КІБЕРНЕТИКА
та КОМП'ЮТЕРНІ
ТЕХНОЛОГІЇ

УДК 004.75:519.83 DOI:10.34229/2707-451X.26.1.2

В.В. ГОДЛЮК

ЗАСТОСУВАННЯ МЕТОДІВ ТЕОРІЇ ІГОР ДЛЯ АНАЛІЗУ ВЗАЄМОДІЇ ВАЛІДАТОРІВ У PROOF-OF-STAKE БЛОКЧЕЙН-СИСТЕМАХ

У статті досліджується стратегічна поведінка валідаторів у блокчейн-системах із механізмом консенсусу Proof-of-Stake (PoS) з використанням апарату теорії ігор. Запропоновано математичну модель некооперативної гри з повною інформацією, у якій валідатори розглядаються як раціональні агенти, що максимізують свій очікуваний виграш. Розглянуто ключові стратегії: чесну валідацію, атаку подвійної витрати та інші форми зловмисної поведінки. Функції корисності враховують винагороди, штрафи (slashing), операційні витрати та ризики. Аналіз рівноваги Неша показує, що стан «усі валідатори діють чесно» є стійким у разі ефективних механізмів покарання, оскільки індивідуальні атаки є економічно нерентабельними. Навпаки, рівновага типу «всі атакують», хоча й теоретично можлива, є практично недосяжною через надмірну вартість контролю над більшістю стейку. Кількісний приклад підтверджує, що стабільність PoS-систем залежить від балансу між стимулами до чесної поведінки та дистимулами до зловмисних дій. Робота підкреслює важливість забезпечення економічної безпеки в архітектурі сучасних блокчейн-протоколів.

Ключові слова: *Proof-of-Stake, валідатори, теорія ігор, рівновага Неша, економічна безпека, slashing, атака подвійної витрати, ігрова модель, блокчейн-протоколи.*

Вступ. У децентралізованих блокчейн-системах із механізмом консенсусу Proof-of-Stake (PoS) валідатори є ключовими учасниками, відповідальними за безпеку та стабільність мережі. Їхня поведінка, зумовлена прагненням максимізувати економічну вигоду, може бути як добросовісною, так і зловмисною, зокрема у формі спроб подвійної витрати коштів або цензури транзакцій [1, 2]. Така стратегічна взаємозалежність робить поведінку валідаторів природним об’єктом дослідження в межах теорії ігор, оскільки виграш кожного учасника залежить не лише від його власної стратегії, а й від дій інших.

Хоча в наявних дослідженнях аналізується поведінка валідаторів, багато з них ґрунтуються на спрощених припущеннях, ігноруючи взаємодію учасників PoS-мереж [3, 4]. У реальних умовах валідатори взаємодіють у складному середовищі, де рішення одного учасника впливає на очікуваний виграш інших, а інформаційна асиметрія та динамічний характер взаємодій ускладнюють прогнозування. У зв’язку з цим актуальною є розробка математично обґрунтованих ігрових моделей, здатних враховувати різноманіття стратегій, економічні стимули та системні параметри, що визначають стійкість PoS-протоколів [1, 4].

Метою цієї статті є побудова та аналіз некооперативної ігрової моделі взаємодії валідаторів у PoS-мережах на основі рівноваги Неша з метою визначення умов, за яких домінує чесна поведінка, а також оцінки стійкості системи до колективних зловмисних дій. Особливу увагу приділено формалізації функцій виграшу, які враховують як законні винагороди, так і ризики штрафів (slashing), а також аналізу рівноважних залежностей від ключових параметрів системи, зокрема розміру заблокованого обсягу криптовалюти (стейку), рівня штрафів та ймовірності виявлення зловмисних дій. Отримані результати демонструють, що ефективні механізми покарання роблять індивідуальні атаки економічно нерентабельними, забезпечуючи домінування рівноваги типу "всі чесні" [1, 2].

Стратегічна поведінка валідаторів у PoS-мережах

У системах, що ґрунтуються на механізмі консенсусу PoS, валідатори виступають ключовими агентами, поведінка яких безпосередньо визначає стійкість, безпеку та функціональність мережі. Їхні рішення формуються під впливом економічних стимулів, спрямованих на максимізацію індивідуального виграшу, який може бути досягнутий як шляхом дотримання протокольних правил, так і внаслідок зловмисних дій. Кожен учасник приймає рішення, балансуючи між потенційними винагородами, ризиками застосування штрафних санкцій та очікуваним впливом дій інших учасників мережі.

Однією з базових стратегій є сумлінна (чесна) валідація, за якої валідатор строго дотримується правил протоколу: коректно перевіряє транзакції, включає їх до блоків без цензури, своєчасно пропонує та підтверджує блоки. Така стратегія орієнтована на отримання регулярних протокольних винагород. У більшості випадків саме чесна поведінка забезпечує найстабільніший і передбачуваний дохід, що робить її фундаментальною для функціонування PoS-систем.

Альтернативною формою взаємодії є утворення валідаційних пулів, у межах яких кілька учасників, особливо з невеликими обсягами стейку, об'єднують свої ресурси з метою підвищення ймовірності обрання для створення блоку. У цій моделі винагороди розподіляються пропорційно внесеним стейкам, що дозволяє дрібним учасникам подолати поріг ефективної участі та зменшити дисперсію доходів. Хоча така практика не є зловмисною за своєю природою, вона вводить елементи кооперації, що ускладнює аналіз стратегічної взаємодії та потребує врахування не лише індивідуальних, а й колективних рішень.

