

УДК 004.057.4

DOI: 10.31891/2219-9365-2019-64-12

БЕЛЬФЕР Р. Е., САВЕНКО О. С.

Хмельницький національний університет

ПРОТОКОЛ КОНСЕНСУСУ PROOF-OF-ACTIVITY НА ОСНОВІ ВІДСЛІДКОВУВАННЯ ПОКАЗНИКІВ УЧАСТІ АКТИВНИХ ВУЗЛІВ МЕРЕЖІ

В роботі здійснено постановку актуальної наукової задачі з розроблення нового соціально орієнтованого протоколу, основними задачами якого є уникнення псевдо-децентралізації та монополізації мережі, збільшення доступності участі у підтримці роботи системи для всіх активних вузлів мережі, чесний відбір потенційних вузлів валідаторів базуючись на продуктивності їхньої участі у роботі мережі та справедлива винагорода за створення нових блоків та додавання їх до блокчейну. Розроблений протокол забезпечує створення та додавання нових блоків до блокчейну нових вузлів валідатор, який створюватиме наступний блок, згідно з його корисною активністю у мережі відповідно до попередньо визначених умов, що можуть бути сформовані відповідно до вимог системи та задовольнятимуть індивідуальні потреби блокчейну. Для застосування протоколу PoA мережа проектується за принципом Layered Peer to Peer (LP2P) архітектури особливістю якої є те, що рівні за своєю взаємодією вузли розміщуються на різних рівнях відповідно до своєї типізації або параметризації, що використовуватиметься для виконання алгоритму, який розроблено, та знаходження консенсусу.

Крім того, протокол може бути одним з етапів впровадження нових принципів податкової локальної політики, де податки будуть прив'язані до активностей окремих членів громадськості, а також, оновлення виборчого права, що базуватиметься на соціальній активності учасників мережі та стане якісно новим принципом проведення нових, експериментальних але якісних виборів.

Ключові слова: протокол, мережа, алгоритм мережного протоколу, блокчейн, архітектура

BELFER R., SAVENKO O.

Khmelnitskyi National University

PROOF-OF-ACTIVITY CONSENSUS PROTOCOL ON THE PARTICIPATION OF INDICATORS ACTIVE NETWORK NODES

The paper deals with the setting of a topical scientific task of developing a new socially oriented protocol, the main tasks of which are to avoid pseudo-decentralization and monopolization of the network, to increase the availability of participation in maintaining the operation of the system for all active nodes of the network, fair selection of potential nodes of validators based on productivity network operation and a fair reward for creating new blocks and adding them to the blockchain. The developed protocol provides creation and addition to blockchain of new blocks, defines a node validator, which will create the next block according to its useful activity in the network according to predefined conditions, which can be formed according to the requirements of the system and will satisfy the individual needs of the blockchain. To apply PoA, the network is designed on a Layered Peer to Peer (LP2P) architecture, the feature of which is that nodes interact at different levels according to their typing or parameterization, which will be used to execute the algorithm developed and find consensus.

In addition, the protocol may be one of the steps in the implementation of new principles of local tax policy, where taxes will be tied to the activities of individual members of the public, as well as the renewal of suffrage based on the social activity of network members and a qualitatively new principle of conducting new ones, experimental but qualitative choices.

Keywords: protocol, network, network protocol algorithm, blockchain, architecture

Постановка задачі. Технологія розподіленого реєстру блокчейн досягла небувалої інформаційної впізнаваності у 2018 році завдяки високому попиту на продукт своєї діяльності - криптовалюту. Незважаючи на різкий спад вартості основних світових криптовалют та зменшенні інформаційного простору навколо технології, блокчейн залишається однією з найперспективніших ІТ сфер наряду зі штучним інтелектом, інтернетом речей, хмарними рішеннями та інших. Зацікавленість проявляють фінансові корпорації та світові банки, підприємства задіяні у сфері агропромисловості та гравці на ринках землі чи нерухомості, урядові структури та соціальні мережі. Найпопулярнішими методами організації блокчейн мереж є протоколи консенсусу Proof-of-Work (PoW) та Proof-of-Stake (PoS). Проте, і перший і другий мають як переваги так, і, суттєві недоліки, що впливають на безпеку, швидкість роботи, доступність, можливість масштабування та навіть енергоефективність.

