УДК 004.056 **DOI:10.30837/rt.2019.4.199.15**

К.В. ІСІРОВА, О.В. ПОТІЙ, д-р техн. наук

ПРИНЦИПИ ПОБУДОВИ ЕЛЕКТРОННОЇ СИСТЕМИ ТАЄМНОГО ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ

Електронні довірчі послуги стають невід'ємною частиною інформаційного простору. Їх використання регулюється Регламентом (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93 / ЄС [1], яка встановлює терміни та умови. Завдяки надійній реалізації таких базових послуг, як електронний підпис та електронна аутентифікація, можна побудувати більш складні системи, які покладаються на них, наприклад, систему електронного голосування.

Віддалене (електронне) голосування має багато переваг. Передбачається, що воно більш зручне для кінцевих користувачів, оскільки люди можуть голосувати, не виходячи з дому; це підвищує активність виборців [13, 15]. Забезпечення електронного голосування дешевше: замість того, щоб постійно друкувати бюлетені, достатньо один раз розробити систему. Крім того, припущення, що ніхто не може втручатися в програму на пристрої для голосування, означає, що електронне голосування менш схильне до корупції, адміністративного тиску та людських факторів [14, 15]. Однак це викликає низку специфічних проблем, які перешкоджають цілісності виборів. Віддалено, набагато складніше авторизувати виборця або переконатися, що ніхто не вплинув на процес голосування. З іншого боку, Інтернет дає більше можливостей для перевірки звичайними виборцями, чи правильно було враховано голос. Наразі електронне голосування є повністю законним або частково застосованим у багатьох країнах світу [2, 13]. Оскільки в електронному голосуванні залучено все більше і більше людей, зростає потреба в безпечніших і ефективніших методах його реалізації, а саме для цього розроблені спеціальні криптографічні протоколи.

Мета статті – формулювання нових принципів побудови систем електронного голосування з використанням DLT, пропозиція дворівневої архітектури такої системи та адаптований протокол голосування, що допомагає нівелювати існуючі недоліки класичних систем електронного голосування.

Принципи електронних систем голосування

Система електронного голосування – сукупність взаємопов'язаних правил, методів, процесів, засобів і технологій, а також правових норм, що в сукупності забезпечують і регулюють дистанційне легітимне волевиявлення авторизованих користувачів(виборців).

Складові частини (підсистеми/рівні) системи електронного голосування (рис. 1):

- нормативно-правовий рівень (закони та інші нормативно-правові документи);
- організаційний рівень (архітектура системи електронного голосування);
- рівень процесів (процеси для користувача, процеси для);
- технологічний рівень (методи, засоби, протоколи, технології).

Таємні протоколи голосування – протоколи обміну даними для реалізації безпечного, таємного електронного голосування через Інтернет з використанням комп'ютерів, телефонів або інших спеціальних комп'ютерів.

Можна виділити такі обов’язкові вимоги до безпеки систем електронного голосування [3, 9]:

- ніхто, крім виборця, не повинен знати свого вибору;
- лише легітимні виборці можуть голосувати, крім того, вони повинні мати можливість голосувати лише один раз;
- рішення виборця не може бути таємно або явно змінено будь-ким (крім, можливо, самого виборця).

