**Гоша Д.О.**, студент 4 курсу

*кафедра Програмних систем і технологій*

*Факультет інформаційних технологій*

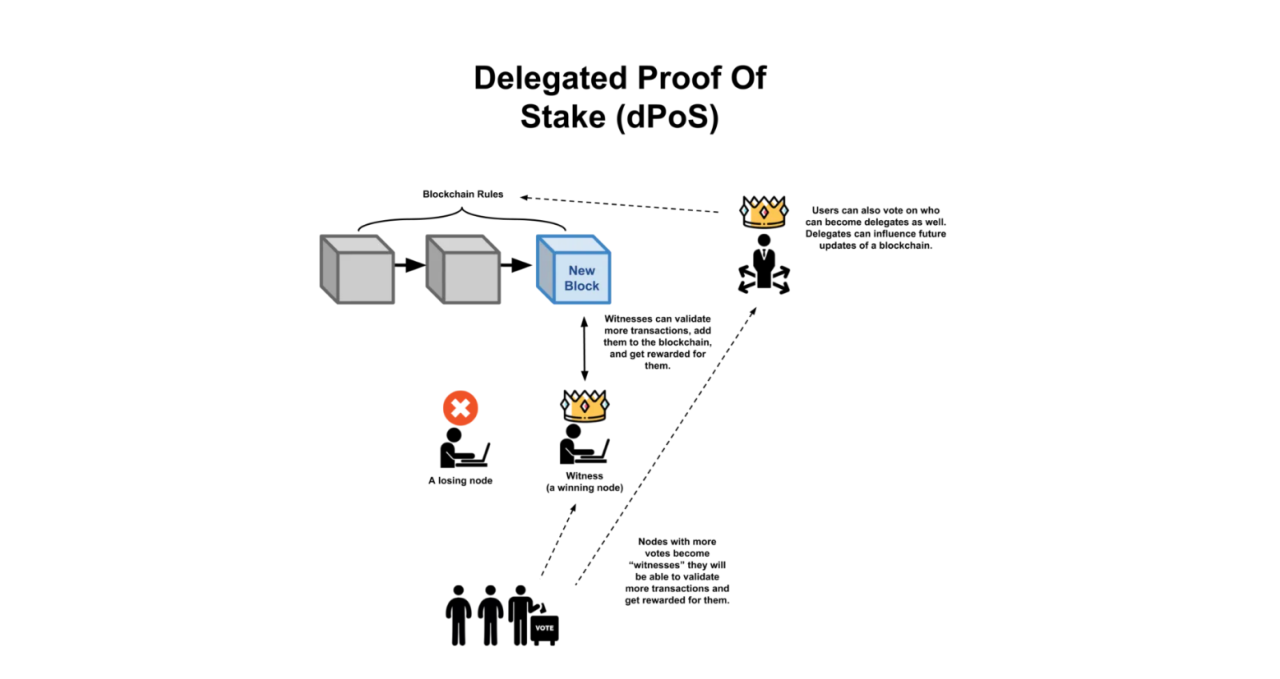
*Київський національний університет імені Тараса Шевченка, м. Київ, Україна*

**Розробка протоколу консенсусу для блокчейн-платформи на основі делегованого доказу частки володіння та багатопідписів**

В роботі пропонується новий протокол консенсусу для блокчейн-платформ, який поєднує переваги алгоритмів делегованого доказу частки володіння (DPoS) та криптографічних багатопідписів.

Однією з ключових проблем існуючих блокчейн-систем є забезпечення балансу між масштабованістю, безпекою та децентралізацією. Алгоритми сімейства Proof-of-Stake дозволяють досягти вищої пропускної здатності порівняно з Proof-of-Work за рахунок відбору валідаторів на основі їх частки токенів. Проте базові реалізації DPoS мають певні недоліки, зокрема ризик змови між делегатами.

Пропонований протокол на основі DPoS передбачає вибір фіксованого числа делегатів, які по черзі формують і підписують блоки. Для підвищення безпеки процесу додатково використовуються багатопідписи, коли для валідації блоку потрібна згода не менше 2/3 делегатів. Це виключає можливість одноосібного контролю над мережею.



*Алгоритм працює наступним чином:*

* Усі власники токенів голосують за делегатів пропорційно до своєї частки. Обирається K делегатів з найбільшою кількістю голосів.
* Делегати по черзі стають лідерами раунду і пропонують новий блок транзакцій.
* Блок розсилається іншим делегатам, які перевіряють його і підписують за допомогою криптографічної схеми багатопідпису, наприклад BLS.
* Якщо блок набирає підписи від 2/3+1 делегатів, він вважається підтвердженим і додається в ланцюжок.
* Процес повторюється з п.2 для наступного раунду.

У роботі проаналізовано стійкість протоколу до різних векторів атак, зокрема Selfish Mining, Nothing-at-Stake, Long Range. Показано, що завдяки багатопідписам зловмисники не зможуть провести розгалуження ланцюжка або повторно використати старі ключі для переписування історії.

Для оцінки продуктивності протоколу розроблено прототип блокчейн-платформи на базі фреймворку Cosmos SDK. Проведено тестування пропускної здатності і часу підтвердження транзакцій у мережі з різною кількістю вузлів. Результати показали, що протокол дозволяє досягти показників до 5000 TPS при середньому часу фіналізації блоків менше 5 с.

Підсумовуючи, запропонований протокол консенсусу на основі DPoS та багатопідписів забезпечує оптимальне поєднання високої продуктивності, безпеки та децентралізації блокчейн-платформи. Його можна застосовувати для побудови масштабованих рішень в галузях, де критичними є швидкість і надійність обробки транзакцій.

**Література:**

* *Larimer D. Delegated Proof-of-Stake (DPoS) Whitepaper. 2014. URL: https://bitshares.org/technology/delegated-proof-of-stake-consensus/*
* *Boneh D., Drijvers M., Neven G. BLS Multi-Signatures With Public-Key Aggregation. 2018. URL: https://crypto.stanford.edu/~dabo/pubs/papers/BLSmultisig.html*
* *Kwon J. Tendermint: Consensus Without Mining. 2014. URL: https://tendermint.com/static/docs/tendermint.pdf*
* *Baghdasaryan R. Consensus Algorithms: DPoS. 2019. URL: https://medium.com/coinmonks/consensus-algorithms-dpos-2b9c784f3b5e*