PoW тісно пов'язаний з витратами електроенергії для здійснення обчислень, які необхідні для основ функціонування блокчейн систем з використанням цього протоколу. За деякими оцінками найбільші блокчейн системи що використовують PoW - оціночно у 2020 році сукупно Bitcoin та Ethereum зможуть спожити електроенергії для майнінгу на 4.5 млрд. \$, тобто більше 14 млн. \$ щоденно [2, 3]. Для порівняння, ці дві мережі, для забезпечення власних потреб у майнінгу, використовують більше енергії, ніж Фінляндія. Серед інших недоліків PoW - недостатня швидкість проведення транзакцій (формування одного блоку транзакцій займає 10 хв - саме такий час займає обчислення необхідної задачі для підтвердження, а складність самої задачі формується таким чином, щоб на її виконання витрачалося саме така кількість

часу [1]), псевдо-децентралізація при якій основна “влада” концентрується поміж вузлів з найпотужнішим обладнанням, поступова втрата мотивації учасників брати участь у підтримці роботи мережі, оскільки з часом винагорода за майнінг зменшується, що може призвести до зниження безпеки у системі шляхом зменшення загальної кількості активних вузлів.

Альтернативою PoW став новий принципово інший за своєю суттю протокол PoS [4]. Протокол ставлять у протизвагу PoW беручи до уваги такі переваги як відсутність залежності від електроенергії, оскільки відсутня необхідність проведення значних обчислень, зацікавленість учасників в підтримці безпеки системи, оскільки вони самі володіють монетами у мережі, більш задовільна швидкість проведення транзакцій. Проте, у протокола залишаються такі проблеми як псевдо-децентралізація [5], що і у випадку з PoW можуть призводити до зниження мотивації щодо участі у мережі. Оскільки учасники з більшими частками володіння монетами будуть обиратися алгоритмом частіше, тобто виконуватиметься правило, що багаті стають багатшими - отримуємо зав'язаність на основних гравців у системі, що встигли накопичити або придбати основну кількість монет.

Такі недоліки змушують дослідників вдаватись до розробок нових протоколів консенсусу, які б дозволяли системі слідувати визначеним цілям та уникати недоліків уже існуючих алгоритмів.

Саме в цьому **мета дослідження** - створення нового соціально орієнтованого протоколу, основними задачами якого є уникнення псевдо-децентралізації та монополізації мережі, збільшення доступності участі у підтримці роботи системи для всіх активних вузлів мережі, чесний відбір потенційних вузлів валідаторів базуючись на продуктивності їхньої участі у роботі мережі та справедлива винагорода за створення нових блоків та додавання їх до блокчейну.

Протокол консенсусу Proof-of-Activity (PoA) забезпечує створення та додавання до блокчейну нових блоків, визначає вузол валідатор, який створюватиме наступний блок, згідно з його корисною активністю у мережі відповідно до попередньо визначених умов, що можуть бути сформовані відповідно до вимог системи та задовольнятимуть індивідуальні потреби блокчейну.

Для застосування протоколу PoA мережа проектується за принципом Layered Peer to Peer (LP2P) архітектури особливістю якої є те, що рівні за своєю взаємодією вузли розміщуються на різних рівнях відповідно до своєї типізації або параметризації що використовуватиметься для виконання алгоритму та знаходження консенсусу.

Протокол консенсусу PoA може бути впроваджений у будь-яких соціально орієнтованих структурах: соціальних мережах, краудфінансових платформах, громадських платформах та муніципальних системах - будь які організаційні форми у яких чітко прослідковується рівень корисної активності учасників, учасники можуть бути типізовані за видом активності або ж можуть бути параметризовані згідно до їх можливостей у системі.

Особливості протоколу PoA можуть бути використані для створення муніципальних урядових платформ що об'єднуюватимуть громадські ініціативи та надаватимуть можливості для участі населення у їх реалізації. Інтегровані у такі платформи фінансові системи зможуть проводити розрахунок внутрішньою криптовалютою, що буде продуктом діяльності такої децентралізованої системи на основі протоколу консенсусу PoA.

