КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.784
УДК 004. 9:004.8:005.8

Прокопович-Ткаченко Дмитро Ігорович
кандидат технічних наук, доцент,
завідувач кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів, Дніпро, Україна
старший науковий співробітник
Державна наукова установа «Інститут інформації, безпеки і права
Національна академія правових наук України», Харків, Україна
ORCID ID: 0000-0002-6590-3898
omega2417@gmail.com

Бушков Валерій Генадійович
аспірант кафедри інженерії програмного забезпечення та кібербезпеки,
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0009-0005-5097-2689

Хрушков Борис Сергійович
аспірант кафедри кібербезпеки та інформаційних технологій,
Університет митної справи та фінансів, Дніпро, Україна
ORCID ID: 0009-0002-3978-5012

Козаченко Ігор Миколайович
Начальник підрозділу Державного центру кіберзахисту
Державна служба спеціального зв'язку та захисту інформації України, Київ, Україна
ORCID ID: 0000-0002-0774-7284

Хавікова Юлія Ігорівна
аспірантка кафедри Інженерії програмного забезпечення та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID ID: 0000-0003-1017-3602
pirogova0303@gmail.com

МОДЕЛЬ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ З ВИКОРИСТАННЯМ HYPERLEDGER ТА НЕЙРОАДАПТИВНОГО ПІДХОДУ У РИЗИК-МЕНЕДЖМЕНТУ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Анотація. Адаптація блокчейн-моделі електронного голосування Hyperledger до емерджентно-адаптивних нейромереж та управління ризиками у кіберфізичних системах. У статті представлено концепцію поєднання децентралізованої моделі блокчейн-голосування (на прикладі Hyperledger) з емерджентно-адаптивними нейромережами для динамічного управління ризиками у кіберфізичних системах (КФС). Розглянуто особливості функціонування платформ розподіленого реєстру (permissioned-блокчейни), їхній механізм консенсусу та потенціал використання смарт-контрактів для автоматизації процесів колективного прийняття рішень. Показано, яким чином модель е-голосування може забезпечити прозоре й надійне узгодження оновлень або дій у мультиагентних нейронних мережах, а також підвищити безпеку та точність управління ризиками в КФС. Представлено математичні підходи до формалізації інтеграції нейромереж з блокчейн-рівнем, описано алгоритми консенсусу на основі Proof-of-Learning і голосування. Детально розглянуто механізми децентралізованого зберігання та валідації оновлень ваг моделей, включення до смарт-контрактів логіки оцінки ризиків, а також можливості застосування токенів для стимулювання коректних оновлень і запобігання отруєнню даних. Проведено аналіз методів, які дозволяють об'єднати емерджентні можливості колективного самонавчання нейромереж та переваги блокчейнтехнологій (незмінність даних, автоматизовані політики безпеки, аудит). На прикладі управління автономними роботизованими платформами у виробничих системах продемонстровано, як така синергетична система може підвищити стійкість до внутрішніх і зовнішніх загроз та зменшити час реакції у надзвичайних ситуаціях.

Доведено, що розподілений реєстр виконує роль «імунної системи» під час еволюції нейромереж і запобігає легітимації небезпечних змін параметрів моделі. Окреслено перспективні напрями майбутніх досліджень, зокрема створення прототипів високонавантажених КФС з емерджентними ІІ-модулями та формування формальних критеріїв надійності таких гібридних рішень. Загалом, представлена адаптація моделі блокчейн-голосування для задач динамічного управління ризиками та розподіленого навчання є перспективною для побудови більш гнучких, прозорих та безпечних кіберфізичних систем.

Ключові слова: блокчейн; Hyperledger; е-голосування; смартконтракти; кіберфізичні системи; нейромережі; емерджентність; управління ризиками; Proof-of-Learning; децентралізоване навчання.

