УДК 681.3:519.72:003.26

А.М. КУДІН, Б.А. КОВАЛЕНКО, І.В. ШВІДЧЕНКО

ТЕХНОЛОГІЯ БЛОКЧЕЙН: ПИТАННЯ АНАЛІЗУ ТА СИНТЕЗУ

Анотація. Розглянуто роль технології блокчейн у реалізації однієї з тенденцій розвитку сучасних інформаційних систем, а саме децентралізації. Проаналізовано загальну модель функціонування блокчейн-системи, запропоновано ідею побудови нового типу протоколів консенсусу (протокол «proof-of-accuracy»), який об'єднує переваги протоколів типу «proof-of-works» і «proof-of-stake». Досліджено шляхи реалізації протоколу «proof-of-accuracy».

Ключові слова: розподілені комп'ютерні системи, безпека інформації, криптологія, блокчейн, криптовалюти, протоколи консенсусу, загальна теорія оптимальних алгоритмів, протокол узгодження типу «proof-of-accuracy».

ВСТУП

Основні тенденції розвитку сучасних інформаційних технологій є такими:

• подальший розвиток розподіленого оброблення інформації, реалізованого в сучасних грід- та хмарних інформаційно-телекомунікаційних системах;

• поява нових моделей обчислень та їхня практична реалізація (квантові обчислення і квантова криптографія);

• міграція принципів побудови інформаційно-комунікаційних систем загального призначення у галузь автоматизованих систем управління критичною інфраструктурою;

• перехід від інформаційно-комунікаційних систем до кіберпростору, тобто від безпосередньо керованого інформаційно-комунікаційного середовища до децентралізованих систем управління, спроможних надати поведінці деякої області кіберпростору «інтелектуальний» характер.

Остання тенденція потребує пояснення. Визначимо кіберпростір (приставка «кібер» означає «управління») як систему, в якій самостійно виникають сигнали, що забезпечують керування процесами збереження певного стану системи. Тоді інформаційна система повинна мати здатність до самоорганізації і децентралізації та бути розподіленою за функціями та ресурсами. Відомо [1], що структури даних і процеси, які використовуються в системі, мають відповідати принципам функціонування системи, саме тому тенденція децентралізації управління інформаційно-комунікаційними сервісами зумовила виникнення технології блокчейн [2] та її «похідних» — криптовалют [2], інтелектуальних контрактів [3] тощо. Технологія блокчейн є основою розподіленої децентралізованої захищеної технології оброблення інформації, призначеної для розв'язання широкого кола прикладних задач — від децентралізованого випуску та обігу електронної готівки (криптовалюти), аутентифікації та електронного нотаріату до розподіленого підписання контрактів і проведення електронних виборів. З іншого боку, для ефективного використання технології блокчейн потрібно розв'язати низку теоретичних та практичних задач, зокрема:

1. Розроблення та вдосконалення протоколів узгодження в розподілених ненадійних системах.

2. Дослідження моделей даних у блокчейн-системах. Традиційною для технології блокчейн є модель збереження даних із максимальною надлишковістю, коли на кожному вузлі мережі зберігається повна копія бази даних. Альтернативною моделлю збереження даних є модель мінімальної надлишко-

вості, коли частки бази даних розподіляються між усіма вузлами блокчейну і для відновлення повної бази даних потрібна участь усіх вузлів. Між цими двома граничними випадками існують інші моделі збереження даних із різними ступенями надлишковості. Актуальною є задача побудови механізму реплікації таких розподілених баз даних для різних ступенів надлишковості збереження даних.

3. Модифікація наявних криптографічних механізмів блокчейну, наприклад, заміна дерев Меркла, використання групових цифрових підписів, заміна задачі пошуку прообразу геш-функцій на інші складні для обчислення задачі.

4. Аналіз стійкості геш-функцій до обернення з урахуванням особливості їх використання в блокчейні, який відрізняється від традиційного аналізу колізій стійкості та обернення (пошуку прообразу) геш-функцій.

5. Аналіз та побудова клептографічних лазівок блокчейну.