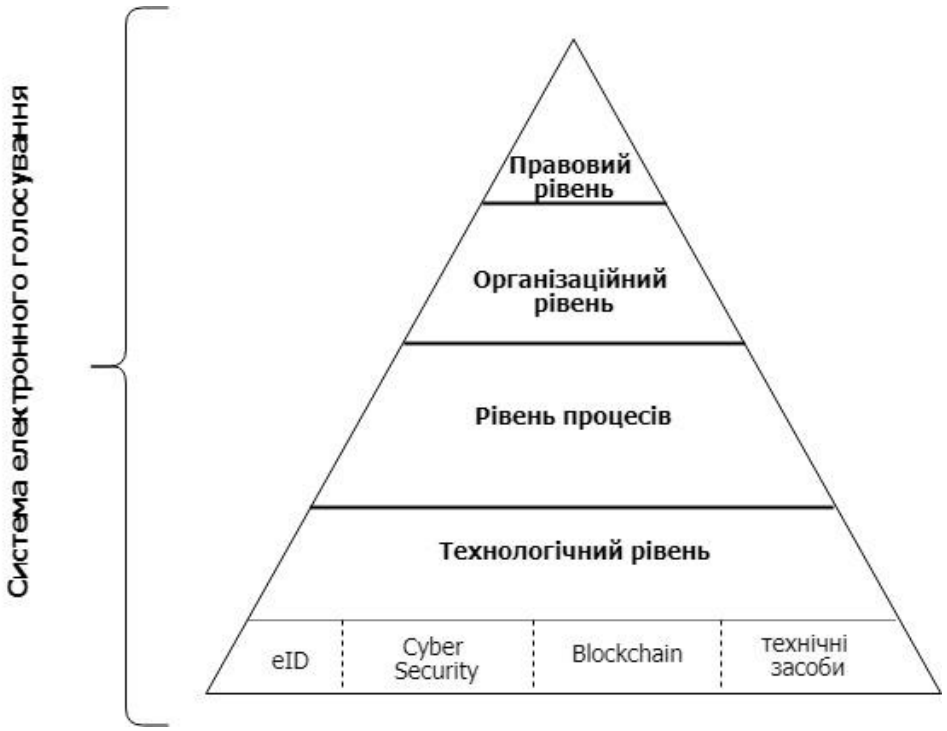

Рис. 1. Складові частини системи електронного голосування

Додатково до них, висуваються додаткові вимоги [3, 9]:

- кожен законний виборець може перевірити, чи правильно підраховано його голос;
- кожен законний виборець може змінити свою думку і змінити свій вибір протягом певного періоду часу;
- система повинна бути захищена від продажу голосів виборцями;
- у разі неправильного підрахунку голосів кожен законний виборець може повідомити про це систему, не виявляючи його особистості;
- неможливо відстежити, звідки віддалено проголосував виборець;
- аутентифікація оператора;
- підтримка системи не повинна вимагати великих ресурсів;
- система повинна бути відмовостійкою у разі технічних несправностей (втрата електроживлення), ненавмисних (втрата виборцем ключа) і зловмисних (навмисного маскування себе як іншого виборця, DoS / DDoS) атак.

Основні загрози для систем такого типу:

- легітимний виборець не може голосувати;
- втрата анонімності;
- неіснуюча реєстрація виборців;
- використання пустих бюлетенів виборців, які зареєструвалися, але не вийшли на вибори.

Існуючі протоколи електронного голосування. Виклики та труднощі

Простий алгоритм електронного голосування (рисунок 2) [9, 11], по суті, являє собою процес обміном повідомлень із електронними підписам між виборчим комітетом і масивом виборців.

Припустимо, що:

A – агентство електронного голосування;

E – виборець;

B – цифровий виборчій бюлетень.

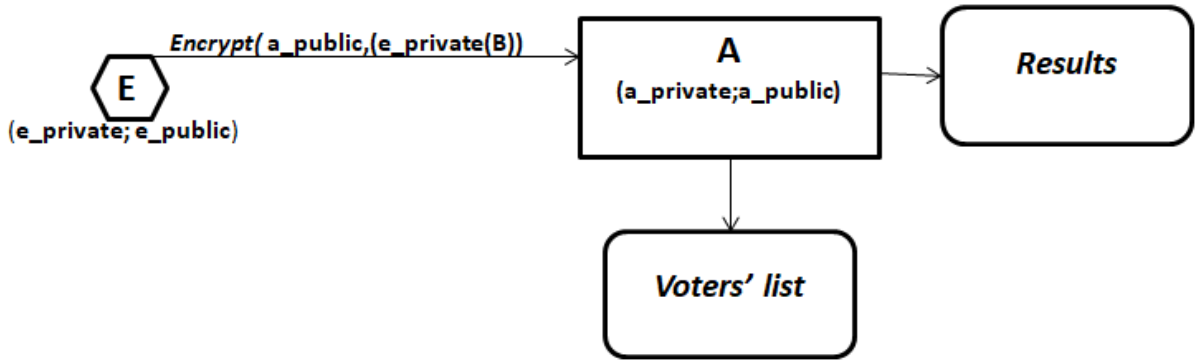

Рис. 2. Простий алгоритм електронного голосування

Алгоритм складається з шести основних кроків.

Крок 1. A розміщає списки можливих виборців.