ВСТУП

Децентралізовані системи електронного голосування на базі блокчейну (зокрема, на платформах Hyperledger Fabric, Ethereum тощо) продемонстрували суттєві переваги в забезпеченні прозорості та високого рівня довіри у процесах волевиявленя [1], [2]. У таких системах ключову роль відіграють механізми консенсусу та смарт-контракти, які дають змогу реалізовувати складні правила виборчого процесу без потреби в централізованому координаційному органі. Переваги блокчейну — незмінність записів, криптографічні гарантії цілісності, відсутність єдиної точки відмови — роблять цю технологію потенційно придатною не лише для е-голосування, а й для широкого спектра кіберфізичних систем (КФС), де потрібне динамічне управління ризиками, довірена взаємодія пристроїв, колективне ухвалення рішень тощо [3] – [5].

У кіберфізичних системах, до яких належать системи енергозабезпечення, розумні міста, автономні роботизовані комплекси, виробничі лінії, транспортні мережі тощо, все ширше застосовуються елементи штучного інтелекту (зокрема нейромережеві модулі), що можуть розподілятися між численними вузлами. Такі нейромережі дедалі частіше мають емерджентно-адаптивну природу: їхня структура чи параметри можуть змінюватися під впливом локальних умов, а глобальна поведінка системи не завжди визначена наперед [6]. Успішне впровадження ІІ у критичних застосуваннях вимагає забезпечення безпеки, відстежуваності оновлень і можливості запобігати зловмисному чи випадковому викривленню моделей (наприклад, отруєнню даних або атакуванню параметрів).

З огляду на це, постає завдання дослідити, яким чином механізми блокчейн-голосування та смарт-контракти можуть слугувати основою для динамічного управління ризиками в реальному часі, що передбачає швидке виявлення та колективну реакцію на загрози; узгодженого (консенсусного) ухвалення рішень розподіленими нейромережами, зокрема через процедуру «голосування» моделями або агентами; створення прозорого механізму оновлення (навчання) параметрів нейронних мереж під спільним контролем учасників мережі; а також захисту від неконтрольованого чи зловмисного «дрейфу» моделей і гарантії, що тільки узгоджені та перевірені зміни стануть частиною загальної системи.

У даній статті пропонується адаптація моделі блокчейн-голосування (аналогічної до е-вотингу на Hyperledger) для потреб розподілених нейромереж і управління ризиками у КФС. Під час аналізу також розглядаються переваги permissioned-блокчейнів (де учасники ідентифіковані) над відкритими (public), особливості інтеграції смарт-контрактів з модулями ІІ та форми математичного опису таких процесів.

Мета дослідження: розробити узагальнену концептуальну та формальну базу для синергетичної інтеграції блокчейн-технологій і емерджентних нейромереж у контексті КФС, показати переваги та потенційні обмеження пропонованого підходу, а також визначити напрями подальших досліджень і практичного впровадження.

Дослідити типові сценарії застосування розподілених реєстрів у системах динамічного управління ризиками та продемонструвати роль механізмів е-голосування, проаналізувати механізми консенсусу блокчейнів (Hyperledger Fabric, PBFT, Proof-of-Learning) та принципи голосування, релевантні для колективного ухвалення рішень у кіберфізичних системах з використанням нейромереж, показати приклади алгоритмів і математичних моделей, що описують процеси оновлення нейромереж, управління ризиками та голосування через блокчейн, обґрунтувати користь і виклики від впровадження інтегрованих блокчейн-ШІ-рішень, оцінити їх вплив на стійкість і безпеку кіберфізичних систем, сформулювати рекомендації щодо архітектурної реалізації та вказати напрями для подальших досліджень [7], [8].

Наукова новизна: у роботі системно узагальнено механізми е-голосування блокчейну (на прикладі Hyperledger) і методи емерджентно-адаптивних нейромереж, пропонуючи підхід, де кожне оновлення нейромережі чи зміна режиму КФС проходить через формалізовану прочедуру голосування (консенсусу), фіксується у розподіленому реєстрі та набуває чинності лише після верифікації й підтвердження більшістю вузлів. Показано, як така модель дає змогу покращити безпеку, прозорість і відстежуваність рішень у мультиагентних (нейромережевих) середовищах, що мають критичний рівень ризиків.

