ISSN 2074-7888, Наукові праці Донецького національного технічного університету,
серія «Проблеми моделювання та автоматизації проектування» №2 (22), 2025

УДК 004.942:004.056.5:004.75:324.65 DOI: 10.31474/2074-7888-2025-2-22-5-15

МОДЕЛЮВАННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ МЕХАНІЗМІВ ГОЛОСУВАННЯ В БЛОКЧЕЙНІ

Маслова Н.О., Ковальчук Л.В.

У статті представлено математичне моделювання криптографічної стійкості механізмів голосування в блокчейн-середовищі з консенсусом Proof-of-Stake. Запропоновано імовірнісну модель, що формалізує процес колективного підписання та підрахунку голосів із урахуванням параметрів безпеки — частки атакувальників, порогу підписів і затримок синхронізації. На основі моделі побудовано аналітичні залежності для оцінювання ймовірності компрометації підписів Pforge та порушення цілісності голосування Pbreak. Проведено чисельні експерименти методом Монте-Карло для порівняння аналітичних і симуляційних результатів та визначення порогових значень параметрів безпеки. Результати дослідження демонструють вплив конфігурації комітету на стійкість голосування й можуть бути використані для оптимізації архітектури блокчейн-систем голосування.

Ключові слова: *моделювання, блокчейн, голосування, Proof-of-Stake, криптографічна стійкість, порогові підписи, імовірнісна модель, Monte-Carlo-Simulation.*

Вступ. З розвитком блокчейн-технологій з'явилися нові моделі децентралізованого управління (governance), у яких ключові рішення щодо функціонування мережі приймаються шляхом on-chain голосування. Такі системи використовуються у мережах Cardano, Tezos, Polkadot та низці DAO-проєктів для ухвалення технічних оновлень, зміни протоколів або розподілу ресурсів. Їхня перевага полягає у прозорості, відсутності централізованого контролю та можливості автоматичного виконання результатів голосування за допомогою смарт-контрактів. Проте саме цей рівень автоматизації та публічності створює нові виклики безпеки, які потребують глибокого криптографічного та математичного аналізу.

Ключовою проблемою є забезпечення достовірності та цілісності голосів у децентралізованому середовищі без довірених посередників. На відміну від традиційних електронних систем, on-chain голосування не може покладатися на централізовану перевірку виборців чи захист даних сервером. Безпека цілковито залежить від криптографічних механізмів (підписів, шифрування, доказів з нульовим розголошенням) і протоколів консенсусу (зокрема Proof-of-Stake), які гарантують узгодженість результатів між вузлами мережі.

Наразі більшість досліджень зосереджено на загальній безпеці консенсусу, тоді як моделі криптографічної стійкості саме голосувальних процедур залишаються недостатньо формалізованими. Реальні випадки маніпуляцій делегованими токенами, можливість змови валідаторів чи підробки підписів створюють ризик порушення чесності голосування навіть за відсутності атак на сам блокчейн. Додаткову складність становить асинхронність мережі, затримки передачі блоків і наявність анонімних учасників, що ускладнює виявлення підробок.

Висока актуальність проблеми зумовлена також тенденцією до масштабування децентралізованих автономних організацій (DAO), де голосування є базовим механізмом управління активами. У таких системах компрометація криптографічних ключів або підписів може призвести до фальсифікації рішень на рівні мільйонів доларів. Зважаючи на це, оцінка ймовірності компрометації або підробки голосу через математичне моделювання стає критично важливим етапом верифікації безпеки протоколів.

Таким чином, гарантування безпеки on-chain голосування є актуальним науковим і практичним завданням, оскільки поєднує проблеми криптографічної стійкості, теорії ймовірностей і децентралізованих обчислень. Розроблення математичних моделей, що дозволяють кількісно оцінювати рівень стійкості таких механізмів, є необхідною умовою для створення надійних систем блокчейн-управління нового покоління.

Аналіз останніх досліджень та публікацій. Сучасні дослідження у сфері

блокчейн-технологій дедалі більше спрямовані на підвищення рівня безпеки та стійкості систем консенсусу й управління. Особливу увагу наукової спільноти привертають математичні моделі, що дозволяють формально оцінювати ризики атак, компрометації ключів, а також надійність механізмів голосування у розподілених середовищах. У цьому контексті спостерігається розвиток двох взаємопов'язаних напрямів: (1) моделювання ймовірнісної безпеки алгоритмів консенсусу та (2) криптографічне забезпечення процедур on-chain голосування.

Розглянемо дослідження безпеки консенсус-механізмів.

Визначальну роль у цьому напрямі відіграють дослідження, у яких запропоновано низку стохастичних моделей для оцінювання вразливостей протоколів Proof-of-Stake (PoS). Так, у роботі [1] розроблено біноміальну модель, що описує ймовірність успіху атаки типу double spend залежно від частки атакувальника, кількості підтверджень та параметрів мережі. Подальший розвиток ця ідея отримала в [2], де проаналізовано процедуру вибору слот-лідера в Ouroboros Praos і показано, що незначні мережеві затримки здатні суттєво змінювати ризик атаки. Робота [3] розширює модель, вводячи часовий компонент для PoW- та PoS-мереж, що дозволяє враховувати реальні умови синхронізації між вузлами.

Вважаємо, що важливим етапом еволюції цих досліджень стала стаття [4], у якій запропоновано аналітичні вирази для визначення кількості підтверджень у двошарових блокчейн-системах. Таким чином, роботи [1-4] формують математичну основу аналізу консенсусу, придатну для подальшої адаптації до задач оцінювання стійкості процедур голосування.

