УДК 004.75 **doi: 10.26906/SUNZ.2024.3.170**

Є. В. Шевчук, В. М. Федорченко

Харківський національний технічний університет радіоелектроніки, Харків, Україна

АНАЛІЗ ОСНОВНИХ ВРАЗЛИВОСТЕЙ І СПОСОБІВ ЗАХИСТУ МЕХАНІЗМУ КОНСЕНСУСУ В ДЕЦЕНТРАЛІЗОВАНИХ БЛОКЧЕЙН СИСТЕМАХ

Анотація. Актуальність. Захист механізму консенсусу в блокчейн системах – один з найважливіших напрямків у вдосконаленні децентралізованих блокчейн систем, цей механізм відповідає за валідацію транзакцій й підтвердженням що транзакції аутентичні, тобто цей механізм відповідає за захист ресурсів і грошей системі, також за захист від різноманітних вразливостей які створює децентралізація, тож аналіз таких вразливостей і захист механізму консенсусу є ключовою темою захисту децентралізованого блокчейну. **Метою даної роботи** є опис основних вразливостей та надання рекомендації щодо вибору підходу до захисту та побудови механізму консенсусу в децентралізованих блокчейн системах. **Об'єктом дослідження** є блокчейн. **Предметом дослідження** є механізм консенсусу децентралізованих блокчейн систем. **Результати**. В роботі були проаналізовані механізму консенсусу децентралізованих блокчейн систем, їх вразливості та методи захисту від них. **Висновок**. Механізм консенсусу децентралізованого блокчейну вірогідно не зможе бути повністю захищений ніколи через його децентралізовану природу, але можна звести ці ризики до мінімуму, наведені методи, а саме їх розумне комбінування допоможе знизити типові ризики будь яких загроз до мінімуму.

Ключові слова: блокчейн, консенсус, PoS, PoW, DPoS, VRF, double spending attack, selfish mining, censorship attack.

Вступ

Сьогодні блокчейн використовується в багатьох сферах, таких як:

- фінанси: децентралізовані фінанси (DeFi), смартконтракти, криптовалюти;
- логістика: відстеження ланцюгів поставок, запобігання контрафакту;
- охорона здоров'я: зберігання медичних записів, обмін даними;
- державне управління: цифрові ідентифікатори, голосування, прозорість урядових процесів.

Ця технологія має величезний потенціал для зміни світу. Вона може зробити нашу економіку більш ефективною, нашу систему управління більш прозорою, а наше життя – більш безпечним.

Блокчейн – це не просто криптовалюта. Це децентралізована база даних, що ведеться спільною мережею комп'ютерів. Завдяки цьому вона стає прозорою, безпечною та стійкою до цензури. Блокчейн – це не просто технологія, це нова парадигма довіри. Він дає нам можливість створювати децентралізовані системи, які не підлягають контролю жодної особи чи організації. І ця система була б неможливою без механізму консенсусу, технології, яка надає можливості створення чесної децентралізації яку як мінімум складно зламати якимось чином. Консенсус є ключовою технологію для децентралізованих блокчейн систем, він потрібен для того щоб система залишалася чесною для всіх учасників, ця система відповідає за створення нових блоків в блокчейні і за підтвердження цих блоків, отже вона відповідає за всі транзакції, всі операції в блокчейн, а отже його захист від злому є ключовою темою для захисту даних та користувачів в мережі блокчейн

Результати досліджень

1. Що таке блокчейн? Blockchain зобов'язаний своєю назвою тому, як він зберігає дані транзакцій – у блоках, пов'язаних разом, щоб утворити ланцюжок [1–5]. З ростом кількості транзакцій зростає і блокчейн. Блоки записують і підтверджують час і послідовність транзакцій, які потім реєструються в блокчейні в межах окремої мережі, що регулюється правилами, погодженими учасниками мережі. «Кожен блок містить хеш (цифровий відбиток або унікальний ідентифікатор), пакети останніх дійсних транзакцій із мітками часу та хеш попереднього блоку. Попередній хеш блоку пов'язує блоки разом і запобігає зміні будь-якого блоку або вставці блоку між двома існуючими блоками». Теоретично цей метод робить блокчейн захищеним від втручання.

