© Munin V. , Salnikov A, Automation of voting processes for joint-stock companies using a homomorphic cryptosystem and blockchain technology// Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 2, pp. 82-87.

DOI: 10.18372/2225-5036.25.13839

МЕТОД ПРОВЕДЕННЯ ГОЛОСУВАННЯ СЕРЕД ВЛАСНИКІВ АКЦІЙ НА БЛОКЧЕЙНІ, ВИКОРИСТОВУЮЧИ КРИПТОСИСТЕМУ ПЕЙЕ ТА РОЗПОДІЛЕНУ ГЕНЕРАЦІЮ КЛЮЧІВ

Владислав Мунін, Андрій Сальніков

Київський національний університет ім. Т.Шевченка, Україна

МУНІН Владіслав Валентинович

Рік і місце народження: 1996, Краматорськ, Донецька область, Україна.
Освіта: Київський національний університет ім. Т.Шевченка, 2019 рік.
Наукові інтереси: криптографія, розподілені системи.
Публікації: тези доповідей на конференціях молодих вчених.
E-mail: vladcisco.vm@gmail.com.
Orcid ID: 0000-0002-8483-1826.

САЛЬНІКОВ Андрій Олександрович *к.т.н.*

Рік і місце народження: 1986, Чернігів, Україна.
Освіта: Київський національний університет ім. Т.Шевченка, 2009 рік.
Посада: асистент кафедри комп'ютерної інженерії.
Наукові інтереси: високопродуктивні та високодоступні системи., розподілені обчислення, Grid та Cloud-системи.
Публікації: більше 20 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: i@manf.org.ua.
Orcid ID: 0000-0002-1667-1357.

Анотація. *У статті запропоновано метод проведення безпечного голосування серед власників акцій зі збереженням секретності кожного голосу та отриманням довіреного результату на основі використання криптографічної системи Пейе, яка реалізує адитивну властивість шифротекстів. На основі запропонованого методу виконано імплементацію протоколу голосування з використанням технології блокчейн, що забезпечує довірене середовище обробки транзакцій. Коротко викладено теоретичні поняття технології блочного ланцюжку транзакцій, механізму гомоморфного шифрування, розподіленої генерації ключів. Наведено покроковий алгоритм функціювання системи, описано основні технічні аспекти та переваги застосування децентралізованих технологій для збереження та обробки даних. Було досліджено існуючі рішення в галузі проведення голосувань та приведено порівняльний аналіз. На основі проведеного аналізу було сформовано основні критерії проведення безпечного процесу голосування. Стисло описано метод розподіленої генерації ключів серед учасників системи з урахуванням відмінностей ключів криптосистеми Пейе від стандартних RSA ключів. У роботі докладно описано алгоритмом ієрархічної генерації ключів акціонера. Використання цього алгоритму дає можливість оптимізувати процес збереження та обробки криптографічних матеріалів на клієнтському застосунку. Також було розкрито та обґрунтовано доцільність використання технології розумних контрактів, які є децентралізованими застосунками із спільним середовищем зберігання даних та консенсус алгоритмом. Контракти являють собою алгоритм обробки даних транзакцій у мережі, дозволяють перевіряти правила функціювання системи та проводити логічні операції над даними у захищений спосіб. Наведений метод може використовуватись для проведення голосувань у консорціумах, акціонерних товариствах та приватних мережах, бути інтегрований до децентралізованих систем зберігання даних для забезпечення безпечного механізму прийняття рішення.*

Ключові слова: *блокчейн, криптосистема Пейе, консенсус, публічний ключ, приватний ключ, розумний контракт.*

Актуальність проблеми дослідження

Ідея проведення електронного голосування набуває поширення у різних галузях життєдіяльності, починаючи з публічного сектору, а саме проведення виборів та референдумів закінчуючи приватними голосуваннями у бізнес середовищі , корпораціях та консорціумах [1]. Сучасні рішення спираються на централізовану інфраструктуру з використанням єдиного довіреного центру, який буде проводити підрахунок результатів голосування [2, 3]. При застосуванні цього підходу секретність голосу не забезпечуються, тобто виборча комісія має технічну можливість переглянути хто і як проголосував. Слід зауважити, що при використанні стандартних методів шифрування та приховування голосів серед виборців виборчий комітет може дешифрувати голос кожного виборця. Тому постає проблема кінцевого визначення результатів із унеможливленням маніпулюванням даними та забезпеченням подальшої верифікації.

