виборець повинен пройти

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

додатковий процес аутентифікації, інакше його голос ("токен") не повинен використовуватись. Також процес додаткової аутентифікації на виборчій дільниці не дасть можливість третім особам використати "голос" виборця поза його відому.

- Анонімність. Система голосування повинна виключати будь-які зв'язки між особистістю виборця та його "голосом" (токеном). Виборець та його вибір має залишатися повністю анонімним під час та після голосування.
- Точність. Результати повинні бути абсолютно об'єктивними, кожен "голос" (токен) повинен враховуватися, не може бути змінено, продубльовано або видалено.
- Відкритість. Система повинна мати можливість перевірки процесу голосування в режимі реального часу.
- Захищеність. Система має бути абсолютно захищена від різного виду програмних атак, перехоплення інформації третіми особами або втручання у процес голосування.
- Масштабованість. Система має бути розрахована можливість проведення голосувань федерального чи муніципального масштабів.

Обмеження системи. Передбачається, що виборці використовуватимуть захищені пристрої для голосування. Незважаючи на те, що технологія блокчейн гарантує безпеку та об'єктивність процесу голосування, зловмисник має можливість змінити вибір виборця за допомогою шкідливого програмного забезпечення, встановленого на пристрої голосування. Також особливістю технології блокчейн є неможливість зміни вибору у разі помилки користувача. Виборець може віддати свій голос, тобто здійснити вибір, лише один раз.

Пропонована послідовність здійснення процедури електронного голосування на базі технології блокчейн за допомогою смарт-контракту.

Розроблено послідовність здійснення процедури електронного голосування на базі технології блокчейн з використанням смарт-контракту (рис.1).

Смарт-контракт - умова чи алгоритм. призначений для укладання та підтримки контрактів, реалізованих у блокчейні. Смарт-контракти дають можливість здійснювати конфіденційні та надійні операції без участі зовнішніх посередників, оскільки саме ця технологія дозволить автоматизувати та захистити від змін систему цифрового голосування, тож розглянемо її особливості.

Смарт-контракт розміщується у блокчейні, де вся його логічна структура міститься у програмному блоці. Програмний блок пов'язує усі відомості, що

мають відношення до певного смарт контракту. Дані відомості можуть виконувати роль входу та виходу програмного коду і можуть запускати будь-які дії за межами блокчейну.

