УДК 004.056

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

ДЕЦЕНТРАЛІЗОВАНІ ПРОТОКОЛИ КОНСЕНСУСУ: МОЖЛИВОСТІ ТА РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ

Вступ

Побудова систем для надійного надання користувачам послуг, пов’язаних із використанням інформаційних технологій, стає все більш актуальною задачею. Виникає необхідність побудови систем керування, в тому числі критичними інфраструктурами. Такі задачі традиційно вирішувалися за допомогою побудови централізованих систем з центральним "керуючим" або "хабом", на який покладалися обов’язки керування та контролю за системою. Проте, із різким збільшенням спектру електронних систем та кількості користувачів побудова централізованих систем стає менш ефективним рішенням. Будь-яка централізована система має своє максимально допустиме навантаження при перевищенні якого її функціонування стає неефективним. Більше того, необхідно брати до уваги зростаючі ризики з боку кібернетичних атак, які змушують шукати нові стратегії забезпечення безпеки систем. Особливо це стосується систем, які обробляють критичну інформацію. Традиційно "слабким місцем" будь-якої централізованої структури є її вершина (тобто центральний орган управління), вихід із ладу його внаслідок спрямованої атаки фактично означає зупинку функціонування всієї системи. Виходом вбачається перехід на децентралізовані системи. В яких кожен із учасників виконує частину обов’язків керуючого.

На сьогодні найпоширенішим прикладом успішного впровадження децентралізованих систем безумовно слугують криптовалюти. Необхідно зазначити, що такий принцип побудови може бути успішно впроваджений також в інших сферах, в тому числі у сфері електронних довірчих послуг [3].

Особливо важливим питанням при цьому є формулювання політик та вимог, за якими функціонує децентралізована система. Необхідно забезпечити всім користувачам єдине бачення стану системи в кожен конкретний момент часу. Це можливо із використанням технології blockchain. По суті, blockchain – це журнал з фактами (реєстр фактів), який реплікується на кілька комп'ютерів, об'єднаних в мережу рівноправних вузлів (P2P). Фактами може бути що завгодно, від фінансових операцій та до підписання контенту. Члени мережі – анонімні особи, звані вузлами. Всі комунікації всередині мережі використовують криптографію, щоб надійно ідентифікувати відправника і одержувача. Коли вузол хоче додати факт в журнал, в мережі формується консенсус, щоб визначити, де цей факт повинен з'явитися в журналі; цей консенсус називається блоком.

Надійне забезпечення доступності інформації щодо стану системи досягається за допомогою децентралізованих протоколів консенсусу.

Децентралізовані протоколи консенсусу можуть мати досить широкий спектр застосування:

- формування журналу транзакцій цифрових валют;
- кластери;
- контролери баз даних;
- високонадійні обчислювальні системи;
- критичні технічні системи;
- авіоніка (система управління авіаційним обладнанням);
- космічні системи;
- управління ядерними реакторами, тощо.

Мета статті – формулювання вимог до децентралізованих протоколів консенсусу, проведення порівняльного аналізу існуючих за обраними критеріями, а також надання рекомендацій щодо можливості застосування в залежності від вхідних параметрів.

Призначення протоколів консенсусу

Блоки в децентралізованій мережі одночасно формуються безліччю «учасників». Такі блоки, що задовольняють критеріям, відправляються в мережу та включаються в розподілену базу блоків. Виникають ситуації, коли кілька нових блоків в різних частинах розподіленої мережі посилаються на один і той же блок, тобто ланцюжок блоків може ділитися. Спеціально чи випадково можна обмежити ретрансляцію інформації про нові блоки (наприклад, один із ланцюжків може розвиватися в рамках локальної мережі). У цьому випадку можливо паралельне нарощування різних ланцюжків. У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, що увійшли тільки в один ланцюжок. Коли ретрансляція блоків відновлюється, учасники мають дійти згоди (консенсусу) щодо того, який ланцюжок вважати вірним. Це можливо з використанням децентралізованих протоколів консенсусу.

Консенсус – це спосіб, завдяки якому різні вузли мережі досягають згоди про набір даних, який представляє з себе стан цієї мережі. Наприклад, транзакції, баланси на різних рахунках, результати виконання смарт-контрактів. Система на базі технології blockchain може бути представлена у вигляді машини станів. Протокол консенсусу має забезпечувати послідовність дій, які забезпечують кожному вузлу доступ до актуального поточного стану мережі.

Основними вимогами до таких протоколів є [1, 2]:

– Відсутність центральної довіреної сторони (функціонування в середовищі взаємної недовіри: жоден з учасників не довіряє іншому).