Крок 2. Користувачі, включаючи *E*, оголошують про своє бажання голосувати.

*Крок 3***.** *A* розміщає списки законних виборців.

Кроки 1 – 3 є необхідними. Основна мета – визначити та оголосити кількість активних учасників. Хоча деякі з них можуть не брати участі, а деякі взагалі не можуть існувати («мертві душі», зловмисно введені *A*). При цьому здатність маніпулювати голосом в *A* помітно знижується. В подальшому ці кроки будуть розглядатися за один крок «затвердження списків» [11].

Крок 4. A генерує відкритий ключ (*a_public*) і особистий ключ (*a_private*). Особистий ключ надійно зберігається *A*, відкритий публікується для широкого доступу. Кожен може зашифрувати повідомлення, використовуючи опублікований відкритий ключ, але тільки *A* може його розшифрувати.

Крок 5 включає наступне:

- *E* створює свої власні відкритий (*e_public*) і особистий (*e_private*) ключі, а потім публікує відкритий ключ. Кожен може перевірити документ *E*, але підписати його може тільки сам виборець. Цей крок пропускається, якщо *A* вже знає електронні підписи виборців (наприклад, вони були створені під час реєстрації в системі);
- *E* формує цифровий виборчий бюлетень *B*, де в тій чи іншій мірі висловлює свою волю;
- підписує повідомлення власним особистим ключем (*e_private*);
- шифрує повідомлення за допомогою відкритого ключа *A* (*a_public*);
- надсилає зашифроване повідомлення *A.*

Крок 6 включає наступне:

- *A* приймає повідомлення;
- розшифровує їх за допомогою *a_private*;
- перевіряє підпис виборця за допомогою *e_public;*
- підраховує їх і публікує результати.

Цей протокол надзвичайно простий; однак його достатньо, щоб захистити систему від зовнішнього втручання, шахрайства з голосуванням і дискредитації законних виборців. Проте виборці повинні абсолютно довіряти *A*, оскільки його робота не контролюється ніким. З одного боку, *E* може надати зловмиснику доказ голосування, а з іншого, він не може переконатися, що *A* правильно підрахував або навіть отримав його бюлетень. Таким чином, тривіальний метод застосовується тільки в спільнотах, де кожен довіряє один одному і агентству, відповідальному за підрахунок голосів [12].

Існує декілька відомих модифікацій згаданого протоколу. Перший – Протокол двох агентств, що називається також протоколом Нурмі – Салома – Сантіна (Nurmi – Saloma – Santina) [4]. Основна ідея якого – замінити одну виборчу установу на дві, щоб вони контролювали один одного. Таким чином, в системі з'являється додаткова сторона *V*, яка є валіда-

тором, чиї обов'язки включають підготовку списків, а також прийняття або недопущення учасника до голосування. Крім того, згідно з цим протоколом *A* має опублікувати список прийнятих цифрових бюлетенів. В результаті *A* не може згодом відмовити в отриманні повідомлення від *E*, і кожен виборець може перевірити, чи правильно його голос був врахований, що виключає проблему відсутності контролю над *A*. З іншого боку, існує можливість змови між *A* та *V*, що призведе до можливих маніпуляцій з результатами. Крім того, існує проблема "мертвих душ". Якщо *V* внесе до списку завідомо неіснуючих виборців, то *A* зможе фальсифікувати бюлетені від «мертвих душ».

У 1992 р. була розроблена схема Fujioka-Okamoto-Ohta [5], яка базується на протоколі двох агентств і сліпого криптографічного підпису. Протокол вимагає попередньо обраного методу маскую чого шифрування, згідно з яким виборець відправляє бюлетень валідатору. Шифрування, що маскує, – це особливий тип шифрування, який дозволяє переконатися, що документ є автентичним і підписаний уповноваженим користувачем, але не дозволяє виявити дані, що містяться в ньому. Ця схема частково вирішує проблему змови двох установ. Однак це ускладнює протокол.

Однією з найпопулярніших версій вищезгаданого протоколу є протокол Sensus [6]. При його коректній реалізації, навіть якщо агентствам вдасться дійти до змови, *A* не зможе ідентифікувати виборців. Незважаючи на те, що *A* все ще має можливість «не отримувати» повідомлення, більше неможливо ігнорувати повідомлення спеціально від «небажаних» виборців. Залишається тільки проблема голосування виборців, які не вийшли на вибори.