Використання централізованого середовища для збереження та обробки голосів не забезпечує захист від несанкціонованого втручання та підміни даних, навіть які зберігаються у зашифрованому вигляді. Компрометація файлів журналу та записів баз даних дозволяє вплинути на результати голосування з втратою можливості верифікації їх достовірності.

Розробка системи, що позбавлена описаних вразливостей є актуальною сучасною задачею. В даній роботі запропоновано використати децентралізовані технології зберігання даних, які забезпечують незмінну та прозору історію транзакцій, що набувають все більшої популярності в різних галузях науки і техніки. Так, на сьогодні технологія блочного ланцюжку транзакцій (англ. *blockchain*) активно використовується на рівні держави у проектах земельного устрою, проекти в Швеції, Грузії, Україні, публічних реєстрах, фінансових установах [4-6], та може бути адаптовано для поставленої задачі.

Метою цього дослідження є створення методу приватного голосування власників акцій з використанням системи Пейе, дистрибутивною генерацію ключів та обробкою даних у мережі блокчейн з детальним складових частин системи.

Аналіз існуючих досліджені у галузі проведення голосувань

На сьогодні дослідження у галузі використання децентралізованих середовищ зберігання даних, зокрема, технології блокчейн, що позитивно зарекомендувала себе в різних галузях активно ведуться в світі. З'являються прототипи проектів для проведення публічних голосувань за допомогою цих технологій. Так, наприклад, проект NEM підписав меморандум про співпрацю з державними виконавчими органами України про проведення виборів, використовуючи децентралізовані технології [7]. Рішення використовує публічну мережу блокчейну NEM та спеціально розроблений гаманець NanoWallet з підтримкою відправки multisig транзакцій, тобто транзакцій, які мають бути підписані більш ніж одним учасником мережі. Особливістю блокчейну Nem є побудова модульної архітектури, яка дозволяє проводити інтеграцію між різними типами цифрових активів. Недолік рішення полягає в тому, що секретність голосу окремого виборця не забезпечується з використанням вбудованих механізмів, де кожен голос і є цифровим активом, що потребує фінансових витрат на підтримку дієздатності користувачів системи.

Питання побудови анонімізованої системи голосування розглядають Ю Лі та Кю Ванг в своїй роботі "An E-voting Protocol Based on Blockchain" [2]. Автори пропонують використовувати технологію сліпих підписів, що забезпечують неможливість розпізнавання справжнього відправника транзакції. При цьому слабким місцем системи залишається зміст транзакції ,який буде видно усім учасникам мережі. Автори намагаються вирішувати цю проблему шифруванням голосу публічним ключем системи зі зберіганням приватного ключа у довіреного посередника чи просто використовувати приватну систему доступу до блокчейну.

Інший підхід було представлено у науковій роботі "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy" Королівського коледжу Гелловею. Використання токенів, спеціальніх активів, для голосування частково вирішує проблему надання ваги голосу. Такий підхід створює можливість проводити розподілення активів при реєстрації але створює єдину точку відмови системи за рахунок централізованого емітента та валідатора[3].

Найбільш популярними серед працюючих блокчейн рішень у галузі проведення голосувань є платформи Agora та FollowMyVote.У проекті Agora всі операції здійснюються на анонімізованих даних. Анонімізація відбувається на рівні протоколу та імплементації мережевої інфраструктури [8]. Потім анонімізовані дані розшифровуються і усі підрахунки проводяться над відкритими текстами У проекті FollowMyVote реалізована складна схема реєстрації виборців з використанням сліпих токенів, що робить процес реєстрації максимально анонімізованим та безпечним [9].Проте автори проекту не приділяють уваги проблемі надання голосу ваги.

Проблема приватності голосу вирішується у рішенні «Large-scale Election Based On Blockchain» [10] за рахунок використання криптосистеми ElGamal, яка реалізує властивості мультиплікативності та адитивності шифротекстів [11], але потребує фази довіреного налаштування публічного та приватного ключів системи.