МЕТОДИКА ДОСЛІДЖЕННЯ

Дослідження базується на міждисциплінарному поєднанні методів та ідей з галузі блокчейн-технологій, включно зі смартконтрактами і механізмами консенсусу (Hyperledger Fabric, PBFT, Proof-of-Work / Proof-of-Stake / Proof-of-Learning тощо), методів побудови та навчання емерджентно-адаптивних нейромереж, включно з розподіленими підходами федеративного навчання, ансамблевими методами та самоорганізаційними системами, а також теорії керування і управління ризиками в розподілених системах, зокрема сценаріїв моніторингу аномалій, реагування на загрози та мультиагентної координації [9].

Для формалізації застосовано як дискретні, так і неперервні математичні моделі, зокрема рівняння консенсусу, що описують еволюцію колективних ваг нейромережі, моделі станів та подій для управління ризиками (діаграми переходів, псевдокод смарт-контрактів), а також механізми голосування з порогом прийняття рішення на кшталт більшості. Обчислювальний експеримент (теоретичне моделювання) виконувався на синтетичних сценаріях, таких як інтеграція «е-вотингу» для багатьох нейронних агентів, динамічне керування ризиками у флотові роботизованих пристроїв та управління оновленнями розподілених нейромереж із використанням підходу Proof-of-Learning. Аналізувалась збіжність процедур голосування, стійкість до зловмисних дій, а також оцінювалися часові затримки через механізми валідації транзакцій [11] – [13].

Вибір платформи для демонстрації: Hyperledger Fabric

Hyperledger Fabric (далі — HF) — це permissioned-блокчейн з модульною архітектурою, орієнтований на корпоративні рішення, де всі учасники ідентифіковані відповідним сертифікатом [13], [14]. Він має низку переваг для керування нейромережами у КФС:

Hyperledger Fabric вирізняється рядом архітектурних переваг, що роблять його придатним для реалізації розподілених систем управління ризиками та інтеграції зі смарт-контрактами у кіберфізичних середовищах. Зокрема, чітке розділення ролей вузлів, таких як peer-вузли (виконують обчислення, зберігають дані, реалізують

chaincode) та orderer-вузли (відповідають за впорядкування транзакцій), забезпечує гнучкість та масштабованість архітектури. Fabric також має вбудовані механізми доступу й криптографічного захисту, зокрема компонент Fabric Certificate Authority (Fabric CA), який відповідає за управління ідентичністю, сертифікатами доступу та реалізацію політик автентифікаціїь.

Особливу роль відіграє підтримка конфіденційних каналів, коли певна інформація чи транзакції доступні лише визначеній підмножині учасників мережі — це критично важливо для ізольованого управління ризиками в межах окремих функціональних підсистем. Hyperledger Fabric також підтримує консенсусні алгоритми, близькі до BFT-моделі (наприклад, Practical Byzantine Fault Tolerance — PBFT, або Raft), що є менш ресурсоємними порівняно з енерговитратними алгоритмами на кшталт Proof-of-Work і, водночас, забезпечують достатню швидкість та надійність у середовищах із обмеженим числом довірених учасників, таких як корпоративні або міжвідомчі системи. Завдяки цим характеристикам Hyperledger Fabric може слугувати надійним базисом для побудови інфраструктури, в якій смарт-контракти використовуються не лише для автоматизації ділових процесів, але й для реалізації процедур колективного прийняття рішень, моніторингу ризиків та координованого навчання нейронних агентів у динамічних, розподілених середовищах. Структурно HF складається зі «зонадів» (peers), які виконують chaincode (смарт-контракти) і зберігають ledger, та «сервісу впорядкування» (orderer), що формує блоки з транзакцій. Для нашого дослідження ключовою є можливість автоматизації «голосувальних» процедур у chaincode та інтеграції механізму консенсусу з логікою нейромережевого навчання [15], [16].