Щоб уникнути недоліків Fujiok – Okamoto – Ohta, у тому числі протоколу його модифікацій, необхідне подальше ускладнення алгоритму, що призводить до труднощів практичної реалізації (наприклад, протокол He-Su [6, 10]).

На даний момент протокол Fujiok – Okamoto – Ohta (а також його модифікації, включаючи Sensus) є одним з найбільш перевірених протоколів дистанційного електронного голосування. Саме його варіація застосовувалася на електронних виборах в Естонії.

Система електронного голосування на основі децентралізованих принципів розвитку PKI

Принципи побудови децентралізованої PKI

Принципи побудови децентралізованої PKI були сформульовані авторами [7, 8]:

1. Кожен користувач (користувач виступає вузлом) зберігає свою ключову пару самостійно. Сертифікат відкритого ключа передається разом із підписаним повідомленням.
2. Запис про транзакції за законами blockchain зберігається в розподіленої базі.
3. Блок транзакцій містить реєстр станів сертифіката.
4. При перевірці правильності транзакції (фактично дійсності сертифіката відкритого ключа), перевіряючому необхідно простежити реєстр стану сертифіката відправника аж до його першої публікації (аналогічні дії проходять в системі BitCoin для перевірки наявності «коштів» на «рахунку» клієнта, тобто виключення «подвійної трати»).
5. Первинна ідентифікація нового користувача, однак, є обов'язковою і повинна бути надійно підтверджена. Для цієї і тільки для цієї мети необхідний довірений вузол (аналог уповноваженого на сертифікацію в ієрархічній структурі). Його роль буде полягати в первинному випуску сертифіката нового користувача, а також у випадках необхідних для зміни статусу сертифіката. Після першої транзакції, проведеною новим користувачем, звернення до довіреного вузла більше не виникає. Таким чином, цей вузол буде забезпечувати нових користувачів «батьківським» блоком («genesis block») для того, щоб вже існуючі вузли могли перевіряти статуси сертифіката нового користувача. Доцільним представляється покласти цю роль на структуру, яка підлягає сертифікації з боку контролюючих органів.

Для опису децентралізованої PKI введемо наступні умовні позначення [8]:

M – повідомлення;

$Sign$ – цифровий підпис відправника;

H – криптографічна геш-функція;

$Sert$ – сертифікат відкритого ключа відправника;

ID – унікальний ідентифікатор відправника виданий йому на етапі первинної ідентифікації;

$Status$ – статус сертифіката відкритого ключа відправника.

Основні процедури всередині системи:

- процедура первинної ідентифікації користувача;
- процедура генерації підпису;
- процедура перевірки підпису.

Як зазначалося вище, первинна ідентифікація повинна проводитися сертифікованою структурою (довірчим вузлом). При зверненні до якої користувачу видається (генерується) його унікальний ідентифікатор ID та відповідний йому сертифікат відкритого ключа $Sert$, який пов'язаний із особистим ключем користувача. Слід зазначити, що довічний вузол не зберігає у себе ID користувача, більше того, він його не знає.

Перша транзакція нового користувача повинна бути звернена до довіреного вузла для того, щоб при наступних транзакціях інші користувачі мережі могли прослідкувати реєстр станів даного сертифіката відкритого ключа за законами blockchain. Так як для надійного підтвердження транзакції необхідно обчислення 3 – 5 блоків, наступних за блоком з даної транзакцією, рекомендується відправляти транзакцію не тільки до одного представника довіреного вузла, а до кількох (наприклад, оператор реєстрації, оператор сертифікації, адміністратор безпеки).

Після проходження первинної ідентифікації дані поширюються в розподілену базу, в якій вони зберігаються в наступному вигляді (табл. 1).

Таблиця 1

Вигляд розподіленої БД (blockchain) [7]

$H(Sert,ID)$	$H(Sert,Status)$	$Status$
…	…	…

Транзакція в такій системі матиме вигляд: *M; Sign; H(Sert, ID); Sert; Status*

Запропонована система побудована таким чином, що алгоритм формування підпису ніяк не відрізняється від того, який використовується в класичних системах, і залежить лише від типу підпису. Алгоритм верифікації в децентралізованій PKI складається із двох етапів: по-перше стороні, що перевіряє, необхідно переконатися, що підпис був накладений саме із використанням заявленого відкритого ключа, а другий етап полягає в перевірці чи дійсно даний відкритий ключ належить стороні, що його використовує [7, 8].

