УДК 004.75

ПОРІВНЯННЯ АЛГОРИТМІВ КОНСЕНСУСУ ДЛЯ ІНТЕРНЕТ РЕЧЕЙ

Мурин М.В.[1)], Васильків В.О.[2)]
Тернопільський національний економічний університет
[1)]магістрант; [2)]студент

І. Постановка задачі

Інтернет речей змінить світ, зробивши багато технологічних процесів можливими без участі людини. Інтернет речей – одна з найпопулярніших концепцій в сучасній футурології. І більш того, одна з тих небагатьох, що вже перестають бути концепціями і втілюються в життя. Згідно з найбільш поширеним формулюванням, Інтернет речей – це концепція обчислювальної мережі фізичних предметів (речей), які оснащені технологіями для взаємодії один з одним.Для реалізації IoT необхідна екосистема, яка включала б у себе «розумні речі» – різні пристрої, оснащені сенсорами; мережу доступу і передачі інформації, а також платформи для управління мережею, пристроями і додатками.Концепція передбачає, що Інтернет речей здатний серйозно вплинути на розвиток сучасного суспільства, оскільки дозволить багатьом процесам відбуватися без участі людини[1].

Для використання технології блокчейн в середовищі Інтернет речей необхідна розробка нових алгоритмів консенсусу, які не вимагають значних обчислювальних та енергозатрат.

ІІ. Мета роботи

Метою роботи є порівняння алгоритмів консенсусу IOTA і IOTW для Інтернет речей.

ІІІ. Алгоритми консенсусу для Інтернет речей

Консенсус – це процес прийняття рішень групою, в якій всі члени групи погоджуються підтримати рішення в інтересах цілого. Це загальна згода і солідарність один з одним.

Proof of Assignment – це алгоритм консенсусу нового покоління, який вимагає менших енерговитрат і може працювати на відносно недорогому обладнанні. Цей алгоритм позиціонується як менш енерговитратний в порівнянні з алгоритмами доказ виконаної роботи (PoW) і доказ частки володіння (PoS), які вимагають значного обсягу обчислювальної потужності і пам'яті. PoA розглядається як відповідь на недоліки найпопулярніших в даний час алгоритмів - PoW і PoS - які виявляються, коли ми намагаємося застосувати ці алгоритми в Internet of Things (IoT). IoT – це мережа фізичних пристроїв, транспортних засобів, побутової техніки та інших предметів оснащених електронікою, програмним забезпеченням, датчиками, приводами і можливістю підключення до Інтернету [2].

Для інтернету речей розроблена цифрова валютаIOTA. IOTA не використовує блокчейн, замість блоків в ланцюжки об'єднуються транзакції, утворюючи направлений ациклічний граф (Directed Acyclic Graph,DAG) (рис.1). Емісія в системі одноразова і централізована. Перша транзакція в системі - породжує genesisблок, де розробник присвоїв собі всі монети системи. Всього було створено 2.779.530.283.277.761 монет IOTA. Кожна наступна транзакція в системі вимагає від учасника доказу виконаної роботи і підтвердження двох попередніх транзакцій. Таким чином всі транзакції в системі об'єднуються в складний ланцюжок транзакцій, де кожна наступна посилається на певні дві попередні і таким чином підвищує ступінь їх підтвердження. Такий механізм зв'язку транзакцій розробники назвали Tangle.

IOTA – це і криптовалюта, і система для здійснення миттєвих мікроплатежів без будь-якої комісії [3].

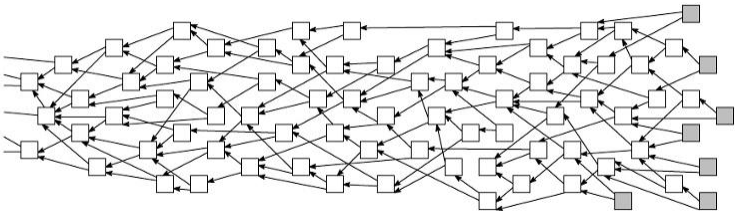

Рисунок 1 – Схема транзакцій IOTA

Блокчейн IOTW використовує алгоритм консенсусу PoA і надає мікро-майнінг, який дозволяє виконувати легкий майнінг на IoT-пристроях, усуваючи необхідність зберігання та обслуговування блокчейна на рівні самих IoT-пристроїв. Зберіганням і обслуговуванням блокчейне займаються попередньо налаштовані довірені ноди. IoT-пристрої виконують обмежену, доступну і просту задачу пошуку відповідного значення хеша і відправляють інформацію довіренійноді. Ноди збирають передану ним інформацію про транзакції, перевіряють її та створюють шаблон блоку з відповідної кількістю перевірених транзакцій [4].

Порівняння алгоритмів консенсусу для мереж Інтернет речейприведено в таблиці 1.

Переваги алгоритму «Proof of Assignment»:1) побутові пристрої можуть бути використані для майнінгу, пропонуючи реалістичне вирішення проблем масштабованості і відкладеної обробки транзакцій, з якими стикаються сучасні популярні криптовалютні мережі; 2) власники пристроїв можуть самі планувати, коли їх пристрої будуть брати участь в майнінгу; 3) власник пристрою може охоче ділитися або продавати дані, згенеровані і оброблені його пристроєм для майнінгу криптовалют, тому що ці дані можуть бути корисні організаціям, які займаються, наприклад, дослідженнями ринку.

Таблиця 1

Порівняння алгоритмів консенсусу для інтернет речей

	IOTW	IOTA
Спеціальне обладнання / CPU необхідний	Не потрібно	Повинні працювати на власних CPU / платах
Mining	+	–
Миттєві транзакція	+	–
Гнучкість системи винагороди	+	–
Витрати на будівництво системи	Низькі	Високі
Безпека	Висока	Низька
Масове партнерство по розгортання в напівпровідникові, IoT апаратній індустрії	+	–
Застосування	Децентралізована платформа електронної комерції, платіжна система, збір великихданих	Мікро-транзакції
Token Utility	Оплата, мікро-транзакція, купівля великих даних	Мікро-транзакції

IOTA не схожа на біткоіни або ефір, так як вона фактично не використовує блокчейн. Ця платформа використовує спеціальний журнал Tangle, що працює на основі DAG – спрямованого ациклічного графа. У блокчейн Bitcoin або Ethereum все тримається на блоках, куди і записується інформацію про транзакції. У Tangle IOTA блоків немає, а транзакції пов'язані за своєю особливою схемою: кожна нова транзакція (назвемо її A) підтверджує дві попередні (B і C). Верифікація також може відбуватися побічно - виникла транзакція D, яка підтвердила A і умовну Z.

Висновок

В роботі проведено аналіз та порівняння алгоритмів консенсусу в мережах Інтернет речей. ПлатформаIOTA здатна зв'язувати практично всі процеси в екосистемі IoT за рахунок налаштування мереж транзакцій та здатності проводити мікро транзакції у величезних кількостях. При цьому платформа реалізована так, що пристрій для взаємодії з іншими вузлами не повинні мати постійного доступу до Інтернету, що дозволить заощадити заряд батареї.

Список використаних джерел

1. Яцків Н.Г., Яцків С.В.Перспективи використання технології блокчейн в мережі Інтернет. речей. Науковий вісник НЛТУ України. - 2016. - Вип. 26.8. – С. 381-387.
2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
3. Andreas M. Antonopoulos. Mastering Bitcoin: unlocking digital cryptocurrencies. "O'Reilly Media, Inc.", 2014, 298 p.
4. Iota: a cryptocurrency for Internet-of-Things. See http://www.iotatoken.com/