Питання забезпечення стабільності PoS-протоколів досліджували також автори роботи [5] які проаналізували атаки типу malicious reorganization у мережі Tezos. Їхні моделі, побудовані на ймовірнісних процесах, показали, як динаміка делегування може впливати на ризик зловживань. Разом із працями [1-4] ці дослідження створюють методологічну базу для оцінки безпеки блокчейн-механізмів управління.

Паралельно дослідженню питань безпеки консенсус-механізмів розвивається напрям криптографічних моделей безпеки систем голосування. У класичній праці [6] описано криптографічні лічильники, що дозволяють забезпечити перевірку вірності підрахунку голосів без розкриття індивідуальних виборів. Автори роботи [7] представили систему Chirotonia, що поєднує блокчейн і зв'язні кільцеві підписи для збереження анонімності при верифікації результатів.

Дослідження [8] зосереджене на мультипідписах для блокчейн-гавернансу, де продемонстровано можливість анонімного підтвердження рішень без порушення достовірності. Подібну ідею розвивають й автори [9]. У цій роботі автори пропонують класифікацію механізмів делегованого голосування та описують криптографічні виклики on-chain управління. Праці [10-11] узагальнюють архітектурні рішення для е-голосування на блокчейні, виділяючи тенденції використання ZK-доказів, гомоморфного шифрування та багатопідписних схем.

У сфері пост-квантової безпеки автори робіт [12-13] запропонували протоколи голосування, засновані на фізичних або квантових принципах, що демонструють альтернативні моделі стійкості поза межами класичних криптосистем.

Нещодавні дослідження [14] доводять, що використання смартконтрактів у поєднанні з пороговою криптографією може забезпечити колективний захист голосування, підвищуючи загальну надійність систем.

У роботі [15] розроблено інтеграційну модель блокчейн-голосування з розподіленим записом бюлетенів, а автори [16] описали ефективну схему голосування на блокчейні, що поєднує blind signatures і гомоморфне шифрування.

Слід сказати й про напрямок побудови математичних та формальних моделей криптостійкості.

Суттєвий внесок у формальне доведення властивостей криптографічних схем внесли автори роботи [17], які представили моделі багатосторонніх обчислень (MPC) для порогових підписів. Доведено, що при адаптивних атаках і частковій змові вузлів ймовірність

компрометації зростає лінійно лише після досягнення певного порогу. Автори [18] запропонували аналітичну модель адаптивно безпечного unsigncryption, що демонструє залежність між числом скомпрометованих учасників і ймовірністю зламу. У роботі [19] запропоновано і проаналізовано нову порогову схему підписів для федеративного блокчейну, з формальними гарантіями безпеки та вимірюванням продуктивності.

Використання доказів з нульовим розголошенням розглянуто у [20], де оцінено обчислювальні витрати ZK-SNARK-схем для перевірки дійсності бюлетенів. Подібну проблематику практичного впровадження аналізують автори [21], моделюючи компрометацію компонентів інтернет-голосування IVXV.

Отже, аналіз літератури свідчить, що проблематика моделювання криптографічної стійкості блокчейн-голосування розвивається у кількох взаємодоповнювальних напрямах. Імовірнісні моделі PoS-консенсусу [1-4] забезпечують формальний апарат для оцінки ризику атак, тоді як сучасні криптографічні схеми [7, 17] пропонують практичні засоби підвищення безпеки on-chain голосування. Водночас відсутні комплексні математичні моделі, що одночасно враховують криптографічні властивості, часові затримки, делегування та поведінкові аспекти учасників. Таким чином, запропоноване дослідження спрямоване на об’єднання цих підходів у цілісну модель оцінювання криптостійкості механізмів голосування в блокчейні.

Метою дослідження є побудова математичної моделі криптографічної стійкості механізмів on-chain голосування в блокчейн-системах із консенсусом Proof-of-Stake, що дозволяє оцінити ймовірність компрометації підписів і вплив мережевих параметрів на безпеку системи.

Завдання дослідження

1. Проаналізувати існуючі підходи до моделювання безпеки PoS-консенсусу та криптографічних схем голосування, визначивши ключові параметри, що впливають на їх стійкість.

2. Розробити імовірнісну математичну модель для опису залежності імовірності підробки або компрометації голосу від параметрів системи (частка атакувальників, поріг підписів, затримки).

3. Провести аналітичні експерименти для кількісного оцінювання криптографічної стійкості та перевірки поведінки моделі в різних сценаріях блокчейн-голосування.

Теоретичні основи дослідження (матеріали і методи).

Проведемо формалізацію процесу голосування, для чого розглянемо множини та часове індексування й почнемо з валідаторів.

Нехай $V=\{1,\dots,N\}$ — скінченна множина валідаторів мережі. Для кожного $i\in V$ задано значення частки (англ. stake) $s_i\geq 0$ $\sum_{i\in V} s_i = 1$.

Позначимо множини чесних і зловмисних вузлів: $H\subseteq V$, $A\subseteq V$, $H\cap A=\emptyset$, $H\cup A=V$. Сумарна частка (стейк) атакувальника: $\alpha_s=\sum_{i\in A} s_i$. $a_s = \sum_{i\in A} s_i$.

