КІЛЬКІСНЕ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ПРОТОКОЛУ DOUBLY-PIPELINED PALA З УРАХУВАННЯМ РЕКОНФІГУРАЦІЇ КОМІТЕТІВ

Дубініна О. М., Риндіна М. С.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

За останнє десятиліття стало очевидним, що технологія блокчейн впевнено займає лідируючі позиції при прийнятті децентралізованих рішень у багатьох виробництвах і галузях. Фундуючим принципом означеної технології є принципова гарантованість того факту, що після включення транзакції до блокчейну, її неможливо ані модифікувати ані відмінити. Саме така концепція має генеральну вагу для будь-якої системи побудованої на блокчейні, оскільки забезпечує незмінність та довіру всередині мережі [1]. Через високу затребуваність і конкуренцію в означеній царині блокчейн-протоколи безперервно удосконалюються і оновлюються, що вимає постійно вирішувати проблеми забезпечення safety, liveness і fault tolerance [2].

Розглянуто сценарій застосування реконфігурації комітету для Doubly-pipelined PaLa, запропонований у [3], який формується виокремленням вузлів інфраструктури як «акселераторів», тобто розробників пропозицій, при цьому учасники комітету, відповідальні за голосування, обираються з вузлів, які підтримують систему. Наприклад, спирається на сукупність повідомлень про обсяг даних, що вони зберігають. Мета дослідження полягає в аналітичному обґрунтуванні кількості вузлів-зловмисників, або таких, що відмовили в обслуговуванні з гарантією забезпечення safety, liveness та fault tolerance.

У кожному із підкомітетів візантійських вузлів менше $f/3$. Для того щоб блок був нотаріально завірений, має існувати принаймні $2f/3$ голосів від кожного з підкомітетів. Враховуючи, що 1) може змінитися лише один із двох підкомітетів, 2) два підкомітети у комітеті можуть бути однаковими, 3) вузли повинні мати нотаріальне завірення батьківським перед голосуванням за наступний блок і при цьому відрізається 1 нормальний блок для фіналізації, перехід від C_{old} до C_{new}, стає можливим через перехід від $(C_{old};C_{old})$ до $(C_{old};C_{new})$ до $(C_{new};C_{new})$ за два нормальні блоки.

У результаті дослідження доведено, що $(2f-1)/3$ – це максимально можлива кількість зловмисників у всьому комітеті, якщо він не підлягає діленню; а для комітета який має ділитися ця величина дорівнюватиме $2(2f-1)/3$.

Література:

1. Blockchain and decentralized systems: in three volumes. V. 3 / P. Kravchenko, B. Skriabin, O. Kurbatov, O. Dubinina, S. Kozlov. – Kharkiv: PROMART, 2023. – 344 p. ISBN 978-617-7634-27-9 / 978-617-7634-79-8

2. Lewis A. The basics of bitcoinsand blockchains: an introduction to cryptocurrencies and the technology that powers them / FL, USA: Mango Publishing Group. – 2018. – 408 p. ISBN 978-1-63353-800-9