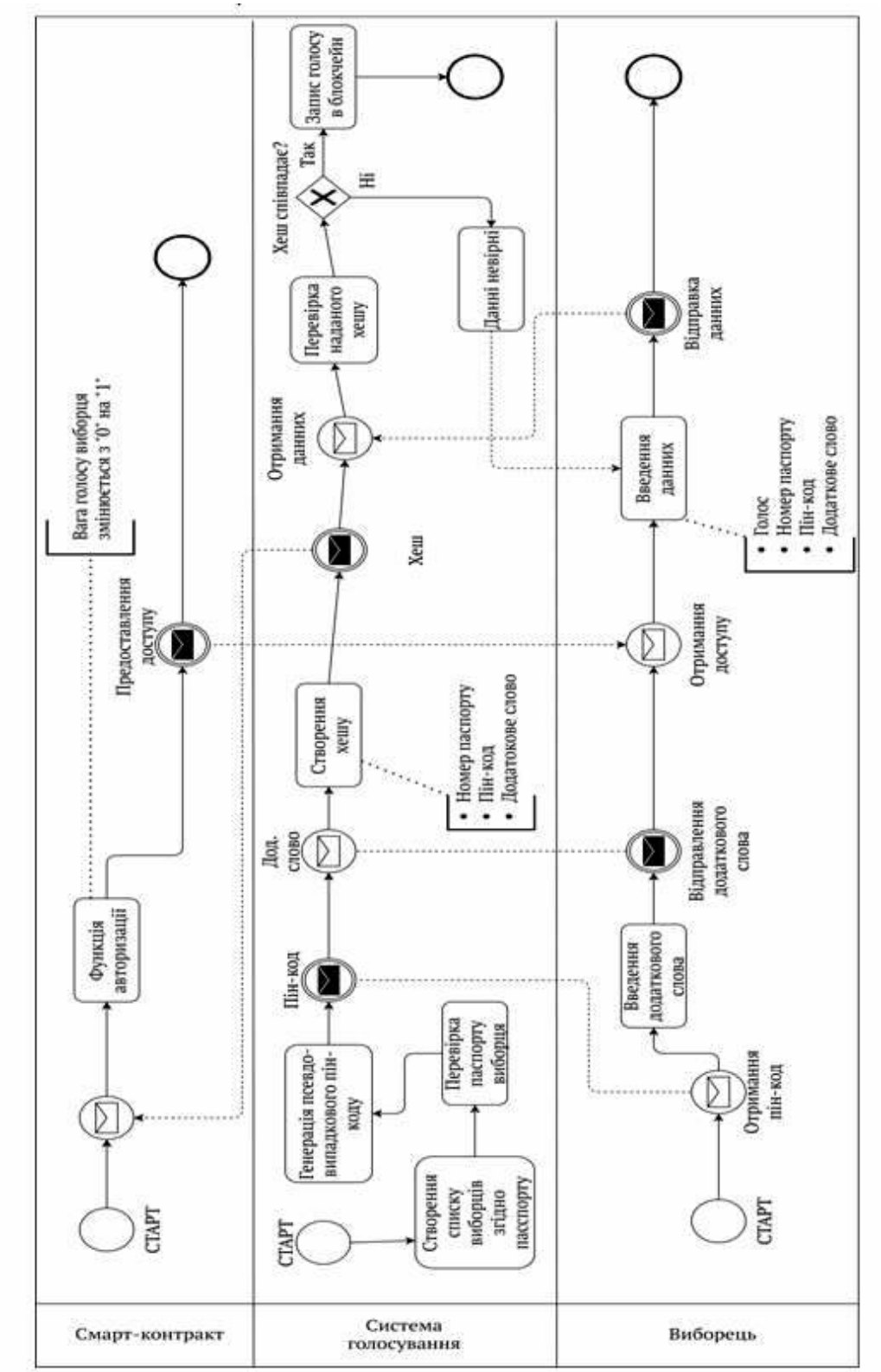

Рисунок 1 - Процедура електронного голосування на базі технології блокчейн

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Обов'язковими властивостями смарт контракту є:

- застосування методу електронного підпису на базі публічних або приватних ключів, що знаходяться у двох і більше сторін угоди;
- існування приватної децентралізованого середовища, в якому вноситься смарт контракт;
- суть договору та існування обов'язкових для його виконання інструментів;
- точно відображені умови його виконання, що підтверджуються підписом учасників договору, та надійність джерел даних.

Значна кількість різних договірних відносин як між людьми, так і між людським і державними органами можна реалізувати частково або повністю автоматизованими. Криптографія, яка лежить в основі смарт-контрактів, надає більш високий рівень безпеки та захищеності, ніж традиційні договори, засновані виключно на державному праві. Також смарт-контракти можуть знижувати економічні витрати, ризики неоднозначних трактувань договору, ризики використання "юридичних махінацій" та людський фактор.

У цій послідовності продуманий процес від приходу виборця на дільницю, його автентифікації до голосування за конкретного кандидата. Для роботи подібної системи розроблено смарт контракт, який включає:

1. Структури (програми) "Голосуючий" та "Кандидат". Для реалізації функціонування системи структура "Кандидат" містить поля: ім'я та підрахунок голосів, відданих за даного кандидата. Структура "Голосуючий" включає в себе поля для:

- зарахування токена (голосу) після успішної авторизації для здійснення голосування;
- даних про кандидата, за якого виборець віддав свій голос;
- одержаного хеша виборця;
- індикатора, чи голосував виборець.

2. Функції (програми) "Голосування", "Авторизації", "Створення голосування", "Підрахунки голосів". "Завершення голосування". Встановлення запропонованої системи на виборчих дільницях відбувається наступним чином: на першій ділянці вручну запускається genesis block, що створюється за описом і міститься в конфігураційному файлі.

Також при створенні процедури голосування до смарт-контракту завантажуються:

• список із номерами паспортів виборців (надає сторонній відповідальний орган);

• список кандидатів;

• час проведення голосування.