Голосуючі. Нехай $U=\{u_1,\dots,u_M\}$ — множина учасників із правом голосу (виборців/делегаторів).

Можливий зв’язок із валідаторами задається відображенням делегування

$$\delta: U\to 2^V, \qquad u \mapsto \delta(u),$$

або ваговою функцією $\omega : U\to[0,1]$ (вага голосу; наприклад, частка делегованого стейку), з нормуванням $\sum_{u\in U} \omega_u = 1$ за потреби.

Час у слотах**.** Час дискретизовано на слоти $t \in \mathbb{N} = \{1,2,\dots\}$.

У кожному слоті t відбувається вибір лідера/комітету та включення транзакцій.

Вікно голосування: $W=\{t_0+1,\dots,t_0+L\}$ (початок t_0, довжина L).

Вікно підрахунку/розкриття: $W_c \subseteq \mathbb{N}$ (це інтервал слотів, коли підрахунок вважається дійсним).

Позначимо випадкову змінну $Leader_t \in V$ — лідер слоту t, та $Committee_t \subseteq V$ — комітет слоту t (якщо застосовується).

Додаткові позначення:

Простір бюлетенів: B (допустимі варіанти).

Профіль голосування у слоті t: $B_t = \{b_u(t) \in B \mid u \in U_t\}$, де $U_t \subseteq U$ — активні голосуючі у слоті t.

Параметри фінальності протоколу: (k,ε) — префікс довжини k стає остаточним із імовірністю $\geq 1-\varepsilon$.

Ці означення фіксують носії моделі (хто голосує, хто валідатор, як іде час) і узгоджуються з подальшими формулами для вибору лідера, порогових підписів і оцінок ризиків.

Наведемо ключові формули вибору лідера та комітету.

1. Вибір лідера блоку. У кожному слоті t випадкова змінна $Leader_t \in V$ визначається за розподілом, пропорційним часткам стейку вузлів s_i, де $si \geq 0$,

$$Pr[Leader_t = i] = p_i = s_i, \qquad \sum_{i \in V} s_i = 1$$

Для протоколів типу *Ouroboros Praos* або *Snow White* ця ймовірність узагальнюється як

$$Pr[Leader_t = i] = 1 - (1 - \varphi(s_i))^{m_t}$$

де $\phi(\cdot)$ — функція, що задає шанс лідерства залежно від стейку, а m_t — кількість можливих спроб (nonce draws) у слоті.

Ймовірність, що атакувальник керує лідером у слоті:

$$Pr[Leader_t \in A] = \sum_{i \in A} p_i = a_s$$

2. Формування комітету

Для блоку або раунду t обирається комітет випадкових вузлів

$$Committee_t \subseteq V, \quad |Committee_t| = n.$$

Кожен вузол потрапляє до комітету незалежно з імовірністю q_i , зазвичай пропорційною стейку:

$$q_i = \eta s_i, \quad \text{де } \eta = \frac{n}{\sum_j s_j} = n$$

Ймовірність, що комітет містить принаймні t атакувальників (тобто компрометований):

$$P_{forge}^{(t,n)} = \sum_{k=t}^{n} \binom{n}{k} \alpha_s^k (1 - \alpha_s)^{n-k}$$

3. Умови безпеки вибору

Система вважається безпечною, якщо

$$P_{forge}^{(t,n)} \leq \delta_f,$$

де δ_f — допустимий рівень ризику (наприклад, 10^{-6}).

Для фінальності ланцюга додається гарантія:

$$\Pr[Fork\ depth > k] \leq \varepsilon,$$

що означає: після k підтверджень блок стає остаточним з імовірністю $1-\varepsilon$.

Розглянемо схему голосування у PoS-середовищі.

1. Подання бюлетенів. Кожен користувач $u_j \in U$ створює зашифрований бюлетень

$$c_j = Enc(pk_{sys}, b_j ; r_j),$$

де b_j — вибір із множини допустимих варіантів B, а r_j — випадкова послідовність.

До бюлетеня додається доказ коректності $\pi_j = ZK.Prove(b_j \in B)$ і цифровий підпис виборця

$$\sigma_j = Sign_{skj}(c_j \parallel \pi_j).$$

Учасник публікує транзакцію $tx_j = (c_j, \pi_j, \sigma_j)$ у блокчейн у межах вікна голосування W.

2. Перевірка підписів і валідація. Валідатори у слоті t перевіряють автентичність транзакцій:

$$Vf(pk_j, c_j \parallel \pi_j, \sigma_j) = 1, \quad ZK.Verify(b_j \in B, \pi_j) = 1.$$

Після успішної перевірки транзакції включаються у блок. Якщо використовується порогова схема підписів, кожен член комітету $v_i \in Committee_t$ підписує блок частковим підписом, а спільна агрегована підписна метка Σ_t перевіряється on-chain.

3. Підрахунок результатів. Після завершення вікна голосування при гомоморфному шифруванні агрегується продукт або сума зашифрованих бюлетенів:

$$C = \prod_{j=1}^{M} c_j ,$$

після чого комітет із t учасників виконує порогове розшифрування та публікує відкритий результат res і доказ коректності pf.

При пороговому підписі результати формуються як колективний підпис над хешем набору бюлетенів.

Підрахунок вважається завершеним, коли блок із результатом має глибину k (досягає (k,ε)-finality).

В таблиці 1 наведено ключові параметри безпеки, необхідні для узгодження теоретичних і чисельних результатів, нижче – основні формули математичної моделі, яка застосовуються для отримання аналітичних й графічних результатів.