6. Побудова криптографічних протоколів на основі блокчейнів, наприклад, протоколів доказу з нульовими знаннями, анонімізації, доказу інтелектуальної власності тощо.

7. Розрахунки параметрів практичних блокчейн-систем (оцінювання надійності реальних блокчейнів, довжини буферів транзакцій, що очікують на включення у блокчейн та ін.).

У цій роботі проаналізовано теоретичні основи функціонування технології блокчейн та криптовалют, аспекти їх практичного використання, переваги та недоліки зазначених технологій. Запропоновано нову математичну модель для опису технології блокчейн на базі загальної теорії оптимальних алгоритмів [4–6]. Розроблено новий метод розв'язання задачі вдосконалення протоколів узгодження під час формування ланцюга транзакцій, який дає змогу поліпшити оцінки швидкості та стійкості за умови збереження децентралізації внесення змін до ланцюга блоків транзакцій.

СКЛАДОВІ ЧАСТИНИ ТА МАТЕМАТИЧНІ МОДЕЛІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Згідно з класичним визначенням «блокчейн» — це ланцюг блоків транзакцій, побудований за спеціальним правилом [2]. Ланцюг утворюється за допомогою так званої конструкції «геш-показника», коли в одному блоку зберігаються дані та геш-код попереднього блоку (рис. 1). Дані в кожному блоці можуть мати будь-яку природу, наприклад, у блокчейні криптовалюти Bitcoin це реєстр платежів усіх абонентів системи Bitcoin разом із механізмом забезпечення його цілісності. Тут для забезпечення цілісності використовується результат обчислення геш-кодів за методом бінарного дерева Меркла [7] (рис. 1). Таким чином, для верифікації цілісності i-го блоку даних ($i = 0, 1$) на n-ому рівні ієрархії потрібна інформація про геш-коди відповідної гілки дерева на $n, n-1, \ldots, 1$ рівнях ієрархії та «корінь геш-дерева», тобто кортеж $< (h_n^i, h_n^{i+1}), (h_{n-1}^i, h_{n-1}^{i+1}), \ldots, (h_1^i, h_1^{i+1}), h_0 >$. Усього для верифікації блоку даних потрібно не більше ніж $O(\log_2 n)$ обчислень геш-кодів.

Видно, що першою складовою блокчейну є розподілена база даних [8]. Відомо, що є чотири основних стратегії розподілу даних між вузлами — централізація, розподіл, дублювання та змішана стратегія. Існують також різні моделі даних: ієрархічна, мережева, реляційна, об'єктна тощо. Поки що у блокчейнах широко використовуються лише примітивні моделі збереження даних. Якщо розглядати модель пошуку та збереження даних у блокчейнах у загальному випадку, то достатньо адекватною моделлю можна вважати орієнтований граф.

Другою складовою технології блокчейн є протоколи зміни (модифікації, додавання) розподіленої бази даних або протоколи узгодження. Стисло про-