Чотири ключові концепції блокчейну:

Спільна книга. Спільна книга – це розподілена система записів, яка «тільки для додавання» використовується в бізнес-мережі. «Завдяки спільній книзі транзакції реєструються лише один раз, усуваючи дублювання зусиль, типове для традиційних бізнес-мереж».

Дозволи. Дозволи забезпечують безпеку транзакцій, їх автентифікацію та можливість перевірки. «Завдяки можливості обмежувати участь у мережі організації можуть легше дотримуватися правил захисту даних, таких як ті, що передбачені в Законі про перенесення та підзвітність медичного страхування (HIPAA)» та Загальному регламенті ЄС щодо захисту даних (GDPR).

Розумні контракти. Розумний контракт – це «угода або набір правил, які регулюють бізнес-операцію; він зберігається в блокчейні та виконується автоматично як частина транзакції».

Консенсус. Завдяки консенсусу всі сторони погоджуються на транзакцію, перевірену мережею. Блокчейни мають різні механізми консенсусу, включаючи підтвердження частки, мультипідпис і PBFT (практична візантійська відмовостійкість).

У кожній блокчейн-мережі є різні учасники, які виконують такі ролі, зокрема:

Користувачі блокчейну. Учасники (зазвичай бізнес-користувачі) з дозволами приєднуватися до мережі

блокчейн і проводити транзакції з іншими учасниками мережі. ***Регулятори.*** Користувачі блокчейну зі спеціальними дозволами для контролю за транзакціями, що відбуваються в мережі. ***Оператори мережі блокчейн.*** Особи, які мають спеціальні дозволи та повноваження на визначення, створення, керування та моніторинг мережі блокчейн. ***Центри сертифікації***. Особи, які видають і керують різними типами сертифікатів, необхідних для запуску дозволеного блокчейну. На рис. 1 можна побачити просту схему блокчейна, кожен блок має в собі хеш і хеш минулого блоку, цей хеш збирається із кореня дерева меркла яке в свою чергу перевірити всі минулі транзакції, також воно слугує у вигляді ідентифікатора блоку транзакцій.