– Рівноправність вузлів (мережа складається з рівноправних вузлів. Якщо зовнішня сторона або зловмисник намагається вивести з дії певну кількість вузлів, мережа продовжує нормально функціонувати до тих пір, поки чесні учасники складають необхідну більшість серед працюючих).

– Більшість вузлів є «чесними».

– «Чесні» учасники не знають, які вузли контролюються зловмисниками (список збійних («атакованих») вузлів невідомий чесним учасникам та може динамічно оновлюватися).

– у кожного вузла або їх деякої множини можливі збої, повне відключення, довільна поведінка (в тому числі і скоординована зловмисником для проведення атаки мережі)

– Мережа не є надійною (можливі довільні затримки і втрати (пропуски) повідомлень)

Перші дві вимоги формулюються виходячи із принципу децентралізації системи. Необхідна кількість чесних вузлів залежить від типу протоколу консенсусу (можливі варіанти: >1/2 чесних учасників, >2/3 чесних учасників). При цьому кожний чесний вузол приходить в один і той же стан в умовах збоїв частини вузлів (або скоординованої роботи злочинних вузлів) та працює за наперед відомим формалізованим протоколом (без участі людини або будь-якої додаткової інформації)

Виділяються такі припущення, за яких протоколи мають продовжувати функціонувати [12]:

– чесні функціонуючі вузли складають більшість (понад 1/2 або більше 1/3 учасників);

– час прийняття рішення не є фіксованим;

– використовується значна надмірність (можна виконувати ідентичні завдання).

Порівняльний аналіз протоколів консенсусу

В залежності від того, які правила використовуються для досягнення згоди між учасниками, можна виділити такі групи протоколів консенсусу.

Proof of Work протоколи [4, 5]

Основні характеристики:

– кількість вузлів-учасників є необмеженою;

– вузли анонімними;

– репутація вузлів невідома;

– необхідна кількість «чесних вузлів» 51 % для надійного функціонування протоколу;

– існує можливість централізації;

– вразливість до атаки 51 %;

– простота масштабування. Додавання нового вузла проходить без змін правил функціонування системи;

– низька пропускна здатність (швидкість формування блоку досягає в деяких випадках 10 хвилин);

– високі енергетичні витрати.

Учасники починають вважати головним ланцюжок з урахуванням рівня складності геш-значення і довжини ланцюжка (правило найдовшого ланцюжка). У разі рівного розподілу складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше. Найяскравішим прикладом є протокол консенсусу Bitcoin.

Існують також інші правила вибору головного ланцюжку, наприклад кількість блоків у дереві, що утворює певний ланцюжок (як у алгоритмі GHOST) [4] (рис.1).

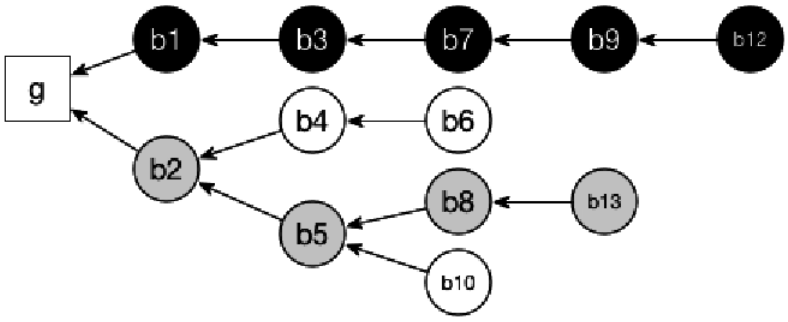

Рис. 1. Протокол консенсусу GHOST [4]

Транзакції, що увійшли тільки в відхилений ланцюжок, втрачають статус підтверджених. У 2017 – 2018 рр. були запропоновані нові алгоритми PoW консенсусу SPECTRE та PHANTOM [5], в яких використовується структура циклічного направленого графу (рис. 2) завдяки чому відсутня втрата блоків. Недоліком протоколів SPECTRE та PHANTOM слід зазначити необхідність зберігання великої кількості інформації.

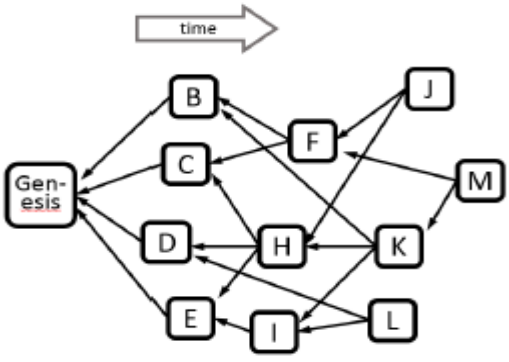

Рис. 2. Протокол консенсусу PHANTOM [5]

Proof of Stake протоколи [6, 7].

