Ймовірнісно-вартісна модель стратегій перевірки фінальності для легких клієнтів блокчейнів із доказом частки

A Probabilistic Cost Model of Finality Verification Strategies for Proof-of-Stake Light Clients

Валентин Чернушевич
аспірант кафедри кібербезпеки інформаційних систем, мереж і технологій, e-mail: valentyn.chernushevych@student.karazin.ua, ORCID ID: https://orcid.org/0009-0007-4186-1981

Valentyn Chernushevych
PhD student, Department of Cybersecurity of Information Systems, Networks and Technologies, e-mail: valentyn.chernushevych@student.karazin.ua, ORCID ID: https://orcid.org/0009-0007-4186-1981

Харківський національний університет імені В. Н. Каразіна, Харків, Україна

V. N. Karazin Kharkiv National University, Kharkiv , Ukraine

Received: October 4, 2026 | Revised: October 25, 2026 | Accepted: October 31, 2026

УДК 004.056.5:004.75

DOI: https://doi.org/10.33445/sds.2026.16.5.17

Мета роботи. Розробити ймовірнісно-вартісну модель оцінювання стратегій перевірки фінальності блоків для легких клієнтів блокчейнів із механізмом консенсусу Proof of Stake (PoS) з урахуванням криптографічної стійкості, розподілу стейку та вартості перевірки.

Методологія дослідження. Застосовано ймовірнісне моделювання, комбінаторний аналіз, методи чисельного інтегрування, динамічного програмування та багатокритеріального порівняння. Для оцінювання ймовірності успішної атаки використано гіпергеометричний розподіл і нецентральний гіпергеометричний розподіл Валеніуса. Досліджено повну перевірку підписів, рекурсивні криптографічні докази, випадкову вибіркову перевірку та штатний протокол легкого клієнта NEAR.

Результати дослідження. Встановлено залежність безпеки й вартості перевірки від кількості валідаторів, концентрації стейку та можливостей супротивника щодо маніпулювання випадковістю. Для системи зі 100 валідаторами за концентрованого розподілу стейку детермінована перевірка мінімального кворуму є економнішою, ніж вибіркова перевірка з ймовірністю успішної атаки 2^{-64}. Для 1000 валідаторів зазначена перевага виникає за вимог до ймовірності атаки, суворіших за 2^{-80}.

Наукова новизна. Запропоновано комплексне порівняння стратегій перевірки фінальності на основі інтеграції ймовірнісної моделі атак із моделлю обчислювальних і транзакційних витрат для блокчейнів із підписами Ed25519.

Практичне значення. Результати можуть використовуватися для обґрунтування вибору механізмів перевірки фінальності під час проєктування легких клієнтів і міжланцюгових мостів.

Тип статті: дослідницька стаття.

Purpose. To develop a probabilistic cost model for evaluating block finality verification strategies for light clients of Proof-of-Stake (PoS) blockchains, considering cryptographic security, stake distribution, and verification costs.

Methodology. The study employs probabilistic modeling, combinatorial analysis, numerical integration, dynamic programming, and multicriteria comparison. Hypergeometric and Wallenius' noncentral hypergeometric distributions are used to estimate the probability of a successful attack. Four strategies are examined: full signature verification, recursive cryptographic proofs, random sampling-based verification, and the native NEAR light-client protocol.

Findings. Verification security and costs depend on the number of validators, the concentration of stake, and an adversary's ability to manipulate randomness. For a system with 100 validators and a concentrated stake distribution, deterministic verification of a minimum quorum is less costly than sampling-based verification at an attack success probability of 2^{-64}. For 1,000 validators, this advantage emerges only when the required attack success probability is lower than 2^{-80}.

Originality. The study provides an integrated comparison of finality verification strategies by combining a probabilistic attack model with computational and transaction-cost models for blockchains that use Ed25519 signatures.

Practical implications. The findings support evidence-based selection of finality verification mechanisms when designing blockchain light clients and cross-chain bridges.

Article type. Research Article.

Ключові слова:. блокчейн; Proof of Stake; легкий клієнт; фінальність блоків; криптографічна стійкість; вибіркова перевірка; міжланцюгові мости.

Key words: blockchain; Proof of Stake; light client; block finality; cryptographic security; random sampling; cross-chain bridges.

Вступ

Міжланцюгові мости — одна з найуразливіших ланок інфраструктури цифрових активів. Систематизації інцидентів показують, що зловмисники найчастіше атакують компоненти, які

перевіряють стан чужого ланцюга, і користуються недостатньо суворою перевіркою підписів або доказів (Lee et al., 2023; Augusto et al., 2024). Автори zkBridge оцінили збитки користувачів від повторюваних атак на мости понад 1,5 млрд доларів США (Xie et al., 2022). Тому правило, за яким легкий клієнт або смартконтракт мосту визнає заголовок блоку фінальним, – це засіб захисту. Від нього залежить цілісність усіх подальших міжланцюгових операцій.

Збитки не обмежуються окремими платформами. За висновком ФБР, 620 млн доларів США в ефірі з мосту мережі Ronin у березні 2022 року викрали угруповання Lazarus Group і APT38, пов'язані з КНДР (Federal Bureau of Investigation, 2022). Група експертів Ради Безпеки ООН у заключній доповіді 2024 року розслідувала 58 імовірних кібератак КНДР на криптовалютні компанії у 2017–2023 роках на суму близько 3 млрд доларів США. За наявними в групи даними, ці кошти допомагають фінансувати розроблення зброї масового знищення (United Nations Security Council, 2024). Слабке правило перевірки в мості, таким чином, стає каналом фінансування підсанкційних державних програм і чинником міжнародної безпеки. Вибір такого правила належить до управління ризиками інформаційної безпеки, і для нього потрібні кількісні критерії.

У блокчейнах з консенсусом на основі доказу частки володіння (proof of stake, PoS) фінальність засвідчують підписи валідаторів, які сукупно володіють понад двома третинами стейку, тобто токенів, заблокованих валідаторами для участі в консенсусі. Легкий клієнт має чотири варіанти: (а) перевірити всі ці підписи; (б) перевірити лише випадкову вибірку підписів (Bhatt et al., 2025); (в) перевірити один стислий доказ того, що підписи перевірено, побудований недовіреним доводжувачем (Xie et al., 2022; Danezis et al., 2026); (г) скористатися штатним протоколом легкого клієнта конкретної мережі. Для ланцюгів з агрегованими підписами BLS (Boneh–Lynn–Shacham) ці варіанти досліджено більш широко (Chatzigiannis et al., 2022; Ciobotaru et al., 2022). NEAR натомість використовує окремі підписи Ed25519 (NEAR Protocol, n.d.), а у віртуальній машині Ethereum (EVM) прекомпільованого контракту для Ed25519 немає: пропозиція щодо вдосконалення Ethereum (Ethereum Improvement Proposal, EIP) EIP-665 має статус "Stagnant", тобто роботу над нею зупинено (Oberstein, 2018). Для такого класу ланцюгів досі невідомо, за яких умов кожна стратегія є безпечною й економічною.

Мета дослідження – побудувати відтворювану ймовірнісно-вартісну модель чотирьох стратегій перевірки фінальності. Вхідні величини моделі: кількість валідаторів n, розподіл стейку, частка зловмисного стейку f і кількість r реалізацій випадковості, які може перебрати супротивник. Вихідні величини: стійкість – $log_2 P$, де P — ймовірність успішної атаки, і вартість одного кроку синхронізації легкого клієнта. Завдання дослідження: формалізувати модель загроз; вивести мінімальний розмір вибірки $k^*(\varepsilon)$ для рівних і зважених стейків; побудувати модель вартості (обчислення перевірки, обсяг даних, газ Ethereum, тобто плату за обчислення і дані в одиницях мережі Ethereum); знайти точки перетину $n*$ і межу Парето "вартість — стійкість"; сформулювати рекомендації операторам мостів і легких клієнтів.

Наукова новизна результатів полягає в такому. По-перше, до задачі перевірки фінальності застосовано точне інтегральне подання ймовірності атаки для вибірки без повернення, зваженої за стейком; це подання відоме для нецентрального гіпергеометричного розподілу Валеніуса (Fog, 2008). Воно враховує стратегію розміщення зловмисного стейку і дає змогу обчислювати ймовірності аж до 2^{-128}, недосяжні для методу Монте-Карло. По-друге, в одній моделі зіставлено вибіркову перевірку з рекурсивним доказом фінальності для ланцюга з підписами Ed25519, причому параметри доказу взято з опублікованих вимірів. У доступній автору літературі такого порівняння не знайдено. По-третє, показано, що для ста валідаторів із концентрованим стейком детермінована перевірка мінімального за стейком кворуму дешевша за вибірку вже з рівня стійкості 2^{-64}. Для тисячі валідаторів ця перевага з'являється лише на рівнях, жорсткіших за 2^{-80}.

Огляд літератури

Систематизацію легких клієнтів і їхніх припущень довіри запропонували Chatzigiannis et al. (2022), а ризики міжланцюгової взаємодії розглянуто в оглядах Augusto et al. (2024) і Lee et al. (2023). У ланцюгах з доказом роботи стислу синхронізацію забезпечує FlyClient (Bünz et al., 2020). Для PoS-ланцюгів відомі три напрями: докази із сублінійною складністю на основі ігор бісекції (Agrawal et al., 2023; Tas et al., 2025), легкі клієнти для комітетних ланцюгів (Armknecht et al., 2024) і клієнт, що зберігає безпеку без припущення про чесну більшість завдяки криптоекономічним механізмам (Moshrefi et al., 2024). Підзвітні легкі клієнти дають змогу покарати валідаторів, які підписали хибний заголовок (Ciobotaru et al., 2022).

Найближча до цієї статті робота — Bhatt et al. (2025). Автори пропонують інтерактивний протокол. Ретранслятор заявляє бітову карту підписантів, а сторона, що перевіряє, після розкриття випадковості перевіряє m підписів, вибраних рівноймовірно з повторенням. Для валідаторів з однаковим стейком доведено межу $2 - m$; автори зауважують, що за m, більшого за кількість зловмисних валідаторів, перевірка стає детермінованою. Упередженість випадковості Ethereum оцінено як 864-кратну, і її компенсують десять додаткових перевірок; оптимальні стратегії маніпулювання цією випадковістю дослідили Alpturer і Weinberg (2024). Неінтерактивний варіант на основі евристики Фіата–Шаміра потребує $m + q$ підписів, де 2^q — обчислювальний бюджет супротивника; цей результат спирається на компактні сертифікати Micali et al. (2021). Газ оцінено для підписів ECDSA (Elliptic Curve Digital Signature Algorithm) з прекомпільованим контрактом ecrecover і порівняно з перевіркою доказу UltraPLONK. Ланцюгів з Ed25519, вибірки без повернення, зваженої за стейком, і рекурсивних доказів фінальності на основі FRI (Fast Reed–Solomon Interactive Oracle Proof of Proximity) ця праця не розглядає.