В досліджені Масачусетського університету [12] на відміну від попереднього рішення наводиться приклад використання адитивної криптосистеми Пейе, яка є більш простою у реалізації. Шифрування публічним ключем криптосистеми Пейе [13] є семантично безпечним процесом, тобто неможливо виявити закономірності між шифротекстами одного і того самого відкритого тексту. Проблема дистрибутивної генерації ключів описана у роботі "Experimenting with Shared Generation of RSA keys" [14]. Метою роботи є аналіз ефективності розподіленої генерації RSA ключів. Дослідження показали, що з використанням процесора з частотою 333 Mhz генерація розподіленого ключа відбувається за 1,5 хвилини. Враховуючи суттєве вдосконалення обчислювального обладнання виникає необхідність надання оновленої оцінки роботи алгоритму. Ідея безпечного процесу генерації ключів - гомоморфної криптосистеми - розглянуто у роботі "Efficient RSA Key Generation and Threshold Paillier in the Two-Party

Setting" [15]. Автори описують ключові відмінності ключів криптосистеми Пейе та можливість застосування підходу розподіленої генерації до такого типу системи із збереженням властивостей адитивності.

В даній роботі запропоновано метод, що поєднує дистрибутивну генерацію ключів без використання центрального довіреного серверу у приватних системах з урахуванням відсоткових ваг виборців , що дозволить створювати незалежні від центрального нотаріату системи голосування серед власників активів або прав голосу у приватних мережах. Підсумовуючи проведений аналіз порівняємо ключові характеристики наявних систем проведення голосування, використовуючи технологію блокчейн (таблиця 1).

Таблиця 1

Використання ключових механізмів електронного голосування

Рішення / **Механізм**	**Agora**	**FollowMy Vote**	**King's Colleage**	**Yi Liu and Qi Wang**
Анонімізація виборців	+			
Шифрування голосу	+	-	+	-
Зберігання даних	Технологія блокчейн			
Дистрибутивна генерація ключів	RSA	-	-	-
Операції над шифротекстами	-	ElGamal	+	-
Можливість перевірити голос	+	+	+	-
Використання токену	-	-	ERC20	-
Урахування потужності голосу	-	-	Частково	-

Як видно з порівняльного аналізу кожна з розглянутих систем, навіть при використані криптографічних механізмів, не забезпечує урахування потужності голосу, що доводить існування проблеми безпечного цифрового голосування власниками активів.

Для забезпечення можливості проводити математичні операції над шифротекстами у криптографії для процесу шифрування використовують спеціальний підхід, який здобув назву гомоморфне шифрування. Гомоморфне шифрування - це перетворення даних в шифрований текст, який можна проаналізувати та працювати з ним так, якби він був у відкритому вигляді за рахунок особливих властивостей криптосистеми. Гомоморфне шифрування довгий час було лише теоретичним напрямком досліджень, і лише в 2009 році в роботі Крейга Джентрі була розглянута можливість практичного застосування таких методів [16]. Запропонована Джентрі схема є алгоритмом повністю гомоморфного шифрування.

Для вирішення задачі безпечного збереження даних та роботи децентралізованого додатку , тобто такого додатку який не контролюється єдиним сервером і не має єдиної точки відмови системи. Під технологією блокчейн слід розуміти можливість децентралізованого способу збереження даних у вигляді послідовності блоків які алгоритмічно пов'язані один з одним. Кожен блок ідентифікується за допомогою гешу, створеного за допомогою криптографічного геш-алгоритму SHA256 у заголовку блоку. Кожний блок посилається на попередній блок. Такий зв'язок у структурі збереження даних унеможливлює підміну даних, без зміни всієї історії транзакцій, що дуже важливо в процесі голосування і проблеми підробки голосів.

Блок містить геш свого батька всередині власного заголовка. Там розташовується ланцюжок, що йде весь шлях назад до створеного першого блоку, також відомий як блок генезис, з'єднаний послідовністю гешей. Поле «попередній геш блоку» знаходиться всередині заголовка блоку, і таким чином поточний хеш блоку залежить від хешу батьківського блоку. Геш наступного блоку змінюється, якщо змінюється тотожність батьківських блоків. Блок - це структура даних, яка об'єднує транзакції для включення в журнал Блок складається з заголовку, що містять метадані, а потім довгий список транзакцій. Блок може бути ідентифікований двома способами, шляхом посилання на геш-блок або через посилання на висоту блоку. Це забезпечує властивість незмінності даних.