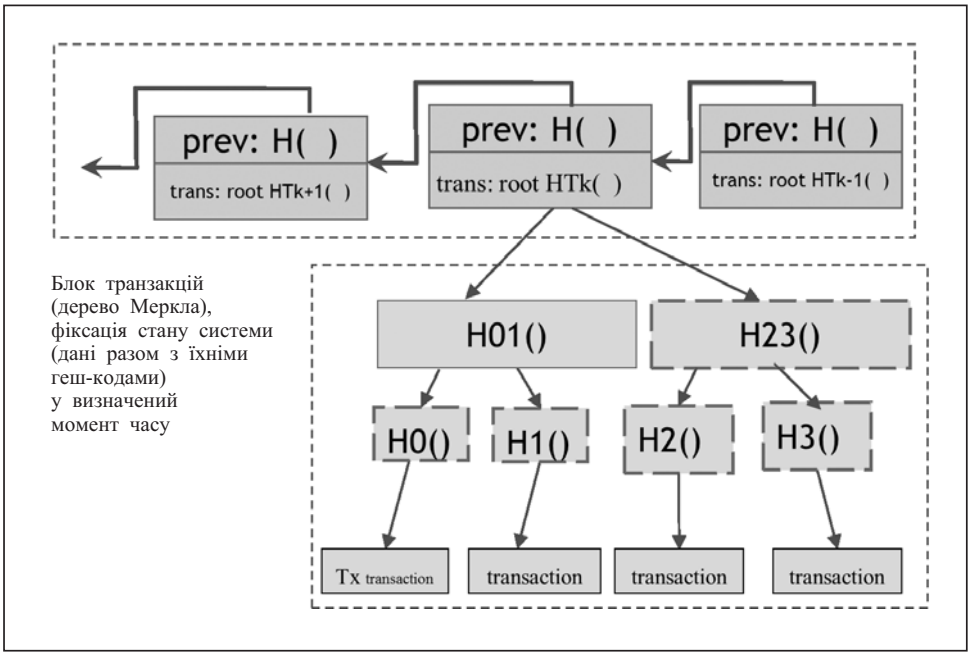

Рис. 1. Ланцюг блоків, що вишиковує блоки транзакцій за порядком їх створення

аналізуємо їхню властивість на прикладі протоколу «proof-of-works» системи Bitcoin. Головною задачею протоколу є генерація нового блоку, що відповідає новому стану системи Bitcoin з проведеними платежами між абонентами. При цьому потрібно уникнути створення абонентами «нечесних» транзакцій (наприклад, повторних витрат монет) та ланцюгів блоків, а також врахувати проблеми ненадійності та асинхронності передачі даних мережею. Проблема побудови протоколів узгодження у розподілених мережах відома як проблема «візантійських генералів» [9]. У випадку візантійських угод для будь-якого початкового входу $x_{i,\, i\in[1,\, n]}$, i-го учасника угоди та деякого параметра d мають виконуватися такі умови.

1. Умова завершення. Всі чесні учасники обчислень у кінці протоколу набувають значення d.

2. Умова коректності. Якщо існує значення x таке, що для чесних учасників $x = x_i$, тоді $d = x$.

Спільна властивість цих протоколів полягає в тому, що загальна кількість учасників повинна перевищувати кількість «нечесних» учасників більше ніж у три рази, $n > 3f$, де f — кількість «нечесних» учасників. Зрозуміло, що такі умови практично унеможливлюють пряме використання зазначених протоколів. Візьмемо до уваги, що більшість цих протоколів створена для розподілених баз даних у мережах із відомою архітектурою без урахування асинхронності та невизначеності архітектури сучасних глобальних інформаційно-телекомунікаційних систем. Тому під час побудови нових асинхронних протоколів узгодження потрібно взяти до уваги такий фактор як неможливість передбачити кількість активних у цей час вузлів мережі. Це зумовлює потребу у здійсненні випадкового вибору учасника протоколу та створенні механізму забезпечення цілісності всіх попередніх транзакцій (далі — «механізму цифрового пломбування»). Додатковою вимогою є створення механізму «заохочення» участі у протоколі для гарантування його роботоздатності.

З огляду на це, основні ідеї створення протоколу узгодження в системі Bitcon є такими:

• забезпечення синхронізації за допомогою ланцюга блоків транзакцій;

• реалізація механізму цифрового пломбування за рахунок цифрового підпису, заснованого на ідентифікаторах;

• реалізація загальноприйнятих для мережі правил генерації наступного блоку транзакцій у ланцюзі блоків;

• забезпечення сталої значної обчислювальної складності розв'язання задачі генерації наступного блоку транзакцій у ланцюзі блоків;

• забезпечення заохочення участі учасників протоколу у розв'язанні задачі генерації наступного блоку транзакцій у ланцюзі блоків;

• можливість перевірки правильності генерації наступного блоку транзакцій у ланцюзі блоків будь-яким учасником протоколу.

З урахуванням зазначеного вище наведемо загальний алгоритм роботи протоколу узгодження блокчейну Bitcoin.

1. Нові транзакції розсилаються всім вузлам мережі.

2. Транзакції розташовуються у списку непідтверджених транзакцій. Вузол обирає транзакції за певним правилом (наприклад, згідно з максимальною грошовою комісією), та об'єднує їх у блок розміром 1–2 Мб (блок містить декілька транзакцій).