Також, протокол може бути одним з етапів впровадження нових принципів податкової локальної політики де податки будуть прив'язані до активностей окремих членів громадськості, а також, оновлення виборчого права, що базуватиметься на соціальній активності учасників мережі та стане якісно новим принципом проведення нових, експериментальних але якісних виборів.

Пов'язані роботи. Серед напрацювань у сфері дослідження блокчейну, які ставили за мету створення соціально орієнтованих мереж на протизвагу популярним PoW та PoS, варто виділити такі, що були проведені компаніями NEM [6] та Mithril [7].

Сінгапурська компанія NEM позиціонує себе як новаторську, використовуючи на 100% оригінальні розробки власної блокчейн платформи та як альтернативу існуючим PoW та PoS. Компанія створила першу криптовалюту використовуючи алгоритм Proof-of-Importance (PoI) [8]. Нова система консенсусу пропонує швидкі транзакції, мінімальні комісійні збори, низьке споживання електроенергії та абсолютну прозорість у роботі - команда розробників позиціонує NEM, як функціональний грошовий засіб у сучасній економіці. Час створення транзакції у гаманці користувача займає 5 секунд, підтвердження - 20 секунд. Мережа готова до обробки 3000 транзакцій за секунду [9].

PoI [10] - це механізм, що використовується для визначення учасника (вузла) мережі, який має право додати блок до блокчейну, процес який у NEM називають harvesting. В обмін на здійснення такого процесу, вузли можуть збирати комісійні збори з транзакцій у блоці. Учасники з найвищим показником важливості матимуть більшу ймовірність бути обраними для процесу створення блоку. Проте, щоб бути потенційно обраним для обчислення показнику важливості, NEM протокол вимагає наявність щонайменше 10000 XEM, криптовалюти у мережі NEM, на рахунку учасника системи.

PoI має на меті вирішення проблеми, яка може виникати у моделі PoS при ідентифікації загальної підтримки мережі учасниками. NEM вирішує цю задачу враховуючи три фактори: вклади, транзакційне партнерство, кількість та розмір транзакцій, проведених за останні 30 днів.

Вклади:

- потрібно буде щонайменше 10000 придбаних монет для участі у harvesting;
- більша кількість придбаних монет є підтвердженням більшої важливості учасника;
- PoI враховує лише ті монети, які є у власності учасника певну кількість часу.

Транзакційне партнерство:

- PoI винагороджує користувачів, які проводили транзакції на рахунки інших учасників NEM мережі;

- користувачі не можуть маніпулювати у мережі проводячи транзакції між акаунтами; алгоритм враховує лише чисті перекази в часі.

Кількість та розмір транзакцій, проведених за останні 30 днів:

- одна транзакція (більша мінімального розміру) підвищує доказ важливості акаунту;
- більші та частіші транзакції мають більший вплив на підтвердження важливості.

Mithril [11] - це соціально медійна платформа децентралізованого типу, започаткована Тайваньським підприємцем Jeffrey Huang, що винагороджує будь-кого, хто створює медійний контент. Користувачі заробляють токени за допомогою процесу "соціального майнінгу", що дозволяє їм взаємодіяти з іншими отримуючи винагороду, чи є вони відомим учасниками соціальних медіа чи основними бренд лідерами. За допомогою блокчейн технології, Mithril спроможний забезпечити безпеку транзакцій та всіх залучених частин мережі. Додатково, технологія децентралізованого зберігання даних блокчейну дозволяє ефективний запис незмінних та перевірених транзакцій. Головною метою Mithril є створення найоптимальнішої та найкращої блокчейн системи для впровадження її у застосунках соціальних мереж. Головним пріоритетом технології є інтеграція з існуючими основними соціально-медійними платформами.

