Обробка інформації в складних організаційних системах

УДК 004.056.5 DOI: 10.30748/soi.2018.155.06

О.М. Букраба, Ф.С. Мазепа, К.Р. Карнишов, О.О. Яковенко, Н.І. Кушніренко

Одеський національний політехнічний університет, Одеса

СИСТЕМА ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Стаття присвячена розробці системи електронного голосування, яка реалізована на основі технології блокчейн. У статті проаналізовані основні недоліки існуючих системи електронного голосування та запропонована принципово нова система електронного голосування, яка гарантує збереження голосів виборців незмінними, дозволяє виборцю віддати свій голос дистанційно за допомогою смартфону або персонального комп'ютеру, а також переконатися, що голос був зарахований вірно, при цьому система забезпечує таємність голосування.

Ключові слова: *система електронного голосування, технологія блокчейн, електронний цифровий підпис, хеш сума.*

Вступ

Постановка проблеми та аналіз публікацій. Вибори – це найпоширеніша форма участі громадян у суспільно-політичному житті держави та місцевих органів самоврядування. Для проведення легітимних виборів необхідно прийняти заходи для запобігання порушенням під час голосування та підрахунку голосів, забезпечити збереження результатів голосування незмінними, спростити процес голосування для забезпечення високої явки виборців. Традиційна система голосування, яка використовується в багатьох державах, до числа яких належить Україна, не може в повній мірі гарантувати, що вибори були проведені з дотриманням усіх вищеперерахованих вимог [1–2]. На відміну від традиційних виборів, запропонована система електронного голосування з використанням технології блокчейн дозволить проводити вибори, які будуть відповідати вищеперерахованим вимогам [3].

Метою статті є проектування структури баз даних, які будуть використовуватися у електронній системі голосуванні, розробка алгоритму голосування, аналіз загроз, які найбільш характерні для системи електронного голосування. Технологія блокчейн буде використовуватися для збереження голосів виборців та "відривних частин бюлетенів" у розподілених базах даних, які будуть зберігатися на смартфонах, планшетах або персональних комп'ютерах виборців, які надалі будемо називати персональними пристроями виборця, завдяки чому буде гарантована незмінність результатів голосування.

Виклад основного матеріалу

Аналіз існуючих систем електронного голосування

Системи електронного голосування можна поділити на два типи: ті, які потребують безпосередньої наявності виборця на виборчій дільниці та ті, які дозволяють проголосувати дистанційно [4]. Прикладами систем, які потребують наявності виборця на дільниці, є КОВБ-2003 та КОВБ-2010, які дозволяють автоматизувати процес підрахунку бюлетенів.

Такі системи як Hart eSlate DRE [5], UE 2000, ДАС "Вибори" відносяться до систем прямого запису. Вони зчитують голос виборця за допомогою електронно-оптичних або механічних компонентів та одразу записують голос виборця на електронний носій, завдяки чому забезпечують вищий рівень автоматизації виборчого процесу у порівнянні з системами КОВБ-2003 та КОВБ-2010.

Перша система електронних виборів з можливістю дистанційного голосування була застосована 16 жовтня 2005 року на муніципальних виборах в Естонії. Для того щоб проголосувати на виборах у Естонії через мережу Інтернет, у виборця має бути ID-паспорт громадянина Естонії, комп'ютер з підключенням до мережі Інтернет та прилад для зчитування інформації з ID-паспорту [6].

Окрім Естонії, досвід з проведення Інтернет-виборів різних рівнів (від місцевих до парламентських) мають Великобританія, Сполучені Штати Америки [7] та Росія [8].