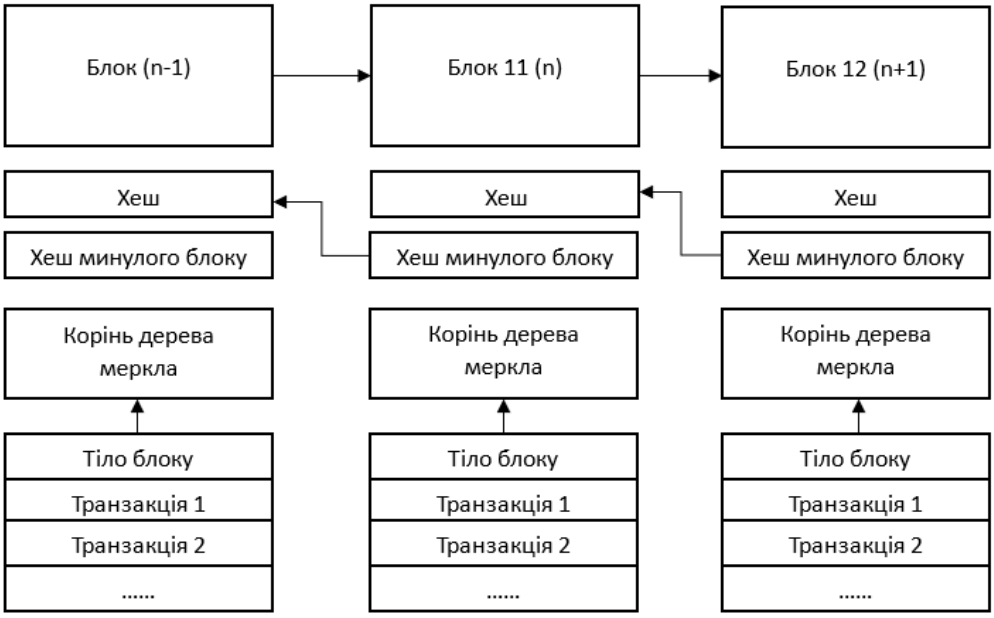

Рис. 1. Схема простого блокчейна

2. Що таке механізм консенсусу? Механізм консенсусу — це саморегульований стек програмних протоколів, записаних у код блокчейну, який синхронізує мережу для узгодження стану цифрової книги [6, 7, 8]. Це робиться шляхом підтримки єдиного набору даних — взаємно узгодженої версії історії транзакцій блокчейну — замість використання кожного вузла або комп'ютера в мережі для окремого збереження власної копії бази даних у повному обсязі. Незважаючи на те, що під час програмування мережевого стандарту верифікації слід враховувати різноманітні консенсусні механізми, кожен підхід спрямований на дискредитацію шахраїв у їхніх спробах заперечити записи.

Консенсус працює таким чином що вузли вводять дані з транзакції, що очікує на розгляд, а потім звітують із статусом схвалення або відхилення, коли запит буде перехресно перевірено з його записами. Наприклад, якщо користувач намагається обробити транзакцію, використовуючи раніше витрачені монети, які вже були враховані, цей запит буде легко відхилено щодо незмінної книги, що підтверджується несхваленням більшості. Користувачів, які не дотримуються консенсусу, часто блокують у мережі. У випадку, якщо вузол хоче оскаржити запис, йому доведеться подати запит на відкликання всієї мережі. Якщо більше ніж дві третини однорангових вузлів схвалюють, транзакція підтверджується, розповсюджується та постійно записується в блокчейн.

3. Основні вразливості механізму консенсусу блокчейн систем. На даний момент, існують три основні механізми консенсусу які блокчейни використовують для створення і валідації блоків транзакцій. PoW – proof of work, широко відомий механізм в якому для того щоб підтверджувати транзакції потрібно використовувати потужності процесорів або відеокарт [9, 10], найвідоміший його представник це Bitcoin. PoS – proof of stake механізм який активно набирає свою популярність, в цьому механізмі консенсусу вузол який створює блоки, відомий як валідатор, вибирається в залежності від того яку частину активів блокчейну вони вносять в якості застави, але й це тільки дає їм шанс бути вибраними, вузли вибираються випадково, чим більше застава ти більше шанс бути вибраним і отримати винагороду [11, 12], і як можна побачити на рис. 2 вибирається не одна нода для обробки а одразу декілька.

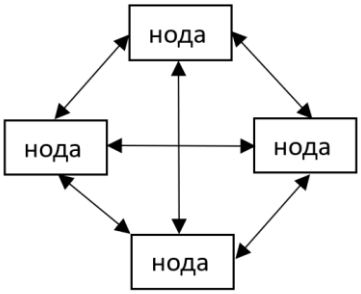

Рис. 2. PoS

Також вони перевіряють результати один одної, цей рисунок також можна віднести до PoW єдиною різницею слугує спосіб, по якому ця нода вибирається. DPoS – delegated proof of stake це механізм консенсусу який трохи нагадує PoS, але в в випадку з DPoS замість

того щоб всі вузли брали участь, власники валюти обирають делегатів, які відповідають за додавання нових блоків [13, 14].

Приклад цього DPoS можна побачити на рис. 3 тут також можна побачити що існують слідуючи ноди, ці ноди нічого не записують в блок транзакцій, але слідкують за тим щоб ці транзакції були правильними (працюють без винагородження).

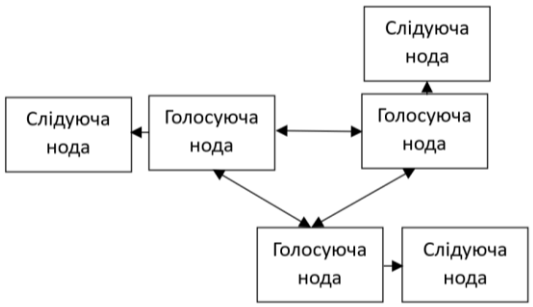

Рис. 3. DPoS

Не зважаючи на те, що в обох методах консенсусу ми отримуємо однаковий результат – валідований блок транзакції, шлях яким вони приходять до нього сильно відрізняється, і відповідно до цього шляху вони мають різні важливі вразливості.