Принципи побудови децентралізованої системи електронного голосування

Процес голосування складається з етапів:

1. Формування списків виборців.

2. Голосування.

3. Підрахунок голосів.

Тут і далі *CA* – центр сертифікації (або довірені вузли у децентралізованій PKI).

Архітектура (рис. 3) складається із двох рівнів та базується на раніше запропонованій децентралізованій PKI. Користувачі використовують існуючі ключові пари. Центри сертифікації (довірені вузли) об’єднуються в мережу блокчейн (CAs’ Blockchain Ledger) – нижній рівень. На верхньому рівні знаходиться децентралізована інфраструктура для електронного голосування (Decentralized e-voting Infrastructure). Представництва Агентства електронного голосування аналогічно до центрів сертифікації ключів об’єднуються в окрему мережу блок-

чейн (Ais' Blockchain Ledger) Необхідно зазначити, що для таких мереж немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки обидві мережі поєднує довірені («чесні») вузли.

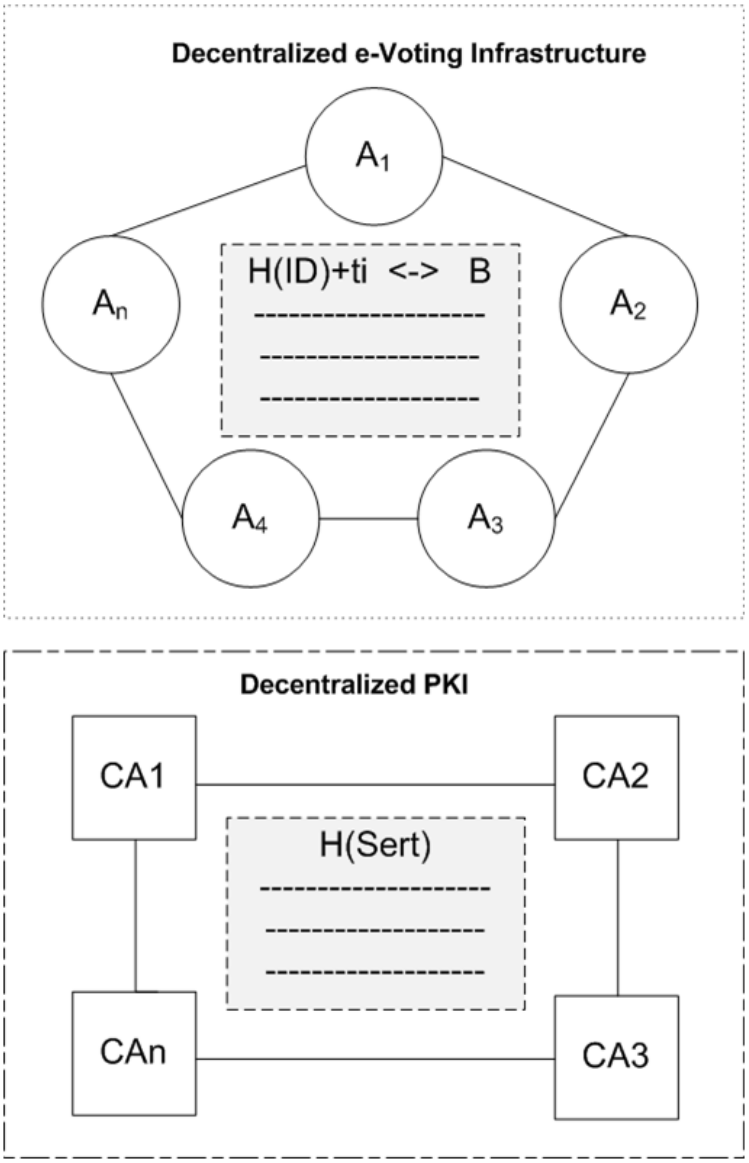

Рис. 3. Архітектура децентралізованої системи електронного голосування

Перший етап: формування списків виборців:

Процес формування списків виборців наступний (рис. 4).