В основі роботи кожного блокчейн застосування полягає використання алгоритму консенсусу, який визначає правила створення нового блоку причому цей алгоритм може адаптований під окремий випадок, наприклад випускати блоки зможуть лише довірені вузли, що зробить неможливим атаки 51 %, коли зловмисник має більшість обчислювальної потужності в мережі. Збереження незмінної та прозорої історії транзакцій є важливою перевагою над існуючими способами зберігання даних.

Проблема контролю з боку централізованої частини системи вирішується розподіленою генерацію секретного ключа системи, яким буде проводитись дешифрування результатів голосування. Етап розподілення ключа Пейе складається з використання двох протоколів. По-перше, генерація ключа , який виконується лише один раз, і не вимагає постійних накладних витрат. У другому протоколі для дешифрування застосовується апарат нульових знань [17]. Схеми шифрування RSA і Пейе мають однаковий формат публічного та секретного ключів, композитного N і його факторів. Більш того, шифровані тексти мають схожу структуру. Таким чином, може здатися, що розшифрування за Пейе повинне бути однаковим до розподіленого дешифрування за алгоритмом RSA. Тим не менш, при на відміну від розшифрування, як у RSA, дешифратор повинен позбутись випадкової складової в зашифрованому тексті, щоб завершити процес дешифрування. Тому схема Пейе потребує додаткових обчислень при дешифруванні. У розподільчих умовах це означає, що сторони повинні зберігати два типи частин дешифрування: частину секретного ключа та підтвердження його отримання.

Запропонована система голосування

Було сформовано критерії, яким повинна задовольняти система голосування власників акцій для проведення безпечного та прозорого процесу:

1. Тільки авторизовані учасники системи можуть бути допущеними до процесу голосування.
2. Жоден учасник голосування не може проголосувати більше одного разу.
3. Вибір учасника повинен зберігатися у секреті від інших учасників.
4. Кожен голос повинен бути врахований при розрахунку результату.
5. Учасник голосування повинен мати можливість перевірити статус обробки його голосу, але голос не повинен ідентифікувати учасника.

Виходячи з базових принципів система голосування має бути побудована з наступними компонентами: комітетом голосування, серверним децентралізованим застосуванням, клієнтським додатком.

1. Технологічний ланцюжок функціонування системи наступний.
2. Комітет голосування відповідає за реєстрацію публічних адрес, з яких можуть відправлятись голоси.
3. Дистрибутивний розподіл ключів здійснюється між вузлами, комітету учасниками якого можуть бути різні структурні підрозділи, організації, тощо.
4. Комітет надає публічний ключ системи, яким буде здійснюватися шифрування голосів. Після проведення голосування дешифрує кінцевий результат.

Клієнтській додаток відповідає за генерацію пар ключів для кожного виборця виходячи з кількості акцій у компанії. Містить функціонал шифрування голосу та відправки транзакції у блокчейн.

Децентралізоване серверне рішення являє собою сукупність блокчейн вузлів, публічних чи приватних, які є вхідними точками для приймання підписаних транзакцій , децентралізованого застосування, яке зберігає зашифровані голоси та реалізує правила голосування.

Загальна ілюстрація технічного ланцюжку системи наведена на рисунку 1.

Розглянемо процес голосування на наступному прикладі. Нехай є три власника акцій V_1, V_2, V_3 з відсотками акцій P_1, P_2, P_3 відповідно у певному консорціуму C . У системі обираються учасники комітету голосування $VK_1 \dots VK_n$, де n – кількість учасників комітету. Далі комітет генерує у дистрибутивний спосіб публічний та приватний ключ консорціуму $PubKey_c$, $PrivKey_c$, якими буде здійснюватися шифрування та дешифрування голосів. Приватний ключ системи представлений у вигляді розподілених часток у кожного учасника комітету. При генерації ключів вказується мінімальне число k – часток приватного ключа необхідних при дешифровці результату. За допомогою клієнтського додатку кожен власник акцій генерує кількість публічних ключів яка відповідає кількості акції ,якими він володіє. Для спрощення будемо уявляти ,що кожен учасник може володіти відсотком акцій з точністю до сотих відсотка.