Основні вразливості PoW:

• Атака 51% - якщо зловмисник контролює більше 50% обчислювальної потужності мережі, він може спробувати атаку 51%. Маючи мажоритарний контроль, зловмисник може переписати історію транзакцій, скасувати транзакції або подвійно витратити монети, підриваючи незмінність і безпеку блокчейну [15–17];

• Selfish mining - майнери можуть брати участь у егоїстичному майнінгу, де вони приховують розкриті блоки в мережі, щоб отримати перевагу. Це порушує справедливість процесу консенсусу та може призвести до ризиків централізації [15, 17];

• Double spending attacks - хоча PoW ускладнює подвійне витрачання, це не неможливо. Зловмисник із достатньою обчислювальною потужністю може спробувати видобути дві конфліктні транзакції одночасно, що потенційно призведе до подвійних витрат у разі успіху [17].

Основні вразливості PoS:

• Nothing at stake problem - у PoS валідаторам не потрібно витрачати ресурси (як у PoW), щоб брати участь у процесі консенсусу. Це відкриває двері до проблеми «Nothing at stake», коли валідатори можуть підтримувати кілька конфліктуючих ланцюжків, полегшуючи виконання мережних розгалужень і атак [17];

• Censorship attacks - заможні валідатори потенційно можуть вступити в змову, щоб цензурувати певні транзакції або надавати перевагу певним учасникам, оскільки вони мають більшу частку в безпеці мережі [15, 17];

• Stake Grinding - зловмисники потенційно можуть маніпулювати процесом відбору для створення блоку, змінюючи свою ставку або участь, підриваючи справедливість і безпеку механізму консенсусу [15, 16].

Основні вразливості DPoS:

• Централізація - влада зосереджена в руках невеликої кількості делегатів. Це може зробити систему більш сприятливою до різних типів атак [18];

• Зловживання владою – делегати можуть зловживати своєю владою, наприклад цензуруючи транзакції (ця проблема є як в PoS так і в DPoS) [19];

• Атака змови – делегати можуть змовитися з метою маніпулювання системою [20].

4. Способи захисту механізму консенсусу блокчейн систем Одним із варіантів для захисту механізму консенсусу є зміна його алгоритму, наприклад з PoW на PoS, але потрібно пам’ятати що такий підхід достатньо складно реалізувати, і можна завжди отримати інші вразливості нового механізму консенсусу [21]. Також важливим підходом до захисту систем є створення великих покарань для учасників системи які провели або намагаються провести атаку на систему, це сильно збільшить ризики для зловмисників, і відіб’є в них бажання атакувати систему, адже навіть неуспішна атака, а просто спроба зробити її призведе до колосальних збитків і зловмисники втратить всі свої ресурси. Також важливим аспектом є постійний аудит системи, він допомагає виявляти виникаючі вразливості, атаки які готуються, а також можливі маніпуляції в системі в минулому [22]. Створення централізованого нагляду, призведе до більшої централізації, але й до більшої безпеки, якщо блокчейн сильно пов’язаний з банківською справою або фінансами це може бути необхідним, це рішення можна використати для запобігання майже всіх існуючих вразливостей.

Захист PoW механізму консенсусу від атак 51% є збільшення часу затримки підтвердження блокчейну, цей варіант збільшує кількість часу для виявлення таких атак, і збільшує вартість таких атак, але також це збільшує час обробки всіх транзакцій, що призведе до падіння продуктивності блокчейна і збільшення вартості транзакції [23]. Для систем які щойно розвернулися і ще не набрали велику кількість валідаторів є можливість взяти на себе частину валідації, можливо навіть тимчасово взяти 51%, це призведе до більшої централізації, але на ранніх етапах до більшої безпеки.