Лінія стислих доказів консенсусу починається з zkBridge (Xie et al., 2022): там доказ консенсусу ланцюга-джерела перевіряють у цільовому ланцюзі. Guppy (Danezis et al., 2026) реалізує легкий клієнт на рекурсивних доказах Plonky2, але свідомо виносить перевірку підписів валідаторів за межі схеми через хеш-ланцюгове зобов'язання і зосереджується на доказах включення до стану. Для NEAR існують і практичні розробки. Electron Labs запропонувала перевірку Ed25519 у Circom для легкого клієнта NEAR на доказах нульового розголошення (Electron Labs, 2022), а Succinct Labs розвиває легкі клієнти на віртуальній машині SP1 з перевіркою в EVM через обгортки Groth16 і PLONK (Succinct Labs, 2024). Рецензованих порівнянь цих систем з вибірковою перевіркою за єдиною моделлю загроз автор не знайшов. Власні виміри рекурсивних доказів на Plonky2 для фінальності NEAR опубліковано раніше (Kuznetsov et al., 2024a, 2024b); тут вони слугують лише вхідними параметрами.

Стійкість самого доказу залежить від параметрів FRI і хеш-функції. За документацією Plonky2 стандартна конфігурація FRI забезпечує 100 біт стійкості, оціненої за гіпотезою про межі близькості кодів Ріда–Соломона (conjectured security), а Poseidon у цій конфігурації, за оцінкою Bariant et al. (2022), — близько 95 біт (Polygon Zero, n.d.). Block et al. (2023) обґрунтували безпеку перетворення Фіата–Шаміра для FRI, тоді як Khovratovich et al. (2025) показали практичні атаки на це перетворення в окремих конструкціях. Межі близькості кодів Ріда–Соломона переглянули Ben-Sasson et al. (2026). Реальні вразливості реалізацій стислих неінтерактивних аргументів знання (SNARK) систематизували Chaliasos et al. (2024), а Chalkias et al. (2020) показали, що неоднозначність правил перевірки EdDSA може спричиняти розбіжності в рішеннях між різними реалізаціями. Стійкість Poseidon до недвійкових диференційних і лінійних атак досліджено в праці Kovalchuk et al. (2021), імовірнісні моделі безпеки PoS-протоколів — в праці Bespalov et al. (2025).

Невирішені частини проблеми такі. Межа 2^{-m} для вибірки з повторенням є консервативною для скінченного n і не враховує нерівномірного розподілу стейку, який у реальних мережах тяжіє до степеневого розподілу (Kwon et al., 2019; Clauset et al., 2009).

Бракує кількісного порівняння вибірки з рекурсивним доказом фінальності для ланцюгів з підписами Ed25519, яке враховувало б обсяг даних і повну вартість транзакції в Ethereum. Нарешті, не проаналізовано, як поводиться кожна стратегія, коли фактична частка зловмисного стейку перевищує проєктну.

Методологія дослідження

Модель системи і загроз

Розглядаємо епоху з n валідаторами (у NEAR — виробниками блоків) зі стейками $s_1, \ldots, s_n$, нормованими до одиниці. Легкий клієнт довіряє набору валідаторів поточної епохи, отриманому з контрольної точки, і приймає заголовок, якщо отримує сертифікат фінальності. Кроком синхронізації називаємо прийняття фінального заголовка нової епохи разом із переходом до наступного набору валідаторів. Ретрансляторам і доводжувачам клієнт не довіряє.

Супротивник контролює множину валідаторів A із сумарним стейком f, усіх ретрансляторів і канал до легкого клієнта, але ключів чесних валідаторів не має. Атака вдається, якщо клієнт прийняв заголовок, якого чесні валідатори не підписували. Ймовірність підробити підпис Ed25519 оцінюємо як 2^{-128} (Bernstein et al., 2012), а ймовірність порушити стійкість доказу — як $2^{-\lambda}$, де λ — стійкість системи доведення. Атаки зі старими ключами валідаторів, що вийшли з набору (Gaži et al., 2018), нейтралізують контрольні точки, тому до моделі їх не включено. Не включено також утримання даних і порушення безпеки самого консенсусу за $f \geq 1/3$: вони однаково зачіпають усі стратегії. Отже, модель стосується лише перевірки сертифіката легким клієнтом, а безпеку консенсусу (узгодженість і живучість ланцюга) приймає як припущення.

Стратегії перевірки

- **S1 — повна перевірка кворуму.** Для рівних стейків перевіряють $\lfloor 2n/3 \rfloor + 1$ підписів, як у "наївному" підході праці Bhatt et al. (2025); клієнт отримує також наступний набір валідаторів. Варіант **S1′** перевіряє наявні підписи в порядку спадання стейку, доки їхня сума не перевищить 2/3; стійкість S1′ така сама, як S1.
- **S2 — рекурсивний доказ фінальності.** Клієнт перевіряє один доказ того, що підписи і перехід набору валідаторів перевірено в схемі. Розмір доказу і час його перевірки взято з опублікованих вимірів (табл. 1). Порівнюється лише вартість перевірки доказу; витрати доводжувача на його побудову в модель не входять.
- **S3 — випадкова вибірка.** Ретранслятор заявляє множину підписантів з понад 2/3 стейку, клієнт перевіряє k випадково вибраних підписів. Розглянуто вибірку, зважену за стейком, без повернення і з поверненням, а також рівноймовірну вибірку без урахування стейку.
- **S4 — штатний легкий клієнт NEAR.** Структура LightClientBlockView містить заголовок, список next_bps наступних виробників блоків і масив approvals_after_next. Клієнт перевіряє всі наявні підписи, суму їхнього стейку (понад 2/3) і збіг SHA-256 (borsh(next_bps)) з полем next_bp_hash (NEAR Protocol, n.d.).

Модель безпеки

Для рівних стейків супротивник включає до заявленої множини всіх $a = \lfloor fn \rfloor$ своїх валідаторів і мінімальну кількість чесних, тож заявлена множина має $m = \lfloor 2n/3 \rfloor + 1$ елементів. Атака вдається, якщо всі k вибраних без повернення підписантів зловмисні:

$$P_{\mathrm{hyp}}(k) = \frac{\binom{a}{k}}{\binom{m}{k}}, \qquad P_{\mathrm{hyp}}(k) = 0 \ \text{ за } \ k > a. \tag{1}$$

Межа з повторенням, що відповідає аналізу Bhatt et al. (2025), дорівнює $(a/m)k \leq (3f/2)k$; вибірка без повернення не гірша за неї (Hoeffding, 1963).

Для зважених стейків супротивник обирає валідаторів, яких контролює, за однією з трьох стратегій: найбільші (компрометація великих операторів), найменші (розпорошення стейку) або

випадкові. Чесних валідаторів він дописує так, щоб їхній сумарний стейк H був мінімальним, але поріг 2/3 було перевищено. Зважену за стейком вибірку без повернення подаємо через незалежні експоненційні моменти $T_i \sim Exp(s_i)$: порядок їх настання збігається з порядком послідовної вибірки, пропорційної стейку (Efraimidis & Spirakis, 2006); відповідне інтегральне подання відоме для нецентрального гіпергеометричного розподілу Валеніуса (Fog, 2008). Мінімум моментів чесних валідаторів має розподіл Exp(*H*), тому

$$P_w(k) = \int_0^\infty H\ e^{-Ht}\ \Pr[N_A(t) \geq k]dt, \qquad N_A(t) = \sum_{i \in A} \mathbf{1}\{T_i \leq t\}, \tag{2}$$

де $N_A(t)$ – має пуассон-біноміальний розподіл з імовірностями $1 - exp(-s_i t)$.

Хвіст цього розподілу обчислюємо динамічним програмуванням одночасно для всіх *k*, а інтеграл — квадратурою на логарифмічній сітці з 3000 вузлів. Для рівних стейків формула (2) збігається з (1).

Якщо супротивник може відкинути *r* невигідних реалізацій випадковості (перебір, англ. grinding), ймовірність успіху зростає до

$$P_r(k) = 1 - (1 - P(k))^{r+1} \leq (r+1)\,P(k). \tag{3}$$

Розглянуто три режими: $r = 0$ — легкий клієнт використовує власну таємну випадковість після отримання заявки; $r = 2^{10}$ — публічна випадковість ланцюга з упередженістю, оціненою в праці Bhatt et al. (2025); $r = 2^{64}$ — неінтерактивна вибірка Фіата–Шаміра за обчислювального бюджету супротивника 2^{64} хешів.

Стійкість стратегій у бітах за $f < 2/3$ визначаємо так:

$$\lambda_{S1} = \lambda_{S4} = \lambda_{\mathrm{Ed}} = 128, \qquad \lambda_{S2} = \min(\lambda_{\mathrm{FRI}}, \lambda_H, \lambda_{\mathrm{Ed}}), \lambda_{S3}(k) = \min(\lambda_{\mathrm{Ed}}, -\log_2 P_r(k)); \tag{4}$$

за $f \geq 2/3$ підробка вдається за будь-якої стратегії. Для S2 взято $\lambda_{FRI} = 100$ і $\lambda_H \approx 95$ біт оціненої стійкості (Polygon Zero, n.d.); на рисунках показано верхнє значення 100 біт. Це оцінки окремих компонентів; стійкість стратегії за формулою (4) визначає найслабша складова, тож для S2 значення 100 біт на рисунках трохи завищене, а в Ethereum стійкість S2 додатково обмежує крива обгортки (див. “Обговорення”). Мінімальний розмір вибірки

$$k^*(\varepsilon) = \min\{k:\ P_r(k) \leq \varepsilon\}, \qquad \varepsilon \in \{2^{-40}, 2^{-64}, 2^{-80}, 2^{-100}, 2^{-128}\}. \tag{5}$$

Для проєктування беремо найбільше k^* серед стратегій розміщення зловмисного стейку. Тому найгірший випадок у результатах визначено лише серед трьох розглянутих способів розміщення, а не серед усіх можливих.

