DOI: https://doi.org/10.26642/ten-2023-1(91)-156-160
УДК 004.02

О.В. Корнійчук, аспірант
М.С. Граф, PhD
Державний університет «Житомирська політехніка»

Аналіз існуючих механізмів прийняття рішень у децентралізованих системах для застосування в державних закупівлях

У роботі детально досліджуються існуючі механізми для системи прийняття рішень Proof-of-Stake і Proof-of-Work у блокчейнах та проводиться їх порівняння. Розглянуто методи знаходження консенсусу як процесу погодження нового блоку, що згодом додається до блокчейну всіма учасниками. В досліджених механізмах виявлено схожість: передбачені правила, що стосуються всіх учасників – майнерів або валідаторів. У разі порушення цих правил на учасників накладаються штрафи. Після успішно доданого блоку учаснику, що розв'язав математичну задачу, передбачається отримання нагороди за активну участь. Суттєвою різницею між механізмами є формування нових блоків, вимоги до обладнання учасників та механізми нагород і штрафів. Розглядаються тенденції держав у впровадженні блокчейнів у державні реєстри та майданчики для державних закупівель. Було виявлено, що блокчейни можуть зменшити рівень корупції та змов лише за правильного їх впровадження та подальшого використання. У результаті дослідження припускається можливість використання саме Proof-of-Stake механізму для інтеграції в майданчики, що проводять державні закупівлі.

Ключові слова: *блокчейн; державні закупівлі; електронні майданчики; Proof-of-Stake; Proof-of-Work; консенсус.*

Актуальність теми. Публічні закупівлі – це процес закриття потреб держави шляхом знаходження найкращого варіантf на ринку. Державні установи та підприємства мають проводити закупки різноманітних товарів, послуг та робіт для повноцінного функціонування та виконання своїх обов'язків. У різних країнах постійно працюють над розробкою нових методів визначення найкращого варіанта, але завжди варто орієнтуватися на кращі умови і баланс ціни та якості. За аналізом організації економічного співробітництва та розвитку бюджети державних закупівель становлять близько 12 % від ВВП та 29 % від загальних витрат країни і склали разом для країн, що входять в організацію, приблизно 4,2 трильйони EUR на 2013 рік, що робить їх потужним інструментом впливу на ринок як з боку виробництва, так і з боку споживання [1].

За даними Організації економічного співробітництва та розвитку за 2016 рік було встановлено, що як мінімум 20–25 % від бюджету державних закупівель було виведено шляхом корупційним схемам [2]. Це означає, що, незважаючи на всі спроби держав максимально спростити та зробити прозорими цей процеси, є частка тендерів, що витрачаються нераціонально та піддаються впливу корупційними схемами. Одним із важливих завдань будь-якої держави та її свідомих громадян є постійний контроль над витратами. Саме тому розвиток систем, що допомагають реалізовувати державні закупівлі та надають інструменти для моніторингу процесів закупівель, має високий пріоритет. Важливо зазначити, що державні закупівлі можуть містити абсолютно різні поняття, такі як закупівлі канцелярії та дозабезпечення військового потенціалу країни.

Аналіз останніх досліджень та публікацій, на які спираються автори. Багато вчених та програмістів працюють над створенням різних нових механізмів знаходження консенсусу чи доопрацюванням вже існуючих. Деякі з цих ідей є революційними та створюють нові блокчейни, але велика кількість з них не здатні набрати необхідної кількості користувачів чи ліквідності для повноцінного функціонування в майбутньому. На 2021 рік 100 найкращих проєктів з платформи CoinMarketCap володіють приблизно 96 % криптовалютної ринкової капіталізації [3]. Найбільші проєкти використовують дві головні технології – Proof-of-Stake та Proof-of-Work, що приблизно становить 21 та 58 % відповідно, що показано на рисунку 1 [4]. Аналітика зроблена в 2020 році та не враховує перехід одного з найбільших проєктів Ethereum на PoS механізм. Крім цього, існують деякі системи, що базуються або використовують модифіковані алгоритми Proof-of-Stake та закриті блокчейни, такі як Hyper Ledger з Byzantine Fault Tolerance механізмом.