Вимоги до нової системи електронного голосування

Згідно зі статтею 71 Конституції України вибори в органи державної влади та органи місцевого самоврядування здійснюються шляхом таємного голосування, тому перш за все система електронного голосування має забезпечувати збереження таємниці голосування [9]. Не менш важливими вимогами, яким має задовольняти система електронного голосування, є неможливість змінити голоси виборців та провести вкидання бюлетенів. Для того щоб забезпечити високий рівень довіри виборців до нової системи електронного голосування, в ній повинен бути реалізований прозорий алгоритм підрахунку голосів та можливість перевірки виборцем стану свого голосу, а саме того, що голос був записаний у базу даних та не був змінений. Вище перелічені вимоги перш за все впливають на архітектурні рішення, які будуть застосовуватися у системі електронного голосування: механізм автентифікації виборця, отримання цифрового бюлетеня та збереження голосів виборців. Але окрім відповідності вище перерахованим вимогам, система має дозволяти виборцям проголосувати дистанційно за допомогою персонального пристрою, оскільки це дозволить залучити до участі в виборах більшу кількість виборців і, як наслідок, отримати більш об'єктивні результати голосування. Вихідний код системи електронного голосування має знаходитися у відкритому доступі.

Аналітичний огляд технології блокчейн

Блокчейн – це розподілена база даних, у якій дані зберігаються у вигляді ланцюжку блоків, який постійно зростає, захищений від підробки та переробки даних. Кожен блок ланцюжку складається з заголовку та списку транзакцій. Заголовок блоку містить інформацію хеші попереднього блоку, хеш-сумах транзакцій, які увійшли у цей блок, свій хеш та час створення блоку. Перший блок в ланцюжку називають первинним блоком і розглядають як окремий випадок, оскільки він не має материнського блоку [10]. Для того щоб новий блок був прийнятим іншими користувачами мережі, він має задовольняти певним вимогам, які варіюються у залежності від обраного протоколу консенсусу. Найбільш поширеними протоколами консенсусу є доказ виконання роботи (Proof of Work (PoW)) та доказ долі власності (Proof of Stake (PoS)) [11]. Інші протоколи консенсусу застосовуються для вирішення вузького спектру задач [12]. Технологія блокчейн отримала широко розповсюдження у сфері криптовалют. В Україні з 2017 року ця технологія використовується в оновленій системі електронних торгів конфіскованим майном СЕТАМ та в інформаційній системі державного земельного кадастру [13].

Структура системи електронного голосування, яка пропонується

Проектування архітектури баз даних є важливим етапом розробки програмного забезпечення. Тому розробку системи електронного голосування доцільно розпочати з проектування архітектури баз даних. Для реалізації системи електронного голосування на основі технології блокчейн пропонується використовувати три бази даних: одну централізовану реляційну базу даних voterRegisterDB, яка буде зберігатися на серверах центральної виборчої комісії, та дві розподілені бази даних bulletinDB та votesDB, побудовані на основі технології блокчейн, які зберігатимуться на персональних носіях виборців. Структури полів вище перелічених баз даних наведені на рис. 1–3 відповідно.

Id виборця
ПІБ виборця
Адреса прописки виборця
Дата народження виборця
Публічний ключ виборця pubKeyN
Вхідні умови задачі taskN
Рішення задачі taskN
Бюлетень bulletinN

Рис. 1. Поля централізованої бази даних voterRegisterDB для зберігання реєстру виборців

Id блоку
Хеш-сума попереднього блоку
Бюлетень bulletinN, підписаний особистим ключем виборця prvKeyN
Час генерації блоку

Рис. 2. Поля розподіленої бази даних bulletinDB, яка реалізована на основі технології блокчейн

Id блоку
Хеш-сума попереднього блоку
Голос виборця
Хеш-сума для ідентифікації голосу hashN
Час генерації блоку

Рис. 3. Поля розподіленої бази даних votesDB, ка реалізована на основі технології блокчейн

Алгоритм голосування

Голосування за допомогою системи електронного голосування складається з наступних кроків:

1. Виборець має з'явитися до органу ведення Реєстру виборців з паспортом та ідентифікаційним кодом. Після перевірки особи виборця йому буде наданий одноразовий ключ oneTimeKeyN, який необхідний для того, щоб виборець міг додати свій відкритий ключ pubKeyN у базу даних voterRegisterDB.