Соціальний майнінг [12], як технологія вперше застосована у Mithril, використовується для забезпечення процесу, що лежить в основі системи. Основою обчислення алгоритму соціального майнінгу є створений користувачем цінний контент у мережі згідно якого він може отримати монету MITN. Винагорода буде напряму пов'язана з їхнім впливом та успіхом як контрибуторів мережі. Чим більше мережеву значимість користувач привнесе у платформу, тим більше монет він отримає. Наприклад, варіант діяльності трьох нових користувачів – X, Y та Z, можна описати наступним алгоритмом. Вони нові користувачі та на їхніх балансах 0 монет. Через тиждень X генерує 4 історії та отримує 400 переглядів і 0 вподобань. Y генерує 5 історій та в свою чергу отримує 200 переглядів та 80 вподобань. А Z не згенерувала жодного контенту. В результаті X отримує 400 одиниць ore, Y - 600 одиниць а Z - 0. Після проведення відповідних розрахунків, загальна Mithril винагорода за тиждень становить 10000 монет MITN. Відповідно X отримує 4000 монет MITN, Y - 6000 MITN, Z не отримує нічого.

Основна частина.

1. Мережна архітектура Layered Peer-to-Peer (LP2P)

Для проектуванням блокчейну за принципами PoA потрібно внести ясність у архітектуру задіяної мережі. В основі канонічних мереж блокчейн, як Bitcoin що базується на протоколі консенсусу PoW, використовується однорангова архітектура Peer-to-Peer (P2P). У такому випадку кожен вузол мережі є рівноправною одиницею у загальній роботі системи. Проте, для реалізації PoA необхідна типізація чи параметризація учасників мережі. Це необхідно для проходження визначених стадій роботи алгоритму консенсусу та відбору потенційних вузлів валідаторів серед загальної множини.

У такому випадку, однорангова мережа потребує додаткового уточнення для такого використання. Саме тому запропоновано використовувати множину рівнів для кожного окремого типу або параметра вузлів мережі. Кожен рівень (layer) містить підмножину вузлів, що поєднуються за певною ознакою, проте не втрачають ознак класичної P2P мережі при знаходженні у одноранговому зв'язку між собою. Таким чином, уточнена архітектура набуватиме нового виду, а для її визначення пропонується ввести нову назву багаторівневої однорангової мережі - Layered Peer-to-Peer (LP2P). Схематичне зображення різних видів мережевих архітектур (серверно-орієнтована, однорангова, багаторівнева однорангова) представлено на рис. 1 та 2. Відповідно до кількості та якості своєї активної діяльності у мережі, вузол може переміщатися рівнями, тим самим підвищувати вірогідність обрання валідатором. Таким чином, розташування вузла у багаторівневій мережі не є статичним і може змінюватися. Таким чином, згідно зі схемою зображеною на рис. 2., при виконанні умови $activityIndex(node) \geq index1$ для вузла node0K отримуємо перетворення node0K node1L+1. Отже, якщо вузол рівня N досягає такого індексу активності, що є щонайменше рівним індексу активності рівня N+1, то такий вузол переміщується і стає вузлом рівня N+1.

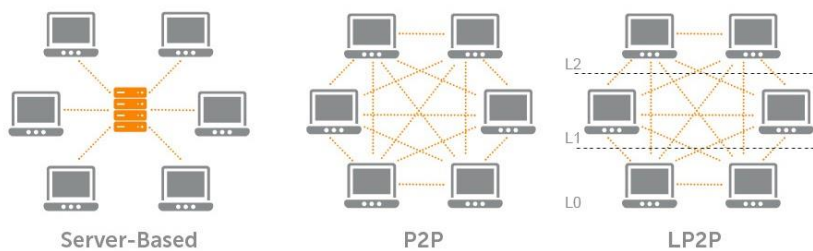


Рис. 1. Схематичне зображення різних видів мережних архітектур: серверно-орієнтована, однорангова, багаторівнева однорангова

Серед усієї множини вузлів мережі, рівневному поділу підлягатимуть лише активні вузли мережі, тобто ті, діяльність яких буде обчислюватися за коефіцієнтами активності і вони матимуть право брати участь у відборі на роль валідатора (Рис. 3.).