Поряд із добросовісними стратегіями, існують і такі стратегії, що спрямовані на отримання недозволеної вигоди. Однією з них є атака подвійної витрати (double spending), за якої валідатор намагається створити альтернативну гілку блокчейну з метою скасування вже підтвердженого переказу коштів. Успіх такої атаки залежить від контролю над значною часткою загального стейку мережі, зазвичай – понад 50 %. Водночас ризик її виявлення є високим, оскільки сучасні PoS-протоколи передбачають суворі механізми slashing, що призводять до втрати значної частини або всього застейканого капіталу [1, 2].

Ще однією потенційною загрозою є цензура транзакцій, коли валідатор навмисно не включає певні транзакції до блоків, які він пропонує, або відмовляється підтверджувати блоки, що містять такі транзакції. Така поведінка може мати економічну, політичну або регуляторну мотивацію. Хоча механізми її виявлення є менш очевидними, ніж у випадку подвійної витрати, така стратегія може підривати децентралізацію та незалежність мережі, особливо якщо вона набуває поширення серед великих валідаційних пулів.

Іншим типом зловмисної поведінки є атака на живучість (liveness attack), за якої валідатор навмисно припиняє участь у консенсусі, не підтверджуючи блоки у моменті, коли має таку можливість. Це може призводити до уповільнення або навіть повної зупинки роботи мережі, що знижує рівень довіри до системи. Хоча така поведінка зазвичай карається штрафами за бездіяльність, вона може використовуватися як інструмент тиску з метою примусового внесення змін до протоколу.

Окремо слід згадати атаку типу nothing-at-stake attack, характерну для ранніх моделей PoS-протоколів. Вона полягає в тому, що валідатори можуть одночасно підтримувати кілька конфліктних гілок блокчейну без істотних витрат, оскільки відсутність обчислювальної роботи притаманної у Proof-of-Work (PoW), дозволяє грати на всіх гілках паралельно. Хоча ця загроза була актуальною для перших PoS-систем, сучасні протоколи, такі як Ethereum 2.0, ефективно нейтралізують її за допомогою механізмів slashing за подвійне підтвердження блоків [1, 2].

Таким чином, поведінка валідаторів у PoS-мережах є результатом складної стратегічної взаємодії, у межах якої кожне рішення оцінюється з погляду очікуваного виграшу, ризику штрафів та

впливу на інших учасників. Для побудови адекватної ігрової моделі необхідна формалізація можливих стратегії і відповідних функцій корисності, що створює основу для подальшого аналізу рівноважних станів мережі.

Формалізація функцій виграшу

Для побудови ефективної ігрової моделі поведінки валідаторів у PoS-мережах необхідно формалізувати їхні цільові функції, які визначають раціональний вибір стратегій. У цьому контексті виграш (або корисність) кожного валідатора визначається як очікувана чиста фінансова вигода, що виникає внаслідок його дій, з урахуванням як протокольних винагород, так і потенційних штрафів, операційних витрат та інших економічних чинників. Функція корисності є центральним елементом аналізу, оскільки саме вона формує стимули до чесної або зловмисної поведінки.

Основу позитивного виграшу становлять протокольні винагороди, спрямовані на заохочення активної та добросовісної участі у механізмі консенсусу. Насамперед, це винагорода за створення блоку – фіксована або динамічна кількість токенів, яка нараховується валідатору, що успішно запропонував новий блок і який був прийнятий мережею. Позначимо R_b – розмір протокольної винагороди. Він є параметром протоколу і зазвичай залежить від загальної емісії та економічної моделі мережі. Ймовірність отримання такої винагороди прямо пропорційна частці стейку валідатора відносно загального стейку мережі, що забезпечує пропорційний і справедливий розподіл прав на створення блоків.

Додатковим джерелом доходу є комісії за транзакції (R_t), які сплачуються користувачами за включення їхніх операцій до блоку. У багатьох сучасних PoS-системах, зокрема після переходу Ethereum на механізм PoS, валідатори отримують частину цих комісій, тоді як інша частина може спалюватися з метою зменшення загальної пропозиції токенів [1, 2]. Загальний обсяг комісій залежить від інтенсивності транзакційної активності у мережі, рівня попиту, а також від стратегії валідатора щодо відбору транзакцій для включення до блоку.

Окрім винагород за створення блоків, PoS-протоколи передбачають винагороди за підтвердження (атестацію) інших блоків. Це дозволяє валідаторам, які не були обрані для пропозиції блоку, отримувати невеликі, але регулярні винагороди за підтвердження коректності стану мережі. Такий механізм стимулює високу участь у консенсусі та підвищує безпеку системи, оскільки кожен валідатор зацікавлений у постійній участі в процесі підтвердження блоків. Загалом очікуваний дохід від чесної валідації можна подати у вигляді:

$$U_{\text{чесний}} = p_i \cdot (R_b + R_t) + R_a - C_{\text{опер.}}, \quad (1)$$

де $p_i = \frac{s_i}{S}$ – ймовірність вибору валідатора i для створення блоку, S_i – розмір його стейку, S – загальний стейк мережі, R_a – винагорода за атестацію, $C_{\text{опер.}}$ – операційні витрати на утримання та функціонування вузла.

Протилежністю позитивних складових виграшу є негативні компоненти, зокрема штрафи, втрати та ризики, пов'язані з недобросовісною поведінкою. Найсерйознішим механізмом покарання є slashing – автоматичне списання частини або всього застейканого капіталу валідатора у разі виявлення зловмисних дій, таких як подвійне підтвердження блоків, спроба подвійної витрати або створення недійсного блоку. Розмір штрафу, можна подати у вигляді

$$P_s = \lambda \cdot s_i,$$

де λ – частка стейку, що втрачається.

У сучасних протоколах λ може бути динамічним і залежати від масштабу порушення та кількості одночасних порушників [1, 2].