У цьому випадку кожен учасник голосування має таку кількість ключів:

$$N_i=P_i*100 \qquad (1)$$

і реєструє їх у сервісі для того щоб контролювати доступ до процесу голосування (це може бути як і централізований сервіс так і розподілений додаток у вигляді смарт-контракту). Комітету відомі тільки публічні адреси виборців і він не має уявлення про конкретних осіб , що ними володіють.

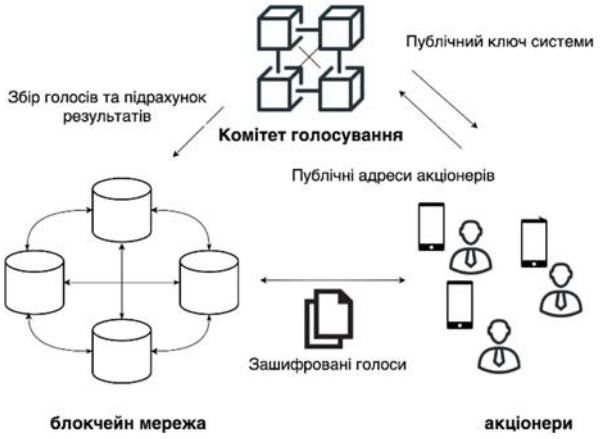

Рис. 1. Архітектура застосування

Далі у клієнтському додатку створюється та підписуються транзакції для відправки у блокчейн з метою зберігання результатів. З одної публічної адреси може бути відправлений лише один голос. Голос передається у зашифрованому вигляді публічним ключем консорціуму

$$vote=E(PubKey_c, option_{1\dots m}), \qquad (2)$$

де $option_{1\dots m}$ – код опції голосування. Кодування опцій робиться у вигляді піднесення в степінь основи системи числення, що має бути більша за максимальну кількість голосів в системі. У даному прикладі при максимальних 10000 голосах за одну опцію основа системи – 10001.При наявності двох опцій кодування 10001^0 та 10001^1 , це буде використовуватись при визначенні фінального результату голосування. Шифрування голосу повинно бути семантично безпечним , тобто щоб шифр від одного і того самого коду виглядали по-різному. Це буде унеможливлювати збір статистики, деанонімізування та визначення результатів у ході голосування. Зашифрований голос, підписаний приватним ключем виборця $PrivKey_v$ відправляється у мережу блокчейн (приватну чи публічну залежить від консорціуму) ти записується у смарт-контракт. Процес реєстрації голосів зображений на рисунку 3.

Контроль правил голосування здійснюється в коді смарт-контракту. Після того як всі учасники проголосували комітетом збираються всі зашифровані голоси. За допомогою властивості адитивності криптосистеми Пейе над зашифрованими даними проводяться арифметичні операції множення .Результат дешифрується за допомогою розподілених часток приватного ключа системи (диференційне дешифрування) та приводиться до системи числення яка використовувалась при кодуванні , отриманий результат – арифметична сума кодів. Кількість голосів за кожну опцію легко виокремлюється з результату.

Процес генерації адрес, з яких буде здійснюватися відправка транзакцій до мережі потребує більш детального розгляду. Так як клієнтське застосування може бути представлене у вигляді мобільного додатку, воно буде мати суттєві обмеження у процесі роботи: пам'яті та потужності процесору та дотримання безпеки. При генерації пар ключів для власника акцій, наприклад 50, і при урахуванні сотих, потрібно згенерувати 5000 пар. При проведенні декількох голосувань одночасно – кількість гаманців збільшується дуже швидко , потрібно оптимізувати пошук необхідного та що більш важливо підписувати кожну транзакцію різним приватним ключем. При втраті доступу до файлу приватного ключа стандартними засобами його неможливо відновити, а з цього слідує неможливість відправити транзакцію з публічної адреси .Для того ,що зробити процес більш ефективним та безпечним слід використовувати механізм HD-wallet, який дає змогу генерувати ієрархічну структуру ключів. Дерево ключів починається з вузла. Гаманець створюється за допомогою випадкової послідовності даних, які називаються мнемонікою. При цьому не обов'язково завжди зберігати всі ключі, а лише знати необхідну глибину для генерації пари. При цьому майстер ключ потрібно надійно зберігати і залишати в секреті від усіх учасників голосування.