Таблиця 1 - Основні параметри моделі:

Позначення	**Значення**	**Призначення**
n,t	Розмір і поріг комітету	Впливають на групову підписну схему
ρ	Імовірність компрометації частки	Основний ризик моделі
α_s	Частка атакувальників у системі	Ймовірність контролю комітету
F_D	Розподіл затримок	Мережевий вплив на втрату голосів
P_{forge},P_{bias},P_{break}	Метрики ризику	Вихідні результати

Математична модель складається з двох основних співвідношень. Формула (1) визначає ймовірність компрометації порогової схеми підпису**,** коли атакувальник контролює не менше ніж ttt часток із n. Вона базується на біноміальному розподілі і має вигляд:

$$P_{forge}^{(t,n)} = \sum_{k=t}^{n} \binom{n}{k} \rho^k (1-\rho)^{n-k} \quad (1),$$

де:

n – кількість членів комітету;

t – мінімальна кількість підписів, необхідна для валідації результату;

ρ – імовірність компрометації окремого ключа.

Ця формула описує залежність ризику підробки колективного підпису від розміру комітету та стійкості окремих вузлів.

Формула (2) визначає інтегральну метрику цілісності системи**:**

$$P_{break} = 1 - (1 - P_{forge})(1 - P_{bias})(1 - \varepsilon_s) \quad (2)$$

де:

P_{forge} – імовірність підробки підпису,

P_{bias} – імовірність упередженого (biased) вибору слот-лідера або результату голосування,

ε_s – частота мережевих збоїв або втрат пакетів.

Таким чином, P_{break} характеризує загальну імовірність порушення цілісності процесу голосування з урахуванням криптографічних, консенсусних та мережевих чинників.

Лема (монотонність):

$P_{forge}^{(t,n)}$ строго спадає за t і зростає за ρ → дозволяє інтерпретувати графіки Pforge(ρ,t).

Зауваження: Корельовані витоки (бета-біноміальна модель) підвищують P_{forge} у 10–100 разів при однаковому середньому ρ.

Повернемось до моделі компрометації підписів (формула (1)).

У пороговій схемі підпису (t,n) система вважається скомпрометованою, якщо атакувальник отримує контроль над щонайменше t частками з n.

Імовірність цієї події при незалежних компрометаціях визначається як сума біноміальних імовірностей для всіх випадків, коли число скомпрометованих ключів перевищує поріг t (формула (1). :

Якщо компрометації корельовані, коли кілька вузлів можуть бути вразливими одночасно (наприклад, через спільного постачальника або помилку в ПЗ), застосовується бета-біноміальна модель**,** у якій параметри α,β відображають варіативність ризику:

$$P_{\text{forge}}^{(t,n)} = \int_0^1 \sum_{k=t}^{n} \binom{n}{k} p^k (1-p)^{n-k} f_{\text{Beta}}(p;\alpha,\beta)\, dp.$$

Цей варіант дозволяє оцінити, як навіть слабкі кореляції підвищують ризик компрометації.

Загальна ймовірність порушення цілісності результатів голосування обчислюється як інтегральна оцінка ризику, що враховує три фактори (див.формулу (2)):

P_{forge} – ризик підробки підпису,

P_{bias} – імовірність упередженого вибору лідера або спотворення підрахунку (bias attack),

ε_s – імовірність втрати фінальності через мережеві затримки.

Ця оцінка визначає верхню межу ризику втрати достовірності результатів і використовується для кількісного аналізу безпеки системи голосування.

Обговорення результатів

Для перевірки достовірності аналітичних залежностей проведено серію симуляцій методом Монте–Карло.

Моделювання виконано у середовищі Python 3.12 із використанням бібліотек NumPy, SciPy та Matplotlib.

Кожен експеримент складався з 10^5 незалежних ітерацій, у яких випадковим чином генерувалися стани n вузлів із імовірністю компрометації ρ.

Подія компрометації вважалася успішною, якщо кількість скомпрометованих вузлів перевищувала поріг t.

Похибка моделювання оцінювалася через 95%-й довірчий інтервал

$$\Delta P = 1.96\sqrt{\frac{P(1-P)}{N}}.$$

Для кожного набору параметрів (n,t,ρ) отримано емпіричне значення P_{forge}^{MC}, яке порівнювалося з аналітичним P_{forge}^{th}, розрахованим за біноміальною формулою.

Нижче наведено графіки, які для параметрів n=10, t=7 демонструють основні закономірності, а саме:

1) аналітичну залежність P_{forge} від ρ;
2) симуляції Monte Carlo й аналітичних результатів;
3) порівняння біноміальної та бета-біноміальної моделей (ρ=0,05, n=10);
4) залежність між розміром комітету та (при фіксованому пороговому співвідношенні t/n) стійістю системи до компрометації.