Крім прямих фінансових штрафів, валідатори також зазнають втрат потенційного доходу (opportunity cost) у разі бездіяльності або застосування санкцій. Якщо валідатор тимчасово або пос-

тійно виключений з процесу консенсусу, він втрачає можливість отримувати винагороди, що зменшує його сумарний дохід. Такі штрафи за не активність, хоча й менш жорсткі за slashing, відіграють важливу роль у забезпеченні високої доступності та стабільності мережі.

Важливим, хоча й не завжди формалізованим, чинником є репутаційний ризик. Для великих валідаційних пулів втрата довіри спільноти може призвести до відтоку делегованих стейків, що безпосередньо впливає на їхній дохід. Хоча цей ефект складно кількісно оцінити, його можна інтегрувати в модель у вигляді зниження майбутніх очікуваних винагород або зменшення ймовірності залучення нових учасників.

На основі зазначених компонентів можна визначити очікуваний виграш для різних стратегій поведінки. Для валідатора, який дотримується чесної стратегії, виграш є відносно стабільним і передбачуваним. Для валідатора, що обирає стратегію спроби подвійної витрати, очікуваний виграш залежить від ймовірності успіху атаки q та ймовірності її виявлення δ . У цьому випадку очікуваний виграш можна подати у вигляді:

$$U_{\text{атака}} = q \cdot G - \delta \cdot \lambda \cdot s_i - C_{\text{опер.}}, \quad (2)$$

де G – потенційна вигода від успішної атаки (наприклад, вартість подвійно витрачених коштів). Якщо атака зазнає невдачі, що є ймовірним у разі контролю лише меншої частки загального стейку, валідатор зазнає суттєвих фінансових втрат унаслідок застосування механізмів slashing, а його чистий виграш стає від'ємним.

Аналогічно можна формалізувати виграш для інших стратегій, зокрема, цензури транзакцій або участі у валідаційних пулах. Наприклад, для валідатора, що приєднується до пулу, очікуваний дохід залежить не лише від розміру його власного стейку, але й від загальної винагороди пулу, комісії оператора пулу та рівня його ефективності:

$$U_{\text{пул}} = \frac{s_i}{S_{\text{пул}}} \cdot R_{\text{пул}} - f_{\text{комісія}} - C_{\text{опер.}}, \quad (3)$$

де $R_{\text{пул}}$ – загальна винагорода пулу, $f_{\text{комісія}}$ – комісія, що утримується оператором пулу.

Таким чином, функції виграшу дозволяють перейти від якісного опису стратегій до кількісного аналізу їх економічної доцільності. Вони слугують основою для побудови математичної ігрової моделі, у якій кожен валідатор максимізує свій очікуваний виграш з урахуванням дій інших учасників мережі.

Ключові параметри системи

Для побудови реалістичної та конкретної ігрової моделі поведінки валідаторів у PoS-блокчейн-системах необхідно чітко визначити сукупність параметрів, що впливають на їхні стратегічні рішення. Ці параметри є основою для кількісного аналізу функцій виграшу, визначення рівноважних станів і оцінки стійкості мережі. Вони формують економічні стимули, обмеження та визначають структуру взаємодії між учасниками.

Центральним параметром є розмір стейку окремого валідатора s_i , тобто кількість токенів заблокованих ним для участі у консенсусі. Цей параметр безпосередньо визначає вплив валідатора в мережі, оскільки пропорційний ймовірності бути обраним для створення або підтвердження блоку. Водночас, s_i визначає масштаб потенційних штрафів у разі порушення протоколу, адже механізми slashing застосовуються як частка від застейканого капіталу.

Індивідуальний стейк пов'язаний із загальним стейком мережі $S = \sum_{j=1}^{N} s_j$, який слугує нормуючим фактором для оцінювання відносного впливу кожного валідатора. Загальний стейк визначає рівень децентралізації мережі, конкуренцію між учасниками та ступінь концентрації влади. Високе значення S порівняно з окремими s_i знижує ймовірність домінування одного учасника, що підвищує стійкість системи. Натомість, значна концентрація стейку може створювати передумови для коаліційних атак.

На основі цих параметрів визначається ймовірність вибору валідатора для участі в консенсусі p_i, яка у базовій моделі задається як відносна частка його стейку: $p_i = \frac{s_i}{S}$. Хоча в реальних PoS-протоколах цей механізм може доповнюватися елементами випадковості, часовими факторами або віком стейку, пропорційна залежність залишається ключовою для моделювання очікуваних винагород.

Винагороди, які стимулюють добросовісну участь, визначаються кількома параметрами. По-перше, це базова винагорода за створення блоку R_b – фіксована або динамічна кількість токенів, що призначається валідатору за успішне внесення блоку до ланцюжка. Цей параметр є центральним стимулом участі у процесі консенсусу. По-друге, важливим додатковим джерелом доходу є середні комісії за транзакції R_t , які залежать від попиту на мережу, обсягу транзакцій та стратегії валідатора щодо включення операцій. Разом із винагородою за підтвердження блоків (атестацію), ці компоненти формують очікуваний позитивний виграш від чесної поведінки.

З іншого боку, для стримування зловмисної поведінки критичну роль відіграють параметри, пов'язані з покараннями. Найважливішим із них є розмір штрафу за зловмисні дії (slashing penalty) λ, що визначає частку стейку валідатора, яку він втрачає у разі виявлення порушення, наприклад, подвійного підтвердження або спроби подвійної витрати. Цей параметр може бути фіксованим або динамічним залежно від масштабу порушення та кількості одночасних порушників. Ефективність механізму slashing безпосередньо залежить від λ: чим вищий штраф, тим сильніший дистимул до використання ризикованих стратегій.

Додатковим фактором є штраф за бездіяльність (inactivity penalty) P_{in}, який застосовується до валідаторів, що не виконують свої обов'язки з підтвердження блоків. Хоча цей штраф менший за slashing, він відіграє важливу роль у підтриманні високої доступності мережі та заохочує постійну участь валідаторів у консенсусі.