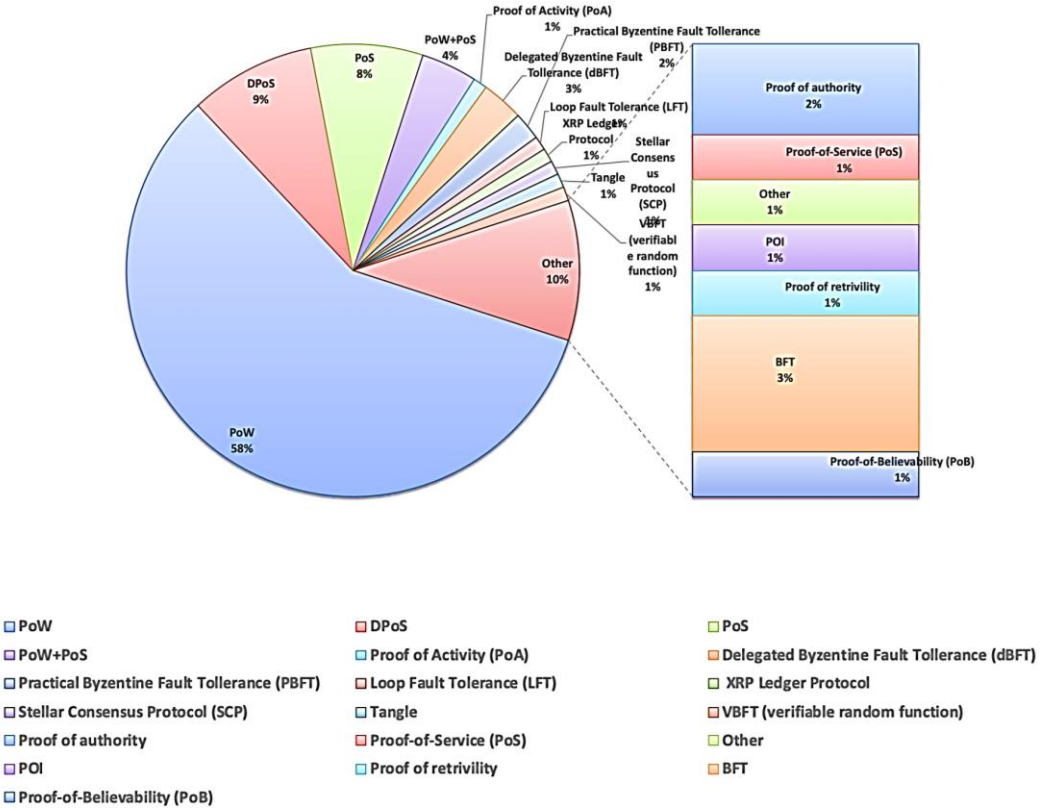

Рис. 1. Алгоритми консенсусу в 100 найкращих криптовалютах [4]

Проаналізувавши переваги закритих блокчейнів зі схеми на рисунку 2, можна зробити висновок, що вони є найбільш придатні до використання в державних системах, оскільки це дозволить швидше приймати рішення та надасть державі можливість контролювати всю мережу. Для подібних закритих систем є ризик корупції всередині та вірогідність можливих змов. Якщо більшість нод будуть у змові між собою, це може призвести до незворотних наслідків, таких як зміна правил знаходження консенсусу чи перезапис важливої інформації. На сьогодні прийняття рішення використання блокчейну, що поєднує всі бажані функції, неможливе без істотних компромісів. Саме тому варто зосередити увагу на більш відкритих блокчейнах, де кожен учасник має виконувати певні правила задля того, щоб надалі мати можливість брати участь у процесі формування блоку.

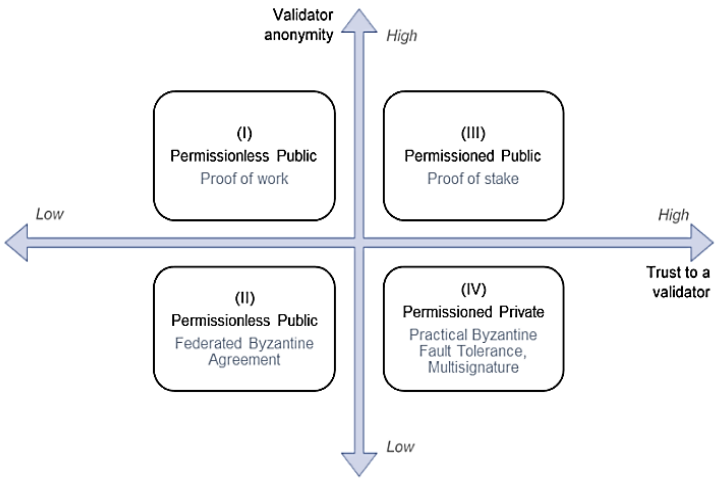

Рис. 2. Топологія блокчейнів [5]

Метою статті є проведення аналізу найбільш вживаних систем прийняття рішень, що використовують у блокчейнах.