3. Кожен вузол намагається підібрати геш-код блоку спеціального вигляду (геш-код прообразу повинен мати префікс визначеного виду). Обчислювальна складність цієї задачі має бути постійною незалежно від обчислювальних можливостей мережі. Відомим прикладом такої задачі є обчислення геш-коду для заданих даних (так званої «геш-головоломки»), а саме знаходження такого значення *nonce*, щоб геш-код $nonce \| hcode_{i-1} \| block_i < t$, де $hcode_{i-1}$ — геш-код попереднього блоку, $block_i$ — дані поточного блоку, t — деяке граничне значення, однакове для усіх учасників протоколу. Відомо, що для сильної геш-функції ця задача розв'язується тільки методом прямого перебору за всіма значеннями *nonce*. Значення t змінюється так, щоб у середньому час розв'язання задачі становив приблизно 10 хвилин. У разі знаходження належного геш-коду відповідний блок відправляється всім вузлам мережі.

4. Вузли перевіряють «справжність» цього блоку (обчислюють геш-функцію, перевіряють спеціальну умову, коректність транзакцій (геш-коди та відсутність витрат коштів, які вже використовувалися) тощо).

5. Якщо перевірки пройдено, новий блок додається до ланцюга та його геш-код використовується як нові вихідні дані.

6. «Винагорода» за генерацію нового блоку може бути повернена. Рекомендовано користуватися нею після 20 підтверджених блоків. Інформацію в транзакціях можна вважати підтвердженою (у системі Bitcoin це «входи»-монети) тільки після підтвердження в середньому п'ять транзакцій.

7. У випадку приблизно одночасної генерації наступного блоку двома і більше майнерами (коли другий майнер публікує інформацію про новий блок перш ніж йому прийде інформація про новий блок від першого) у направленому графі блоків відбувається розгалуження. Далі кожен майнер обирає один з нових блоків (наприклад, той, що побачили першим) і намагається згенерувати новий блок на основі обраного, продовжуючи «відгалуження» у графі. Зрештою один з цих двох ланцюжків стає довшим (той, який обрала більша кількість майнерів) і саме його визнають основним.

Зловмисник намагається згенерувати більш довгий ланцюг блоків аніж «чесні» вузли. Змагання у швидкості між зловмисником та «чесними» вузлами можна представити математичною моделлю масового обслуговування або біноміальним випадковим рухом [2]. Нехай p — ймовірність додавання блоку

в «чесному» ланцюзі, q — ймовірність створення блоку зловмисником, q_z — ймовірність зміни зловмисником z «власних» блоків

$$q_z = \begin{cases} 1, & \text{якщо } p \le q, \\ (q/p)^z, & \text{якщо } p > q. \end{cases}$$

Ймовірність того, що зловмисник переможе «чесних» учасників, можна визначити за законом Пуасона

$$P = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)}),$$

де $\lambda = z\frac{q}{p}$.

У реальній ситуації маємо $p > q$, а $p \le q$ відповідає ситуації, коли 50% та більше обчислювальних потужностей мережі сконцентровані у зловмисника, тобто децентралізацію системи порушено. Підвищення ефективності протоколу узгодження полягає у створенні умов, за яких $p >> q$. Зрозуміло, що у разі застосування підходу лише на основі «обчислювального» або «чистого» принципу «proof-of-works» задача не може бути розв'язана. Тому зазвичай змінюють саму ідею протоколів «доказу роботи». У табл. 1 наведено аналіз деяких протоколів узгодження, альтернативних протоколам «proof-of-works».