Ще одним ключовим параметром є ймовірність виявлення зловмисної дії δ. Вона визначає надійність протокольних механізмів доведення недобросовісної поведінки (proof-of-misbehaviour). Для таких атак, як подвійна витрата, сучасні PoS-протоколи передбачають високу ймовірність виявлення ($\delta \approx 1$), що робить подібні атаки економічно нерентабельними [1, 2]. Натомість, для атак типу цензури ця ймовірність може бути значно нижчою, що ускладнює їх ефективне стримування.

Окрім протокольних параметрів, важливу роль відіграють операційні витрати валідатора $C_{\text{опер.}}$, які включають витрати на обладнання, електроенергію, технічне обслуговування та мережеве з'єднання. Ці витрати зменшують чистий виграш і можуть впливати на рівень входу до системи, особливо для дрібних учасників. У моделі вони зазвичай вважаються фіксованими або такими, що залежать від масштабу діяльності.

Нарешті, для аналізу зловмисних стратегій необхідно враховувати потенційну вигоду від успішної атаки G, тобто фінансовий прибуток, який валідатор може отримати в разі її реалізації, наприклад, вартість подвійно витрачених коштів або вигоду від цензури. Цей параметр виступає як зовнішній стимул, що не залежить від протокольних винагород, але безпосередньо впливає на стратегічні рішення валідатора.

Зазначені параметри взаємодіють між собою у межах функцій виграшу, формуючи складну систему стимулів. Наприклад, очікуваний виграш від чесної поведінки залежить від s_i, S, R_b, R_t та $C_{\text{опер.}}$, тоді як вибір зловмисної стратегії оцінюється шляхом порівняння величини G , з параметрами λ , δ та ризиком втрати стейку і майбутніх винагород $p_i \cdot (R_b + R_t)$. Зміна будь-якого з цих параметрів може призвести до зсуву рівноважного стану системи, що робить їх ключовими для аналізу стійкості PoS-протоколів.

Формалізація математичної ігрової моделі

Для аналізу стратегічної взаємодії валідаторів у PoS блокчейн-системах необхідно побудувати формальну модель, засновану на принципах теорії ігор. Така модель дай змогу визначити раціональні стратегії учасників, проаналізувати можливі рівноважні стани та оцінити стійкість системи до зловмисних дій. У цьому розділі представлено структуру гри, визначено гравців, їхні стратегії, функції корисності та ключові припущення щодо типу гри.

Гравці та множини учасників

У розглянутій моделі гравцями виступають валідатори – учасники мережі, які володіють застейканими токенами і беруть участь у процесі консенсусу. Нехай загальна кількість валідаторів у мережі дорівнює N, і кожен валідатор $i \in \{1,2,\dots,N\}$ характеризується розміром свого стейку s_i, який визначає його вплив на процес створення блоків та рівень потенційних штрафів.

Для спрощення аналізу розглядається некооперативна гра, в якій кожен валідатор діє як незалежний раціональний агент, прагнучи максимізувати свій очікуваний виграш [5]. Хоча валідатори можуть об'єднуватися в пули, що вносить елементи кооперації, індивідуальний вибір стратегії залишається автономним, що відповідає парадигмі некооперативної теорії ігор.

Множина стратегій

Кожен валідатор обирає стратегію з множини можливих дій. У рамках базової моделі розглядаються дві основні стратегії, які відображають фундаментальний вибір між добросовісною та зловмисною поведінкою:

- Чесна валідація (H). Валідатор дотримується протокольних правил, коректно перевіряє транзакції, пропонує та підтверджує блоки, не намагаючись маніпулювати станом мережі. Ця стратегія спрямована на отримання легітимних винагород за участь у консенсусі.
- Атака (A). Валідатор намагається здійснити зловмисну дію, зокрема атаку подвійної витрати (double spending). Ця стратегія передбачає спробу отримати додаткову вигоду шляхом порушення протоколу за умови виявлення та застосування штрафних санкій.

Таким чином, для кожного валідатора і множина чистих стратегій визначається як $S_i = \{H, A\}$, а загальний простір стратегій гри має вигляд $S = S_1 \times S_2 \times \cdots \times S_N$.

Функції виграшу

Функція корисності (виграшу) кожного валідатора визначається як очікувана чиста фінансова вигода, що залежить від його власної стратегії, стратегій інших учасників та системних параметрів. Нехай $u_i(s_i, s_{-i})$ – виграш валідатора i, де s_{-i} – стратегії всіх інших гравців.

Якщо валідатор i обирає стратегію H, його виграш складається з очікуваних винагород за створення блоку та підтвердження інших блоків, зменшених на операційні витрати:

$$U_{i(H,s_{-i})} = p_i \cdot (R_b + R_t) + R_a - C_{\text{опер.}}, \quad (4)$$

де $P_i = \frac{si}{S}$ – ймовірність бути обраним для створення блоку, R_b – базова винагорода за блок, R_t – середні комісії за транзакції, R_a – винагорода за атестацію, $C_{\text{опер.}}$ – операційні витрати валідатора.

Якщо валідатор і обирає стратегію A, його виграш залежить від ймовірності успіху атаки q, потенційної вигоди G, імовірності виявлення δ та розміру штрафу $\lambda \cdot s_i$:

$$U_{i(A,s_{-i})} = q \cdot G - \delta \cdot \lambda \cdot s_i - C_{\text{опер.}}, \quad (5)$$

При цьому імовірність успіху атаки q залежить від сукупного стейку атакувальників S_A. У спрощеній моделі можна припустити, що $q \approx 1$, якщо $S_A > 0.5S$ (атака більшості), і $q \approx 0$, якщо $S_A \leq 0.5S$ (атака меншості). Відповідно, імовірність виявлення δ є високою для атак меншості та значно нижчою для атак більшості.