Далі система генерує пари виду [номер паспорта, псевдовипадковий пін-код] Голосуючий пред'являє паспорт співробітнику виборчої комісії, і його просять вигадати довільне додаткове число або слово.

Після цього система обчислює хеш від трьох параметрів: номер паспорта, псевдовипадковий пін-код, згенерований системою, додаткове число]. Дане додаткове число (слово) використовується як "salt" (сіль), для того, щоб:

- виключити перехоплення працівниками виборчого органу пін-кодів виборців;
- унеможливити підбір зловмисниками хеша.

Далі отриманий хеш автоматично відправляється до смарт-контракту в функцію auth (авторизації), і у користувача з'являється можливість проголосувати. Після цього користувач у терміналі голосування вводить свої дані, пін-код, додаткове слово або код - на підставі цих даних зчитується хеш і порівнюється з тим, який записаний у смарт-контракт. Після повної авторизації він голосує.

За бажанням розроблену систему голосування можна інтегрувати з державними сервісами, що значно спростить процес верифікації, і додаткове число (salt) не буде потрібно. Для цього необхідна завчасна реєстрація кожного учасника голосування у сервісі державних послуг. У такому разі ЦВК зобов'язана надавати сервісу список з номерами паспортів громадян, які мають право брати участь у конкретному голосуванні, а система державних послуг повинна видавати пін-код кожному учаснику голосування, за допомогою якого він зможе пройти ідентифікацію на виборчій дільниці.

Висновки. На підставі огляду систем голосування та аналізу їх недоліків, було запропоновано цифрове вирішення проблеми на основі блокчейн технології та розроблено повністю алгоритмічне вирішення проблеми. розроблено функціонально повну систему електронного голосування та схему проведення виборів на основі технології блокчейн при використанні смарт-контракту.

Ця система при подальшому доопрацюванні та впровадженні може дозволити створювати та проводити достовірну та прозору процедуру голосування, скоротити витрати держави на проведення виборчих компаній.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Спроектовану систему голосування можна застосувати у багатьох випадках, наприклад, у таких:

- Вибори президента, мера міста, голови регіону, але в цьому випадку потрібно буде додатково реалізувати систему мережевих вузлів для рівномірного розподілу навантаження на мережу.
- Вибори в наукових та освітніх закладах (вибори в Академії наук, вибори кращого викладача в університеті, голови студентської ради і т.д.)
- Державні вибори.

Особливістю результатів даного дослідження є той факт, що систему електронного голосування з запропонованою структурою при доопрацюванні для конкретних завдань, а також за допомогою вирішення питань масштабування можна впровадити в роботу державних органів, наукових та освітніх установ.

Крім того, передбачено можливість інтеграції підсистеми авторизації користувача з існуючими державними електронними послугами.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Gerlach J., Grasser U. Three Case Studies from Switzer land: E-voting // Berkman Center Research Publication. 02.04.09.URL: https://www.alexandria .unisg.ch/52680/ (дата запиту: 04.09.21).

2. Ibrahim S., Kamat M., Salleh M., Aziz S. R. A. Secure E-Voting with Blind Signature // Proceeding of the 4th Na tional Conference of Communication Technology. 14.01.03. URL: https://ieeexplore.ieee.org/document/1188334/ (дата запиту: 05.09.21).

3. Barnes A., Brake C., Perry T. Digital Voting with use of Blockchain Technology, available at: https://www.economist.com/sites/default/files/ plyoumouth.pdf (дата запиту: 04.09.21).

4. Ben Ayed A. A conceptual Secure Blockchain Electronic Voting System // International Journal of Network Security & Its Applications (IJNSA). 2017. Vol. 9, N. 3. URL: http:// aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf (дата запиту: 02.09.21).

5. Boucher P. What if blockchain technology revolutioni zed voting European Union. 2016.URL: http://europarl.europa.eu/RegData/etudes/ATAG/2016/ 581918 /EPRS_ATA(2016)581918_EN.pdf (дата запиту: 04.09.21).

REFERENCES

1. Gerlach J., Grasser U. Three Case Studies from Switzer land: E-voting // Berkman Center Research Publication. 02.04.09.URL: https://www.alexandria .unisg.ch/52680/ (access date: 04.09.21).