Одним із найкращих способів захисту від selfish mining є зміна систем винагородження майнерів таким чином, що вигоди від використання цієї вразливості буде менше ніж в звичайних чесних майнерів.

Для того щоб захиститися від double spending атаки можна додати одноразові криптографічні записи які називаються nonce, значення цих записів має бути створене до того як блок буде добутий, його значення можна використати тільки один раз, такі записи слугують для того щоб переконуватися в унікальності блока, так само можна додати часові мітки на блоки, вони також слугують для підтвердження унікальності добутого блока [24].

Захиститися від nothing at stake можна впровадивши систему репутації валідатора, наприклад збільшення нагород для чесних валідаторів з гарною репутацією, або збільшення шансу що їх оберуть для валідації блоку, і протилежно для цього знижувати

нагороди і шанс на валідацію валідаторам з низькою репутацією, також можна додати штрафи для валідаторів які будуть помічені в конфліктуючих форках. Створення чекпоінтів це періодичне збереження блокчейну в певному моменті, всі валідатори мають будувати блокчейн далі тільки з цього чекпоінту, що унеможливить підтримку конфліктних форків.

Захистом від censorship attaks є використання спеціальних нод стеження, які будуть слідкувати за валідаторами і створювати звітність вірогідних порушень, створення методів валідації які будуть порівнювати транзакції з найдовшим ланцюжком блоків також допоможе уникнути long range attaks.

Від stake grinding захистом може стати використання перевіреної випадкової функції (VRF) для генерації випадковості блоків. VRF дозволяє власникам монет генерувати випадкові значення так, що ніхто крім власника не зможе створити їх за допомогою його приватного ключа, при цьому всі інші зможуть перевірити правильність згенерованого значення.

Захист від централізації в DPoS механізмі консенсусу можна впровадити використанням алгоритмів з множинними делегатами, це розподіляє владу між більшою кількістю учасників, і робить систему більш стійкою до атак, таким чином навіть учасники з найменшою долею зможуть приймати певну участь у голосуванні.

Захиститися від зловживання владою можна за допомогою створення механізмів відкликання, це дозволить користувачам видаляти делегатів, які зловживають своїми повноваженнями і використати смарт контракти для автоматизації виконання правил, і ускладнення зловживання повноваженнями.

Від атак змови можна захиститися використовуючи наведені вище системи репутації і порівнянням транзакцій з найдовшим кодом, це допоможе виявити зловмисних валідаторів завчасно.

Якщо все ж таки зловмисники змогли успішно атакувати ваш блокчейн, вихід все ще існує і це хард форк, як зображено на рис. 4. Хард форк можна зробити якщо валідатори погодяться в випадку з PoW це майнери, а у випадку з PoS і DPoS це стейк холдери, що чинний ланцюг має бути перетертий, то можна перестати вважати дійсним ланцюжок транзакцій в якому є сліди активності зловмисників, і почати новий, чистий, але якщо ми зробимо так, то всі транзакції в минулих блоках просто перетруться, а там суміщені не тільки транзакції зловмисників, а всі транзакції які були створені в цьому блокчейні в певний час, для цього також є вихід, можна взяти транзакції не пов'язані зі зловмисниками, і інтегрувати їх вже в новий ланцюжок, репутаційні збитки і можливо реальні залишаться, але будуть значно зменшені.

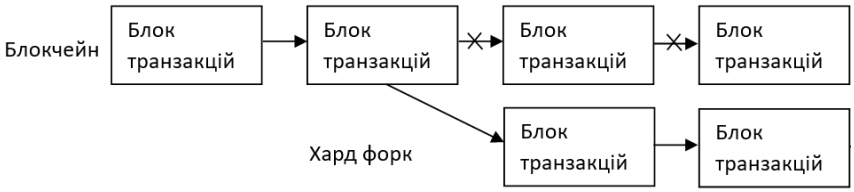

Рис. 4. Хард форк

Треба пам'ятати що головна вразливість механізму консенсусу це той факт що він контролюється не однією організацією, а великою групою людей, це як його головна особливість так і головний недолік, не зважаючи на те що абсолютного захисту на разі не існує, можна впровадити комбінацію захисних мір які зможуть не впливаючи на швидкість блокчейна збільшити його безпеку.