Тип гри та припущення

Модель класифікується як некооперативна гра в нормальній формі з повною інформацією, що означає, таке:

- усі гравці знають множину стратегій, функції виграшу та параметри системи;
- рішення приймаються одночасно або без знання вибору інших учасників, що відповідає статичній грі;
- метою кожного гравця є максимізація власного виграшу без урахування суспільного блага.

Такий підхід дозволяє використовувати концепцію рівноваги Неша для визначення стабільних станів системи, у яких жоден учасник не має стимулу відхилятися від обраної стратегії [6], та є узгодженим із сучасними тенденціями застосування математичних моделей для аналізу цифрових платформ, де формалізовані методи використовуються для оптимізації взаємодії учасників, балансування навантаження та прогнозування стратегічної поведінки [7].

Аналіз функцій виграшу та пошук рівноважних станів

Після формалізації гри, визначення гравців, їхніх стратегій і функцій виграшу наступним кроком є аналіз моделі з метою визначення рівноважних станів. Центральним поняттям у цьому контексті є рівновага Неша – такий стан гри, у якому жоден гравець не може збільшити свій виграш шляхом одноосібної зміни власної стратегії, за умови незмінності стратегій інших гравців. Її існування та стійкість дають змогу зробити висновки щодо передбачуваної поведінки валідаторів у PoS-мережах.

Як було зазначено раніше, функції виграшу кожного валідатора i залежать не лише від його власної стратегії, а й від сукупної поведінки інших учасників, зокрема від загального стейку тих, хто обирає стратегію атаки. Нехай $S_A = \sum_{j \in A} s_j$ – це сукупний стейк усіх валідаторів, які обрали стратегію Атака (A). Ця величина є критичним параметром, що визначає як імовірність успіху атаки q, так і ймовірність її виявлення δ.

У сучасних PoS-протоколах, зокрема в Ethereum 2.0, безпека системи ґрунтується на припущенні, що більшість учасників діє добросовісно. У зв'язку з цим можна визначити два ключові сценарії, які визначають динаміку виграшів.

1. Атака меншості $(S_A \leq 0.5S)$.

У цьому випадку сукупний стейк атакувальників є недостатнім для контролю над процесом консенсусу. Спроби створити альтернативну гілку блокчейну будуть відхилені більшістю чесних валідаторів. Отже, імовірність успіху атаки $q \approx 0$, а імовірність її виявлення $\delta \approx 1$, оскільки механізми slashing ефективно фіксують подвійне підтвердження блоків. Таким чином, атака меншості – економічно нерентабельна.

2. Атака більшості $(S_A > 0.5S)$.

Якщо зловмисники контролюють понад половину загального стейку, вони отримують можливість домінувати в консенсусі. У цьому випадку $q \approx 1$ (атака успішна), а $\delta \approx 0$ (атака не виявляється), оскільки більшість підтверджує зловмисну гілку. Хоча така стратегія теоретично можлива, у добре спроєктованих системах вона економічно малоймовірна через надмірну вартість набуття контролю над більшістю стейку.

На основі цих припущень можна проаналізувати два потенційні стійкі стани: рівновагу "всі чесні" та рівновагу "всі атакують".

Рівновага "всі чесні" (All-Honest Equilibrium)

Розглянемо стан, у якому всі $N - 1$ інших валідаторів обирають стратегію H. Для окремого валідатора i, який розглядає можливість відхилення до стратегії A, сукупний стейк атакувальників S_A дорівнюватиме лише s_i, що, за великого N, становить незначну частку від загального стейку S. Отже, виконується умова $S_A \leq 0.5S$, і маємо:

$$q \approx 0, \delta \approx 1.$$

Тоді очікуваний виграш валідатора i від атаки становить:

$$u_i(A) = q \cdot G - \delta \cdot \lambda \cdot s_i - C_{\text{опер.}} \approx -\lambda \cdot s_i - C_{\text{опер}}. \quad (6)$$

Тоді як, виграш від чесної поведінки дорівнює:

$$u_i(H) = p_i \cdot (R_b + R_t) + R_a - C_{\text{опер}}. \quad (7)$$

Оскільки $u_i(H) > u_i(A)$ (додатній дохід порівняно зі значними втратами), валідатор i не має стимулу відхилятися. Це підтверджує, що рівновага "всі чесні" – стійка за наявності ефективних механізмів slashing [1, 2].

Рівновага "всі атакують" (All-Attacker Equilibrium)

Розглянемо протилежний сценарій, у якому всі N валідаторів обирають стратегію A. У цьому випадку $S_A = S$, отже $S_A > 0.5S$, і виконується:

$$q \approx 1, \delta \approx 0.$$

Виграш від атаки:

$$u_i(A) = q \cdot G - \delta \cdot \lambda \cdot s_i - C_{\text{опер.}} \approx G - C_{\text{опер.}}. \quad (8)$$

Якщо потенційна вигода G від успішної атаки (наприклад, вартість подвійно витрачених коштів) є значною, відповідний виграш може перевищувати виграш від чесної поведінки. При цьому виграш від відхилення до стратегії H у такій мережі буде незначним, оскільки блоки запропоновані чесними валідаторами не прийматимуться зловмисною більшістю. Отже, $u_i(H) \approx -C_{\text{опер.}}$, і якщо $G > 0$, то $u_i(A) > u_i(H)$.

Це означає, що рівновага "всі атакують" також може бути стійкою, але лише за умови, що зловмисна більшість уже існує. Водночас досягнення такого стану вимагає контролю над більшістю стейку, що є економічно надзвичайно витратним. У реальних системах вартість набуття контролю над 51% стейку часто істотно перевищує потенційну вигоду G, що робить цю рівновагу теоретично можливою, але практично малоймовірною.