1. Користувач надсилає запит на включення його до списку виборців до довіреного вузла.

Запит формується як транзакція, яка може бути в цілому використана в децентралізованій PKI:

$$M; Sign; H(Sert, ID); Sert; Status; \quad (1)$$

де $M=H(ID)$

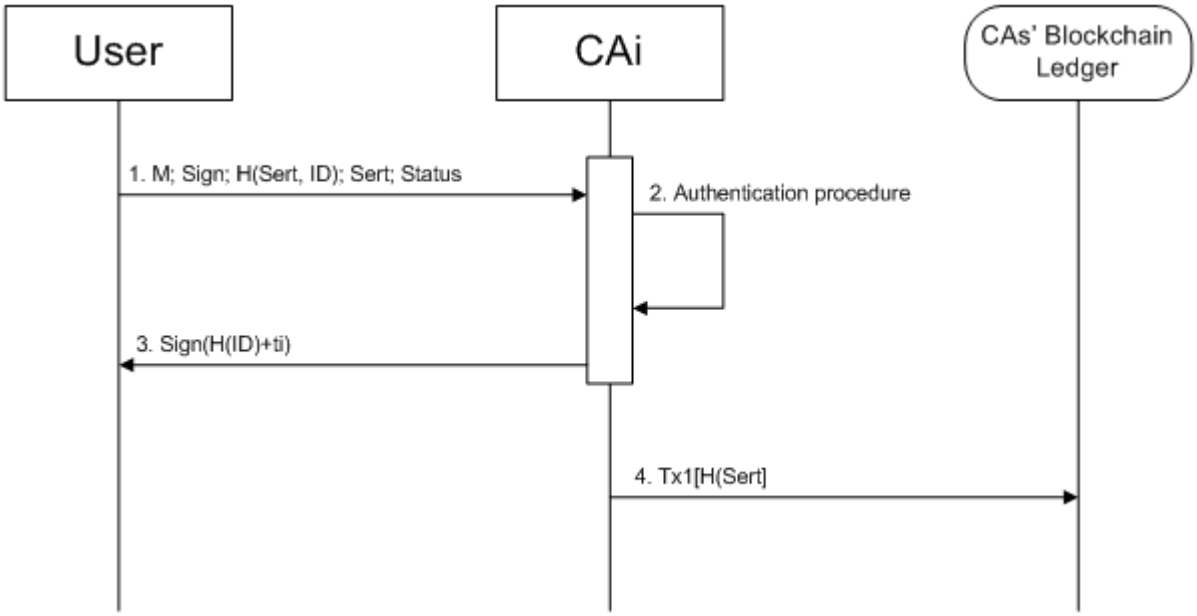

Рис. 4. Процес формування списку виборців

2. Орган з сертифікації на підставі даних, отриманих під час первинної ідентифікації, перевіряє легітимність виборця (фактично проходить процедура аутентифікації виборця). Під час перевірки орган з сертифікації також перевіряє чи не був даний користувач раніше включений до списку легітимних виборців. Таку перевірку можливо здійснити на основі даних із розподіленого реєстру мережі Blockchain (CAs' Blockchain Ledger).

3. Якщо процедура аутентифікації пройшла успішно, у відповідь на запит орган із сертифікації надсилає користувачу його мітку підписану власним особистим ключем:

$$Sign(H(ID)+t_i)\ ; \tag{2}$$

де – t_i є ідентифікаційною позначкою (міткою).

4 Орган із сертифікації формує транзакцію Tx1, в яку включає геш-значення від сертифікату виборця (H(Sert)). Учасники мережі блокчейн (CAs' Blockchain Ledger) досягають консенсусу щодо включення такої транзакції до розподіленого реєстру.

Таким чином, коли вичерпався час, виділений на формування легітимних списків виборців, у цьому блокчейні створено деперсоналізований список потенційних легітимних виборців.

Після закінчення періоду, призначеного для формування списків законних виборців, всі довірені вузли передають Агентству дані про мітки, які вони видали виборцям (без відомостей про відповідність між міткою та користувачем):

$$H(ID)+t \tag{3}$$

Таким чином, Агентство отримує список всіх зареєстрованих легітимних виборців, але виборці зберігають свою анонімність.