Модель вартості

Вартість кроку синхронізації описано трьома показниками. Обчислення перевірки виражено в тактах процесора: перевірка підпису Ed25519 коштує 273 364 такти окремо або 134 000 тактів на підпис у пакетному режимі (64 підписи) (Bernstein et al., 2012), хешування списку валідаторів — 15 тактів на байт (Kuznetsov et al., 2024a). Час перевірки доказу S2 переведено в такти за робочою частотою процесора стенда 4,7 ГГц: 4,0–5,1 мс відповідають 18,8–24,0 млн тактів, номінальні 4,5 мс — 21,2 млн (Kuznetsov et al., 2024b). У цій праці час перевірки наведено для компонентних доказів; для фінального агрегованого доказу прийнято той самий діапазон, що узгоджується з оцінкою близько 4 мс в анотації праці. На с. 102 тієї самої праці часом перевірки для легкого клієнта названо 0,47 с, але за с. 101 це тривалість кроку фінальної агрегації, тобто частина побудови доказу, тому в моделі це значення не використано. Такти Ed25519 і час перевірки доказу виміряно на різних процесорах, через це точки перетину за обчисленнями слід вважати модельними оцінками. Обсяг даних для S1 і для S3 із зобов’язанням набору валідаторів на основі дерева Меркла:

$$B_{S1} = B_h + \lceil n/8 \rceil + 64\,m + B_V(n), \quad B_{S3} = B_h + \lceil n/8 \rceil + k\,(113 + 32\lceil \log_2 n \rceil) + 32, \tag{6}$$

де B_h = 304 Б — поля LightClientBlockView без списків, $B_V(n)$ — серіалізований список валідаторів (ідентифікатор, ключ 33 Б, стейк 16 Б), 113 Б — підпис, ключ і стейк одного вибраного валідатора. Для S2 обсяг дорівнює розміру агрегованого доказу (180 112 Б) плюс 72 Б публічних входів; доказ лише компонента підписів (133 080 Б) не засвідчує переходу до наступного набору валідаторів і тому як S2 не розглядається. Поле next_bp_hash у NEAR є плоским хешем списку, а не коренем дерева Меркла, тому в чинному протоколі S3 мусить завантажувати повний next_bps; цей варіант розраховано окремо.

Газ транзакції Ethereum після оновлення Prague обчислюємо за спрощеною формулою EIP-7623 (без складника для створення контракту) (Wahrstätter & Buterin, 2024):

$$G_{tx}(d, e) = 21\,000 + \max(4\tau(d) + e,\ 10\,\tau(d)), \qquad \tau(d) = z + 4\,(d - z), \qquad (7)$$

де d – байти calldata (вхідних даних транзакції);
z – нульові байти (консервативно z = 0);
e – газ виконання.

Для S2 припущено обгортання доказу в Groth16 (Groth, 2016) над кривою BN254 з ℓ = 3 публічними входами. За EIP-1108 (Salazar Cardozo & Williamson, 2018) перевірка коштує 45 000 + 4·34 000 + ℓ·(6 000 + 150) газу, до чого додаються calldata обсягом 256 + 32ℓ Б і запис зобов'язання нового набору валідаторів у сховище (20 000 газу); разом 246 082 газу. Така обгортка потребує довіреного налаштування параметрів, а її криптографічний рівень обмежує крива BN254 (див. "Обговорення"). Як верхню оцінку взято 0,94 млн газу для перевірки доказу UltraPLONK (Bhatt et al., 2025) з тим самим записом у сховище. Для S1 calldata містить заголовок, бітову карту, $\lfloor 2n/3 \rfloor + 1$ підписів, а також поточний і наступний набори валідаторів по 48 Б на валідатора, бо контракт зберігає лише їхні хеші. За n = 100 це 14 205 Б, тож за формулою (7) діє нижня межа EIP-7623: 21 000 + 10·4·14 205 = 589 200 газу. Для S3 враховано дві транзакції (заявка і відповідь), відкриття шляхів у дереві Меркла через KECCAK256 (30 газу плюс 6 на слово) і два записи стану заявки у сховище по 20 000 газу (Ethereum Foundation, n.d.); як і для S1 та S2, у другій транзакції враховано запис зобов'язання нового набору валідаторів. Вартість перевірки одного підпису Ed25519 в EVM G_{Ed} у первинних джерелах не наведено, тому її задано сценаріями: 2 000 газу (ціна, запропонована в EIP-665), 3 000 (як для ecrecover), 10^5 і 10^6 газу (виконання байт-кодом). Обчислено також граничне значення G_{Ed}, за якого стратегії коштують однаково.

Точка перетину n^* – найменше n, за якого вартість однієї стратегії перевищує вартість іншої.

Параметри і процедура

Вхідні параметри наведено в табл. 1. Знімок NEAR отримано 04.10.2026 через публічний інтерфейс віддаленого виклику процедур (RPC): EXPERIMENTAL_protocol_config (epoch_length = 43 200 блоків, num_block_producer_seats = 100) і next_light_client_block для блоку 218 416 559 та попередньої епохи (стейки ста виробників блоків і наявність їхніх підписів).

Таблиця 1. Вхідні параметри моделі

Параметр	Значення	Джерело
Розмір доказу фінальності S2	180 112 Б (агрегований доказ; доказ компонента підписів — 133 080 Б)	Kuznetsov et al. (2024b), с. 94, 100–101
Час перевірки доказу S2	4,0–5,1 мс (компонентні докази; номінально 4,5 мс)	Kuznetsov et al. (2024b), с. 94, 100–101
Частота процесора стенда	4,7 ГГц (базова 4,5 ГГц, максимальна 5,7 ГГц)	Kuznetsov et al. (2024b), с. 99

Параметр	Значення	Джерело
Перевірка рекурсивного доказу (Ryzen 7)	5,5–7,0 мс	Kuznetsov et al. (2024a), с. 275, табл. 4
Перевірка Ed25519	273 364 такти; до 134 000 у пакеті з 64	Bernstein et al. (2012), с. 78
Стійкість Ed25519 / S2	128 біт / 100 біт (FRI), ≈95 біт (Poseidon)	Bernstein et al. (2012); Polygon Zero (n.d.)
Розміри підпису і ключа	64 Б / 32 Б	Josefsson & Liusvaara (2017)
Газ: база; calldata; BN254; KECCAK256; запис	21 000; 4/10 на токен; 150 / 6 000 / 45 000 + 34 000·k; 30 + 6; 20 000	Wahrstätter & Buterin (2024); Salazar Cardozo & Williamson (2018); Ethereum Foundation (n.d.)
Газ перевірки Ed25519 G_{Ed}	2 000 (EIP-665, не впроваджено) … 10^6	припущення, аналіз чутливості
Перебір випадковості r	0; 2^{10}; 2^{64}	припущення за Bhatt et al. (2025)
Розподіли стейку	рівні; Ципф α = 0,5; 1,0; Парето ξ = 1,2; 2,0; знімок NEAR	припущення, аналіз чутливості

Джерело: складено автором (results/T0_parameters.csv).

Усі таблиці й рисунки генерує один скрипт finality_model.py (Python 3.11, numpy, scipy, pandas, matplotlib; початкове значення генератора випадкових чисел 20261004). Інтеграл (2) перевірено двома способами. Для рівних стейків він збігається з формулою (1) до третього знака в $\log_2 P$. Для чотирьох розподілів і двох стратегій супротивника 28 значень порівняно з методом Монте-Карло ($4 \cdot 10^5$ повторень на точку, ключі $-\ln U/s_i$): жодне відхилення не перевищує 2,4 стандартної похибки, 25 із 28 лежать у межах 95-відсоткового довірчого інтервалу. За такої кількості повторень метод Монте-Карло перевіряє лише ймовірності, не менші приблизно за 10^{-4}; для глибших хвостів правильність обчислень спирається на збіг із формулою (1) і точність інтегрування.

Результати дослідження

Розмір вибірки для рівних стейків

Мінімальний розмір вибірки для $f = 1/3$ наведено в табл. 2. За скінченного n вибірка без повернення потребує менше підписів, ніж межа з повторенням: для $n = 100$ рівень 2^{-40} досягається за 27 підписів, а з 34 підписів атака стає неможливою, бо серед 33 зловмисних валідаторів не можна вибрати 34 різних (рис. 1, а). Для $n = 1000$ рівню 2^{-80} відповідають 74 підписи проти 80 за межею з повторенням, для $n = 10\,000$ різниця зникає. Перебір випадковості за $f = 1/3$ додає близько $\log_2(r + 1)$ підписів: 8–10 для $r = 2^{10}$ і 45–63 для $r = 2^{64}$ (за $n \geq 1000$).

Таблиця 2. Мінімальний розмір вибірки $k^*(\varepsilon)$ для рівних стейків, $f = 1/3$

n	r	2^{-40}	2^{-64}	2^{-80}	2^{-100}	2^{-128}
100	0	27	34	34	34	34
100	2^{10}	30	34	34	34	34
1000	0	39	60	74	90	112
1000	2^{10}	48	69	82	98	120
1000	2^{64}	93	112	124	138	157
10 000	0	40	64	80	99	127
10 000	2^{64}	103	127	142	162	189
∞ (з повторенням)	0	40	64	80	100	128

Примітка: для n = 100 значення 34 означає детерміновану перевірку (k = a + 1). Джерело: розраховано автором (results/T1_kstar_equal_stake.csv).

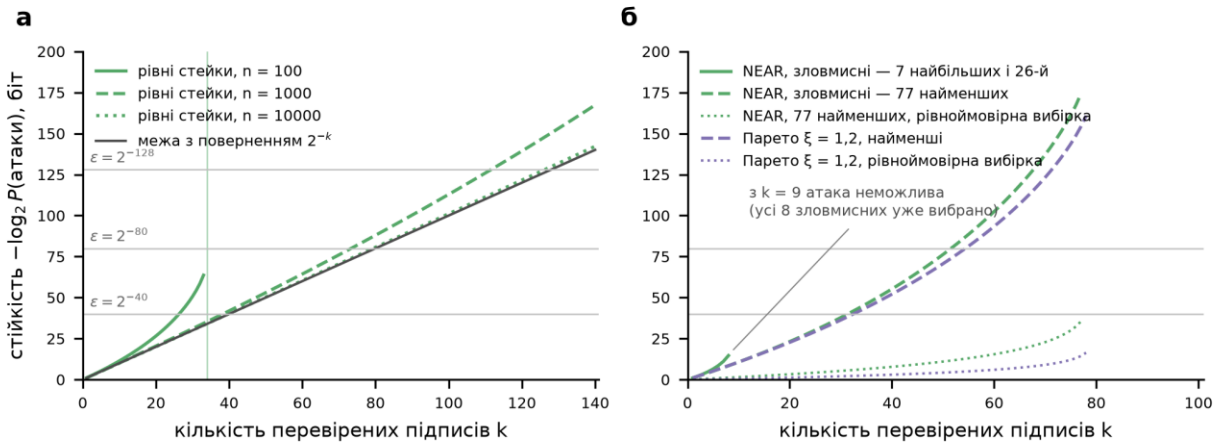


Рисунок 1. Стійкість вибіркової перевірки залежно від кількості перевірених підписів:
а — рівні стейки (*n* = 100, 1000, 10 000) і межа з повторенням;
б — зважені стейки (знімок NEAR і розподіл Парето) за різного розміщення зловмисного стейку.

Джерело: розраховано автором.

Зважені стейки і знімок NEAR

У знімку NEAR вісім найбільших виробників блоків володіють понад третиною стейку, а 23 — понад двома третинами; частка найбільшого становить 6,3 %, десяти найбільших — 41,7 %, коефіцієнт Джині дорівнює 0,57. На момент знімка 71 зі 100 слотів approvals_after_next містили підпис, що відповідає 76,8 % стейку. Тому за $f = 1/3$ супротивник може контролювати сім найбільших валідаторів і ще одного, 26-го за стейком (разом 33,3 % стейку). У цьому разі зважена вибірка стає детермінованою вже з дев'яти підписів (рис. 1, б). Найгірший для захисника з розглянутих сценаріїв — розпорошення третини стейку на 77 найменших валідаторів: тоді для рівня 2^{-80} треба перевірити 52 підписи, вибрані зважено без повернення. Рівноймовірна вибірка без урахування стейку потребує 78 підписів, тобто фактично перевірки всієї зловмисної частини (табл. 3, рис. 2). Знімок відображає розподіл стейку на одну дату; для інших епох розрахунок треба повторити на новому знімку.