Приклад та ілюстрація моделі

Для наочної демонстрації працездатності запропонованої ігрової моделі та підтвердження отриманих теоретичних висновків, розглянемо гіпотетичний приклад PoS-мережі з фіксованими параметрами. Такий приклад дає змогу кількісно оцінити очікувані виграші для різних стратегій, проаналізувати умови існування рівноваг Неша та проілюструвати механізми, що забезпечують стійкість системи.

Нехай у мережі функціонує $N = 1000$ валідаторів, із загальним стейком $S = 1000000$ токенів. Припустимо, що всі валідатори є гомогенними, тобто мають однаковий розмір стейку $s_i = 1000$ токенів. Базова винагорода за створення блоку становить $R_b = 5$ токенів, середні комісії за транзакції – $R_t = 1$ токен, а операційні витрати валідатора – $C_{\text{опер.}} = 0.1$ токена. Розмір штрафу за зловмисну дію (slashing penalty) визначено як $\lambda = 0.1$, тобто 10 % від розміру стейку. Потенційну вигоду від успішної атаки подвійної витрати оцінено як $G = 100000$ токенів.

Очікуваний виграш від чесної поведінки

Спочатку розрахуємо очікуваний виграш валідатора, який дотримується чесної стратегії. Імовірність бути обраним для створення блоку визначається як

$$p_i = \frac{s_i}{S} = \frac{1000}{1000000} = 0.001.$$

Винагорода за атестацію (підтвердження блоків інших валідаторів) враховується як $R_a = 0.1$ токена. Тоді очікуваний виграш від чесної поведінки становить:

$$U_i(H) = p_i \cdot (R_b + R_t) + R_a - C_{\text{опер.}} = 0.001 \cdot (5 + 1) + 0.1 - 0.1 = 0.006 + 0.1 - 0.1 = 0.006.$$

Отриманий виграш є додатнім, хоча й невеликим, що забезпечує базовий стимул до чесної участі у протоколі.

Аналіз рівноваги "всі чесні"

Розглянемо стан, у якому всі інші $N - 1 = 999$ валідаторів дотримуються чесної стратегії. Якщо окремий валідатор i вирішить відхилитися та спробувати здійснити атаку, його стейк $s_i = 1000$ токенів становитиме лише 0.1% від загального стейку. Отже, сукупний стейк атакувальників дорівнює $S_A = 1000$, що значно менше критичного порогу у 50 %. У цьому випадку імовірність успіху атаки $q \approx 0$ буде відкинута більшістю чесних валідаторів, а імовірність її виявлення становить $\delta \approx 1$, що зумовлює застосування механізмів slashing.

Тоді очікуваний виграш від атаки визначається як:

$$u_i(A) = q \cdot G - \delta \cdot \lambda \cdot s_i - C_{\text{опер}} \approx 0 - 1 \cdot 0.1 \cdot 1000 - 0.1 = -100.1.$$

Порівняння з виграшем від чесної поведінки $u_i(H) = 0.006$ показує, що $u_i(H) > u_i(A)$. Це підтверджує, що рівновага "всі чесні" – стабільна: жоден окремий валідатор не має стимулу відхилятися від чесної стратегії, оскільки потенційні втрати від штрафних санкцій значно перевищують будь-яку можливу вигоду.

Аналіз рівноваги "всі атакують"

Розглянемо гіпотетичний сценарій, у якому всі $N = 1000$ валідаторів одночасно обирають стратегію атаки. У цьому випадку сукупний стейк атакувальників становить $S_A = 1000000$ токенів, що відповідає 100 % загального стейку мережі. Отже, маємо такі умови:

- імовірність успіху атаки $q \approx 1$, оскільки атакувальники повністю контролюють процес консенсусу;
- імовірність виявлення $\delta \approx 0$, оскільки зловмисна більшість підтверджує власну гілку блокчейну, тому механізм slashing не застосовується.

Тоді очікуваний виграш валідатора від атаки:

$$U_i(A) = 1 \cdot 100000 - 0 \cdot \lambda \cdot s_i - 0.1 = 99999.9.$$

Якщо один із валідаторів спробує відхилитися від цієї стратегії та повернутися до чесної поведінки, його блоки не будуть прийняті зловмисною більшістю, а отже він не отримає жодних протокольних винагород. Його виграш у такому випадку становитиме:

$$U_i(H) = -C_{\text{опер}} = -0.1.$$

Оскільки $u_i(A) > u_i(H)$, рівновага "всі атакують" також є стійкою: жоден учасник не має стимулу виходити з коаліції зловмисників.

Наведений приклад демонструє існування двох рівноважних станів, але із різними рівнями досяжності. Рівновага "всі чесні" є стійкою та легко досяжною, оскільки її реалізація потребує лише ефективних механізмів slashing. Натомість, рівновага "всі атакують" – теоретично можлива, але практично недосяжна, оскільки вимагає контролю над більшістю стейку мережі, що є економічно надзвичайно витратним. У реальних системах вартість придбання 51 % стейку часто перевищує потенційну вигоду від атаки, що робить таку рівновагу неактуальною.

Аналіз поведінки валідаторів у PoS-блокчейн-системах за допомогою ігрової моделі дає змогу сформулювати важливі висновки щодо економічної безпеки, стійкості та передбачуваності функціонування таких мереж. Отримані результати підтверджують, що раціональна поведінка учасників значною мірою визначається системою економічних стимулів, яка має бути ретельно збалансованою для забезпечення домінування добросовісної поведінки.