Таблиця 1. Аналіз протоколів узгодження

Тип протоколу узгодження	Аналіз алгоритмів визначення пріоритету учасника під час генерації нового блоку
Proof-of-stake	Пріоритет учасника під час генерації нового блоку в ланцюзі блоків залежить від розміру частки розподіленого цінного ресурсу, яким він володіє. За генерацію блоку учаснику збільшується його частка цінного ресурсу. Питання щодо того, як розподілити частки між учасниками на етапі ініціалізації протоколу не розглядається.
Proof-of-activity	Пріоритет учасника під час генерації нового блоку в ланцюзі блоків залежить від його обчислювальних ресурсів, частки цінного ресурсу та «активності» в мережі. Що більшими є частка та час перебування в мережі, то вищим є пріоритет. Прикладом практичної реалізації певною мірою можна вважати криптовалюту DASH.
Proof-of-burn	Пріоритет учасника під час генерації нового блоку в ланцюзі блоків залежить від розміру частки розподіленого цінного ресурсу, який був знищений учасником на попередньому етапі протоколу.
Proof-of-capacity	Пріоритет учасника під час генерації нового блоку в ланцюзі блоків залежить від розміру частки розподіленого цінного ресурсу, яким є місткість простору для зберігання даних.
Proof-of-delegated stake	Пріоритет учасника під час генерації нового блоку в ланцюзі блоків формується у два етапи. На першому відбувається вибір підмножини учасників за результатами процедури голосування. Кількість голосів кожного учасника залежить від частки володіння цінним ресурсом. У другому етапі беруть участь тільки учасники, обрані за результатом першого етапу. Пріоритет учасника на другому етапі залежить від наявності учасника в мережі та його обчислювальних ресурсів. Застосовується у системах Bitshares та Steemit.

ОСНОВНІ ІДЕЇ ТА СТВОРЕННЯ ПРОТОКОЛУ УЗГОДЖЕННЯ «PROOF-OF-ACCURACY»

Результати аналізу різних протоколів узгодження, заснованих як на принципах «proof-of-works», так і на інших (див. табл. 1), дають змогу сформулювати загальну постановку задачі створення ефективного за швидкодією та стійкого до централізації протоколу узгодження для технології блокчейн.

Потрібно розробити протокол узгодження, для якого ймовірність формування блоку чесним учасником набагато більша ніж імовірність створення блоку нечесним учасником протоколу $p >> q$, який залишається стійким до атаки централізації з плином часу, не вимагає значних обчислювальних ресурсів та є ефективним за швидкістю виконання транзакцій.

Перш ніж сформулювати основну ідею створення такого протоколу, зауважимо, що:

• в усіх відомих протоколах узгодження ресурс, за яким визначається пріоритет учасника під час формування угоди, прямо чи опосередковано пов'язаний з деяким реальним цінним ресурсом. У протоколах типу «proof-of-works» це час, обчислювальні ресурси та електроенергія, у протоколах типу «proof-of-stake» це процент від загального цінного ресурсу, наприклад пам'яті («proof-of-capacity»), активності учасника («proof-of-activity»), репутації учасника («proof-of-signature») та ін.; цей зв'язок не дає змоги учасникам генерувати довільну кількість ресурсів і довільно підвищувати свій пріоритет;

• учасники протоколу зацікавлені у проведенні транзакцій з метою додавання блоку за рахунок підвищення свого ресурсу, за яким визначається пріоритет учасника протоколу;

• протоколи містять механізм, який обмежує можливість підвищення пріоритету учасників певною межею для збереження децентралізації протоколу.

Сформулюємо основні ідеї створення нового протоколу узгодження.

1. За основу можна взяти гібрид протоколу типу «proof-of-works» та "proof-of-stake".

2. Для обчислення ресурсу, який визначає рейтинг учасника протоколу в генерації нового блоку, потрібно мати не лише певний поріг обчислювальної складності задачі підвищення рейтингу, але й інформацію про вхідні дані (задані неповно і неточно), що дає змогу розв'язати задачу з потрібною точністю.

3. Для унеможливлення генерації довільної кількості ресурсів учасником протоколу до початку протоколу застосовується три типи обмежень: по-перше, регулюється чисельність учасників, які можуть взяти участь у протоколі; по-друге, окремі дані рейтингу учасників формуються тільки для поточного сеансу протоколу (як сеансові ключі у схемі Діфі–Хелмана); по-третє, інформація про дані, потрібні для обчислення рейтингу, розміщується на кількох ресурсах, за доступ до яких конкурують учасники протоколу угоди («свідома DDOS-атака») і пошук цих даних триває протягом певного непокращуваного часу (принцип «пошуку голки е стіжку сіна»). Через це потрібно розробити метод, який дає змогу забезпечити принципову неможливість розв'язання задачі (на якій засновано генерацію нового блоку) з потрібною точністю до певного часу. Практично станом на певний час не має існувати алгоритм розв'язання задачі з потрібною точністю.