Основні характеристики:

– вузли-учасники не анонімні;

– вузли-учасники мають репутацію;

– монетарна мотивація учасників чесно слідувати протоколу. При спробі атаки "ставка" учасника-порушника згорає.

По суті відбувається голосування (рис. 3). Новий блок формує учасник, який зробив найбільшу «ставку». Логіка протоколів такого типу полягає в тому, що учасникам із великою кількістю монет, невигідно робити спроби атак, оскільки успішна атака призведе до знецінення криптовалюти. Таким чином, для учасника немає більш вигідної стратегії, ніж чесно слідувати протоколу.

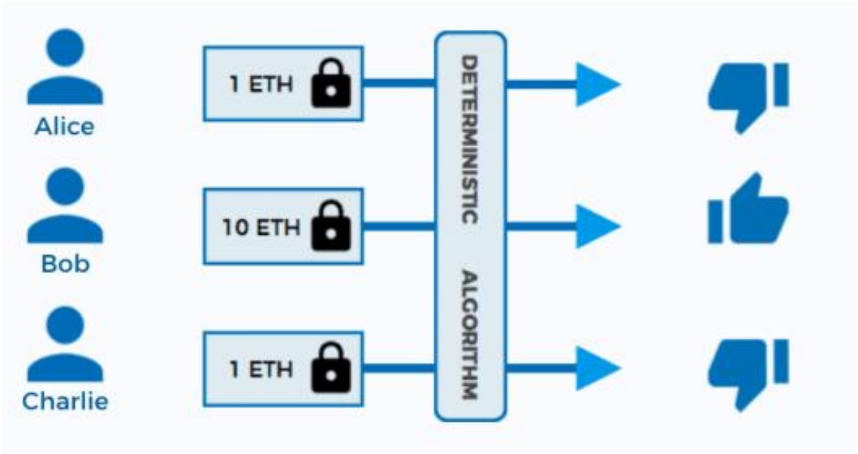

Рис. 3. PoS протокол консенсусу

При цьому вузли можуть передавати свої голоси іншим, які будуть голосувати від їх імені, таким чином утворюючи колегію виборців (Delegated PoS) [7].

BFT протоколи.

Основні характеристики:

– базуються на задачі Візантійських генералів;

– вузли-учасники не є анонімними;

– для надійного функціонування чесних учасників має бути >2/3;

– ймовірність відміни рішення є експоненційно спадною;

– для прийняття рішення необхідна кінцева кількість кроків;

– висока пропускна здатність;

– можливі елементи централізації.

Протоколи BFT історично з'явилися першими. Practical BFT [8, 9] протокол являв собою по суті варіант клієнт-серверної архітектури, коли тільки після звернення клієнта до серверу, транзакція могла бути передана іншим учасникам для підтвердження. Нові протоколи Algorand [10] та Hashgraph [11], наприклад позбавлені цього недоліку. Згідно з протоколом Algorand серед учасників випадковим чином обирається деякий підкомітет, який приймає рішення про підтвердження транзакції. Підтвердження відбувається у декілька етапів, на кожному з яких обирається окремий підкомітет. Протокол має високу пропускну здатність, добре масштабується. Проте, недоліком є погане функціонування у нестабільних мережах з великими затримками.

Табл. 1 містить зведені дані порівняння основних груп протоколів консенсусу.

Таблиця 1

Зведена таблиця порівняння протоколів консенсусу

Протоколи		Анонімність/ відкритість вузлів-учасників	Наявність репутації вузлів-учасників	Мотивація вузлів-учасників	Математична задача	Кількість «чесних вузлів»	Простота масштабування
PoW	GHOST	Вузли є анонімні	Репутація вузлів невідома	Винагородження за вирішення блоку	Пошук прообразу геш-функції	>1/2	Легко масштабувати
	SPECTRE						
	PHANTOM						
PoS	DelPoS DPoS	Вузли не анонімні	Вузли мають репутацію	Мотивація учасників чесно слідувати протоколу полягає в тому, що немає більш вигідної стратегії	Система "голосування"	>1/2	Труднощі у масштабуванні
BFT	Practical BFT	Вузли не анонімні	Вузли мають репутацію	Мотивація учасників чесно слідувати протоколу лежить за межами протоколу	«Проблема Візантійських генералів»	>2/3	Важко масштабувати
	Honey Badger BFT						
	ALGORAND						Легко масштабувати
	HSHGRAPH						

Таким чином, можна зробити висновки, що кожна з груп має свої переваги та недоліки. Табл. 2 наводить їх у зведеній формі.