2. Виборець, використовуючи свій персональний пристрій, генерує електронний цифровий підпис, а саме відкритий ключ pubKeyN та особистий ключ prvKeyN. Авторизувавшись на сайті ЦВК, за допомогою одноразового ключа oneTimeKeyN, виборець публікує свій відкритий ключ pubKeyN. Відкритий ключ pubKeyN публікується у списку виборців voterRegisterDB навпроти відповідного виборця. Генерація ключів є обов'язковою процедурою для усіх виборців, які бажають вперше прийняти участь у електронному голосуванні.

3. Виборець має завантажити та встановити програмне забезпечення для електронного голосування на свій персональний пристрій. Хеш-сума програмного забезпечення programHash має бути опублікована на сайті ЦВК, для того щоб виборець мав змогу переконатися, що було завантажене та встановлене офіційне програмне завантаження та в нього не були внесені будь-які зміни.

4. Виборець має авторизуватися у системі електронного голосування за допомогою особистого ключа prvKeyN.

5. Якщо у поточний момент відбуваються вибори, то система автоматично розпочне завантаження копій баз даних bulletinDB та votesDB, побудованих на основі технології блокчейн, через мережу Інтернет. У іншому випадку завантаження баз даних bulletinDB та votesDB розпочнеться одразу ж після початку голосування, у якому виборець має право прийняти участь.

6. Після закінчення завантаження баз даних bulletinDB та votesDB система електронного голосування автоматично відправить запит на отримання випадкових вхідних даних для вирішення асиметричної задачі taskN до ЦВК. Вхідні данні для задачі taskN генеруються автоматично, підписуються електронним цифровим підписом ЦВК та публікуються у списку виборців навпроти відповідного виборця.

7. Асиметрична задача taskN вирішується на пристрої виборця. Знаходження рішення задачі є ресурсномістким процесом. Отримане рішення задачі taskN, підписане ключем prvKeyN, передається до ЦВК. Рішення задачі taskN є доказом виконаної роботи (Proof of Work (PoW)) та є аналогом підпису виборця у виборчому списку при традиційному голосуванні. Вирішення ресурсномісткої задачі необхідно для захисту системи електронного голосування від можливого масового фіктивного голосування, оскільки воно вимагатиме наявності великої обчислювальної потужності у зловмисників.

8. ЦВК перевіряє правильність вирішення виборцем асиметричної задачі taskN. Якщо задача вирішена вірно, ЦВК розміщує вирішення задачі taskN у відповідній графі у списку виборців voterRegisterDB та генерує бюлетень bulletinN, який складається з унікальної послідовності символів, та публікується у списку виборців.

9. Виборець підписує свій бюлетень bulletinN особистим ключем prvKeyN та відправляє запит на додання підписаного бюлетеня у базу даних bulletinDB.

10. Після перевірки того, що цей бюлетень ще не був доданий до бази даних bulletinDB та підписаний особистим ключем виборця prvKeyN, він додається у мережу блокчейн bulletinDB, а виборцю надається можливість додати свій голос voteN у базу даних votesDB.

11. У залежності від того, які вибори проходять на даний момент, виборець віддає свій голос за одного з кандидатів, політичну партію або рішення референдуму. Після того, як виборець проголосував, йому пропонується впродовж 30 секунд намалювати на екрані смартфону або планшету, чи за допомогою комп'ютерної миші або тачпаду, у випадку голосування через персональний комп'ютер, будь-який випадковий малюнок. Цей малюнок та час голосування буде використаний для генерації хеш-суми hashN. Генерація хеш-суми hashN відбуватиметься на персональному пристрої виборця. Ця хеш-сума hashN буде додана до голосу виборця, який буде записаний у базу даних votesDB, а також збережена на персональному пристрої виборця. Це дозволить виборцю ідентифікувати свій голос серед інших, для того щоб перевірити те, що він записаний у базу даних votesDB та його значення не було змінено. Хеш-сума hashN не передається виборцем у ЦВК, тому ніхто окрім виборця не знатиме, кому належить голос виборця voteN, тому виборець не може бути ідентифікований ні ЦВК, ні іншими виборцями.