Ці ідеї визначають такий підхід до побудови протоколу узгодження [10]: запропоновано змінити обчислення функції формування «цифрової пломби» (алгоритму додавання нового блоку в блокчейн у разі застосування протоколу угоди «proof-of-works») таким чином, щоб необхідні вхідні дані були задані неповно і неточно, а значення функції потрібно обчислити з точністю, що задається деяким порогом. Інформація про вхідні дані розміщується на кількох ресурсах, за доступ до яких конкурують учасники протоколу угоди. Остання властивість дає змогу зрівняти шанси учасників протоколу з високопродуктивними і малопродуктивними обчислювальними ресурсами в боротьбі за право генерації нового блоку. Як теоретичну основу побудови та оцінювання стійкості протоколу узгодження на основі «доказу точності» запропоновано обрати загальну теорію оптимальних алгоритмів [5], яка пов'язує існування і складність алгоритмів з точністю задання вхідних даних.

Існує кілька можливих варіантів реалізації протоколів узгодження з використанням викладених вище ідей.

Варіант 1. Протокол «simple tickets»

Етап ініціалізації. За допомогою криптографічного протоколу спільної генерації випадкової [11] величини генерується випадкове число R. Воно є невідомим для учасників протоколу. Від нього обчислюється та публікується геш-код $H(R)$. За допомогою (k, n) — порогового криптографічного протоколу розподілу секрету з досконалою стійкістю (наприклад, протоколу Шаміра) [11] число R розміщується за різними випадковими адресами мережі (наприклад, обраного пулу IP-адрес мережі Інтернет) таким чином, що деякі адреси не містять частин секрету.

Основний етап. Учасники протоколу намагаються зібрати k частин для відновлення секрету та за допомогою криптографічних протоколів цифрового нотаріату і доведення з нульовими знаннями довести факт відвідування IP-адрес та володіння числом R. Перемагає та генерує блок той, хто перший зібрав k частин для відновлення секрету. Зв'язок із реальними цінними ресурсами — це використання учасником протоколу реальних IP-адрес, кількість яких є обмеженою. Усі сеансові дані після генерації блоку анулюються як сеансові ключі у протоколі Діфі–Хелмана, тобто цінним ресурсом є реальна IP-адреса. Можливим ускладненням для порушників, які будуть намагатися використати велику кількість IP-адрес, може бути потреба у розв'язанні певної складної задачі під час реєстрації IP-адреси для участі в протоколі. Задачу можна сформулювати згідно з тим самим принципом виключення існування алгоритму (даних для її розв'язання) до початку протоколу узгодження.

Під час практичної реалізації зазначеного протоколу виникають окремі труднощі технічного характеру (наприклад, пов'язані з вибором оптимальної кількості IP-адрес тощо), тому розглянемо інший варіант реалізації зазначених ідей.

Варіант 2. Протокол узгодження «proof-of-accuracy» або «доказ точності»

Інформація про вхідні дані, потрібні для розв'язання задачі генерації нового блоку, розміщується на кількох ресурсах, за доступ до яких конкурують учасники протоколу угоди («свідома DDOS-атака»). Як примітиви для створення протоколу узгодження «proof-of-accuracy» («протоколу доведення точності») (далі — «примітиви протоколу») використовують протокол сумісного генерування випадкового біта, протокол передачі із забуванням, протокол часового замка, протоколи доведення при нульових знаннях, протокол розподілу секрету, обчислення з максимально можливою точністю для заданої апріорної інформації [11].

Сформулюємо загальний опис протоколу в термінах визначених примітивів протоколу, а потім наведемо приклади реалізації з урахуванням сучасних можливостей хмарних технологій для проведення криптоаналізу [12].