Другий етап: голосування:

Процес формування голосування відбувається наступним чином наступний (рисунок 5)

1. Виборець, який отримав підтвердження від довіреного вузла, формує повідомлення зі своїм рішенням/вибором і надсилає Агентству наступний набір даних:

$$H(ID)+ti;\ encrypt\ (M^*) \tag{4}$$

де – $M^*= a\_pub, H(ID)+t, B$

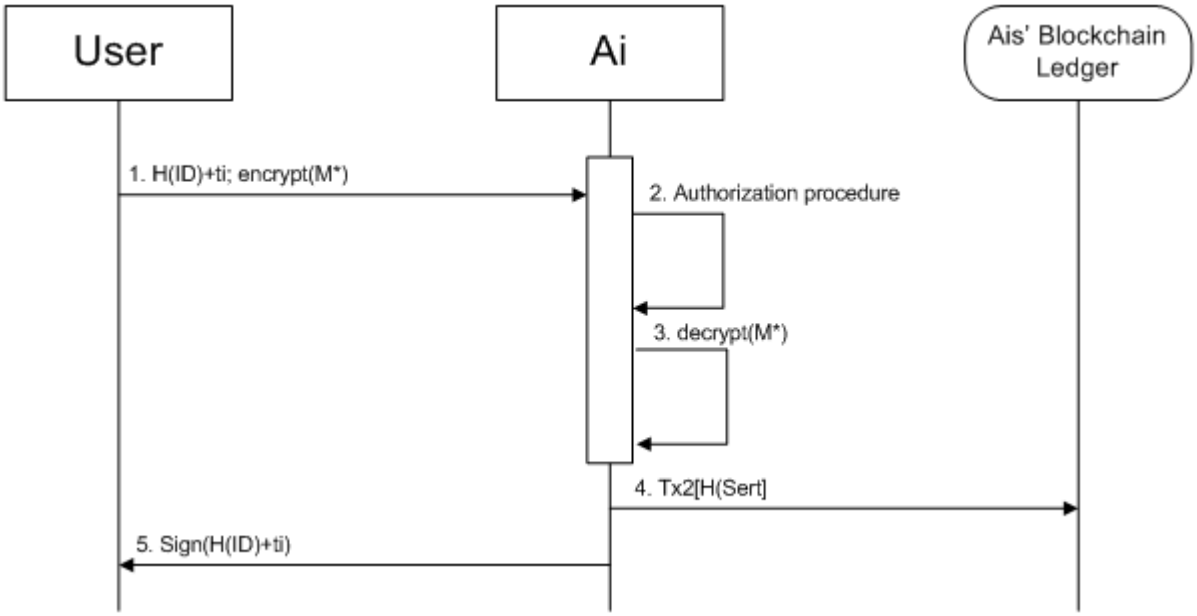

Рис. 5. Процес голосування

2. По зовнішній мітці H (ID) + ti Ai може ідентифікувати, що голос прийшов саме від легітимного виборця (процедура авторизації виборця).

3. Якщо процедура авторизації пройшла успішно, то використовуючи власний e_private, Ai розшифровує повідомлення та проводить перевірку того, чи зовнішня позначка відповідає тій, яка була зашифрована.

4. Якщо вони збігаються, *Ai* формує транзакцію Tx2, в яку включає відповідність між H (ID) + t і B. Учасники мережі блокчейн (Ais' Blockchain Ledger) досягають консенсусу щодо включення такої транзакції до розподіленого реєстру.

При цьому, Агентство, як і будь-який зовнішній спостерігач, досі не знає, хто саме серед легітимних виборців робить цей вибір, таким чином виборці є анонімними без використання сліпих підписів.

5. Якщо перевірки 2 і 3 пройшли успішно, *Ai* в якості підтвердження прийняття його голосу надсилає виборцю його мітку підписану власним особистим ключем.

Перед підрахунком голосів, необхідно виконати наступні перевірки:

$$N(H(Sert))=N(H(ID)+t) \tag{5}$$

Це означає, що кількість геш значень сертифікатів (*N (H(Sert))*) в мережі CAs' Blockchain Ledger, організованому між довіреними вузлами, повинна відповідати кількості *H (ID) + t*, що були надіслані в Агентство довірчими вузлами. Таким чином, виключається можливість *A* не враховувати голоси легітимних виборців:

$$N(H(ID)+t)\geq N(B) \tag{6}$$

Це означає, що кількість поданих бюлетенів не повинна перевищувати кількість зареєстрованих виборців. Дана перевірка виключає можливість використання «мертвих душ».