Для степеневих розподілів картина подібна: найгірші значення $k^*(2^{-80})$ для зваженої вибірки становлять 48–55 за $n = 100$ і 76–77 за $n = 1000$, тоді як рівноймовірна вибірка за $n = 1000$ потребує 829–918 підписів. Отже, вибірка без урахування стейку для мереж з нерівномірним стейком непридатна. Водночас S1′ потребує лише 18–22 підписів для розподілів з $\alpha = 1{,}0$ і $\xi = 1{,}2$ за $n = 100$ і 23 підписів для повного набору NEAR (34 — з урахуванням лише фактично наявних підписів), забезпечуючи 128 біт. Для тисячі валідаторів співвідношення протилежне: S1′ потребує 83–166 підписів, тобто більше, ніж зважена вибірка для рівня 2^{-80} (76–77).

Таблиця 3. Проєктне (найгірше) $k^*(\varepsilon)$ для зважених стейків і розмір мінімального кворуму S1′, $f = 1/3$, $r = 0$

Розподіл	S1′, підписів	Зважена без повернення, 2^{-40} / 2^{-80}	Рівноймовірна, 2^{-40} / 2^{-80}	З повторенням, 2^{-40} / 2^{-80}
Рівні, $n = 100$	67	27 / 34	27 / 34	40 / 80
NEAR, знімок, $n = 100$	23	32 / 52	78 / 78	40 / 80
Ципф $\alpha = 1{,}0$, $n = 100$	18	32 / 54	83 / 83	40 / 80
Парето $\xi = 1{,}2$, $n = 100$	22	33 / 55	79 / 79	40 / 80

Розподіл	S1′, підписів	Зважена без повернення, 2^{-40} / 2^{-80}	Рівноймовірна, 2^{-40} / 2^{-80}	З повторенням, 2^{-40} / 2^{-80}
Ципф α = 1,0, *n* = 1000	83	39 / 76	904 / 918	40 / 80
Парето ξ = 1,2, *n* = 1000	166	40 / 77	742 / 829	40 / 80

Джерело: розраховано автором (results/T2b_design_kstar.csv).

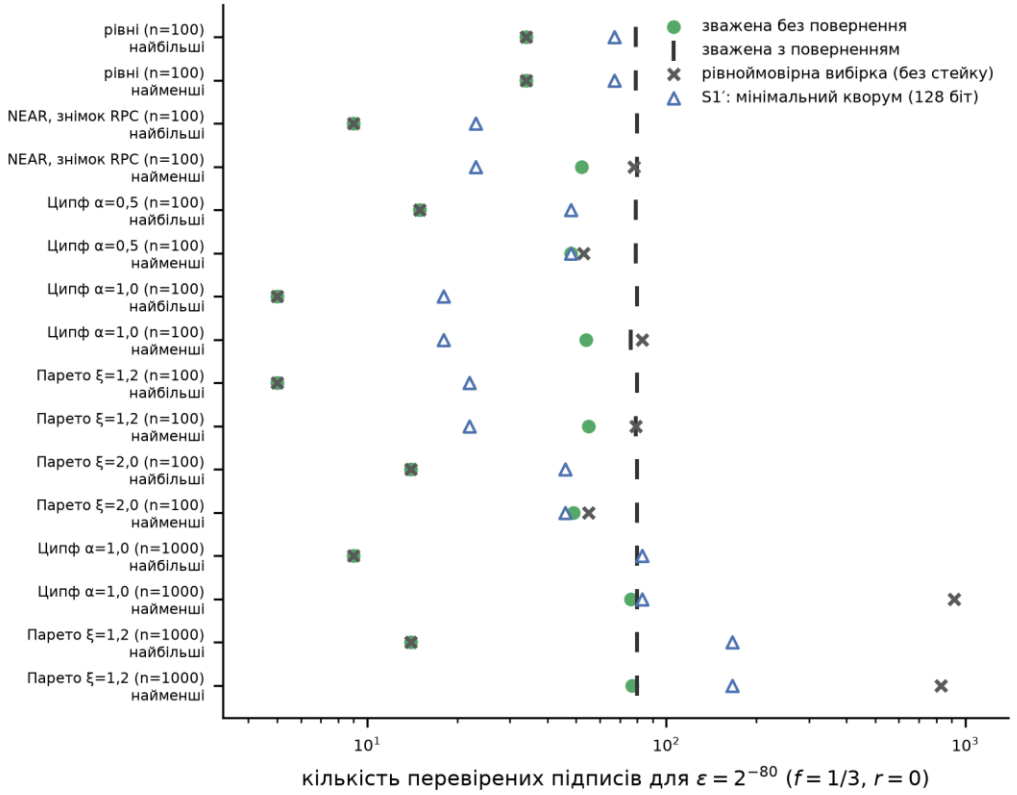


Рисунок 2. Кількість перевірених підписів для рівня 2^{-80} за різних розподілів стейку, стратегій розміщення зловмисного стейку і схем вибірки; трикутник — мінімальний за стейком кворум S1′ зі стійкістю 128 біт. Джерело: розраховано автором.

Вартість кроку синхронізації для NEAR

Стратегії для *n* = 100 і знімка стейків NEAR зіставлено в табл. 4 і на рис. 3. Доказ S2 за обчисленнями (18,8–24,0 млн тактів) того самого порядку, що S1 (18,4 млн) і S4 (19,5 млн). За обсягом даних він у 14 разів більший за модельне двійкове подання S4 (12,5 КБ) і майже в 7 разів — за фактичну відповідь RPC у форматі JSON (JavaScript Object Notation) (26,6 КБ). S3 із зобов'язанням на основі дерева Меркла за рівня 2^{-80} потребує 17,9 КБ, тобто більше, ніж S1, бо кожен вибраний підпис супроводжує шлях у дереві Меркла із семи хешів. Найдешевшою стратегією зі стійкістю 128 біт є S1′: 34 підписи, 9,4 млн тактів, 10,1 КБ.

Таблиця 4. Вартість одного кроку синхронізації, NEAR, *n* = 100

Стратегія	Підписів	Обсяг, Б	Обчислення, млн тактів	Стійкість, біт	Газ EVM
S1 повна перевірка кворуму	67	12 013	18,4 (9,1 у пакеті)	128	589 200 (*G*_Ed = 2 000)
S1′ мінімальний кворум за стейком	34	10 088	9,4	128	—
S4 штатний легкий клієнт	71	12 493 (JSON 26 583)	19,5	128	—

Стратегія	Підписів	Обсяг, Б	Обчислення, млн тактів	Стійкість, біт	Газ EVM
S2 рекурсивний доказ	0	180 184	18,8–24,0 (номінально 21,2)	95–100	246 082 (Groth16) … 963 720
S3, 2^{-40}	32	11 133 (9 867)	9,0	40	524 864 (*G*_Ed = 2 000)
S3, 2^{-80}	52	17 873 (11 167)	14,6	80	793 664 (*G*_Ed = 2 000)
S3, 2^{-100}	60	20 569 (11 687)	16,8	100	—

Примітка: для S3 взято найгірше розміщення зловмисного стейку; у дужках — варіант без зобов'язання на основі дерева Меркла, коли клієнт завантажує повний next_bps. Для S1 кількість підписів 67 = ⌊2n/3⌋ + 1 відповідає моделі рівних стейків. Газ для S1, S2 і S3 враховує запис зобов'язання нового набору валідаторів у сховище (20 000 газу); для S1 діє нижня межа EIP-7623 (*calldata 14 205 Б).*

Джерело: розраховано автором (results/T4_costs_NEAR_n100.csv).

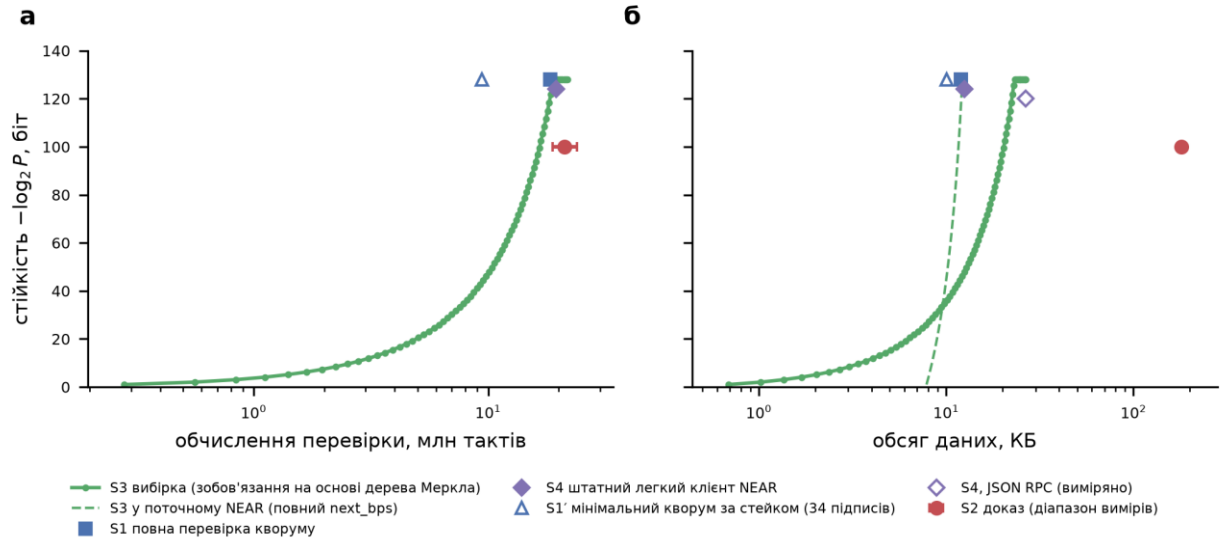


Рисунок 3. Межа Парето "вартість — стійкість" для NEAR, *n* = 100:
а — обчислення перевірки;
б — обсяг даних.
На панелі а відрізок для S2 охоплює діапазон опублікованих вимірів часу перевірки.
Джерело: розраховано автором.

Точки перетину за кількістю валідаторів

Вартість S1 зростає лінійно з *n*, вартість S2 від *n* не залежить, а вартість S3 зростає лише до насичення $k^*(\varepsilon)$ (рис. 4, табл. 5). За обчисленнями (модельна оцінка) S2 стає дешевшою за S1 з n^* = 103–133 для окремих перевірок і з n^* = 211–265 для пакетної. За обсягом даних n^* = 1569. S3 за обсягом даних дешевша за S2 в усьому діапазоні до 10^5 валідаторів навіть за $r = 2^{64}$. За обчисленнями на рівні 2^{-80} S3 порівняння з S2: 21–24 млн тактів проти 18,8–24,0 млн. Якщо ж $r = 2^{64}$, S2 стає дешевшою з n^* = 201–284.