12. Голос виборця voteN записується у базу даних votesDB. Можливість виборця додати голос voteN до бази даних votesDB анулюється.

13. Виборець отримує змогу перевірити те, що його голос voteN був записаний до бази даних votesDB та не був змінений.

Аналіз захищеності запропонованої системи електронного голосування

Запропонований проект системи електронного голосування дозволяє забезпечити високий рівень захисту системи від найбільш вірогідних порушень, які можуть виникнути під час проведення електронних виборів та вплинути на результат чи перебіг голосування.

Захист результатів голосування від зміни та(або) видалення голосів забезпечується завдяки тому, що бюлетені та голоси виборців зберігаються у розподілених базах даних, які реалізовані на основі технології блокчейн та зберігаються на персональних пристроях виборців. Оскільки технологія блокчейн є захищеною за дизайном та відповідає

вимогам задачі візантійських генералів [12], то для того, щоб змінити результати голосування, зловмисники мають виконати атаку 51 відсотка. Така атака може бути проведена шляхом змови більшості виборців, що є майже недосяжною задачею, або завдяки масовому злому облікових записів виборців, який неможливо виконати через високу обчислювальну складність, пов'язану з використанням електронного цифрового підпису для автентифікації виборців.

Окрім захисту від зміни та видалення результатів голосування, використання електронного цифрового підпису виборця дозволяє знизити ризик того, що зловмисники зможуть проголосувати від імені іншого виборця. Електронний цифровий підпис виборця виконується за алгоритмом RSA, надійність якого полягає у високій обчислювальній складності знаходження зворотної функції до функції шифрування. Складність знаходження зворотної функції полягає у факторизації великого цілого числа n на прості множники. Загальний метод решета числового поля, який є найшвидшим алгоритмом факторизації на сьогоднішній день, дозволяє виконати розкладання k-бітного цілого числа на множники зі швидкістю, яка обраховується за формулою (1) [14]:

$$\exp((c + o(1))k^{\frac{1}{3}} \log^{\frac{2}{3}} k), \text{ для } c < 2. \qquad (1)$$

При обраній довжині ключа цифрового підпису ця швидкість є доволі низькою, що не дозволяє зловмисникам виконати масове голосування від імені інших виборців.

У системі реалізований двохфакторний захист від фальсифікації результатів виборів шляхом додавання у список виборців неіснуючих виборців та подальшого голосування від їх імені. По-перше, система вимагає надання доказу виконаної роботи (Proof of Work (PoW)). Це потребує наявності у ЦВК, або інших зловмисників, великих обчислювальних потужностей для проведення масових фальсифікацій. По-друге, публічно оприлюднений список виборців дозволяє виборцям перевірити коректність списку виборців. Колективна перевірка списку виборців дозволить значно скоротити кількість помилок у ньому та ускладнить додання великої кількості неіснуючих виборців до списку виборців.

Повністю автоматизований процес підрахунку голосів дозволяє уникнути помилок під час підрахунку голосів, пов'язаних з людським чинником. Відкритий вихідний код системи гарантує, що алгоритм підрахунку голосів буде прозорим та не буде містити помилок. Також кожен з виборців може власноруч виконати перерахунок голосів та порівняти отриманий результат з результатом, який був опублікований ЦВК.

Збереження таємниці голосування забезпечується завдяки використанню двох розподілених баз даних: у базі даних bulletinDB зберігаються підписані електронним цифровим підписом виборця бюлетені, а голоси виборців, які зберігаються у базі даних votesDB, не підписуються електронними цифровими підписами виборців, через які третя особа могла б ідентифікувати, за кого саме проголосував певний виборець. В той самий час для того, щоб виборець мав змогу перевірити свій голос, до нього додається хеш-сума hashN, яка дозволяє виборцю ідентифікувати свій голос voteN серед голосів інших виборців та перевірити його стан. В той самий час ні ЦВК, ні жодна третя особа не знає, кому з виборців належить хеш-сума hashN, оскільки її значення обчислюється на пристрої виборця та не передається у ЦВК. Реалізувати скритну передачу хеш-суми hashN до ЦВК неможливо, оскільки програмний код системи знаходитиметься у відкритому доступі та може бути перевірений виборцями. Змінити код системи без відома виборців також неможливо, оскільки в цьому випадку хеш-сума програми programHash неминуче зміниться, що дозволить виявити втручання у вихідний код системи електронного голосування.