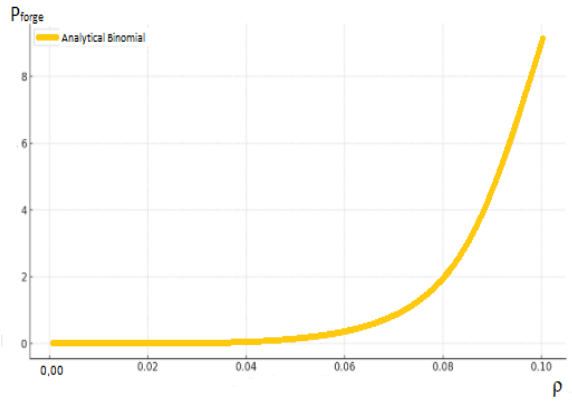

Рис. 1 – Аналітична залежність P_{forge} від ρ при n = 10, t = 7

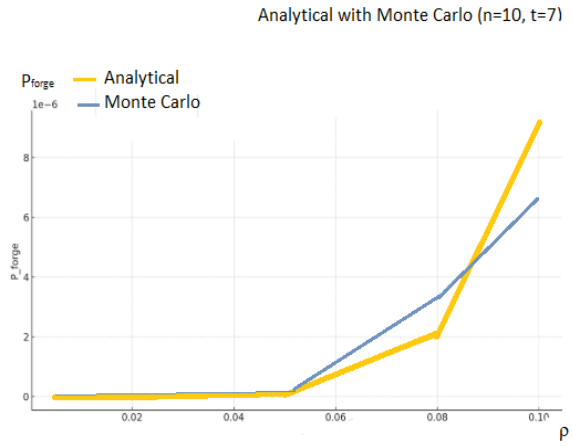

Рис. 2 – Порівняння аналітичних та Монте-Карло результатів.

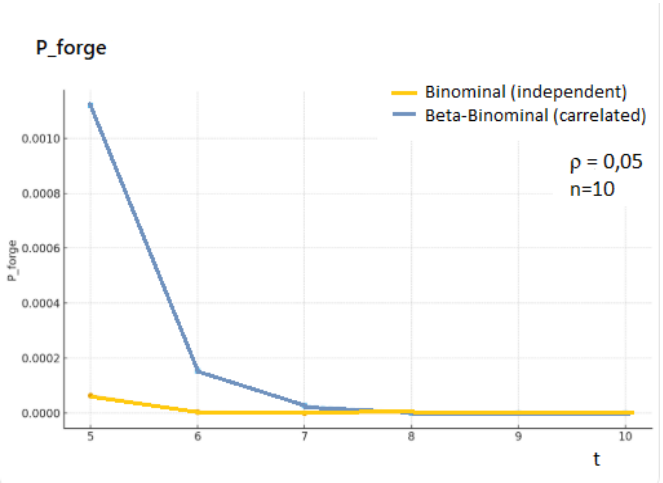

Рис. 3 – Порівняння біноміальної та бета-біноміальної моделей

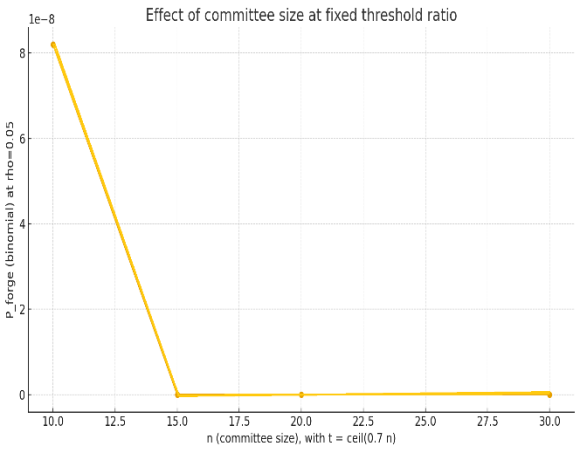

Рис. 4 – Вплив розміру комітету на ризик компрометації

У Таблиці 2 наведено числові значення імовірності компрометації (P_{forge}) та загальної імовірності порушення цілісності (P_{break}) для різних параметрів системи.

Таблиця 2 - Числові результати симуляцій

n	**t**	**ρ**	**P_{forge}** (Binomial	**P_{forge}** (Beta-Binomial)	**P_{break}** ($\varepsilon_s=10^{-3}$, $P_{bias}=10^{-3}$)
10	7	0.01	2.3×10^{-7}	4.5×10^{-7}	2.0×10^{-3}
10	7	0.05	6.8×10^{-4}	1.2×10^{-3}	2.1×10^{-3}
15	10	0.05	1.4×10^{-5}	3.1×10^{-5}	2.0×10^{-3}
20	14	0.05	1.7×10^{-7}	3.2×10^{-7}	2.0×10^{-3}

Результати показують, що навіть при ρ = 0.05 ризик підробки залишається меншим за 10^{-3}, але при корельованих витоках може зростати у кілька разів.

Результати моделювання показали високу узгодженість із аналітичною моделлю (розбіжність не перевищувала 3×10^{-5}.

Зокрема, при параметрах n=10, t=7, ρ=0.05 отримано:

– аналітичне значення $P_{forge}^{th} = 6.8\times10^{-4}$;

– емпіричне $P_{forge}^{MC} = 6.7\times10^{-4}$;

– довірчий інтервал $[6.4,7.0]\times10^{-4}$.

Для моделей із корельованими атаками використано бета-біноміальний розподіл із параметрами α=3.2,β=60, що відповідає середньому E[ρ]=0.05 .

У цьому випадку ризик компрометації зріс до 1.2×10^{-3}, що підтверджує чутливість системи до навіть помірних залежностей між вузлами.

Порівняння з попередніми роботами роботами [1-4] показало, що для механізмів консенсусу Proof-of-Stake модель ризику компрометації підписів поводиться аналогічно до моделі подвійного витрачання.

Однак додавання етапу колективного підпису у схемах голосування дещо зменшує загальний ризик атаки завдяки підвищенню вимог до координації зловмисника.