Ключовий висновок дослідження це те, що рівновага "всі чесні" – стійка та домінуюча в умовах добре спроєктованих PoS-протоколів. Це означає, що окремий валідатор не має стимулу відхилятися від чесної стратегії, оскільки потенційні втрати від неуспішної атаки суттєво перевищують будь-яку очікувану вигоду. Стійкість цієї рівноваги забезпечується двома основними механізмами: економічною неефективністю атаки меншості та ефективністю механізмів slashing [1, 2].

У сценарії, коли валідатор діє індивідуально, його спроба здійснити подвійну витрату або іншу зловмисну дію буде відхилена більшістю чесних учасників, що робить атаку безрезультатною. Водночас, сучасні протоколи передбачають надійні механізми виявлення такої поведінки, які призводять до автоматичного застосування штрафних санкцій. Як показано в кількісному прикладі, втрата частини стейку (наприклад, 10 % або більше) створює значний фінансовий ризик, що робить атаку економічно нерентабельною. Це підтверджує, що механізм slashing є потужним дистимулом, який ефективно стримує індивідуальну зловмисну поведінку.

Водночас, аналіз виявив існування альтернативної рівноваги – "всі атакують", яка також може бути стійкою, але лише за умови контролю зловмисниками більшості стейку мережі. У такому випадку їхні дії не будуть виявлені, оскільки саме вони формують консенсус, і вони можуть отримати значну вигоду від успішної маніпуляції. Однак ця рівновага – теоретична ніж практична. Вартість придбання або контролю над більшістю стейку капіталізованого блокчейну (наприклад, Ethereum) значно перевищує потенційну вигоду від атаки. Це робить подібний сценарій економічно невигідним і підтверджує концепцію економічної безпеки, згідно з якою система захищена не лише технічно, а й тим, що атака є фінансово руйнівною для потенційного атакувальника.

Отримані результати мають безпосереднє практичне значення для розробників блокчейн-протоколів і підкреслюють важливість стратегічного калібрування ключових параметрів системи.

Оптимальний розмір штрафів (slashing penalty). Механізми покарання мають бути досить суворими, щоб потенційні втрати від зловмисної дії суттєво перевищували очікуваний виграш від чесної валідації. Це формує сильний дистимул до використання ризикованих стратегій.

Висока ймовірність виявлення зловмисних дій. Надійність механізмів доказу недобросовісної поведінки (proof-of-misbehaviour) – критично важлива. У PoS-протоколах, зокрема в Ethereum 2.0, подвійне підтвердження блоків легко виявляється, що забезпечує високу ймовірність виявлення ($\delta \approx 1$) для атак меншості [1, 2].

Економічна вартість атаки. Вартість набуття контролю над 51 % стейку має бути настільки високою, щоб перевищувати будь-яку потенційну вигоду від атаки. Це гарантує, що навіть теоретично можливі атаки не будуть реалізовані на практиці.

Привабливість чесної валідації. Окрім стримування зловмисної поведінки, протокол має забезпечувати достатні стимули до чесної участі. Винагороди за валідацію та атестацію повинні компенсувати операційні витрати та забезпечувати позитивний очікуваний дохід, що заохочує довгострокову участь валідаторів у мережі.

Обмеження моделі та напрямки майбутніх досліджень

Запропонована модель – аналітично строга, вона ґрунтується на низці спрощувальних припущень, які відкривають можливості для подальших досліджень:

Гомогенність валідаторів. Модель припускає, що всі валідатори мають однакові обсяги стейків та операційні витрати. У реальних мережах спостерігається значна неоднорідність – від дрібних індивідуальних учасників до великих валідаційних пулів. Перспективний напрямок це аналіз асиметричних моделей із різними типами гравців.

Статичний характер гри. Аналіз базується на одноразовому виборі стратегії. У реальних мережах валідатори взаємодіють протягом тривалого часу, що створює умови для стратегій, заснованих на репутації, довірі та повторюваних взаємодіях. Розширення моделі до повторюваної гри може виявити додаткові рівноважні стани.

Розширений стратегічний простір. У межах моделі розглянуто лише дві базові стратегії – чесну валідацію та атаку подвійної витрати. Інші форми зловмисної поведінки, зокрема як цензура транзакцій або атаки на живість мережі, можуть бути інтегровані в розширені версії моделі.

Моделювання кооперації. Валідаційні пули вносять елементи кооперації, які не повністю враховані в некооперативній моделі. Застосування апарату кооперативної теорії ігор дало б змогу дослідити внутрішню динаміку пулів та стратегії взаємодії між ними.

Динамічні параметри системи. У реальних системах параметри, такі як розмір винагород, комісії або загальний обсяг стейку змінюються з часом. Динамічне моделювання дозволило б аналізувати адаптацію стратегій валідаторів у відповідь на еволюцію мережі.

Незважаючи на значні обмеження, розроблена модель забезпечує міцну аналітичну основу для розуміння фундаментальних економічних механізмів, що лежать в основі стабільності PoS-систем. Вона демонструє, що теорія ігор це ефективний інструмент оцінки безпеки блокчейн-протоколів та оптимізації їхніх механізмів стимулювання.

Висновки. У цій статті було розроблено та проаналізовано математичну ігрову модель, спрямовану на дослідження стратегічної поведінки валідаторів у PoS блокчейн-системах. Застосування апарату теорії ігор дозволило формалізувати взаємодію учасників як некооперативну гру з повною інформацією, визначити функції корисності для ключових стратегій, зокрема, чесної валідації та спроби подвійної витрати, та проаналізувати існування рівноважних станів, насамперед рівноваги Неша.

Основний результат дослідження це демонстрація того, що в добре спроєктованих PoS-протоколах рівновага "всі чесні" – стійка та домінуюча. Це означає, що окремий валідатор, діючи раціонально, не має стимулу відхилятися від протокольних правил, оскільки потенційні втрати від неуспішної атаки – зумовлені механізмами slashing, значно перевищують очікуваний виграш від зловмисної дії. Умова стійкості цієї рівноваги це ефективність механізмів виявлення порушень та досить суворі штрафи, які роблять індивідуальні атаки економічно нерентабельними.