Нехай $N(X)$ — інформація, потрібна для обчислення секрету в (k, n) — пороговій схемі розподілу секрету (будь-яка апріорна інформація про X), $S: X \times \Re_+ \to 2^G$ — оператор (у частковому вигляді функція) відновлення секрету, G — множина значень функції інформації про секрет (наприклад, як G можна використовувати вагу Хемінга, значення біта парності та ін.). Тоді інформаційним порогом складності обчислень секрету (максимально можливою точністю для заданої апріорної інформації, що характеризує можливості виконання транзакції) є інформаційна неповнота N. Як $\Phi(N(X))$ обираємо множину ідеальних алгоритмів φ відновлення секрету. Тоді можна довести, що для будь-яких алгоритмів відновлення секрету, які реалізуються множиною $\Phi(N(X))$, існує $r(N(X)) \geq \varepsilon > 0$, де $r(N(X))$ — радіус інформації $N(X)$. Прикладом описаної задачі може бути задача обчислення коефіцієнтів многочлена за його значеннями у точках.

Розіб'ємо випадковим чином граф G блокчейну на підграфи G_i з розподілом P^R, де R — випадкова величина, що визначає кількість вершин підграфів. Вершини підграфа генерують значення (для кожної задачі свої) випадкових величин Y_i з розподілами P^{Y_i}, які відповідають значенням многочлена в певних точках. Як тільки для якогось підграфа кількість інформації буде дорівнювати $r(N(X))$, відповідна підмножина учасників системи розв'язує задачу отримання всіх коефіцієнтів многочлена, продемонструвати яку вона може іншим учасникам мережі. Ймовірності p та q тут визначаються розподілами ймовірностей P^R та P^{Y_i}.

Етап ініціалізації. За допомогою примітиву протоколу «протокол сумісного генерування випадкового біта» (RBG) учасники протоколу генерують випадкові коефіцієнти многочлена, які за допомогою примітиву протоколу «передачі із забуванням» передаються одному випадково обраному спільнотою (також за допомогою RBG) тимчасовому координатору.

Усі дії користувачів протоколюються за допомогою механізму ЕЦП.

Етап наповнення. Тимчасовий координатор за допомогою довіреного генератора випадкових чисел генерує коєфіцієнти многочлена, які випадковим чином надає учасникам спільноти. Участь самого тимчасового координатора у протоколі узгодження виключається за допомогою криптографічного протоколу часового замка (TL).

Етап здійснення транзакції та завершення узгодження. Перший із спільноти, хто збирає k з n частин секрету, доводить це тимчасовому координатору та іншим за допомогою примітиву протоколу доведення при нульових знаннях. Транзакція вважається узгодженою після таких перевірок та завершення участі у протоколу тимчасового координатора за допомогою примітиву TL.

Зауваження

1. DOS-атака на одного з учасників спільноти не порушує протокол, адже ймовірність вибору його як «завершувача» транзакції є незначною.

2. DOS-атака на тимчасового координатора не порушує протокол, адже ймовірність вибору його як тимчасового координатора є незначною.

3. Для зменшення ймовірності нечесної поведінки тимчасового координатора застосовується довірений зовнішній генератор випадковості та додатковий параметр, пов'язаний із тимчасовим координатором, який застосовується у його примітиві TL.

ВИСНОВКИ

Побудова протоколів узгодження на основі принципів, що поєднують переваги протоколів «доказу роботи» та «доказу частки (володіння, активності та ін.)», вважається перспективною з погляду економії обчислювальних ресурсів та збереження децентралізації. Запропоновані в роботі протоколи забезпечують ефективність за часом на рівні протоколів, що використовують «візантійські угоди», але мають менш суворі вимоги до кількості нечесних учасників протоколу.

СПИСОК ЛІТЕРАТУРИ

1. Таненбаум Э., Ван-Стеен М. Распределенные системы. Принципы и парадигмы. Санкт-Петербург: Питер, 2003. 877 с.
2. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf.
3. A next-generation smart contract and decentralized application platform. URL: https://github.com/ethereum/wiki/wiki/White-Paper.
4. Трауб Дж., Вожьняковский Х. Общая теория оптимальных алгоритмов. Москва: Мир, 1983. 382 с.