Висновки

У статті запропонований принцип дії системи електронного голосування, реалізованої на основі технології блокчейн. Використання публічно доступного списку виборців та двох розподілених баз даних, реалізованих на основі технології блокчейн, дозволить реалізувати систему електронного голосування, яка задовольнятиме висунутим вимогам. Окрім того, запропонована система, на відміну від існуючих аналогів, дозволить не тільки автоматизувати процес підрахунку голосів, а й дасть змогу виборцям проголосувати дистанційно, використовуючи власний смартфон або персональний комп'ютер без додаткового обладнання, власноруч перерахувати результати виборів, а також перевірити те, що їх голос був зарахований та не був змінений, при цьому, запропонований алгоритм підпису голосу дозволить забезпечити таємницю голосування.

Список літератури

1. Постанова Верховної Ради України "Про схвалення Концепції запровадження системи електронного голосування в Україні" [Електронний ресурс]. – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/DF87900A.html/.

2. Сіденко І.Г. Перспективи впровадження електронного голосування в Україні [Електронний ресурс] / І.Г. Сіденко // Харків, 2012. – Режим доступу: http://www.kbuapa.kharkov.ua/ebook/conf/2012-2/doc/1/12.pdf/.

3. Gritzalis Dimitris. Secure Electronic Voting [Electronic resource] / Dimitris Gritzalis // 7th Computer Security Incidents Response Teams Workshop. – 2002. – P. 5-14. – Available at: https://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf.

4. Електронний науковий архів Науково-технічної бібліотеки Національного університету "Львівська політехніка". Впровадження електронного голосування в України: проблеми та перспективи. – Режим доступу: http://ena.lp.edu.ua/bitstream/ntb/33188/1/056-126-127.pdf.

5. The Official Site of Hart Intercivic eSlate. [Electronic resource]. – Available at: https://www.verifiedvoting.org/resources/voting-equipment/hart-intercivic/eslate/.

6. Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance / Sarah P. Everett, Kristen K. Greene, Michael D. Byrne, Dan S. Wallach, Kyle Derr, Daniel Sandler and Ted Torous // Proceedings of Measuring, Business, and Voting. – Florence, Italy. – April 5-10, 2008.

7. Electronic Voting Offers Opportunities and Presents Challenges [Electronic resource]. – Available at: https://www.gao.gov/new.items/d04766t.pdf/.

8. Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed [Electronic resource]. – Available at: https://www.gao.gov/assets/250/247851.pdf/.

9. Конституция Украины, принятая на пятой сессии Верховной Рады Украины 28 июня 1996 года с изменениями и дополнениями согласно Закону Украины "О внесении изменений к Конституции Украины" №2222-IV. – Харьков: ФЛП Спивак Т.К., 2010. – 48 с.

10. Офіціальний сайт Blockchain technology "Advantages & disadvantages of blockchain technology" [Electronic resource]. – Available at: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/.

11. Офіціальний сайт Blockchain Labs "What Are Consortium Blockchains?" [Electronic resource]. – Available at: https://www.blockchainlabs.asia/news/what-are-consortium-blockchains/.

12. Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations / Ethereum. – CreateSpace Independent Publishing Platform. – 2016. – 360 p.

13. Офіціальний сайт Міністерства аграрної політики та продовольства України. Державний земельний кадастр перейшов на технологію Blockchain [Електронний ресурс] – Режим доступу: http://minagro.gov.ua/node/24722/.

14. Coutinho S.C. The Mathematics of Ciphers: Number Theory and RSA Cryptography / S.C. Coutinho. – A K Peters/CRC Press; 1 edition. – 1999. – 198 p.