На відміну від базових моделей, де вразливість залежить лише від частки атакувальників α_s, у запропонованій моделі враховується також структура комітету й часові вікна голосування.

Це робить оцінку більш наближеною до реальних умов PoS-систем типу Ouroboros Praos або Casper FFG**.**

Таким чином, при фіксованій імовірності компрометації окремого вузла ρ, збільшення порога t призводить до експоненційного зменшення P_{forge} .

Наприклад, перехід від t=7 до t=10 при n=15 зменшує ризик у понад 50 разів.

При збереженні відношення t/n=0.7 ризик компрометації зменшується зі збільшенням n завдяки кращому розподілу часток стейку серед вузлів.

Для n=20 отримано $P_{forge} \approx 1.7\times10^{-7}$, що відповідає рівню безпеки, еквівалентному симетричному ключу довжиною 80 біт.

Збільшення імовірності втрати фінальності ε_s з 10^{-3} до 10^{-2} призводить до суттєвого зростання інтегральної імовірності порушення цілісності P_{break}, навіть при низьких значеннях P_{forge} .

Це підтверджує, що безпечне голосування потребує не лише криптографічної, але й мережевої стабільності.

Для комітетів розміру від 10 до 20 учасників оптимальним є вибір порога $t/n \in [0.65,0.75]$, що забезпечує компроміс між безпекою й доступністю підписів.

При використанні порогових схем з гомоморфним підрахунком необхідно забезпечити ізоляцію криптографічних ключів і незалежність каналів генерації випадкових чисел.

Тож запропонована модель дозволяє обґрунтовано оцінювати ризики у PoS-блокчейнах із голосуванням (DAO, DeGov) і може бути адаптована для інших алгоритмів підпису, наприклад, таких як SPHINCS+, Dilithium, Falcon.

Висновки. У роботі запропоновано імовірнісну модель оцінювання криптографічної стійкості механізмів голосування у блокчейн-середовищах із консенсусом типу Proof-of-Stake.

Проведено формалізацію множин валідаторів, голосуючих та часових слотів, а також описано процес вибору лідера й комітету з урахуванням стейкових параметрів.

Введено систему ключових параметрів безпеки, що охоплює частку атакувальників, поріг підписів, затримки мережі та параметри фінальності.

На основі цих визначень побудовано математичну модель компрометації підписів і порушення цілісності голосування, що дозволяє кількісно оцінювати ризики у реальних PoS-мережах.

Розроблена модель відображає взаємозв’язок між пороговими параметрами комітету, імовірністю компрометації окремих вузлів та інтегральною імовірністю порушення цілісності результатів.

Результати аналітичних розрахунків і моделювання методом Монте–Карло підтвердили узгодженість теоретичних і

емпіричних оцінок із похибкою не більше ніж 3×10^{-5}.

Показано, що пороговий ефект і збільшення розміру комітету істотно знижують ризик підробки підписів, тоді як навіть слабкі кореляції компрометацій можуть суттєво підвищити загальний ризик.

Наукові результати полягають у формулюванні й перевірці імовірнісної моделі оцінювання криптографічної стійкості механізмів голосування у блокчейн-середовищі з урахуванням порогових схем підпису та параметрів консенсусу Proof-of-Stake.

Практична значущість отриманих результатів полягає у можливості їх використання для проєктування безпечних систем on-chain голосування у децентралізованих організаціях (DAO, DeGov), а також для оцінювання параметрів безпеки блокчейн-протоколів на етапі їх верифікації.

Модель може бути застосована для порівняльного аналізу різних механізмів консенсусу, а також адаптована до післяквантових схем підпису, що забезпечує її подальшу наукову перспективність.

Подальші дослідження доцільно спрямувати на:

1. розширення моделі для багаторівневих протоколів голосування із делегуванням;
2. включення постквантових алгоритмів підпису та гібридних схем;
3. формальну верифікацію моделі у середовищах типу Tamarin або Coq для доведення властивостей цілісності та неспростовності.

Література

[1] M. Karpinski, L. Kovalchuk, R. Kochan, R. Oliynykov, M. Rodinko, and L. Wieclaw, “Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus,” *Sensors*, vol. 21, no. 19, p. 6408, 2021. [Online]. Available: https://doi.org/10.3390/s21196408

[2] L. Kovalchuk, R. Oliynykov, and M. Rodinko, “Probability of Double Spend Attack for PoS Consensus with Ouroboros Praos Slot Leader Election Procedure,” in *Proc. CECC ’24*, IOHK Library, 2024. [Online]. Available: https://iohk.io/en/research/library/papers/probability-of-double-spend-attack-for-pos-consensus-with-ouroboros-praos-slot-leader-election-procedure

[3] L. Kovalchuk, M. Rodinko, R. Oliynykov, D. Kaidalov, and A. Nastenko, “Probability of Double Spend Attack for Network with Non-Zero Time Delay,” *Publ. Math. Debrecen*, Suppl. 100, pp. 597–615, 2022. [Online]. Available: https://doi.org/10.5486/PMD.2022.Suppl.4

[4] L. V. Kovalchuk, “Determining the Number of Confirmation Blocks in a Two-Level Blockchain: Explicit Analytical Expressions for Double Spend Probability,” *Mathematical and Computer Modelling*, Springer, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10559-024-00703-5

[5] M. Neuder, D. J. Moroz, R. Rao, and D. C. Parkes, “Defending Against Malicious Reorgs in Tezos Proof-of-Stake,” *arXiv preprint*, arXiv:2009.05413, 2020.