Таблиця 2

Переваги та недоліки основних груп протоколів консенсусу

Протоколи	Переваги	Недоліки
PoW	Доказова стійкість Легка масштабованість	Високі енергетичні затрати Втрата частини інформації Необхідність зберігати великий об'єм інформації Низька пропускна спроможність
PoS	Відсутність математичного доведення стійкості	Висока пропускна спроможність Мотивація учасників чесно слідувати протоколу
BFT	Висока пропускна здатність Рішення, яке отримане не може бути відмінено з часом Для отримання рішення необхідна кінцева кількість кроків	Необхідність 2/3 чесних вузлів Відсутність мотивації учасників чесно слідувати протоколу

Можливо виділити наступні рекомендації:

1. Вибір протоколу консенсусу має базуватися насамперед на умовах, в яких передбачається функціонування системи.

2. Можливе поєднання декількох протоколів в один (так звані гібридні протоколи).

3. Якщо система має функціонувати в умовах взаємної недовіри без додаткових інструментів контролю за користувачами, доцільне використання PoW протоколів, не дивлячись на низьку пропускну здатність таких протоколів.

4. Для систем закритого типу із наперед прогнозованою кількістю вузлів і без перспектив швидкого розширення використання BFT протоколів є вигідним. При цьому необхідно

додатково забезпечувати мотивацію вузлів-учасників чесно слідувати протоколу. Необхідною є первинна ідентифікація учасників.

5. Для не анонімних систем відкритого типу доцільним є використання PoS протоколів.

6. Якщо система має специфічну архітектуру та особливі умови функціонування, можливе використання гібридних багатошарових протоколів консенсусу, розроблених відповідно до особливостей даної системи. Одним із прикладів може бути поєднання PoW та PoS протоколу, в якому нові користувачі, які ще не мають попередньої історії транзакцій та, відповідно, особистої репутації, користуються PoW протоколом, який в даному випадку забезпечуватиме їх накопиченням репутації. Після проходження "порогу довіри" користувач переходить на використання PoS протоколу.

Висновки

1. Децентралізовані системи здатні краще забезпечити функціонування електронних систем в умовах збільшення спектру електронних послуг та зростання кількості користувачів.

2. Для надійного функціонування децентралізованих систем (в тому числі у критичних інфраструктурах) можливе використання технології blockchain із децентралізованими протоколами консенсусу.

3. Вибір протоколу консенсусу має базуватися за умов, в яких передбачається функціонування системи. Для систем закритого типу із заздалегідь прогнозованою кількістю учасників доцільним вбачається використання BFT протоколу із додатковим забезпеченням контролю за чесністю учасників. Для анонімних систем із відсутністю можливості контролю передбачається використання доопрацьованих PoW протоколів PoS.

Список літератури:

1. L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone. A prototype eval-uation of a tamper-resistant high performance blockchain-based transaction log for a distributed database // EDCC. IEEE, 2017.

2. C. Cachin, R. Guerraoui, and L. Rodrigues. Introduction to reliable and secure distributed programming // Springer, 2011.

3. K. Isirova and O. Potii. Decentralized public key infrastructure development principles // IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – Kiev, 2018. – P. 305-310.

4. J. A. Garay, A. Kiayias, and N. Leonardos. The Bitcoin Backbone Protocol // Analysis and Applications, volume 9057 of LNCS, pages 281{310. Springer, 2015.

5. Aggelos Kiayias1 and Giorgos Panagiotakos. On Trees, Chains and Fast Transactions in the Blockchain Yonatan Sompolinsky and Aviv Zohar. PHANTOM: A Scalable BlockDAG protocol

6. Bernardo Machado David, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. IACR Cryptology ePrint Archive, 2017:573, 2017.

7. George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies // 23nd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016. The Internet Society, 2016.

8. Stefano De Angelis; Leonardo Aniello1; Roberto Baldoni1,Federico Lombardi;Andrea Margheri and Vladimiro Sassone. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain

9. M. Castro and B. Liskov. Practical byzantine fault tolerance and proactive recovery // ACM Trans. Comput. Syst., 20(4):398{461, 2002.

10. Algorand Whitepaper: https://www.algorand.com/docs/whitepapers/

11. LEEMON BAIRD. THE SWIRLDS HASHGRAPH CONSENSUS ALGORITHM: FAIR, FAST, BYZANTINE FAULT TOLERANCE

12. D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun. A review on consensus algorithm of blockchain.

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

Надійшла до редколегії 29.10.2018