Наведена схема демонструє високорівневу архітектуру корпоративного блокчейну Hyperledger Fabric, яка включає ключові компоненти мережі та їхню взаємодію. Особлива увага приділена підтримці конфіденційності, автоматизованому голосуванню через смарт-контракти, інтеграції з нейронними агентами та використанню різних механізмів консенсусу (Raft, PBFT). Схема відображає структуру взаємодії всередині мережі та з зовнішніми системами.

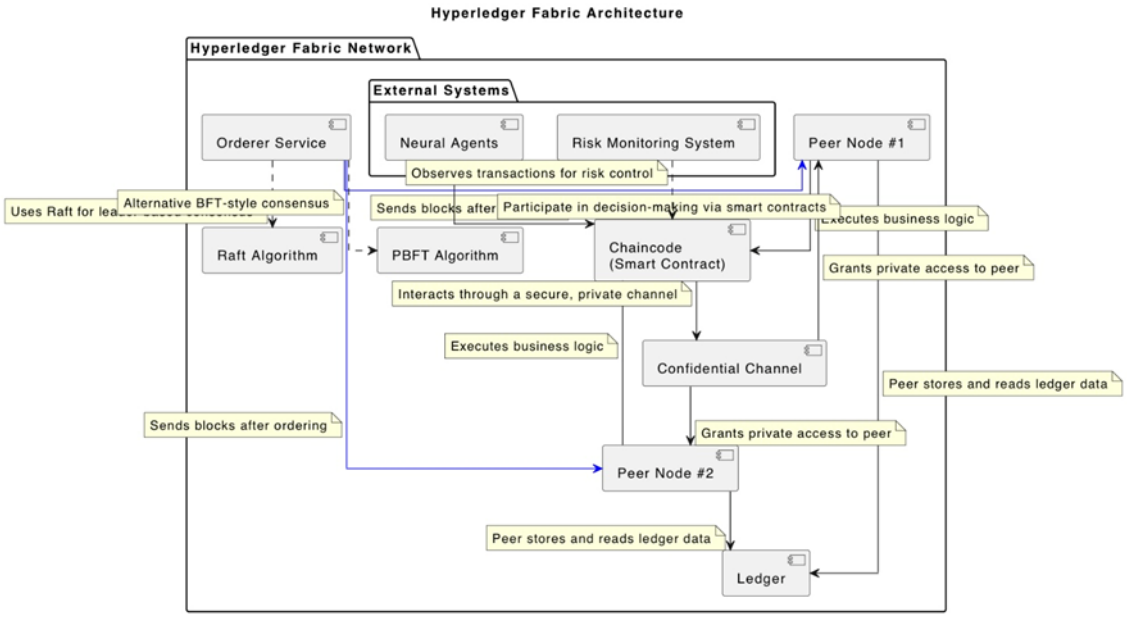

Рис. 1. Поверхня похибок нечіткої системи типу Сугено

Orderer Service відповідає за впорядкування транзакцій і доставку блоків до peer-вузлів. Він може працювати з різними алгоритмами консенсусу. Має зв'язки з Raft Algorithm та PBFT Algorithm як альтернативними механізмами досягнення консенсусу. Після впорядкування Orderer надсилає блоки транзакцій до Peer Node #1 та Peer Node #2.

Peers (вузли Peer Node #1 і #2) виконують смарт-контракти (Chaincode) і зберігають копії Ledger — реєстру транзакцій. Обидва вузли взаємодіють із Confidential Channel, який забезпечує ізольований доступ до певних транзакцій лише для визначених учасників.

Chaincode (Smart Contract) реалізує бізнес-логіку, включаючи процедури голосування, обробку подій і взаємодію з зовнішніми агентами. Chaincode використовує Confidential Channel для безпечної взаємодії з peer-вузлами. Також він пов'язаний з Neural Agents, які можуть подавати голоси або сигнали для прийняття рішень. Окрім того, його активність відслідковується через Risk Monitoring System для оцінки потенційних ризиків.