Висновки та перспективи подальших досліджень

Аналіз процесів проведення голосувань акціонерних товариств та існуючих рішень в цій галузі показав, що базовими принципами голосування є збереження анонімності, врахування ваги голосу учасника, відповідно до кількості його акцій та можливість переконатися у включенні голосу учасника у кінцевий результат.

1. Запропонована архітектура програмного рішення дозволяє автоматизувати процеси голосування акціонерних товариств та шляхом використання гомоморфної криптосистеми та блокчейн забезпечує виконання базових принципів голосування.

2. Використання децентралізованої технології зберігання даних блокчейн (в запропонованому методі забезпечує анонімність користувачів, секретність голосу та контрольовану фазу підрахунку результату.

3. Запропонований механізм розподіленої генерації ключів системи дозволяє позбутись централізованого серверу, який контролює процес підрахунку результатів, а використання методів ієрархічної генерації ключів вирішує проблему використання ресурсів пам'яті мобільного пристрою та швидкодії операцій шифрування.

4. Запропонований механізм розподіленої генерації ключів системи дозволяє позбутись централізованого серверу, який контролює процес підрахунку результатів, а використання методів ієрархічної генерації ключів вирішує проблему використання ресурсів пам'яті мобільного пристрою та швидкодії операцій шифрування.

5. Подальші дослідження в галузі проведення голосувань за допомогою представленої архітектури рішення, полягають у реалізації безпечного протоколу голосування та його впровадження у сучасні інструменти контролю та менеджменту компанійВиходячи з представленої архітектури рішення, подальші дослідження полягають у реалізації безпечного протоколу голосування та його впровадження у сучасні інструменти контролю та менеджменту компаній.

Література

[1]. List of projects that use blockchain. [Електронний ресурс]. Режим доступу: https://en. bitcoinwiki.org/wiki/Blockchain_Projects_List.

[2]. Liu Y. An E-voting Protocol Based on Blockchain. [Електронний ресурс]. Режим доступу: https://eprint.iacr.org/2017/1043.pdf

[3]. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. [Електронний ресурс]. Режим доступу: https://arxiv. org/pdf/1805.10258.pdf.

[4]. National Agency of Public Registry in the Republic of Georgia. [Електронний ресурс]. Режим доступу: https://exonum.com/napr.

[5]. Blockchain and future house purchases. [Електронний ресурс]. Режим доступу: https://chromaway. com/landregistry/.

[6]. Blokchain Escrow service for financial market. [Електронний ресурс]. Режим доступу: https://serenity-financial.io.

[7]. Підпис меморандуму компанією NEM [Електронний ресурс]. Режим доступу: http://land. gov.ua/derzhavnyi-zemelnyi-kadastr-pereishov-na-tekhnolohiiu-blockchain.

[8]. Agora [Електронний ресурс]. Режим доступу: https:// static1. squarespace. com / static / 5b0be2f4e2ccd12e7e8a9be9/t/5b6c38550e2e725e9cad3f18/1533818968655/Agora_Whitepaper.pdf.

[9]. FollowMyVote [Електронний ресурс]. Режим доступу: https:// followmyvote. com/ cryptographically-secure-voting.

[10]. Large-scale Election Based On Blockchain. [Електронний ресурс]. Режим доступу: https://www. sciencedirect.com/science/article/pii/S1877050918302874.

[11]. Meier A. The ElGamal Cryptosystem. [Електронний ресурс]. Режим доступу: http://www.mayr. in.tum.de/konferenzen/Jass05/courses/1/papers/meier_paper.pdf.

[12]. Voting, Homomorphic Encryption. [Електронний ресурс]. Режим доступу: http://web.mit. edu/6.857/OldStuff/Fall02/handouts/L15-voting.pdf.

[13]. O'Keeffe M. The Paillier Cryptosystem. [Електронний ресурс]. Режим доступу: https://owd. tcnj.edu/~hagedorn/papers/CapstonePapers/OKeeffe/CapstoneOKeeffeCryptography.pdf.

[14]. Malkin M. Experimenting with Shared Generation of RSA keys. [Електронний ресурс]. Режим доступу: http:// crypto. stanford. edu/~dabo/ papers/ ShareExp.ps.