Викладення основного матеріалу. Система прийняття рішення або знаходження консенсусу – це процес домовленості всіх учасників системи для того, щоб досягти загальної згоди [6]. Саме при консенсусі блокчейн може функціонувати як система та додавати нові блоки. Для того щоб це зробити, існують різні механізми у системах прийняття рішень. Термін «механізм знаходження консенсусу» означає весь набір протоколів, стимулів та ідей, які дозволяють мережі вузлів погоджувати стан блокчейну. Перелік подібних ідей та правил буде відрізняти механізм від механізму, але в більшості з них мають бути наявні правила для учасників, що передбачатимуть винагороди за правильно обраховані блоки та систему штрафних санкцій за спроби маніпулювання даними.

Одними із перших і найбільш популярних на цей момент є блокчейни Bitcoin та Ethereum. Підтримка та розробка нових ідей проводиться і на теперішній час, але обидва з них починали роботу на Proof-of-Work механізмі.

Proof-of-Work. Proof-of-work механізм використовується в Bitcoin та раніше використовувався в Ethereum. З початку 2022 року Ethereum почали перехід на Proof-of-Stake механізм і вже до кінця року успішно закінчили його. Як відомо, цей механізм має на меті створити певний відкритий «ринок» трансакцій, в якому учасники, надалі в контексті майнери, мають розв'язати математичну задачу певної складності. Рішення цієї задачі буде мати певний хеш, що криптографічно пов'язує поточний і минулий блок. Перемагає той майнери, який швидше вирішить завдання та надішле іншим учасникам відповідь. У Bitcoin наявний певний алгоритм, який задає правила обрахування, одне з яких – обчислення блоку – має займати приблизно 10 хвилин, через це наявний такий параметр – mining difficulty, – який змінюється кожних 2016 блоків. Він автоматично буде підлаштовуватися і збільшувати чи зменшувати час, що потрібен на обчислення, задля того щоб це займало до 10 хвилин.

Варто зазначити, що заробіток майнерів у Bitcoin на даний час формується в формі емітованих біткоїнів і комісійних зборів. Емісія біткоїнів обмежена в 21 мільйон та кожних 210 000 блоків зменшується вдвічі. 2033 року емісія буде зупинена зовсім, а основним джерелом прибутку стануть комісійні збори.

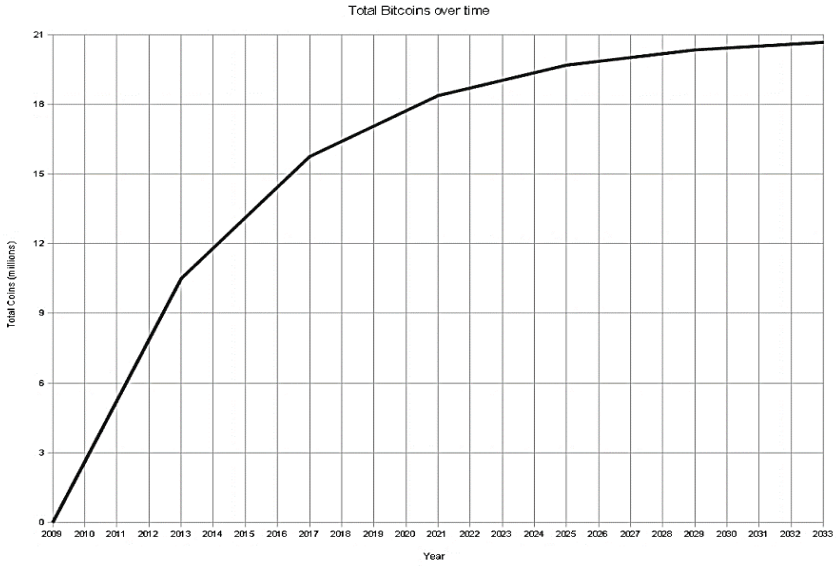

Рис. 3. Кількість біткоїнів за 2009–2033 роки [7]

Proof-of-Stake. У цьому варіанті реалізації механізму блок створює валідатор. Порівняно з Proof-of-Work, де час створення блоку залежить від mining difficulty, час створення нового блоку фіксований. Час розділений на слоти, що складають 12 секунд, та епохи – 32 слоти. Кожному блоку буде випадковим чином обраний валідатор, що пропонуватиме блок для додавання. Цей валідатор відповідає за те, щоб його створити та відправити всім іншим у межах мережі. В кожному слоті буде обрано певну кількість валідаторів, яких називають committee of validators. Вони відповідальні за те, щоб прийняти рішення щодо блоку, та також вибираються випадковим чином.