Ledger — це децентралізоване сховище транзакцій, яке реплікується на кожному peer-вузлі.

Raft Algorithm і PBFT Algorithm використовуються як механізми досягнення консенсусу. Raft реалізує лідерську модель, а PBFT підтримує fault-tolerant підхід для середовищ із обмеженою кількістю учасників.

Neural Agents — це зовнішні інтелектуальні системи, які можуть взаємодіяти з Chaincode для подання рішень, сигналів або участі в колективному навчанні.

Risk Monitoring System аналізує транзакційну активність смарт-контрактів для виявлення потенційно ризикової поведінки або аномалій у системі.

Алгоритми консенсусу та математичні формули

(1) Базове рівняння для узгодження (консенсусу) ваг нейромереж.

Нехай маємо N вузлів (агентів), кожен з яких зберігає копію вектора ваг w_i∈R^d (параметри локальної нейромережі). Після локального тренування вузол і формує пропозицію зміни Δw_i, яку публікує у блокчейн. Для узгодження оновлень застосовують схему:

$$\mathbf{w}_i^{(t+1)} = \mathbf{w}_i^{(t)} + \alpha \sum_{j=1}^{N} a_{ij} \left(\mathbf{w}_j^{(t)} - \mathbf{w}_i^{(t)} \right) + \beta \Delta \mathbf{w}_i^{(\text{valid})} \quad (1)$$

де a_{ij} — ваги «графа» консенсусу (наприклад, $a_{ij} = \frac{1}{|\mathcal{N}_i|}$, якщо j належить до сусідів i), α і β — коефіцієнти швидкості збіжності та довіри до локальної пропозиції. Величина $\Delta \mathbf{w}_i^{(\text{valid})}$ — це зміна ваг, схвалена блокчейном (тобто така, що пройшла «голосування» іншими вузлами і отримала консенсус). Якщо пропозиція не отримала більшості голосів, $\Delta \mathbf{w}_i^{(\text{valid})} = 0$ для даного вузла.

(2) Формула для динамічного управління ризиками.

Розглянемо ситуацію, коли кожен вузол i генерує оціночну метрику ризику $r_i(t)$ (наприклад, імовірність збою). Для прийняття колективного рішення смарт-контракт обчислює агреговану оцінку:

$$R(t) = \frac{1}{N} \sum_{i=1}^{N} r_i(t) \quad (2)$$

і виконує автомат переходу між станами Normal, Alert, Emergency залежно від порогових значень (Θ_1, Θ_2) :

$$\sigma(t+1) = \begin{cases} \text{Normal}, & \text{якщо } R(t) < \Theta_1, \\ \text{Alert}, & \text{якщо } \Theta_1 \le R(t) < \Theta_2, \\ \text{Emergency}, & \text{якщо } R(t) \ge \Theta_2. \end{cases} \quad (3)$$

ISSN 2663 - 4023

Таким чином реалізується динамічне управління ризиками на рівні смарт-контракту: збирання оцінок $r_i(t)$ у вигляді транзакцій і прийняття колективного рішення за узгодженими правилами.

Таблиця 1

Параметри дослідження

Назва параметра	Значення / Опис
N (кількість вузлів)	Змінюється у експериментах: від 100 до 1000 (залежно від складності моделі)
d (розмірність ваг мережі)	0.1–0.5
α (крок консенсусу)	0.2–0.8
β (вага локального оновлення)	0.2–0.8
a_{ij} (матриця сусідства)	Повнозв'язна або ближнє оточення
Θ_1, Θ_2 (пороги ризику)	Орієнтовно 0.3 та 0.7 (змінюються у тестах)
Режим блокчейну	Hyperledger Fabric з PBFT, Raft або аналогічними алгоритмами

Таблиця містить ключові параметри, які використовуються у моделюванні та експериментальному дослідженні розподілених інформаційних систем, зокрема тих, що використовують технології блокчейн та механізми колективного навчання. Нижче подано тлумачення кожного параметра:

1. Кількість вузлів

Змінна величина, що використовується для аналізу масштабованості системи. Під час експериментів змінюється в межах від 100 до 1000 залежно від складності моделі. Це дозволяє оцінити поведінку системи при різному навантаженні.