References

1. The Resolution of the Verkhovna Rada of Ukraine (2018), "*Pro spvalennya Koncepciyi zaprovadzhennya systemy elektronnogo golosuvannya v Ukrayini*" [*On Approval of the Concept for the Implementation of the Electronic Voting System in Ukraine*], available at: https://search.ligazakon.ua/l_doc2.nsf/link1/DF87900A.html/ (accessed 26 November 2018).

2. Sidenko, I.G. (2012), "Perspektyvy vprovadzhennya elektronnogo golosuvannya v Ukrayini" [Prospects for implementing e-voting in Ukraine], *Actual problems of public administration*, No. 2(42), pp. 222-230, available at: www.kbuapa.kharkov.ua/ebook/conf/2012-2/doc/1/12.pdf/.

3. Gritzalis, Dimitris (2002), Secure Electronic Voting, *7th Computer Security Incidents Response Teams Workshop*, pp. 5-14, available at: https://www.terena.org/activities/tf-csirt/meeting7/gritzalis-electronic-voting.pdf (accessed 26 November 2018).

4. Electronic Scientific Archive of the Scientific and Technical Library of the National University "Lviv Polytechnic" (2014), "*Vprovadzhennya elektronnogo golosuvannya v Ukrayiny: problemy ta perspektyvy*" [*Introduction of e-voting in Ukraine: problems and perspectives*], available at: http://ena.lp.edu.ua/bitstream/ntb/33188/1/056-126-127.pdf (accessed 26 November 2018).

5. The Official Site of Hart Intercivic eSlate (2017), *Hart Intercivic eSlate*, available at: https://www.verifiedvoting.org/resources/voting-equipment/hart-intercivic/eslate/ (accessed 26 November 2018).

6. Everett, Sarah P., Greene, Kristen K., Byrne, Michael D., Wallach, Dan S., Derr, K., Sandler, D. and Torous, T. (2008), Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance, *Proceedings of Measuring, Business, and Voting*, April 5-10, Florence, Italy.

7. *Electronic Voting Offers Opportunities and Presents Challenges*, available at: https://www.gao.gov/new.items/d04766t.pdf/ (accessed 27 November 2018).

8. United States Government Accountability Office (2005), *Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed*, available at: https://www.gao.gov/assets/250/247851.pdf/ (accessed at 26 November 2018).

9. (2010), "*Konstytutsyia Ukrayny, pryniataia na piatoi sessyy Verkhovnoi Rady Ukrayny 28 yiunia 1996 hoda s yzmenenyiamy y dopolnenyiamy sohlasno Zakonu Ukrayny «O vnesenyy yzmenenyi k Konstytutsyy Ukrayny» No. 2222-IV*" [*The Constitution of Ukraine, adopted by the fifth session of the Verkhovna Rada of Ukraine on June 28, 1996, with amendments and additions according to the Law of Ukraine "On Amendments to the Constitution of Ukraine" No. 2222-IV*], FLP Spivak T.K., Kharkiv, 48 p.

10. The official site of Blockchain technology (2016), *Advantages & disadvantages of blockchain technology*, available at: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/ (accessed 26 November 2018).

11. The official site of Blockchain Labs (2018), *What Are Consortium Blockchains?*, available at: https://www.blockchainlabs.asia/news/what-are-consortium-blockchains/ (accessed 27 November 2018).

12. Ethereum (2016), *Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, CreateSpace Independent Publishing Platform, 360 p.

13. The official site of the Ministry of Agrarian Policy and Food of Ukraine (2017), "*Derzhavnyi zemelnyi kadastr pereishov na tekhnolohiiu Blockchain*" [*State Land Cadastre switched to Blockchain technology*], available at: www.minagro.gov.ua/node/24722/ (accessed 27 November 2018).

14. Coutinho, S.C. (1999), *The Mathematics of Ciphers: Number Theory and RSA Cryptography*, A K Peters/CRC Press; 1 edition, 198 p.