5. Трауб Дж., Васильковский Г., Вожьняковский Х. Информация, неопределенность, сложность. Москва: Мир, 1988. 184 с.
6. Сергієнко І.В., Задірака В.К., Литвин О.М. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. Київ: Наук. думка, 2012. 400 с.
7. Ralph C.M. Secrecy, authentication, and public key systems. Ph.D. thesis. (El. Eng.). Stanford, 1979. 182 p. URL: http://www.merkle.com/papers/Thesis1979.pdf.
8. Коннолли Т., Бегг К., Страчан А. Базы данных: проектирование, реализация и сопровождение. Теория и практика. Москва: Вильямс, 2000. 1093 с.
9. Pease M., Shostak R. The Byzantine Generals problem. *ACM Transactions on Programming Languages and Systems.* 1982. Vol. 4, Iss. 3. P. 382–401.
10. Кудин А.М. Блокчейн и криптовалюты на основании «доказательства точности». *Математичне та комп'ютерне моделювання. Серія: Технічні науки: Зб. наук. праць.* Інститут кібернетики ім. В.М. Глушкова Національної академії наук України, Кам'янець-Подільський національний університет імені Івана Огієнка. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2017. Вип. 15. С. 104–108.
11. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. Москва: Горячая линия – Телеком, 2007. 320 с.
12. Задирака В.К., Кудин А.М., Селюх П.В., Швидченко И.В. Облачные технологии: новые возможности для вычислительного криптоанализа. *Проблемы управления и информатики.* 2016. № 1. С. 148–155.

Надійшла до редакції 05.07.2018

А.М. Кудин, Б.А. Коваленко, И.В. Швидченко
ТЕХНОЛОГИЯ БЛОКЧЕЙН: ВОПРОСЫ АНАЛИЗА И СИНТЕЗА

Аннотация. Рассмотрена роль технологии блокчейн в реализации одной из тенденций развития современных информационных систем — децентрализации. Проанализирована общая модель функционирования блокчейн-системы и предложена идея построения нового типа протоколов консенсуса (протокол «proof-of-accuracy»), объединяющего преимущества протоколов типа «proof-of-work» и «proof-of-stake». Исследованы пути реализации протокола «proof-of-accuracy».

Ключевые слова: распределенные компьютерные системы, безопасность информации, криптология, блокчейн, криптовалюты, протоколы консенсуса, общая теория оптимальных алгоритмов, протокол согласования типа «proof-of-accuracy».

A.M. Kudin, B.A. Kovalenko, I.V. Shvidchenko
BLOCKCHAIN TECHNOLOGY: ANALYSIS AND SYNTHESIS

Abstract. The role of the blockchain technology in decentralization of the modern computer system is discussed. Authors analyze general model of operation of the blockchain system. The idea of a new type of consensus protocols (proof-of-accuracy protocol) is proposed. According to authors' opinion, the new protocol have the benefits of "proof-of-work" and "proof-of-stake" protocols. The ways of implementation of the "proof-of-accuracy" protocol are discussed.

Keywords: distributed computing systems, information security, cryptology, blockchain, cryptocurrency, consensus protocols, proof-of-accuracy consensus protocol.

Кудін Антон Михайлович,
доктор техн. наук, старший науковий співробітник, професор Фізико-технічного інституту НТУУ «КПІ імені Ігоря Сікорського», заступник директора департаменту безпеки — начальник управління безпеки інформації Національного банку України, Київ, e-mail: pplayshner@gmail.com.

Коваленко Богдан Анатолійович,
здобувач кафедри математичних методів захисту інформації Фізико-технічного інституту НТУУ «КПІ імені Ігоря Сікорського», Київ, e-mail: animantbk@gmail.com.

Швідченко Інна Віталіївна,
кандидат фіз.-мат. наук, старший науковий співробітник Інституту кібернетики ім. В.М. Глушкова НАН України, Київ, e-mail: inetsheva@gmail.com.