З іншого боку, показано, що рівновага "всі атакують", хоча може бути теоретично стабільна, але практично недосяжна в реальних умовах. Її існування передбачає контроль над більшістю стейку мережі, що потребує надзвичайно високих фінансових витрат. У більшості капіталізованих систем, таких як Ethereum, вартість придбання 51 % стейку значно перевищує потенційну вигоду від атаки, що робить цей сценарій економічно невигідним. Це підтверджує концепцію економічної безпеки: система захищена не лише технічно, а й завдяки тому, що атака фінансово руйнівна для потенційного зловмисника.

Ключовий висновок це те, що стабільність PoS-систем безпосередньо залежить від ретельного балансу економічних стимулів.

Ефективний дизайн протоколу повинен одночасно:

- заохочувати чесну поведінку шляхом забезпечення стабільного та привабливого доходу від валідації;
- стримувати зловмисні дії шляхом впровадження суворих та надійно виявлюваних штрафів;
- забезпечувати високу економічну вартість атаки, що робить її практично недосяжною для потенційних зловмисників.

Запропонована модель ґрунтується на певних спрощеннях – зокрема припущення гомогенності валідаторів і одноразового характеру гри, вона формує міцну аналітичну основу для розуміння фундаментальних механізмів безпеки PoS-мереж. Перспективним напрямком подальших досліджень є розширення моделі шляхом урахування неоднорідних агентів, повторюваного характеру гри, динамічної заміни параметрів системи, а також аналіз інших типів атак, зокрема цензури транзакцій, атак на забезпечення живучості системи.

References

1. Buterin V., Griffith V. Casper the Friendly Finality Gadget. Ithaca (NY): arXiv; 2017. https://doi.org/10.48550/arXiv.1710.09437
2. Buterin V. An incomplete guide to rollups Vitalik's website; 2021. https://vitalik.eth.limo/general/2021/01/05/rollup.html (accessed: 12.08.2025)
3. Eyal I., Sirer E.G. Majority is not enough: Bitcoin mining pools and the incentives for selfish mining. In: Christin N. Johnson A, editors. Financial Cryptography and Data Security: *XVIII International Conference*, FC 2014, Christ Church,

Barbados, March 3–7, 2014. Revised Selected Papers. Berlin: Springer; 2014. P. 436–450. (Lecture Notes in Computer Science; vol. 8437). https://doi.org/10.1007/978-3-662-45472-5_28
4. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Katz J, Shacham H, editors. Advances in Cryptology CRYPTO 2017. *XXXVII Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 20–24, 2017. Proceedings, Part I. Cham: Springer; 2017. p. 357–388. (Lecture Notes in Computer Science; vol. 10401). https://doi.org/10.1007/978-3-319-63688-7_12
5. Osborne M.J., Rubinstein A. A course in game theory. Cambridge (MA): MIT Press; 1994. 352 p.
6. Nash J.F. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences of the United States of America. 1950. 36 (1). P. 48–49. https://doi.org/10.1073/pnas.36.1.48
7. Godliuk V. Mathematical Models for Management Information Systems on Digital Platforms: from Resource Management to Demand Forecasting. *Cybernetics and Computer Technologies*. 2025. **2**. P. 37–46. https://doi.org/10.34229/2707-451X.25.2.3 (in Ukrainian)

Received/Одержано 31.10.2025 Accepted/Прийнято 03.03.2026 Published/Надруковано 27.03.2026

Годлюк Віктор Васильович,
аспірант Інституту кібернетики імені В.М. Глушкова, Київ, Україна.
https://orcid.org/0009-0007-4489-7058
goodiniv@ukr.net

UDC 004.75:519.83

Viktor Godliuk

Application of Game Theory Methods to Analyze Validator Interaction in Proof-Of-Stake Blockchain Systems

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Kyiv
Correspondence: goodiniv@ukr.net

This paper investigates the strategic behavior of validators in blockchain systems utilizing the Proof-of-Stake (PoS) consensus mechanism through the application of game theory. A mathematical model of a non-cooperative game with complete information is proposed, where validators act as rational agents aiming to maximize their expected payoff by choosing between honest validation and malicious actions, specifically a double-spending attack. The model incorporates key economic parameters of the system: block and attestation rewards, transaction fees, operational costs, slashing penalties, and the probability of detecting protocol violations. Utility functions for two primary strategies – honest and attacking – are formalized, and conditions for the existence of Nash equilibrium, the central solution concept in game theory, are analyzed.

The analysis demonstrates that under effective punishment mechanisms, the "all-honest" equilibrium is stable: an individual validator has no incentive to deviate from protocol-compliant behavior, as potential losses from penalties significantly outweigh any gains from a failed attack. Conversely, the "all-attackers" equilibrium, while theoretically possible, is practically unattainable due to the prohibitively high cost of acquiring a majority stake, rendering such a strategy economically infeasible. A quantitative example based on a hypothetical network of 1000 validators confirms these findings and highlights the critical importance of balancing incentives for honest behavior with strong disincentives for malicious actions.

The study emphasizes the crucial role of economic security in PoS systems, where stability is ensured not only by technical safeguards but also by carefully designed economic mechanisms. The developed model can be used by blockchain protocol designers to calibrate consensus parameters, thereby promoting decentralization, resilience, and long-term network reliability. Future research can extend the model by incorporating heterogeneous validators, repeated games, and the analysis of other attack vectors.

Keywords: Proof-of-Stake, validators, game theory, Nash equilibrium, economic security, slashing, double-spending attack, game model, blockchain, consensus.