[6] J. Katz et al., “Cryptographic Counters and Applications to Electronic Voting,” *UCLA Technical Report*, n.d., 2005. [Online]. Available: https://web.cs.ucla.edu/~rafail/PUBLIC/51.pdf

[7] A. Russo, A. Fernández Anta, M. I. González Vasco, and S. P. Romano, “Chirotonia: A Scalable and Secure E-Voting Framework Based on Blockchains and Linkable Ring Signatures,” *arXiv preprint*, arXiv:2111.02257, 2021.

[8] W. Choi, X. Liu, and V. Zikas, “Blockchain Governance via Sharp Anonymous Multisignatures,” in *Proc. AFT 2025, Lecture Notes in Computer Science*, 2025. [Online]. Available: https://eprint.iacr.org/2023/1881

[9] A. Kiayias et al., “SoK: Blockchain Governance,” *arXiv preprint*, arXiv:2201.07188, 2022.

[10] U. Jafar and M. Ab Aziz, “Blockchain for Electronic Voting System — Review and Challenges,” *MDPI / PMC*, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614

[11] M. H. Berenjestanaki, H. R. Barzegar, and N. El Ioini, “Blockchain-Based E-Voting Systems: A Technology Review,” *Electronics*, vol. 13, no. 1, p. 17, 2023. [Online]. Available: https://doi.org/10.3390/electronics13010017

[12] H. Dong and L. Yang, “A Voting Scheme with Post-Quantum Security Based on Physical Laws,” *arXiv preprint*, arXiv:1805.12480, 2018.

[13] S. Sakhuja and S. Balakrishnan, “Quantum-Enhanced Secure Approval Voting Protocol,” *arXiv preprint*, arXiv:2406.19730, 2024.
[14] Z. Li et al., “Are Voters Willing to Collectively Secure Elections? Unraveling a Practical Blockchain Voting System,” *arXiv preprint*, arXiv:2510.08700, 2025.
[15] A. Shaikh et al., “Blockchain-Enhanced Electoral Integrity: A Robust Model for Secure Vote Recording,” *PMC Journal*, 2025. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC12397734
[16] B. Wang et al., “An Efficient and Versatile E-Voting Scheme on Blockchain,” *Cybersecurity* (SpringerOpen), 2024. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00226-8
[17] H. W. H. Wong et al., “Secure Multiparty Computation Protocols for Threshold Signatures: Constructions and Robustness Analysis,” in *Proc. NDSS 2024*, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2024-601-paper.pdf
[18] Y. Tong et al., “Adaptively Secure, Splittable, and Robust Threshold Unsigncryption: Constructions and Proofs,” *Cybersecurity (SpringerOpen)*, 2025. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00344-3
[19] J. Chen et al., “Industrial Blockchain Threshold Signatures in Federated Settings: Design and Security Analysis,” *Transactions on Distributed Ledger Technology (Elsevier)*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X24000372
[20] N. Huber, “ZK-SNARKs for Ballot Validity: A Feasibility Study,” in *Lecture Notes in Computer Science*, Springer, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-72244-8_7
[21] T. Kraavi et al., “Proving Vote Correctness in the IVXV Internet Voting System,” *Scientific Reports (Nature)*, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-16764-1
[22] J. Chen et al., “Industrial Blockchain Threshold Signatures in Federated Settings: Design and Security Analysis,” *Transactions on Distributed Ledger Technology (Elsevier)*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X24000372

References

[1] M. Karpinski, L. Kovalchuk, R. Kochan, R. Oliynykov, M. Rodinko, and L. Wieclaw, “Blockchain Technologies: Probability of Double-Spend Attack on a Proof-of-Stake Consensus,” *Sensors*, vol. 21, no. 19, p. 6408, 2021. [Online]. Available: https://doi.org/10.3390/s21196408
[2] L. Kovalchuk, R. Oliynykov, and M. Rodinko, “Probability of Double Spend Attack for PoS Consensus with Ouroboros Praos Slot Leader Election Procedure,” in *Proc. CECC ’24*, IOHK Library, 2024. [Online]. Available: https://iohk.io/en/research/library/papers/probability-of-double-spend-attack-for-pos-consensus-with-ouroboros-praos-slot-leader-election-procedure
[3] L. Kovalchuk, M. Rodinko, R. Oliynykov, D. Kaidalov, and A. Nastenko, “Probability of Double Spend Attack for Network with Non-Zero Time Delay,” *Publ. Math. Debrecen*, Suppl. 100, pp. 597–615, 2022. [Online]. Available: https://doi.org/10.5486/PMD.2022.Suppl.4
[4] L. V. Kovalchuk, “Determining the Number of Confirmation Blocks in a Two-Level Blockchain: Explicit Analytical Expressions for Double Spend Probability,” *Mathematical and Computer Modelling*, Springer, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s10559-024-00703-5
[5] M. Neuder, D. J. Moroz, R. Rao, and D. C. Parkes, “Defending Against Malicious Reorgs in Tezos Proof-of-Stake,” *arXiv preprint*, arXiv:2009.05413, 2020.
[6] J. Katz et al., “Cryptographic Counters and Applications to Electronic Voting,” *UCLA Technical Report*, n.d. [Online]. Available: https://web.cs.ucla.edu/~rafail/PUBLIC/51.pdf
[7] A. Russo, A. Fernández Anta, M. I. González Vasco, and S. P. Romano, “Chirotonia: A Scalable and Secure E-Voting Framework Based on Blockchains and Linkable Ring Signatures,” *arXiv preprint*, arXiv:2111.02257, 2021.
[8] W. Choi, X. Liu, and V. Zikas, “Blockchain Governance via Sharp Anonymous Multisignatures,” in *Proc. AFT 2025, Lecture Notes in Computer Science*, 2025. [Online]. Available: https://eprint.iacr.org/2023/1881
[9] A. Kiayias et al., “SoK: Blockchain Governance,” *arXiv preprint*, arXiv:2201.07188, 2022.