В Ethereum співвідношення інше. Обгорнутий доказ коштує 246 082 газу, тоді як пряма перевірка доказу Plonky2 лише за calldata коштувала б близько 7,2 млн газу (180 112 Б за ціною 10 газу на токен). Навіть якби для Ed25519 існував прекомпільований контракт за 2 000–3 000 газу, S1 залишалася б дешевшою за обгорнутий S2 лише до *n* = 38, а S3 (2^{-80}, $r = 2^{10}$) — до *n* = 35. Відносно оцінки рівня UltraPLONK ці межі становлять 170 і 219. За *n* = 1000 S3 коштує 1,51 млн

газу навіть за безкоштовної перевірки підпису, бо дві транзакції, calldata і шляхи в дереві Меркла 82 вибраних валідаторів дорожчі за перевірку доказу, вартість якої від *n* не залежить.

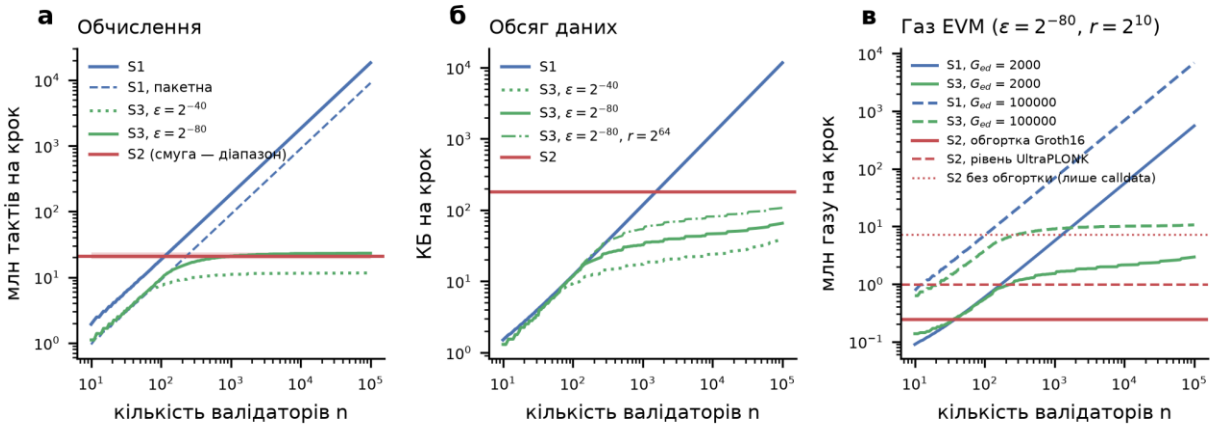


Рисунок 4. Вартість кроку синхронізації залежно від кількості валідаторів (f = 1/3): а — обчислення; б — обсяг даних; в — газ Ethereum.

Джерело: розраховано автором.

Таблиця 5. Точки перетину n^* (найменше n, з якого перша стратегія дорожча за другу)

Показник	Пара стратегій	n^*
Обчислення	S1 / S2	103–133 (пакетна S1: 211–265)
Обчислення	S3 (2^{-80}, $r = 2^{64}$) / S2	201–284
Обсяг даних	S1 / S2	1569
Обсяг даних	S3 / S2	не досягається до 10^5
Газ, G_Ed = 2 000–3 000	S1 / S2 (Groth16; UltraPLONK)	39; 171
Газ, G_Ed = 2 000–3 000	S3 / S2 (Groth16; UltraPLONK)	36; 220
Газ, G_Ed ≥ 10^5	S1 і S3 / S2	≤ 10–21

Джерело: розраховано автором (results/T5_crossovers.csv, results/T6_Ged_breakeven.csv).

Оптимальна стратегія на площині (*n*, *f*)

На рис. 5 показано найдешевшу стратегію, що забезпечує рівень 2^{-80}, залежно від n і проєктної частки зловмисного стейку f для рівних стейків. За обчисленнями і за $f \le 1/3$ S3 оптимальна в 97,9 % клітинок, S2 — у решті (великі n поблизу f = 1/3); за більших f S2 займає область від $n \approx 100$–1000. За обсягом даних і $f \le 1/3$ S3 оптимальна завжди, а S2 — лише за $n \gtrsim 1600$ і $f \gtrsim 0{,}54$. В Ethereum за G_{Ed} = 2 000 S2 оптимальна у 81 % клітинок, за $G_{Ed} = 10^5$ — в усіх.

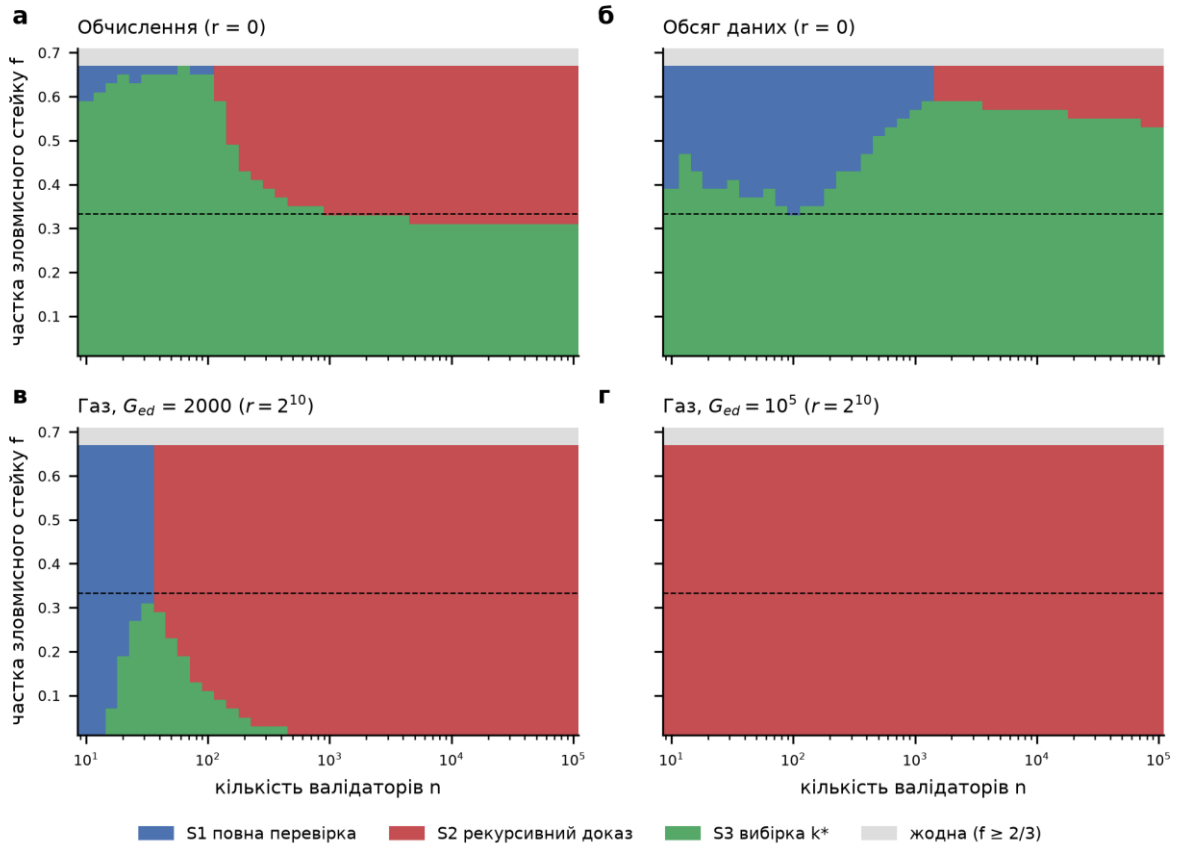


Рисунок 5. Оптимальна стратегія для рівня 2^{-80} на площині (n, f):
а — обчислення; б — обсяг даних; в, г — газ Ethereum за двох значень вартості перевірки Ed25519; штрихова лінія — f = 1/3.

Джерело: розраховано автором.

Чутливість до недооцінки частки зловмисного стейку

Розмір вибірки k^* швидко зростає з f: для n = 1000 і рівня 2^{-80} він дорівнює 74 за f = 1/3 і наближається до повного кворуму 667 поблизу f = 2/3 (рис. 6, а). Якщо k підібрано для f = 1/3, а фактична частка більша, стійкість S3 падає: за f = 0,40 — до 42–59 біт, за f = 0,50 — до 21–33 біт, за f = 0,60 — до 8–12 біт (рис. 6, б). Стійкість S1, S2 і S4 щодо підробки сертифіката за $f < 2/3$ від f не залежить.

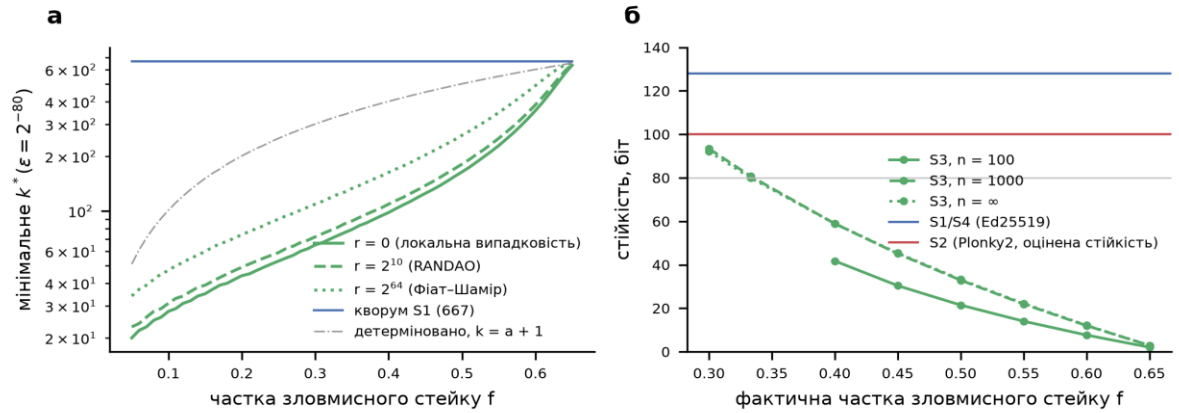


Рисунок 6. Чутливість вибіркової перевірки: а — мінімальний розмір вибірки для рівня 2^{-80} залежно від f і перебору випадковості (n = 1000); б — фактична стійкість, якщо k підібрано для f = 1/3.

Джерело: розраховано автором.