Важливо зменшити кількість вразливостей до мінімуму, бо кожна така вразливість збільшує можливості для створення інших атак, роблячи атаки таких типів дешевшими, а вразливість блокчейну більшою, найважливішими мірами для захисту від всіх типів атак є збільшення покарань в системі, наприклад втрата всіх вкладених монет зловмисником, проведення постійного аудиту системи, для того щоб виявляти атаки і вразливості завчасно і могти покарати зловмисника який ще не встиг завершити атаку, але вже втратить всі ресурси, що сильно збільшить ризики для них, якщо ж блокчейн пов'язаний з банківською інфраструктурою та фінансами можливим рішенням є більша централізація в руках керуючої компанії.

З методів захисту наведених вище можна вивести комбінацію технологій захисту, необхідно додати максимальні покарання за зловмисну діяльність, або за підготовку такої діяльності, в випадку з PoW це буде втрата всіх винагород і повна ануляція балансу пула зловмисників, також заборона працювати в вашому блокчейні для цього пула, в випадку з PoS і DPoS втрата всього стейку. Постійний аудит є дещо дорогою але необхідною мірою для виявлення і запобігання атак які готуються, для виявлення вразливостей до того як ними почнуть користуватися, а також маніпуляцій в системі в минулому.

Висновки

Механізм консенсусу децентралізованого блокчейну вірогідно не зможе бути повністю захищений ніколи через його децентралізовану природу, але можна звести ці ризики до мінімуму, наведені методи, а саме їх розумне комбінування допоможе знизити типові ризики будь яких загроз до мінімуму. Важливо пам'ятати що кожна загроза залишена в блокчейні несе ризики спрощення створення інших загроз, наприклад censorship attacks можуть запобігати виявленню як stake grinding так і nothing at stake.

Потрібно пам'ятати що через децентралізацію можна створити разом з учасниками хард форк, і вичистити всі зміни які зробив зловмисник, але це не означає що не постраждає як репутація цієї блокчейн системи так і вірогідно зловмисники зможуть заробити на ній, що призведе до збитків всіх інших

учасників системи. Важливо пам'ятати що в таких системах ідеальний захист, принаймні поки що неможливий, але варто робити все можливе для збільшення захисту блокчейну від якомога більшої кількості атак.

Треба також відмітити що блокчейн потрібно постійно вдосконалювати, адже постійно з'являються нові вразливості і методи захисту від них, адже ідеального захисту від атак не існує.

І ще однією важливою темою є праця розробників разом з спільнотою учасників децентралізованої системи, це допоможе забезпечити максимальну швидкість реакції на атаку, або швидко знайти вразливість.