Стати валідатором в Ethereum мережі після переходу на Proof-of-Stake набагато простіше. В поточній імплементації необхідно менше обчислювальних потужностей, але варто додати суму в 32 ETH, що становить приблизно $50 000. Цю суму називають stake і валідатор може її втратити, якщо намагатиметься атакувати блокчейн шляхом створення неправильного блоку. Такий механізм штрафних санкцій одразу відсікає певну кількість атак, що вартують менше ніж сума стейку.

Безпека. Використання блокчейну в процесі державних закупівель може бути дуже різноманітним, починаючи від побудови повністю нової системи з імплементацією власного Proof-of-Stake чи Proof-of-Work алгоритму до створення простого смартконтракту в уже існуючій мережі. Якщо розглядати питання впровадження блокчейну в державні системи, то на перше місце виходить саме безпека механізму в системі прийняття рішень.

Для Proof-of-Work існує вірогідність атаки під назвою «51 %». Суть цих дій в тому, щоб заволодіти більше ніж 50 % потужностей майнерів та почати створювати власні блоки. Ці атаки можуть призвести до відхилення деяких транзакцій чи подвійного використання коштів користувачів. Подібний тип атак у великих блокчейнах як Bitcoin буде коштувати в рази більше, ніж потенційні можливі нагороди. Для того щоб заволодіти 51 %, необхідно витратити приблизно 10 більйонів доларів [6].

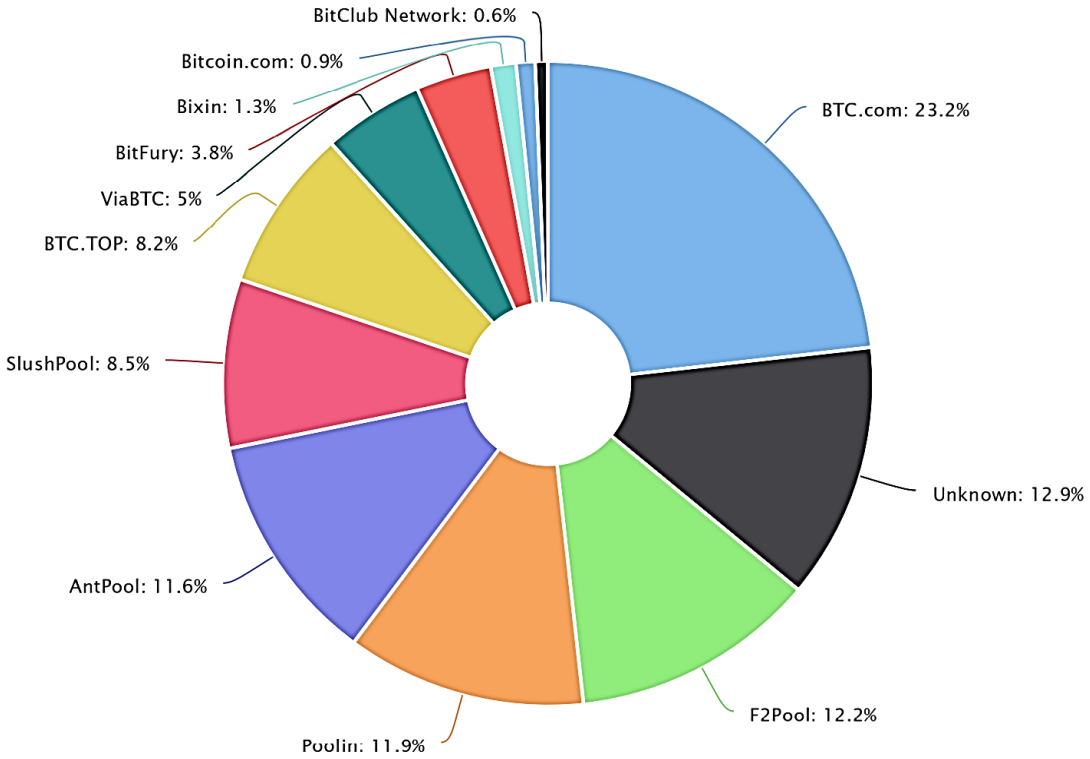

Рис. 4. Розподіл потужностей майнерів у Bitcoin [8]

Але варто також зауважити, що станом на 2022 рік приблизно 75 % потужностей майнерів розподілено між 4 учасниками, тобто в разі змови більшості з них ймовірність подібної атаки все ж зберігається.

Після переходу Ethereum на Proof-of-Stake вартість подібної атаки збільшилась, оскільки в цьому алгоритмі кожен з валідаторів має свій певний стейк, який може втратити у разі спроби підміни інформації в блоці. Додатковим механізмом захисту є також випадковий вибір валідатора та комітету валідаторів, що приймають рішення з приводу нового блоку. Кількість валідаторів у мережі Ethereum на момент 12 січня 2023 року становить більше ніж 500 000, що набагато зменшує вірогідність змови [9].