Обговорення

Отримані результати узгоджуються з висновком Bhatt et al. (2025), що вибірка суттєво дешевша за повну перевірку: за $n = 1000$ і рівня 2^{-80} вона скорочує кількість перевірок з 667 до 74–82. Відмінностей дві. По-перше, точна модель без повернення і зважена за стейком схема дають менші k^* для малих n, але для ста валідаторів із концентрованим стейком детермінований мінімальний кворум S1′ дешевший за вибірку вже з рівня 2^{-64}. Цієї альтернативи Bhatt et al. не розглядали: вони аналізували валідаторів Polkadot з однаковим стейком. По-друге, висновок цих авторів про перевагу вибірки над SNARK за газом отримано для ECDSA з прекомпільованим ecrecover і без урахування calldata та відкриттів шляхів у дереві Меркла. Для ланцюгів з підписами Ed25519 повна вартість транзакції змінює висновок: обгорнутий доказ дешевший за вибірку вже з кількох десятків валідаторів.

Щодо zkBridge (Xie et al., 2022) і Succinct Labs (2024) модель кількісно підтверджує доцільність стислих доказів для перевірки в Ethereum і уточнює її межу. Перевага S2 за газом виникає лише після обгортання в доказ із перевіркою білінійного спарювання: пряма передача доказу обсягом 180 КБ коштує близько 7,2 млн газу. Guppy (Danezis et al., 2026) виносить перевірку підписів за межі схеми, щоб зменшити витрати доводжувача; вартість для перевіряльника в моделі цієї статті від цього не змінюється, тож підходи доповнюють один одного, а порівняння витрат доводжувача потребує окремого дослідження. Розробки Electron Labs (2022) засвідчують, що перевірку Ed25519 у схемі для легкого клієнта NEAR пропонували ще 2022 року. Внесок цієї статті — не сама конструкція S2, а умови її застосовності.

З погляду безпеки головне таке. Щодо підробки сертифіката, тобто заголовка, якого не підписав жоден чесний валідатор, S1 і S2 зберігають стійкість за будь-якої частки зловмисного стейку, меншої за 2/3. Гарантія S3 натомість залежить від проєктної оцінки f. Помилка в цій оцінці, наприклад через непомічену концентрацію стейку або підкуп частини валідаторів, перетворює 80-бітну гарантію вибірки на 21–33 біти. Безпеки самого консенсусу за $f \geq 1/3$ не гарантує жодна стратегія.

Водночас S2 має нижчий криптографічний рівень, ніж S1: 95–100 біт оціненої стійкості за прийнятих параметрів проти 128 біт Ed25519. До того ж реалізація схеми додає власну поверхню атаки (Chaliasos et al., 2024). У Ethereum рівень S2 обмежує ще й обгортка. Стійкість кривої BN254 після вдосконалення алгоритмів решета числового поля нижча за 128 біт (Barbulescu & Duquesne, 2019); автори EIP-2537 оцінюють її у 80 біт (Vlasov et al., 2020). Groth16, крім того, потребує довіреного налаштування параметрів (Groth, 2016), і компрометація цього налаштування дає змогу підробляти докази. З оновлення Prague Ethereum має прекомпільовані контракти для кривої BLS12-381 з рівнем понад 120 біт (Vlasov et al., 2020). Обгортка над цією кривою усуває обмеження BN254, але її вартості ця модель не оцінює. Отже, доказова фінальність рівноцінна повній перевірці щодо порогу 2/3, проте не щодо криптографічного рівня, доки параметри FRI, хеш-функції та кривої обгортки не підібрано під 128 біт.

Умови застосовності доказової фінальності. За результатами моделі рекурсивний доказ виправданий, якщо виконується хоча б одна з умов: (1) перевірка відбувається в середовищі без дешевої перевірки Ed25519, насамперед в EVM, і доказ обгорнуто в систему з перевіркою білінійного спарювання; (2) кількість підписантів перевищує приблизно 1600 за обсягом даних або 100–270 за обчисленнями; (3) потрібна стійкість до f, вищої за 1/3, без лінійного зростання вартості. Для штатного легкого клієнта NEAR із нинішніми ста виробниками блоків доказ на один крок синхронізації не дає виграшу ні за обчисленнями, ні за обсягом даних; його можливі переваги за тривалих перерв у синхронізації ця модель не охоплює.

Рекомендації операторам. Легким клієнтам на пристроях за концентрованого стейку доцільно перевіряти підписи в порядку спадання стейку до перевищення 2/3 (S1′): це не змінює протоколу і зберігає 128 біт. Вибірку варто застосовувати лише із зважуванням за стейком,

таємною випадковістю клієнта ($r = 0$) і консервативною проєктною оцінкою f; неінтерактивна вибірка за $r = 2^{64}$ потребує в 1,4–2,6 раза більше підписів. Мостам в Ethereum, що обслуговують ланцюги з підписами Ed25519 і мають $n \geq 39$ валідаторів, доцільно використовувати обгорнутий доказ фінальності, віддаючи перевагу кривій BLS12-381 перед BN254, а вибірку розглядати лише за наявності прекомпільованого контракту для Ed25519. Для NEAR передумовою вибіркової перевірки без завантаження повного списку валідаторів був би перехід від плоского хешу next_bp_hash до кореня дерева Меркла.

Обмеження. Такти Ed25519 виміряно на процесорах Nehalem/Westmere, а час перевірки доказу — на Ryzen 9 7950X. Сучасні ядра перевіряють Ed25519 за меншу кількість тактів, тому наведені точки перетину за обчисленнями слід розглядати як модельні оцінки, зміщені на користь S2: на однаковому обладнанні перевага доказу настала б за більшої кількості валідаторів. Модель газу S2 спирається на припущення про обгортання доказу і не враховує вартості побудови обгортки. Побудова доказу у вимірах Kuznetsov et al. (2024b) тривала 13–18 хв на блок, тож для мостів, яким потрібна фінальність кожного блоку, S2 додає затримку, якої модель не враховує. Бібліотеку Plonky2 її розробники позначили як застарілу (Polygon Zero, n.d.), тому для нових реалізацій параметри доказу слід виміряти заново. Розподіли стейку, крім знімка NEAR, параметричні, а сам знімок відображає один момент часу. Модель охоплює один крок синхронізації і не розглядає накопичення витрат за тривалу відсутність зв'язку та атаки на доступність даних.

Висновки

Побудовано відтворювану ймовірнісно-вартісну модель чотирьох стратегій перевірки фінальності для легких клієнтів PoS-ланцюгів з підписами Ed25519. Модель поєднує точне інтегральне подання зваженої за стейком вибірки без повернення, перевірене методом Монте-Карло, з аналітичною оцінкою обчислень, обсягу даних і газу Ethereum.

Для рівних стейків і $f = 1/3$ рівню 2^{-80} відповідає 34 перевірки за $n = 100$ (детерміновано) і 74 — за $n = 1000$. Перебір випадковості додає 8–10 перевірок за $r = 2^{10}$ і до 63 — за $r = 2^{64}$.

Для знімка NEAR від 4 жовтня 2026 року (100 виробників блоків, коефіцієнт Джині 0,57) найгірше з розглянутих розміщень зловмисного стейку вимагає перевірити 52 підписи у зваженій вибірці для рівня 2^{-80}, тоді як мінімальний за стейком кворум дає 128 біт за 34 перевірки. Вибірка без урахування стейку для таких мереж непридатна.

Перевірка рекурсивного доказу фінальності на один крок синхронізації дешевша за повну перевірку підписів за обчисленнями зі 103–133 валідаторів, за обсягом даних — з 1569, в Ethereum після обгортання в Groth16 — з 39. Для штатного клієнта NEAR за нинішніх параметрів виграшу немає.

Вибірка втрачає більшу частину гарантій, якщо частку зловмисного стейку недооцінено: за $f = 0{,}5$ стійкість падає з 80 до 21–33 біт. Доказова фінальність стійка до такої помилки, але її криптографічний рівень за стандартної конфігурації (95–100 біт) нижчий за 128 біт повної перевірки, а в Ethereum його додатково обмежує крива обгортки.

Перспективи подальших досліджень — урахування накопичення витрат за багато епох і агрегації доказів, моделювання затримки доводжувача, підбір параметрів FRI для 128-бітної доведеної стійкості та аналіз динаміки концентрації стейку NEAR за тривалий період.

Фінансування

Це дослідження не отримало зовнішнього фінансування.

Конкуруючі інтереси

Автор є співавтором праць Kuznetsov et al. [30, 31], виконаних у компанії Zpoken OÜ, виміри з яких використано як вхідні параметри моделі. Інших конфліктів інтересів автор не має.

Використання штучного інтелекту

Під час підготовки рукопису автор використовував мовну модель Claude Opus 5.5 (Anthropic) лише для мовного редагування тексту. Ідея, модель, програмний код, розрахунки й висновки належать автору, який несе повну відповідальність за зміст рукопису.

Доступність даних і коду

Скрипт finality_model.py, перелік версій бібліотек (requirements.txt), вхідні знімки NEAR RPC від 04.10.2026 (data/*.json), вхідні параметри моделі з посиланнями на джерела (results/T0_parameters.csv), таблиці результатів (results/T1–T8) і рисунки відтворюються однією командою python finality_model.py (початкове значення генератора випадкових чисел 20261004, тривалість близько двох хвилин). Матеріали розміщено у відкритому репозиторії https://github.com/Valentine1898/finality-verification-model.

Список використаних джерел

1. Agrawal S., Neu J., Tas E. N., Zindros D. Proofs of proof-of-stake with sublinear complexity. 5th Conference on Advances in Financial Technologies (AFT 2023). 2023. Vol. 282. P. 14:1–14:24. DOI: https://doi.org/10.4230/LIPIcs.AFT.2023.14.
2. Alpturer K., Weinberg S. M. Optimal RANDAO manipulation in Ethereum. 6th Conference on Advances in Financial Technologies (AFT 2024). 2024. Vol. 316. P. 10:1–10:21. DOI: https://doi.org/10.4230/LIPIcs.AFT.2024.10.
3. Armknecht F., Karame G., Mohamed M., Weis C. Practical light clients for committee-based blockchains. 2024 Annual Computer Security Applications Conference (ACSAC). IEEE, 2024. P. 473–487. DOI: https://doi.org/10.1109/ACSAC63791.2024.00049.
4. Augusto A., Belchior R., Correia M., Vasconcelos A., Zhang L., Hardjono T. SoK: Security and privacy of blockchain interoperability. 2024 IEEE Symposium on Security and Privacy (SP). IEEE, 2024. P. 3840–3865. DOI: https://doi.org/10.1109/SP54263.2024.00255.
5. Barbulescu R., Duquesne S. Updating key size estimations for pairings. Journal of Cryptology. 2019. Vol. 32, No. 4. P. 1298–1336. DOI: https://doi.org/10.1007/s00145-018-9280-5.
6. Bariant A., Bouvier C., Leurent G., Perrin L. Algebraic attacks against some arithmetization-oriented primitives. IACR Transactions on Symmetric Cryptology. 2022. No. 3. P. 73–101. DOI: https://doi.org/10.46586/tosc.v2022.i3.73-101.
7. Ben-Sasson E., Carmon D., Haböck U., Kopparty S., Saraf S. On proximity gaps of Reed–Solomon codes. Proceedings of the 58th Annual ACM Symposium on Theory of Computing. ACM, 2026. P. 1157–1167. DOI: https://doi.org/10.1145/3798129.3800827.
8. Bernstein D. J., Duif N., Lange T., Schwabe P., Yang B.-Y. High-speed high-security signatures. Journal of Cryptographic Engineering. 2012. Vol. 2, No. 2. P. 77–89. DOI: https://doi.org/10.1007/s13389-012-0027-1.
9. Bespalov Y., Kovalchuk L., Nelasa H., Oliynykov R. Binomial distribution with delay in analysis and parametrization of Ouroboros Praos proof of stake blockchain protocol. Probability in the Engineering and Informational Sciences. 2025. Vol. 39, No. 4. P. 520–550. DOI: https://doi.org/10.1017/S0269964825000014.
10. Bhatt B. N., Shirazi F., Stewart A. Trustless bridges via random sampling light clients. 7th Conference on Advances in Financial Technologies (AFT 2025). 2025. Vol. 354. P. 31:1–31:24. DOI: https://doi.org/10.4230/LIPIcs.AFT.2025.31.
11. Block A. R., Garreta A., Katz J., Thaler J., Tiwari P. R., Zając M. Fiat–Shamir security of FRI and related SNARKs. Advances in Cryptology – ASIACRYPT 2023. Lecture Notes in Computer Science. Springer, 2023. Vol. 14439. P. 3–40. DOI: https://doi.org/10.1007/978-981-99-8724-5_1.