2. Ibrahim S., Kamat M., Salleh M., Aziz S. R. A. Secure E-Voting with Blind Signature // Proceeding of the 4th Na tional Conference of Communication Technology. 14.01.03. URL: https://ieeexplore.ieee.org/document/1188334/ (access date: 05.09.21).

3. Barnes A., Brake C., Perry T. Digital Voting with use of Blockchain Technology, available at: https://www.economist.com/sites/default/files/ plyoumouth.pdf (access date: 04.09.21).

4. Ben Ayed A. A conceptual Secure Blockchain Electronic Voting System // International Journal of Network Security & Its Applications (IJNSA). 2017. Vol. 9, N. 3. URL: http:// aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf (access date: 02.09.21).

5. Boucher P. What if blockchain technology revolutioni zed voting European Union. 2016.URL: http://europarl.europa.eu/RegData/etudes/ATAG/2016/ 581918 /EPRS_ATA(2016)581918_EN.pdf (access date: 04.09.21).

Received 06.09.2021.
Accepted 09.09.2021.

Концепция электронного голосования на основе технологии Блокчейн

В настоящее время демократическое голосование является одним из самых популярных методов решения общественно важных вопросов в развитых странах. Наиболее распространенным методом голосования является бумажная система. Данный метод имеет некоторые недостатки, среди которых технические (фальсификации, ошибки в подсчетах, отсутствие прозрачности проведения), социальные и экономические (высокая стоимость для бюджета). Электронные системы голосования не получили своего распространения из-за проблем с безопасностью, верификацией результатов или некорректной работой программного обеспечения [1, 2].

Concept of digital voting based on the Blockchain technology

Democratic voting is one of the most popular methods of resolving socially important issues in developed countries. The most common method of voting is the paper system. This method has certain disadvantages, including technical (falsifications, calculation errors, lack of transparency), social and economic (high cost to the budget). Electronic voting systems have not become widespread due to security issues, verification of results or incorrect operation of software [1, 2].

Blockchain technology offers new opportunities to develop completely different types of digital services due to the key features of this technology, such as transparency and security of the data transfer process. Developers have the opportunity to bring the voting system to a new information technology level that meets modern requirements. The use of smart contracts in combination with blockchain technology will help solve most of the existing problems of modern voting systems

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

Blockchain technology is based on a transactional model. The principle of operation of blockchain technology is shown in Pic. 1. Each user has his "wallet" with unique public / private keys, which confirm any action of the user. Transactions (agreement, shipment), which are carried out by all users of the system, are stored in successive blocks. Since the hash of the data of the previous block is used when generating the next, the consistency of the data within the blockchain is ensured.

Волковський Олег Степанович - кандидат технічних наук, доцент кафедри комп'ютерних наук та інформаційних технологій Дніпровського національного університету імені Олеся Гончара (м. Дніпро).

Пачевський Михайло Володимирович - асистент, кафедра комп'ютерних наук та інформаційних технологій Дніпровського національного університету імені Олеся Гончара (м. Дніпро).

Обидєнний Євген Олександрович – асистент кафедри інформаційних технологій та комп'ютерної інженерії Національного ТУ «Дніпровська політехніка».

Волковский Олег Степанович, кандидат технических наук, доцент кафедры компьютерних наук и информационных технологий Днепровского национального университета имени Олеся Гончара (г. Днепр).

Пачевский Михаил Владимирович, ассистент, кафедра компьютерних наук и информационных технологий Днепровского национального университета имени Олеся Гончара (г. Днепр).

Обыденный Евгений Александрович – ассистент кафедры информационных технологий и компьютерной инженерии Национального ТУ "Днепровская политехника".

Volkovskyi Oleg - Candidate of Sciences in Technology, docent of Department of Computer Science and Information Technologies, Oles Honchar Dnipro National University, Dnipro, Ukraine.

Pachevskyi Mykhailo - assistant, Department of Computer Science and Information Technologies, Oles Honchar Dnipro National University, Dnipro, Ukraine.

Obydennyj Evgeniy – Assistant of the Department of Information Technologies and Computer Engineering of the National Technical University "Dneprovsk Polytechnic".