

ОРГАНІЗАЦІЯ ДЕЦЕНТРАЛІЗОВАНОГО ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ BLOCKCHAIN

Д. О. Кочубей^{1, а}, А. М. Родіонов¹

¹ Національний технічний університет України «Київський політехнічний інститут»

Анотація

У даній роботі представлений спосіб побудови децентралізованої системи голосування з використанням технології Blockchain.

Ключові слова: децентралізована система, Blockchain

Вступ

Наше життя нерозривно пов'язане з різного роду даними, документами та фінансами. Через це нам постійно потрібно співпрацювати з різними посередниками, котрі видають нам ці дані, документи чи фінанси, гарантують їх справжність, зберігають або перевіряють. При цьому всьому ми вимушені довіряти зазначеним посередникам як гарантам, що забезпечують безпеку угод.

Інформаційні відносини в інтернеті використовують таку саму модель, якою люди користуються в повсяденному житті: при взаємодії через інтернет користувачі вдаються до послуг посередника, якому можна довіряти.

У даній роботі ми розглянемо спосіб організації децентралізованого анонімного голосування, яке буде звільнено від участі третьої сторони і захищене таким чином від її втручання.

Насьогодні для проведення такого роду голосування використовується сліпий електронний цифровий підпис. Це такий різновид ЕЦП, при якому підписуюча сторона не може знати зміст документа, який підписує. Голосування на основі сліпого електронного підпису вже організовувалося на різних рівнях виборів. Для проведення таємного цифрового голосування існують декілька алгоритмів: протокол двох агенств, протокол Фудзіока-Окамото-Охта, протокол He-Su та інші. Проте кожен з них має один або декілька з наступних недоліків:

- можливість фальсифікування голосування з боку органу, що його проводить;
- можливість подачі голосів від імені тих виборців, які не брали участь у голосуванні;
- велика складність і внаслідок цього вразливість до DoS-атаки.

І ключовим недоліком є залежність від посередника, що проводить голосування.

Для вирішення наведених проблем в даній роботі розглядається спосіб проведення голосування, яке не залежить від центрального органу, що його про-

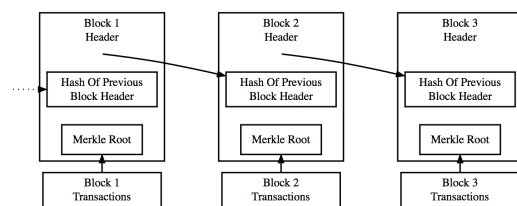


Рис. 1. Схема ланцюга блоків

водить. Для цього розглянемо принципи технології Blockchain, яка є простою у реалізації і одночасно має високий рівень надійності і захищеності.

1. Опис технології Blockchain на прикладі криптовалюти BitCoin

Популярність технології Blockchain у 2009 році принесла криптовалюта BitCoin, що була побудована на її основі. У цьому розділі ми дамо визначення технології Blockchain, а також розглянемо принципи її роботи.

1.1. Поняття технології Blockchain

Blockchain представляє собою набір блоків, структурно об'єднаних в ланцюг. Кожен блок містить набір транзакцій. В сукупності усі блоки становлять послідовність, яка зберігає інформацію про всі проведені у системі транзакції [1]. Користувачі блокчейну утворюють мережу комп'ютерів, на кожному з яких зберігається копія ланцюга блоків. Завдяки цьому вимкнути таку систему неможливо, доки працює хоча б один вузол мережі. Кожен новий користувач лише розширює й укріплює таку мережу. Всі комп'ютери мережі рівноправні і не контролюються центральним органом.

1.2. Принципи роботи технології Blockchain

Ланцюг блоків у спрощеному вигляді представлений на рис. 1.

Кожен блок містить інформації про набір транзакцій, проведених у системі. На основі хешів кожної

^аden.kochubey@gmail.com

транзакції будується дерево Меркла. В такому дереві транзакції пов'язані одна з одною. Кожен блок також зберігає хеш заголовка попереднього блоку. Вкупі це гарантує, що окрема транзакція не може бути змінена без зміни блоку, в якому вона записана [2].

Нові блоки, що поступово додаються до блокчейну, генеруються майнерами [2]. Майнери підтримують роботу мережі, отримуючи грошову винагороду у вигляді комісії за підтвердження транзакцій. Щоб згенерувати новий блок, майнеру необхідно знайти хеш заголовка блоку транзакцій, який є меншим за певне число. Це число характеризує складність генерування нового блоку і змінюється разом з тим, як зростають потужності обчислювальних пристроїв.