12. Bünz B., Kiffer L., Luu L., Zamani M. FlyClient: Super-light clients for cryptocurrencies. 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020. P. 928–946. DOI: https://doi.org/10.1109/SP40000.2020.00049.
13. Chaliasos S., Ernstberger J., Theodore D., Wong D., Jahanara M., Livshits B. SoK: What don't we know? Understanding security vulnerabilities in SNARKs. 33rd USENIX Security Symposium (USENIX Security 24). USENIX Association, 2024. P. 3855–3872. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/chaliasos.
14. Chalkias K., Garillot F., Nikolaenko V. Taming the many EdDSAs. Security Standardisation Research (SSR 2020). Lecture Notes in Computer Science. Springer, 2020. Vol. 12529. P. 67–90. DOI: https://doi.org/10.1007/978-3-030-64357-7_4.
15. Chatzigiannis P., Baldimtsi F., Chalkias K. SoK: Blockchain light clients. Financial Cryptography and Data Security (FC 2022). Lecture Notes in Computer Science. Springer, 2022. Vol. 13411. P. 615–641. DOI: https://doi.org/10.1007/978-3-031-18283-9_31.
16. Ciobotaru O., Shirazi F., Stewart A., Vasilyev S. Accountable light client systems for proof-of-stake blockchains. Cryptology ePrint Archive. 2022. Paper 2022/1205. URL: https://eprint.iacr.org/2022/1205.
17. Clauset A., Shalizi C. R., Newman M. E. J. Power-law distributions in empirical data. SIAM Review. 2009. Vol. 51, No. 4. P. 661–703. DOI: https://doi.org/10.1137/070710111.
18. Danezis G., Maram D., Roy A., Sonnino A., Wüst K. Guppy: Efficient light clients via recursive zero-knowledge proofs. arXiv. 2026. arXiv:2609.07963. DOI: https://doi.org/10.48550/arXiv.2609.07963.
19. Efraimidis P. S., Spirakis P. G. Weighted random sampling with a reservoir. Information Processing Letters. 2006. Vol. 97, No. 5. P. 181–185. DOI: https://doi.org/10.1016/j.ipl.2005.11.003.
20. Electron Labs. [PROPOSAL] Audit for Circom-Ed25519 for standardization of NEAR ZK light client. NEAR NEPs. 2022. Issue 440. GitHub. URL: https://github.com/near/NEPs/issues/440.
21. Ethereum Foundation. Ethereum execution layer specifications: Prague fork, vm/gas.py : computer software. GitHub. URL: https://github.com/ethereum/execution-specs/blob/master/src/ethereum/forks/prague/vm/gas.py (дата звернення: 04.09.2026).
22. Federal Bureau of Investigation. FBI statement on attribution of malicious cyber activity posed by the Democratic People's Republic of Korea : press release. 14 April 2022. URL: https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea.
23. Fog A. Calculation methods for Wallenius' noncentral hypergeometric distribution. Communications in Statistics – Simulation and Computation. 2008. Vol. 37, No. 2. P. 258–273. DOI: https://doi.org/10.1080/03610910701790269.
24. Gaži P., Kiayias A., Russell A. Stake-bleeding attacks on proof-of-stake blockchains. 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, 2018. P. 85–92. DOI: https://doi.org/10.1109/CVCBT.2018.00015.
25. Groth J. On the size of pairing-based non-interactive arguments. Advances in Cryptology – EUROCRYPT 2016. Lecture Notes in Computer Science. Springer, 2016. Vol. 9666. P. 305–326. DOI: https://doi.org/10.1007/978-3-662-49896-5_11.
26. Hoeffding W. Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association. 1963. Vol. 58, No. 301. P. 13–30. DOI: https://doi.org/10.1080/01621459.1963.10500830.
27. Josefsson S., Liusvaara I. Edwards-curve digital signature algorithm (EdDSA). RFC 8032. Internet Research Task Force, 2017. DOI: https://doi.org/10.17487/RFC8032.

28. Khovratovich D., Rothblum R. D., Soukhanov L. How to prove false statements: Practical attacks on Fiat–Shamir. Advances in Cryptology – CRYPTO 2025. Lecture Notes in Computer Science. Springer, 2025. Vol. 16005. P. 3–26. DOI: https://doi.org/10.1007/978-3-032-01887-8_1.
29. Kovalchuk L., Oliynykov R., Rodinko M. Security of the Poseidon hash function against non-binary differential and linear attacks. Cybernetics and Systems Analysis. 2021. Vol. 57, No. 2. P. 268–278. DOI: https://doi.org/10.1007/s10559-021-00352-y.
30. Kuznetsov O., Kuznetsova K., Yezhov A., Chernushevych V. Implementing recursive proofs for efficient blockchain verification: A zk-SNARKs approach. Mathematical Modeling and Simulation of Systems / ed. by V. Kazymyr et al. Lecture Notes in Networks and Systems. Springer, 2024. Vol. 1091. P. 266–280. DOI: https://doi.org/10.1007/978-3-031-67348-1_20.
31. Kuznetsov O., Yezhov A., Kuznetsova K., Yusiuk V., Chernushevych V. Enhancing blockchain scalability through zero-knowledge proofs: A novel block finality system for NEAR protocol. Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024). CEUR Workshop Proceedings. 2024. Vol. 3826. P. 94–104. URL: https://ceur-ws.org/Vol-3826/paper9.pdf.
32. Kwon Y., Liu J., Kim M., Song D., Kim Y. Impossibility of full decentralization in permissionless blockchains. Proceedings of the 1st ACM Conference on Advances in Financial Technologies. ACM, 2019. P. 110–123. DOI: https://doi.org/10.1145/3318041.3355463.
33. Lee S.-S., Murashkin A., Derka M., Gorzny J. SoK: Not quite water under the bridge: Review of cross-chain bridge hacks. 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2023. P. 1–14. DOI: https://doi.org/10.1109/ICBC56567.2023.10174993.
34. Micali S., Reyzin L., Vlachos G., Wahby R. S., Zeldovich N. Compact certificates of collective knowledge. 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021. P. 626–641. DOI: https://doi.org/10.1109/SP40001.2021.00096.
35. Moshrefi N., Sheng P., Deb S., Kannan S., Viswanath P. Unconditionally safe light client. arXiv. 2024. arXiv:2405.01459. DOI: https://doi.org/10.48550/arXiv.2405.01459.
36. NEAR Protocol. Light client. NEAR Protocol Specification (Nomicon). URL: https://nomicon.io/ChainSpec/LightClient (дата звернення: 04.09.2026).
37. Oberstein T. EIP-665: Add precompiled contract for Ed25519 signature verification. Ethereum Improvement Proposals. 2018. URL: https://eips.ethereum.org/EIPS/eip-665.
38. Polygon Zero. Plonky2 : computer software. GitHub. URL: https://github.com/0xPolygonZero/plonky2 (дата звернення: 04.09.2026).
39. Salazar Cardozo A., Williamson Z. EIP-1108: Reduce alt_bn128 precompile gas costs. Ethereum Improvement Proposals. 2018. URL: https://eips.ethereum.org/EIPS/eip-1108.
40. Succinct Labs. SP1 Helios: On-chain Ethereum light client built with SP1 : computer software. GitHub. 2024. URL: https://github.com/succinctlabs/sp1-helios.
41. Tas E. N., Tse D., Yang L., Zindros D. Light clients for lazy blockchains. Financial Cryptography and Data Security (FC 2024). Lecture Notes in Computer Science. Springer, 2025. Vol. 14745. P. 3–21. DOI: https://doi.org/10.1007/978-3-031-78679-2_1.
42. United Nations Security Council. Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023). S/2024/215. United Nations, 2024. URL: https://undocs.org/en/S/2024/215.
43. Vlasov A., Olson K., Stokes A., Sanso A. EIP-2537: Precompile for BLS12-381 curve operations. Ethereum Improvement Proposals. 2020. URL: https://eips.ethereum.org/EIPS/eip-2537.
44. Wahrstätter T., Buterin V. EIP-7623: Increase calldata cost. Ethereum Improvement Proposals. 2024. URL: https://eips.ethereum.org/EIPS/eip-7623.
45. Xie T., Zhang J., Cheng Z., Zhang F., Zhang Y., Jia Y., Boneh D., Song D. zkBridge: Trustless cross-chain bridges made practical. Proceedings of the 2022 ACM SIGSAC Conference on Computer

and Communications Security. ACM, 2022. P. 3003–3017. DOI: https://doi.org/10.1145/3548606.3560652.