Якщо всі перевірки є успішними, проводиться підрахунок голосів.

Третій етап: підрахунок голосів

У Ais' Blockchain Ledger – мережі блокчейн, організованій між представництвами Агентства, формується остаточний список відповідності між мітками виборців та їхнім вибором. Потім кожен користувач перевіряє, чи правильно враховано його голос. У разі помилки виборці повідомляють про це.

Підрахунок голосів здійснюється автоматично.

Висновки

1. Класичні системи голосування не відповідають усім необхідним вимогам для систем голосування (наприклад, виборець не може перевірити, чи правильно його голос враховано і, якщо необхідно, повідомити про це уповноважені органи).

2. Запропонований підхід до розробки системи електронного голосування допомагає зберегти всі переваги децентралізованої PKI. Крім того, слід зазначити, що цей підхід може бути реалізований не тільки за допомогою децентралізованої PKI, але й з існуючою. У цьому випадку ідентифікатори ID мають бути додатково надійно розповсюджені поміж виборців перед впровадженням.

3. Система використовує децентралізовану PKI, відповідно, немає необхідності повторно генерувати списки виборців.

4. Запропонований підхід зберігає переваги існуючих систем електронного голосування, таких як Fujiok-Okamoto-Ohta, Sensus, а також протоколу He-Su без реалізації сліпих підписів. Це допомагає зменшити складність впровадження.

5. Зменшення матеріальних витрат на кожному етапі голосування (оскільки не потрібно друкувати бюлетені, доставляти їх на виборчі дільниці, тощо).

Список літератури:

1. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

2. E-voting world map

3. Hannu Nurmi, Arto Salomaa. Conducting secret ballot elections in computer networks: Problems and solutions // Annals of Operations Research 51 (1994) 185-194 / University of Turku.

4. Nurmi H., Salomaa A. and Santean, L. Secret ballot elections in computer networks // Computers and Security. 36, 10 (1991). P. 553 – 560.

5. Fujioka A., Okamoto T., Ohta K. A Practical Secret Voting Scheme for Large Scale Elections // ASIACRYPT ’92. LNCS, Springer (1993) 244 – 251

6.Qi He, Zhongmin Su. A New Practical Secure e-Voting Scheme (1998).

7. Isirova K. Decentralized Public Key Infrastructure Development Principles / Kateryna Isirova, Oleksandr Potii // The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT’2018, 24-27 May, 2018, Kyiv, Ukraine. P. 320 – 326.

8. Isirova K Blockchain Technology as the Prospective Instrument for Ensuring Electronic Trust Services in Conditions of Cyberthreats // European Cybersecurity Journal. 2019.

9. Julien P. Stern. A New and Efficient All-Or-Nothing Disclosure of Secrets Protocol

10. Brassard G., Crepeau C. and Robert J.-M. All-or-nothing disclosure of secrets // Springer Lecture Notes in Computer Science 263 (1987).

11. Hannu Nurmi, Arto Salomaa. Conducting secret ballot elections in computer networks: Problems and solutions // Annals of Operations Research 51 (1994) 185-194 / University of Turku.

12. Kohno T., Stubblefield A., Rubin A. D. and Wallach D. S. Analysis of an electronic voting system // IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, Berkeley, CA, USA, 2004. P. 27-40.

13. Delis A. et al. Pressing the button for European elections: verifiable e-voting and public attitudes toward internet voting in Greece // 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE). Lochau, 2014. P. 1-8.

14. Stein R. and Wenda G. The Council of Europe and e-voting: history and impact of Rec(2004)11 // 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE). Lochau, 2014. P. 1 – 6.

15. Pomares J., Levin I., Alvarez R. M., Mirau G. L. and Ovejero T. From piloting to roll-out: voting experience and trust in the first full e-election in Argentina // 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE). Lochau, 2014. P. 1 – 10.

АТ «Інститут інформаційних технологій»;
Харківський національний
університет імені В.Н. Каразіна;

Надійшла до редколегії 09.10.2019