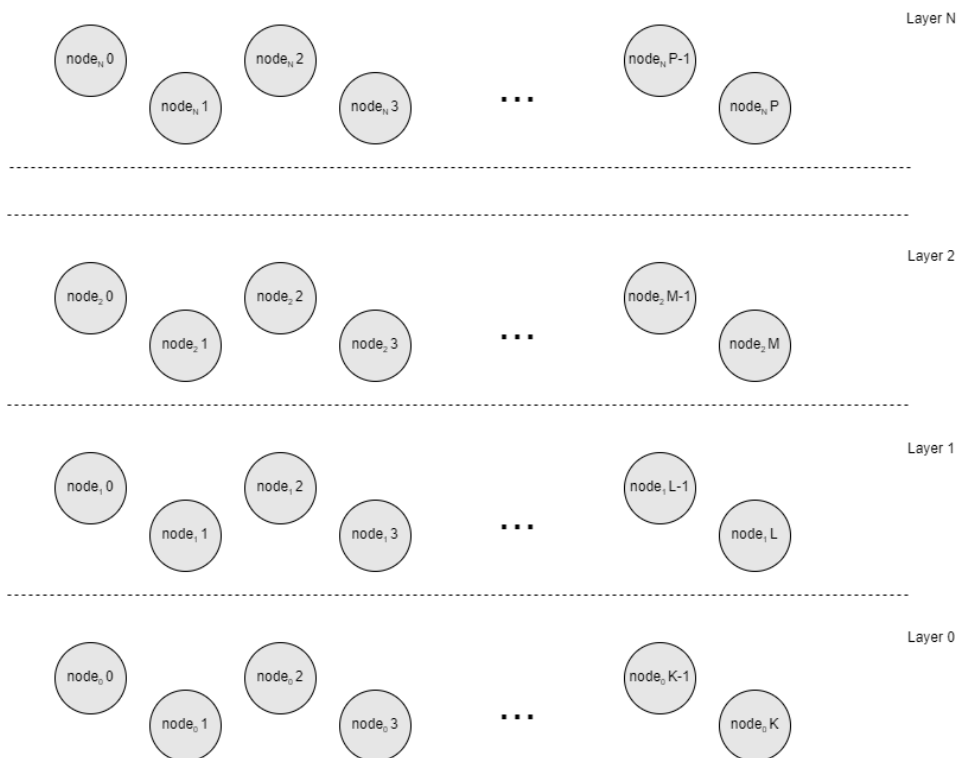


Рис. 2. Схематичне зображення багаторівневої однорангової мережі та вузлів розміщених на рівнях

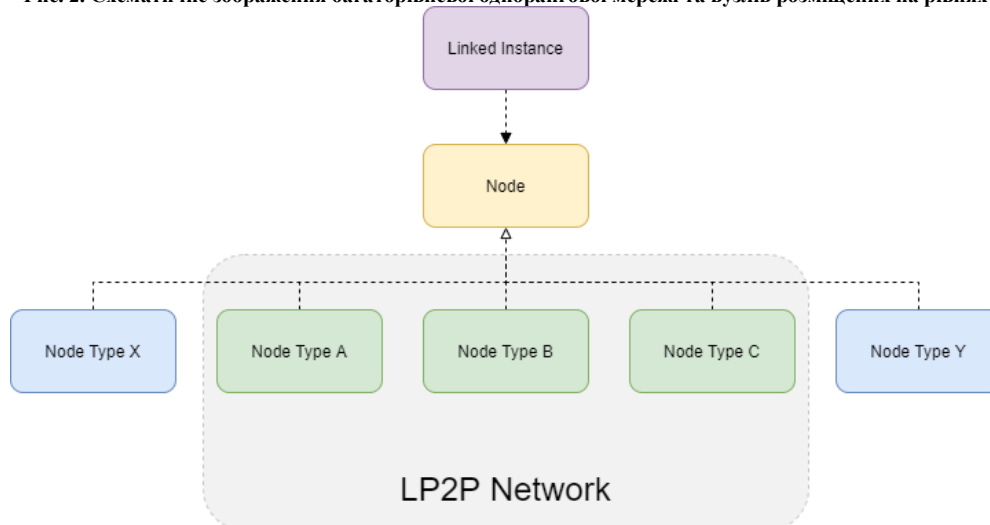


Рис. 3. Діаграма класів типів вузлів мережі що є активними (Node Type A, Node Type B, Node Type C) або пасивними (Node Type X, Node Type Y)

2. Протокол консенсусу activity.

Задача протоколу консенсусу PoA полягає у забезпеченні енергоефективного, справедливого у винагороді, соціально орієнтованого процесу підтвердження транзакцій методом додавання блоків у блокчейн.