Висновки та перспективи подальших досліджень. У результаті дослідження було проведено аналіз публікацій існуючих механізмів прийняття рішень у децентралізованих системах, було описано базові алгоритми та принципи роботи Proof-of-Work та Proof-of-Stake, що дало змогу детальніше проаналізувати та зрозуміти майбутні вектори атак на подібні системи. Було розглянуто декілька теоретичних атак та можливий вплив на стан блокчейну.

Проміжний підсумок потенційних атак показав, що Proof-of-Stake збільшив вартість високо ймовірних атак порівняно з Proof-of-Work. Незважаючи на те, що в першому алгоритмі все одно наявні деякі малоймовірні атаки, Ethereum має певні оборонні стратегії, що покликані продовжувати стабільну роботу блокчейну. Саме тому вибір Proof-of-Stake є більш раціональним, але впровадження такої технології в системи державних закупівель має потенційні труднощі, що залежать від конкретного вибраного підходу до інтеграції.

Через різноманітність варіантів реалізації на цьому етапі неможливо однозначно оцінити та зробити висновки щодо вибору найкращого механізму консенсусу для використання в майданчиках для державних закупівель.

References:

1. OECD (2016), *Preventing corruption in public procurement*, [Online], available at: https://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf
2. Chan Yang (2019), *Is there a role for blockchain for enhancing public procurement integrity?*, 20-21 March, [Online], available at: https://www.oecd.org/corruption/integrity-forum/academic-papers/Chan-Yang-blockchain-public-procurement-integrity.pdf
3. Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A. Hoque and Colman, Alan (2020), *Blockchain Consensus Algorithms: A Survey*, 7 Feb., [Online], available at: https://arxiv.org/pdf/2001.07091.pdf
4. *CoinMarketCap*, [Online], available at: https://coinmarketcap.com
5. Chan Yang (2019), *Is there a role for blockchain for enhancing public procurement integrity?*, 20-21 March, [Online], available at: https://www.oecd.org/corruption/integrity-forum/academic-papers/Chan-Yang-blockchain-public-procurement-integrity.pdf
6. *Ethereum Foundation*, [Online], available at: https://ethereum.org/en/developers/docs/consensus-mechanisms/#what-is-consensus
7. Jake Frankenfieldm (2022), *51 % Attack: Definition, Who Is At Risk, Example, and Cost*, 28 September, [Online], available at: https://www.investopedia.com/terms/1/51-attack.asp
8. Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad Hoque, A. and Colman, Alan (2020), *Blockchain Consensus Algorithms: A Survey*, 7 Feb., [Online], available at: https://arxiv.org/pdf/2001.07091.pdf
9. *Beaconscan*, [Online], available at: https://beaconscan.com/statistics

Корнійчук Олександр Валерійович – аспірант факультету інформаційно-комп'ютерних технологій Державного університету «Житомирська політехніка».

https://orcid.org/0000-0001-8075-2146.

Наукові інтереси:

– блокчейн;
– децентралізовані системи.

Граф Марина Сергіївна – PhD, завідувач кафедри комп'ютерних наук Державного університету «Житомирська політехніка».

https://orcid.org/0000-0003-4873-548X.

Наукові інтереси:

– інтелектуальні системи;
– веборієнтовані технології та аналіз даних.

Korniichuk O.V., Graf M.S.

Analysis of existing decision-making mechanisms in decentralized systems for government procurement use

Existing mechanisms for the Proof-of-Stake and Proof-of-Work decision-making systems in blockchains are thoroughly studied and compared at work. Consensus methods are considered a process of agreeing on a new block that is subsequently added to the blockchain by all participants. Similarities are found in the studied mechanisms: rules are provided that apply to all participants – miners or validators. Penalties are imposed on participants who violate these rules. After successfully adding a block, the participant who solved the mathematical problem is expected to receive a reward for active participation. Significant differences between the mechanisms are the formation of new blocks, the requirements for participant equipment, and mechanisms for rewards and penalties. Trends in the implementation of blockchains in state registers and procurement platforms are considered. It has been found that blockchains can reduce the level of corruption and conspiracy only through proper implementation and further use. As a result of the research, it is assumed that the Proof-of-Stake mechanism can be used for integration into procurement platforms that conduct government procurement.

Keywords: blockchain; government procurement; electronic platforms; Proof-of-Stake; Proof-of-Work; consensus.

Стаття надійшла до редакції 03.05.2023.