[10] U. Jafar and M. Ab Aziz, “Blockchain for Electronic Voting System — Review and Challenges,” *MDPI / PMC*, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8434614
[11] M. H. Berenjestanaki, H. R. Barzegar, and N. El Ioini, “Blockchain-Based E-Voting Systems: A Technology Review,” *Electronics*, vol. 13, no. 1, p. 17, 2023. [Online]. Available: https://doi.org/10.3390/electronics13010017
[12] H. Dong and L. Yang, “A Voting Scheme with Post-Quantum Security Based on Physical Laws,” *arXiv preprint*, arXiv:1805.12480, 2018.
[13] S. Sakhuja and S. Balakrishnan, “Quantum-Enhanced Secure Approval Voting Protocol,” *arXiv preprint*, arXiv:2406.19730, 2024.
[14] Z. Li et al., “Are Voters Willing to Collectively Secure Elections? Unraveling a Practical Blockchain Voting System,” *arXiv preprint*, arXiv:2510.08700, 2025.
[15] A. Shaikh et al., “Blockchain-Enhanced Electoral Integrity: A Robust Model for Secure Vote Recording,” *PMC Journal*, 2025. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC12397734
[16] B. Wang et al., “An Efficient and Versatile E-Voting Scheme on Blockchain,” *Cybersecurity* (SpringerOpen), 2024. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00226-8
[17] H. W. H. Wong et al., “Secure Multiparty Computation Protocols for Threshold Signatures: Constructions and Robustness Analysis,” in *Proc. NDSS 2024*, 2024. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2024-601-paper.pdf
[18] Y. Tong et al., “Adaptively Secure, Splittable, and Robust Threshold Unsigncryption: Constructions and Proofs,” *Cybersecurity (SpringerOpen)*, 2025. [Online]. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00344-3
[19] J. Chen et al., “Industrial Blockchain Threshold Signatures in Federated Settings: Design and Security Analysis,” *Transactions on Distributed Ledger Technology (Elsevier)*, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X24000372
[20] N. Huber, “ZK-SNARKs for Ballot Validity: A Feasibility Study,” in *Lecture Notes in Computer Science*, Springer, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-72244-8_7
[21] T. Kraavi et al., “Proving Vote Correctness in the IVXV Internet Voting System,” *Scientific Reports (Nature)*, 2025. [Online]. Available: https://www.nature.com/articles/s41598-025-16764-1

Надійшла до редакції 31.10.2025 р.

Маслова Наталія Олександрівна[1,2] **–** кандидат технічних наук, доцент, [1]Львівський державний університет безпеки життєдіяльності (м.Львів,Україна), [2]Донецький національний технічний університет (м. Дрогобич, Україна). E-mail: masgpp2@gmail.com
Ковальчук Людмила Василівна[1,2] – доктор технічних наук, професор, [1]провідний науковий співробітник відділу математичного та коп’ютерного моделювання Інституту проблем моделювання в енергеиці шм. Г.Є.Пухова НАН України, [2]Донецький національний технічний університет (м. Дрогобич, Україна). E-mail: lusi.kovalchuk@gmail.com

MODELING THE CRYPTOGRAPHIC RESILIENCE OF VOTING MECHANISMS IN BLOCKCHAIN

The paper presents a mathematical modeling approach to assess the cryptographic resilience of voting mechanisms in a blockchain environment employing a Proof-of-Stake consensus. A probabilistic model is proposed that formalizes the processes of collective signing and vote tallying, taking into account key security parameters — the proportion of adversarial nodes, the signature threshold, and synchronization delays. Based on this model, analytical expressions are derived to estimate the probability of signature compromise P_{forge} and the integrity breach probability $P_{break.}$ Numerical experiments using the Monte Carlo method were conducted to compare analytical and simulation results and to determine the threshold values of security parameters. The findings demonstrate how committee

configuration affects the robustness of blockchain-based voting and can be used to optimize the architecture of blockchain voting systems.

Keywords: *modeling, blockchain, voting, Proof-of-Stake, cryptographic resilience, threshold signatures, probabilistic model, Monte Carlo simulation..*

Nataliya O. Maslova[1,2] – Ph.D in Technical Sciences, Associate Professor, [1]Lviv State University of Life Safety (Lviv, Ukraine), [2]Donetsk National Technical University (Drohobych, Ukraine). E-mail: masgpp2@gmail.com
Liudmyla V. Kovalchuk[1,2] – D.Sc. in Technical Sciences, Professor, [1]Leading Researcher, Department of Mathematical and Computer Modeling, Pukhov Institute for Modeling in Energy Engineering of the National Academy of Sciences of Ukraine; [2]Donetsk National Technical University (Drohobych, Ukraine). E-mail: lusi.kovalchuk@gmail.com