Розглянемо енергоефективність. У алгоритмі схожому до PoS та відмінному від PoW відсутня задача, вирішення якої є єдиним шляхом досягнення консенсусу та створення і підпису нового блоку. Це не вимагає апаратних потужностей для завершення верифікації транзакції та не стає початком майнінгової лихоманки, що завершується витрачанням колосальних ресурсів для обчислення хеш функції, яка з кожним разом стає все складнішою і вимагає залучення все більших потужностей для швидкого обчислення.

Розглянемо вимогу справедливої винагороди. На відміну від PoS не обов'язково володіти найбільшою часткою криптовалюти для того, щоб мати шанс стати валідатором та отримати винагороду. Це посилює децентралізацію та знижує мотивацію отримання якомога більшої частки монет. На відміну від PoW не потрібно розширювати обчислювальні потужності для підвищення шансів стати валідатором та отримати винагороду. Вірогідність обрання валідатором напряму залежить від рівня активності учасника мережі та спонукає всі вузли до підвищення активності, що може бути соціально корисним.

Соціально орієнтованість може зацікавити соціальні структури у впровадженні блокчейну, що використовує алгоритм PoA. Соціальна орієнтованість спонукає учасників бути більш активними у вирішенні різноманітного пулу задач та проблем. До прикладу, таким чином, мешканці міста, у випадку запуску такої системи муніципалітетом, зможуть долучитись до громадської діяльності отримуючи реальну винагороду та мотивацію до дій. Така система може стати першим кроком до впровадження цифрової фінансової системи, перегляду податкових принципів та зміни виборчого права.

3. Алгоритм роботи протоколу при створення нового блоку.

Передумовою початку роботи алгоритму є наявність у множині вхідних транзакцій готових до запису у блок. Аналогічно до стандарту Bitcoin, розмір блоку транзакцій дорівнює 1 mb інформації. Отже, на вхід алгоритму подається така кількість транзакцій, що $\sum_{i=1}^n size_i = const_{size}$, де $size$ - розмір транзакції, N - кількість транзакцій готових до запису в блок, $const_{size}$ - сталий розмір блоку транзакцій = 1 mb.

Етапи алгоритму знаходження консенсусу між вузлами та виділення єдиного вузла валідатора, що матиме право здійснити створення блоку, його підпис та додавання до блокчейну, схематично зображені на рис. 4 та описані нижче.

Етап 1: Для множини з N рівнів $[A, B, C \dots N]$, розміщених згідно мережевої архітектури LP2P, та множини вузлів кожного рівня, де вузол $a_i \in A$, де $i \leq k$, вузол $b_i \in B$, де $i \leq l$, вузол $c_i \in C$, де $i \leq k$, ..., вузол $n_i \in N$, де $i \leq p$, для кожного з рівнів виконуються визначена функція відбору потенційного валідатора f . Отже, для множини рівнів $[A, B, C \dots N]$ та множинам вузлів що належать кожному з рівнів, отримуємо множину функцій: $f_a(a_1, a_2, a_3 \dots a_k)$, $f_b(b_1, b_2, b_3 \dots b_l)$, $f_c(c_1, c_2, c_3 \dots c_m) \dots f_n(n_1, n_2, n_3 \dots n_p)$. Результатом виконання функції f для кожного з рівнів з множини $[A, B, C \dots N]$ та множини вузлів, що належать кожному з рівнів, є потенційний валідатор. Відповідно отримано результуючу множину потенційних валідаторів $[a', b', c' \dots n']$.