СПИСОК ЛІТЕРАТУРИ

1. What is blockchain URL: https://www.ibm.com/topics/blockchain
2. Blockchain Facts: What Is It, How It Works, and How It Can Be Used URL: https://www.investopedia.com/terms/b/blockchain.asp
3. Understanding Blockchain Technology URL: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/
4. What is Blockchain Technology URL: https://www.coindesk.com/learn/what-is-blockchain-technology/
5. How does blockchain work URL: https://online.stanford.edu/how-does-blockchain-work
6. What Is a Consensus Mechanism URL: https://builtin.com/blockchain/consensus-mechanism
7. What Are Consensus Mechanisms in Blockchain and Cryptocurrency URL: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp
8. Consensus Mechanisms In Blockchain: A Deep Dive Into The Different Types URL: https://hacken.io/discover/consensus-mechanisms/
9. What Is Proof-of-work (PoW)? All You Need to Know URL: https://blockworks.co/news/what-is-proof-of-work
10. What Is Proof of Work (PoW) in Blockchain URL: https://www.investopedia.com/terms/p/proof-work.asp
11. What Does Proof-of-Stake (PoS) Mean in Crypto URL: https://www.investopedia.com/terms/p/proof-stake-pos.asp
12. What is proof of stake URL: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-proof-of-stake
13. What is Delegated Proof of Stake (DPoS)? Your Comprehensive Guide to DPoS URL: https://medium.com/unicorn-ultra/what-is-delegated-proof-of-stake-dpos-your-comprehensive-guide-to-dpos-07fd5185b108
14. What Is Delegated Proof-of-Stake (DPoS) URL: https://www.ledger.com/academy/what-is-delegated-proof-of-stake-dpos
15. Blockchain Common Vulnerability List URL: https://github.com/slowmist/Cryptocurrency-Security-Audit-Guide/blob/main/Blockchain-Common-Vulnerability-List.md
16. Blockchain Security: Common Vulnerabilities and How to Protect Against Them URL: https://hacken.io/insights/blockchain-security-vulnerabilities/
17. Blockchain Vulnerabilities and Attacks URL: https://www.linkedin.com/pulse/blockchain-vulnerabilities-attacks-yeshwanth-n/
18. Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Yu., Yevstrat, D., Chyrva, Yu. & Kuchuk, H. (2022), "Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples", *Eastern-European Journal of Enterprise Technologies*, 2022, 6 (4(120)), pp. 40–49, doi: https://doi.org/10.15587/1729-4061.2022.269128
19. Kovalenko, A., Kuchuk, H., Kuchuk, N. and Kostolny, J. (2021), "Horizontal scaling method for a hyperconverged network", 2021 International Conference on Information and Digital Technologies (IDT), Zilina, Slovakia, doi: https://doi.org/10.1109/IDT52577.2021.9497534
20. Petrovska, I. and Kuchuk, H. (2023), "Adaptive resource allocation method for data processing and security in cloud environment", Advanced Information Systems, vol. 7(3), pp. 67–73, doi: https://doi.org/10.20998/2522-9052.2023.3.10
21. Datsenko, S., and Kuchuk, H. (2023), "Biometric authentication utilizing convolutional neural networks", Advanced Information Systems, vol. 7, no. 2, pp. 67–73. Doi: https://doi.org/10.20998/2522-9052.2023.3.10
22. Kovalenko, A. and Kuchuk, H. (2022), "Methods to Manage Data in Self-healing Systems", Studies in Systems, Decision and Control, Vol. 425, pp. 113–171, doi: https://doi.org/10.1007/978-3-030-96546-4_3
23. 51% Attack: The Concept, Risks & Prevention URL: https://hacken.io/discover/51-percent-attack/
24. Understanding Double-Spending and How to Prevent Attacks URL: https://www.investopedia.com/terms/d/doublespending.asp

Received (Надійшла) 11.04.2024
Accepted for publication (Прийнята до друку) 12.06.2024

Analysis of the main vulnerabilities and ways of protection of the consensus mechanism in decentralized blockchain systems

Eugene Shevchuk, Volodymyr Fedorchenko

Abstract. **Topicality**. The protection of the consensus mechanism in blockchain systems is one of the most important directions in the improvement of decentralized blockchain systems, this mechanism is responsible for validating transactions and confirming that transactions are authentic, that is, this mechanism is responsible for protecting resources and money in the system, as well as protecting against various vulnerabilities created by decentralization. so analyzing such vulnerabilities and protecting the consensus mechanism is a key topic of decentralized blockchain security **The goal of this work** is a description of the main implications and recommendations for choosing an approach to protection and promoting a consensus mechanism in decentralized blockchain systems. **The subject of the research** is the impact of the consensus mechanism in decentralized blockchain systems. The subject of research is the consensus mechanism of decentralized blockchain systems. **Results**. The work analyzed the consensus mechanism of decentralized blockchain systems, their differences and methods of protection from them. **Conclusions**. The consensus mechanism of a decentralized blockchain is unlikely to be susceptible to theft through its decentralized nature, but it is possible to reduce the risks to a minimum by introducing methods, and their reasonable combination to help reduce the type of risks and any threats to a minimum.

Keywords: blockchain, consensus, PoS, PoW, DPoS, double spending attack, selfish mining, censorship attack.