References

1. Agrawal, S., Neu, J., Tas, E. N., & Zindros, D. (2023). Proofs of proof-of-stake with sublinear complexity. In 5th Conference on Advances in Financial Technologies (AFT 2023) (LIPIcs, Vol. 282, Article 14, pp. 14:1–14:24). Schloss Dagstuhl – Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPIcs.AFT.2023.14
2. Alpturer, K., & Weinberg, S. M. (2024). Optimal RANDAO manipulation in Ethereum. In 6th Conference on Advances in Financial Technologies (AFT 2024) (LIPIcs, Vol. 316, Article 10, pp. 10:1–10:21). Schloss Dagstuhl – Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPIcs.AFT.2024.10
3. Armknecht, F., Karame, G., Mohamed, M., & Weis, C. (2024). Practical light clients for committee-based blockchains. In 2024 Annual Computer Security Applications Conference (ACSAC) (pp. 473–487). IEEE. https://doi.org/10.1109/ACSAC63791.2024.00049
4. Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2024). SoK: Security and privacy of blockchain interoperability. In 2024 IEEE Symposium on Security and Privacy (SP) (pp. 3840–3865). IEEE. https://doi.org/10.1109/SP54263.2024.00255
5. Barbulescu, R., & Duquesne, S. (2019). Updating key size estimations for pairings. Journal of Cryptology, 32(4), 1298–1336. https://doi.org/10.1007/s00145-018-9280-5
6. Bariant, A., Bouvier, C., Leurent, G., & Perrin, L. (2022). Algebraic attacks against some arithmetization-oriented primitives. IACR Transactions on Symmetric Cryptology, 2022(3), 73–101. https://doi.org/10.46586/tosc.v2022.i3.73-101
7. Ben-Sasson, E., Carmon, D., Haböck, U., Kopparty, S., & Saraf, S. (2026). On proximity gaps of Reed–Solomon codes. In Proceedings of the 58th Annual ACM Symposium on Theory of Computing (pp. 1157–1167). ACM. https://doi.org/10.1145/3798129.3800827
8. Bernstein, D. J., Duif, N., Lange, T., Schwabe, P., & Yang, B.-Y. (2012). High-speed high-security signatures. Journal of Cryptographic Engineering, 2(2), 77–89. https://doi.org/10.1007/s13389-012-0027-1
9. Bespalov, Y., Kovalchuk, L., Nelasa, H., & Oliynykov, R. (2025). Binomial distribution with delay in analysis and parametrization of Ouroboros Praos proof of stake blockchain protocol. Probability in the Engineering and Informational Sciences, 39(4), 520–550. https://doi.org/10.1017/S0269964825000014
10. Bhatt, B. N., Shirazi, F., & Stewart, A. (2025). Trustless bridges via random sampling light clients. In 7th Conference on Advances in Financial Technologies (AFT 2025) (LIPIcs, Vol. 354, Article 31, pp. 31:1–31:24). Schloss Dagstuhl – Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPIcs.AFT.2025.31
11. Block, A. R., Garreta, A., Katz, J., Thaler, J., Tiwari, P. R., & Zając, M. (2023). Fiat–Shamir security of FRI and related SNARKs. In Advances in cryptology – ASIACRYPT 2023 (Lecture Notes in Computer Science, Vol. 14439, pp. 3–40). Springer. https://doi.org/10.1007/978-981-99-8724-5_1
12. Bünz, B., Kiffer, L., Luu, L., & Zamani, M. (2020). FlyClient: Super-light clients for cryptocurrencies. In 2020 IEEE Symposium on Security and Privacy (SP) (pp. 928–946). IEEE. https://doi.org/10.1109/SP40000.2020.00049
13. Chaliasos, S., Ernstberger, J., Theodore, D., Wong, D., Jahanara, M., & Livshits, B. (2024). SoK: What don't we know? Understanding security vulnerabilities in SNARKs. In 33rd USENIX Security Symposium (USENIX Security 24) (pp. 3855–3872). USENIX Association. https://www.usenix.org/conference/usenixsecurity24/presentation/chaliasos
14. Chalkias, K., Garillot, F., & Nikolaenko, V. (2020). Taming the many EdDSAs. In Security

standardisation research (SSR 2020) (Lecture Notes in Computer Science, Vol. 12529, pp. 67–90). Springer. https://doi.org/10.1007/978-3-030-64357-7_4

15. Chatzigiannis, P., Baldimtsi, F., & Chalkias, K. (2022). SoK: Blockchain light clients. In Financial cryptography and data security (FC 2022) (Lecture Notes in Computer Science, Vol. 13411, pp. 615–641). Springer. https://doi.org/10.1007/978-3-031-18283-9_31
16. Ciobotaru, O., Shirazi, F., Stewart, A., & Vasilyev, S. (2022). Accountable light client systems for proof-of-stake blockchains (Cryptology ePrint Archive, Paper 2022/1205). International Association for Cryptologic Research. https://eprint.iacr.org/2022/1205
17. Clauset, A., Shalizi, C. R., & Newman, M. E. J. (2009). Power-law distributions in empirical data. SIAM Review, 51(4), 661–703. https://doi.org/10.1137/070710111
18. Danezis, G., Maram, D., Roy, A., Sonnino, A., & Wüst, K. (2026). Guppy: Efficient light clients via recursive zero-knowledge proofs (arXiv:2609.07963). arXiv. https://doi.org/10.48550/arXiv.2609.07963
19. Efraimidis, P. S., & Spirakis, P. G. (2006). Weighted random sampling with a reservoir. Information Processing Letters, 97(5), 181–185. https://doi.org/10.1016/j.ipl.2005.11.003
20. Electron Labs. (2022). [PROPOSAL] Audit for Circom-Ed25519 for standardization of NEAR ZK light client (NEAR NEPs, Issue 440). GitHub. https://github.com/near/NEPs/issues/440
21. Ethereum Foundation. (n.d.). Ethereum execution layer specifications: Prague fork, vm/gas.py [Computer software]. GitHub. Retrieved October 4, 2026, from https://github.com/ethereum/execution-specs/blob/master/src/ethereum/forks/prague/vm/gas.py
22. Federal Bureau of Investigation. (2022, April 14). FBI statement on attribution of malicious cyber activity posed by the Democratic People's Republic of Korea [Press release]. https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea
23. Fog, A. (2008). Calculation methods for Wallenius' noncentral hypergeometric distribution. Communications in Statistics – Simulation and Computation, 37(2), 258–273. https://doi.org/10.1080/03610910701790269
24. Gaži, P., Kiayias, A., & Russell, A. (2018). Stake-bleeding attacks on proof-of-stake blockchains. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 85–92). IEEE. https://doi.org/10.1109/CVCBT.2018.00015
25. Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Advances in cryptology – EUROCRYPT 2016 (Lecture Notes in Computer Science, Vol. 9666, pp. 305–326). Springer. https://doi.org/10.1007/978-3-662-49896-5_11
26. Hoeffding, W. (1963). Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association, 58(301), 13–30. https://doi.org/10.1080/01621459.1963.10500830
27. Josefsson, S., & Liusvaara, I. (2017). Edwards-curve digital signature algorithm (EdDSA) (RFC 8032). Internet Research Task Force. https://doi.org/10.17487/RFC8032
28. Khovratovich, D., Rothblum, R. D., & Soukhanov, L. (2025). How to prove false statements: Practical attacks on Fiat–Shamir. In Advances in cryptology – CRYPTO 2025 (Lecture Notes in Computer Science, Vol. 16005, pp. 3–26). Springer. https://doi.org/10.1007/978-3-032-01887-8_1
29. Kovalchuk, L., Oliynykov, R., & Rodinko, M. (2021). Security of the Poseidon hash function against non-binary differential and linear attacks. Cybernetics and Systems Analysis, 57(2), 268–278. https://doi.org/10.1007/s10559-021-00352-y
30. Kuznetsov, O., Kuznetsova, K., Yezhov, A., & Chernushevych, V. (2024a). Implementing recursive proofs for efficient blockchain verification: A zk-SNARKs approach. In V. Kazymyr, A. Morozov, A. Palagin, S. Shkarlet, N. Stoianov, D. Vinnikov, & M. Zheleznyak (Eds.),

Mathematical modeling and simulation of systems (Lecture Notes in Networks and Systems, Vol. 1091, pp. 266–280). Springer. https://doi.org/10.1007/978-3-031-67348-1_20

31. Kuznetsov, O., Yezhov, A., Kuznetsova, K., Yusiuk, V., & Chernushevych, V. (2024b). Enhancing blockchain scalability through zero-knowledge proofs: A novel block finality system for NEAR protocol. In Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024) (CEUR Workshop Proceedings, Vol. 3826, pp. 94–104). CEUR-WS.org. https://ceur-ws.org/Vol-3826/paper9.pdf
32. Kwon, Y., Liu, J., Kim, M., Song, D., & Kim, Y. (2019). Impossibility of full decentralization in permissionless blockchains. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (pp. 110–123). ACM. https://doi.org/10.1145/3318041.3355463
33. Lee, S.-S., Murashkin, A., Derka, M., & Gorzny, J. (2023). SoK: Not quite water under the bridge: Review of cross-chain bridge hacks. In 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 1–14). IEEE. https://doi.org/10.1109/ICBC56567.2023.10174993
34. Micali, S., Reyzin, L., Vlachos, G., Wahby, R. S., & Zeldovich, N. (2021). Compact certificates of collective knowledge. In 2021 IEEE Symposium on Security and Privacy (SP) (pp. 626–641). IEEE. https://doi.org/10.1109/SP40001.2021.00096
35. Moshrefi, N., Sheng, P., Deb, S., Kannan, S., & Viswanath, P. (2024). Unconditionally safe light client (arXiv:2405.01459). arXiv. https://doi.org/10.48550/arXiv.2405.01459
36. NEAR Protocol. (n.d.). Light client. In NEAR Protocol specification (Nomicon). Retrieved October 4, 2026, from https://nomicon.io/ChainSpec/LightClient
37. Oberstein, T. (2018). EIP-665: Add precompiled contract for Ed25519 signature verification (Ethereum Improvement Proposals; status: Stagnant). https://eips.ethereum.org/EIPS/eip-665
38. Polygon Zero. (n.d.). Plonky2 [Computer software]. GitHub. Retrieved October 4, 2026, from https://github.com/0xPolygonZero/plonky2
39. Salazar Cardozo, A., & Williamson, Z. (2018). EIP-1108: Reduce alt_bn128 precompile gas costs (Ethereum Improvement Proposals; status: Final). https://eips.ethereum.org/EIPS/eip-1108
40. Succinct Labs. (2024). SP1 Helios: On-chain Ethereum light client built with SP1 [Computer software]. GitHub. https://github.com/succinctlabs/sp1-helios
41. Tas, E. N., Tse, D., Yang, L., & Zindros, D. (2025). Light clients for lazy blockchains. In Financial cryptography and data security (FC 2024) (Lecture Notes in Computer Science, Vol. 14745, pp. 3–21). Springer. https://doi.org/10.1007/978-3-031-78679-2_1
42. United Nations Security Council. (2024). Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023) (S/2024/215). United Nations. https://undocs.org/en/S/2024/215
43. Vlasov, A., Olson, K., Stokes, A., & Sanso, A. (2020). EIP-2537: Precompile for BLS12-381 curve operations (Ethereum Improvement Proposals; status: Final). https://eips.ethereum.org/EIPS/eip-2537
44. Wahrstätter, T., & Buterin, V. (2024). EIP-7623: Increase calldata cost (Ethereum Improvement Proposals; status: Final). https://eips.ethereum.org/EIPS/eip-7623
45. Xie, T., Zhang, J., Cheng, Z., Zhang, F., Zhang, Y., Jia, Y., Boneh, D., & Song, D. (2022). zkBridge: Trustless cross-chain bridges made practical. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 3003–3017). ACM. https://doi.org/10.1145/3548606.3560652

This is an open access journal and all published articles are licensed under a Creative Commons «Attribution» 4.0.