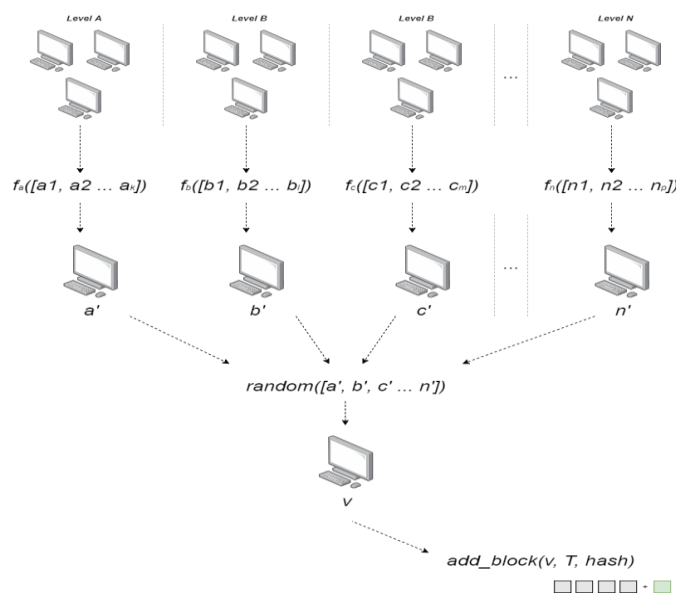


Рис 4. Схема алгоритму роботи протоколу PoA по знаходженню консенсусу між вузлами та довананню нового блоку до блокчейну

Еман 2: Множина потенційних валідаторів $[a', b', c' \dots n']$ використовується як параметр для функції випадкового визначення результуючого вузла валідатора - $random([a', b', c' \dots n'])$. Результатом виконання функції є кінцевий вузол v - визначений випадковим чином серед вузлів множини $[a', b', c' \dots n']$.

Еман 3: Кінцевий вузол v використовується як параметр для додавання блоку транзакцій до блокчейну та підпису цього блоку хеш значенням, отриманого в результаті попереднього виконання хеш функції, - $block(v, T, hash)$, де v - вузол валідатора, T - множина валідних транзакцій готових до запису в блок, $hash$ - хеш ключ, яким буде підписано блок.

На рис. 5 зображено візуалізацію роботи алгоритму для знаходження консенсусу серед вузлів LP2P мережі з трьохрівневою типізацією - множина рівнів $[A, B, C]$.

Висновки. Запропоновано новий соціально орієнтований протокол, основними задачами якого є уникнення псевдо-децентралізації та монополізації мережі, збільшення доступності участі у підтримці роботи системи для всіх активних вузлів мережі, чесний відбір потенційних вузлів валідаторів базуючись на продуктивності їхньої участі у роботі мережі та справедлива винагорода за створення нових блоків та додавання їх до блокчейну. Він забезпечує створення та додавання до блокчейну нових блоків, визначає вузол валідатор, який створюватиме наступний блок, згідно з його корисною активністю у мережі відповідно до попередньо визначених умов, що можуть бути сформовані відповідно до вимог системи та задовольнятимуть індивідуальні потреби блокчейну.

Для застосування протоколу PoA мережа проектується за принципом Layered Peer to Peer (LP2P) архітектури особливістю якої є те, що рівні за своєю взаємодією вузли розміщуються на різних рівнях відповідно до своєї типізації або параметризації, що використовуватиметься для виконання алгоритму, який розроблено, та знаходження консенсусу.