[15]. C. Hazay, G. Mikkelsen, T. Rabin, T. Toft, A. Nicolosi, Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting. [Електронний ресурс]. Режим доступу: https://eprint.iacr.org/ 2011/494.pdf.

[16]. C. Gentry, A fully homomorphic encryption scheme. [Електронний ресурс]. Режим доступу: https://crypto.stanford.edu/craig/craig-thesis.pdf.

[17]. Distributed Paillier Cryptosystem without Trusted Dealer. [Електронний ресурс]. Режим доступу: https://link.springer.com/chapter/10.1007/978-3-642-17955-6_4.

УДК 004.043

Мунин В., Сальников А. Метод проведения голосования среди акционеров на блокчейне используя криптосистему Пейе и распределенную генерацию ключей

Анотация. *В работе предложен метод проведения безопасного голосования среди владельцев акций с сохранением секретности каждого голоса и получением доверенного результата на основе использования криптографической системы Пейе, которая реализует аддитивное свойство зашифрованных текстов. На основе предложенного метода выполнено имплементацию протокола голосования с использованием технологии блокчейн, которая обеспечивает доверительную систему обработки транзакций. Кратко изложены теоретические понятия технологии блочной цепочки транзакций, механизма гомоморфного шифрования, распределенной генерации ключей. Приведен пошаговый алгоритм функционирования системы, описаны основные технические аспекты и преимущества применения децентрализованных технологий для хранения и обработки данных. Были исследованы существующие решения в области проведения голосований и приведен сравнительный анализ. На основе проведенного анализа были сформированы основные критерии проведения безопасного процесса голосования. Кратко описан метод распределенной генерации ключей среди участников системы с учетом различий ключей криптосистемы Пейе от стандартных RSA ключей. В работе подробно описано алгоритм иерархической генерации ключей акционера. Использование этого алгоритма дает возможность оптимизировать процесс хранения и обработки криптографических материалов в клиентском приложении. Также была раскрыта и обоснована целесообразность использования технологии умных контрактов, которые являются децентрализованными приложениями с общим средой хранения данных и консенсус алгоритмом. Контракты представляют собой алгоритм обработки данных транзакций в сети, позволяют проверять правила функционирования системы и проводить логические операции над данными в защищенный способ. Приведенный метод может использоваться для проведения голосований в консорциумах, акционерных обществах и частных сетях, быть интегрирован в децентрализованных систем хранения данных для обеспечения безопасного механизма принятия решений.*

Ключевые слова: *блокчейн, криптосистема Пейе, консенсус, публичный ключ, приватный ключ, смарт контракт.*

Munin V., Salnikov A. Automation of voting processes for joint-stock companies using a homomorphic cryptosystem and blockchain technology

Abstract. *In the article is proposed a method for conducting a safe voting among shareholders with the preservation of the secrecy of each vote and obtaining a trusted result on the basis of the use of the Paillier cryptographic system, which implements the additive property of ciphertexts. On the basis of the proposed method, the voting protocol using the blockchain technology was implemented. This technology provides a trusted transaction processing environment. The theoretical concepts of technology of the block transaction chain, the mechanism of homomorphic encryption, distributed key generation are briefly outlined. The step-by-step algorithm of operation of the system is given, the main technical aspects and advantages of using decentralized technologies for data storage and processing are described. Existing decisions in the area of voting systems were investigated and a comparative analysis was made. On the basis of the analysis, the main criteria for holding a safe voting process were formed. The method of distributed key generation among participants of the system is briefly described taking into account the differences between the keys of the Paillier cryptosystem from the standard RSA keys. The paper describes in detail the algorithm of the hierarchical generation of shareholder keys. Using this algorithm allows to optimize the process of storing and processing cryptographic materials on a client application. The feasibility of using smart contract technology, which is a decentralized application with a shared data storage environment and consensus algorithm, was also disclosed and substantiated. Contracts represent an algorithm for processing transaction data in the network, allowing to check the rules of operation of the system and conduct logical operations on the data in a secure way. This method can be used to conduct voting in consortia, joint stock companies and private networks, to be integrated into decentralized data storage systems to provide a secure decision mechanism.*

Key words: *blockchain, Paillier cryptographic system, consensus, public key, private key, smart contract.*

Отримано *15 травня 2019 року*, затверджено редколегією *30 травня 2019 року*