Надійшла до редколегії 17.10.2018
Схвалена до друку 11.12.2018

Відомості про авторів:

Букраба Олександр Михайлович
студент 6-го курсу
Одеського національного політехнічного університету,
Одеса, Україна
https://orcid.org/0000-0002-6859-2941

Мазепа Федір Сергійович
студент 6-го курсу
Одеського національного політехнічного університету,
Одеса, Україна
https://orcid.org/0000-0002-6054-7660

Карнишов Кирилло Романович
студент 6-го курсу
Одеського національного політехнічного університету,
Одеса, Україна
https://orcid.org/0000-0002-0006-7593

Яковенко Олександр Олександрович
старший викладач кафедри Одеського національного політехнічного університету,
Одеса, Україна
https://orcid.org/0000-0003-1013-9463

Кушніренко Наталія Ігорівна
кандидат технічних наук доцент кафедри Одеського національного політехнічного університету,
Одеса, Україна
https://orcid.org/0000-0003-3722-0229

Information about the authors:

Oleksandr Bukraba
sixth year Student of Odesa National Polytechnic University,
Odesa, Ukraine
https://orcid.org/0000-0002-6859-2941

Fedir Mazepa
sixth year Student of Odesa National Polytechnic University,
Odesa, Ukraine
https://orcid.org/0000-0002-6054-7660

Kyrylo Karnyshov
sixth year Student of Odesa National Polytechnic University,
Odesa, Ukraine
https://orcid.org/0000-0002-0006-7593

Oleksandr Iakovenko
Senior Instructor of Odesa National Polytechnic University,
Odesa, Ukraine
https://orcid.org/0000-0003-1013-9463

Natalya Kushnirenko
Candidate of Technical Sciences Associate Professor of Odesa National Polytechnic University,
Odesa, Ukraine
https://orcid.org/0000-0003-3722-0229

СИСТЕМА ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

А.М. Букраба, Ф.С. Мазепа, К.Р. Карнышов, А.А. Яковенко, Н.И. Кушниренко

Статья посвящена разработке системы электронного голосования, которая реализована на основе технологии блокчейн. В статье проанализированы основные недостатки существующих систем электронного голосования и предложена принципиально новая система электронного голосования, которая гарантирует сохранение голосов избирателей неизменными, позволяет избирателю отдать свой голос дистанционно при помощи смартфона или персонального компьютера, а также убедиться, что голос был засчитан верно, при этом система обеспечивает сохранность тайны голосования.

Ключевые слова: *система электронного голосования, технология блокчейн, электронно-цифровая подпись, хэш сумма.*

ELECTRONIC VOTING SYSTEM BASED ON THE BLOCKCHAIN TECHNOLOGY

O. Bukraba, F. Mazepa, K. Karnyshov, O. Iakovenko, N. Kushnirenko

This article is devoted to development of electronic voting system based on the blockchain technology. Voting is the bridge between the governed and government. The current voting system has many security holes, and it is difficult to prove even simple security properties about them. There are also some reasons for a government to use electronic voting systems are to increase elections activities and to reduce the elections expenses. This article provides an overview of the experiences of other countries using electronic voting systems. Disadvantages of existing electronic voting systems were analyzed in this paper. Fundamentally new open source electronic voting system was supposed based on the analysis of existing electronic voting systems. Supposed electronic voting system uses blockchain for saving electronic votes on devices of voters. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. Each block of blockchain contains a cryptographic hash of the previous block, a timestamp, and transaction data. By design, a blockchain is resistant to modification of the data. Using of blockchain guarantees immutability of votes. This system allows voter to vote remotely using his own smartphone, tablet or personal computer and verify immutability of his vote. Voting secret is also guaranteed by this proposed electronic voting system. Main threats to the proposed electronic voting system were investigated. Investigation of these threats allows to design protected electronic voting system. Implementation of proposed electronic voting system will allow to increase legitimacy of elections, involve more voters to take participation in the elections.

Keywords: *electronic voting system, blockchain technology, digital signature, hash.*