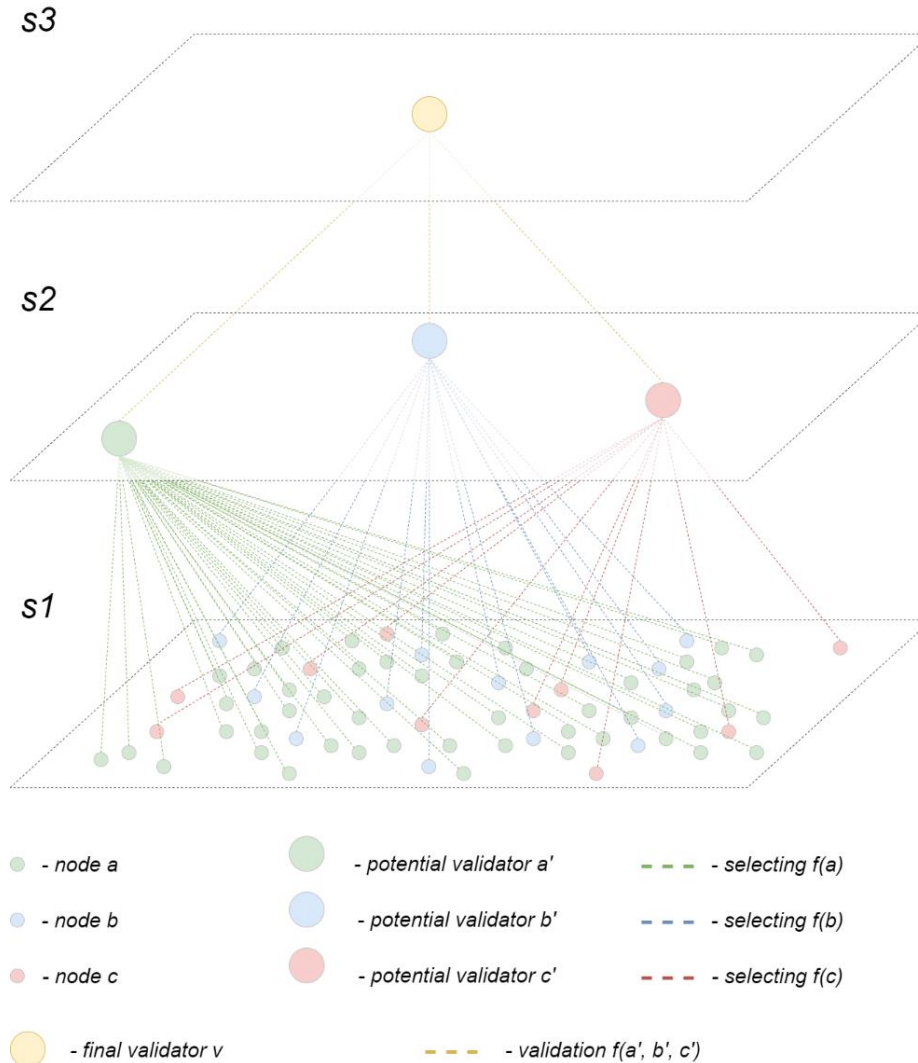


Рис. 5. Візуалізація роботи алгоритму PoA для знаходження консенсусу серед вузлів LP2P мережі з трьохрівневою типізацією

Протокол консенсусу PoA може бути впроваджений у будь-яких соціально орієнтованих структурах: соціальних мережах, краудфандингових платформах, громадських платформах та муніципальних системах - будь які організаційні форми у яких чітко прослідковується рівень корисної активності учасників, учасники можуть бути типізовані за видом активності або ж можуть бути параметризовані згідно до їх можливостей у системі.

Крім того, протокол може бути одним з етапів впровадження нових принципів податкової локальної політики, де податки будуть прив'язані до активностей окремих членів громадськості, а також, оновлення виборчого права, що базуватиметься на соціальній активності учасників мережі та стане якісно новим принципом проведення нових, експериментальних але якісних виборів.

Напрямок подальших досліджень є розробка складових архітектури мережної системи та методів взаємодії компонентів системи і захисту інформації в ній.

Reference

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, <https://bitcoin.org/bitcoin.pdf>.
2. Ethereum Energy Consumption Index, <https://digiconomist.net/ethereum-energy-consumption>.
3. Bitcoin Energy Consumption Index, <https://digiconomist.net/bitcoin-energy-consumption>.
4. A Next-Generation Smart Contract and Decentralized Application Platform, <https://github.com/ethereum/wiki/wiki/White-Paper>.
5. Redefining Internet Protocols Through Effective Decentralization, <https://hackernoon.com/defining-internet-protocols-through-effective-decentralization-b2afbc874d9>.
6. NEM, New Economy Movement, <https://nem.io/>.
7. Mithril, The Future of Social Networks, <https://mith.io/>.
8. What is PoI? <https://docs.nem.io/ja/gen-info/what-is-poi>.
9. Introduction to NEM (XEM): The Proof-of-Importance Coin, <https://cryptoslate.com/nem/>
10. Proof of Importance Explained, <https://www.mycryptopedia.com/proof-of-importance/>.
11. Beginner's Guide to Mithril: Social Platform Which Rewards Content Creators, <https://blockonomi.com/mithril-guide/>.
12. The Future of Social Networks. Mithril (MITH) Whitepaper, <https://whitepaperdatabase.com/mithril-mith-whitepaper/>.

Рецензія/Peer review : 19.09.2019

Надрукована/Printed : 08.01.2020