2. Організація децентралізованого голосування на основі технології Blockchain

Найяскравішим прикладом використання технології Blockchain є криптовалюта BitCoin. Проте це не єдина сфера, де її можна ефективно задіяти. Прикладом ефективного використання технології Blockchain може стати проведення децентралізованого, прозорого голосування [3].

2.1. Концепція голосування на основі Blockchain

Основою такого голосування може бути блокчейн, подібний до блокчейну BitCoin, але замість транзакцій з криптовалютою будуть відбуватись транзакції з голосами. Організатор голосування видає кожному виборцю пару ключів: секретний та публічний. Відповідність між парою ключів та виборцем не встановлюється, а лише затверджується факт видачі. За допомогою секретного ключа виборець отримує доступ до акаунта, на рахунку якого зберігається 1 голос, що є неподільною одиницею при голосуванні. При виборі однієї з запропонованих у голосуванні відповідей, проводиться транзакція переведення голосу. За принципом проведення така схема схожа на традиційні вибори, але з однією ключовою відмінністю – результати голосування зберігаються не на бюлетенях, а в одному ланцюгу блоків. Причому зберігається такий ланцюг не в центральному сховищі, а розподілено на комп'ютерах усіх виборців.

2.2. Проблема дострокових результатів

Децентралізоване зберігання блокчейну дає свої переваги, проте і має певні недоліки. Проблемою є те, що виборці, на комп'ютерах яких зберігається ланцюг блоків, можуть спостерігати за процесом голосування і передчасно бачити результати. Проте вирішення цієї проблеми вже існує, і запозичити його ми можемо з блокчейна криптовалюти BitCoin.

Особливістю ланцюга блоків BitCoin є те, що в ньому немає понять рахунку та балансу. Всі кошти зберігаються в об'єктах, які називаються «виходами транзакцій». Для того, щоб дізнатися про кіль-

кість коштів на якомусь рахунку, необхідно пробігти вздовж всього ланцюга блоків і підрахувати баланс за допомогою інформації у «виходах транзакцій». Зі збільшенням кількості проведених транзакцій, збільшується об'єм дискового простору, необхідного для зберігання ланцюга блоків. Зберігання блокчейна у повному обсязі для звичайного виборця є надлишковим. Для вирішення цієї проблеми були створені клієнти, що зберігають полегшену версію блокчейна: в них містяться лише блоки та транзакції, що стосуються окремого користувача, а отже він може отримати інформацію про стан лише свого рахунку, тому що інші його не цікавлять.

Запропоноване рішення гарно вписується до концепції організації голосування на основі технології Blockchain. На момент проведення голосування виборці мають можливість отримати лише полегшену версію ланцюга блоків. Така версія буде містити одну єдину інформацію – його власний вибір. Після завершення голосування виборцям стає доступний клієнт, що вже містить повний ланцюг блоків і транзакцій.

2.3. Підрахунок результатів

Після отримання повної версії блокчейна, кожний виборець отримує дві важливі можливості:

- перевірити, що його голос переведений коректно (тому кандидату, за якого голосував);
- переглянути весь ланцюг блоків і підрахувати результати голосування.

При цьому всьому виборцю більше не потрібно довіряти та покладатись на виборчі органи, адже ланцюг блоків зберігається одночасно на комп'ютері кожного виборця і його неможливо підробити.

Висновки

У даній роботі розглянуто принципи роботи технології Blockchain, а також наведено приклад використання цієї технології при організації децентралізованого голосування. Було проведено порівняння з альтернативними рішеннями, що наразі використовуються для організації онлайн-голосування, а також визначено ряд питань, які дозволяє вирішити технологія Blockchain.

Представлене у роботі рішення дозволяє провести захищене, незалежне від посередника голосування, результати якого може перевірити кожний виборець.

Перелік використаних джерел

1. Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System, BITCOIN.ORG 3. — 2009. — P. 9 с.
2. Bitcoin Developer Guide. — URL: <https://bitcoin.org/en/developer-guide#block-chain>.
3. Wright Aaron, Filippi Primavera De. Decentralized blockchain technology and the rise or lex cryptographic. — 2015. — P. 58 с.