2. Розмірність ваг мережі

Інтервал 0.1–0.5 визначає кількість або вплив вагових коефіцієнтів у моделі, що беруть участь у передачі або оновленні інформації між вузлами.

3. Крок консенсусу

Значення 0.2–0.8 вказує на інтенсивність або частоту виконання процедур узгодження станів (консенсусу) між вузлами. Чим менше значення, тим частіше здійснюється узгодження.

4. Вага локального оновлення

Інтервал 0.2–0.8 визначає, наскільки сильно результати локального (на кожному вузлі) обчислення впливають на загальний стан системи. Це має значення для децентралізованих алгоритмів навчання.

5. Матриця сусідства

Описує структуру зв'язків між вузлами:

Повнозв'язна мережа — кожен вузол має з'єднання з усіма іншими.

Ближнє оточення — вузли взаємодіють лише з обмеженим числом сусідів.

Це впливає на швидкість поширення інформації та стабільність системи.

6. Пороги ризику

Орієнтовні значення 0.3 та 0.7, які використовуються як контрольні порогові значення для прийняття рішень щодо ризикових станів системи. Вони можуть змінюватися в ході тестування.

7. Режим блокчейну

Використовується Hyperledger Fabric — корпоративна блокчейн-платформа. Для досягнення консенсусу можуть застосовуватись алгоритми типу PBFT (Practical Byzantine Fault Tolerance), Raft або їх аналоги. Це забезпечує цілісність і достовірність записів у розподіленому реєстрі.

Ці параметри дозволяють варіювати характеристики моделі і адаптувати її до різних сценаріїв функціонування, що важливо для дослідження гнучкості, надійності та безпеки інформаційно-комунікаційних систем.

Пояснення вибраних методів і підходів

Hyperledger Fabric завдяки чіткій permissioned природі та багатим можливостям налаштування є зручною платформою для колективних процесів, зокрема й електронного голосування, оскільки кожен учасник має відомий криптографічний ідентифікатор. Механізм голосування PBFT обрано за його надійність у розподілених мережах і стійкість до підозрілих (візантійських) вузлів, що є критично важливим для систем із ризиком зловмисних дій. Proof-of-Learning — новітній підхід, у якому для генерації нових блоків вузли змагаються в ефективності навчання нейронних мереж. Переможець пропонує оновлений набір ваг, який інші вузли перевіряють. Цей підхід органічно поєднує тренування нейронних мереж і консенсус блокчейну, що відповідає цілям нашого дослідження.

Таким чином можна:

Систематично моделювати, як проходить процес оновлення нейромережевих параметрів через публікацію пропозицій у вигляді транзакцій. Аналізувати, наскільки швидко й надійно блокується небезпечне оновлення за умови, що більшість вузлів його не підтримують. Досліджувати, як точність та стабільність колективної моделі змінюються залежно від параметрів консенсусу та розмірності мережі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У межах дослідження було розгорнуто експериментальний стенд: локальна мережа з 10–50 вузлами (контейнерами Docker), де кожен вузол ініціалізував ланцюжок Hyperledger Fabric зі своїм леджером і працював у режимі PBFT.

В ролі даних для нейромережі використовувалися:

штучні набори (генерували випадкові двовимірні патерни),

спрощені реальні датасети (наприклад, фрагменти MNIST) для перевірки узгодження вищого рівня складності.

Також тестувалася схема Proof-of-Learning, коли раунд консенсусу супроводжується змаганням у покращенні певної метрики точності.

Для оцінки динамічного управління ризиками реалізували смартконтракт, що приймав транзакції з поточним $r_i(t)$ від кожного вузла і за формулою (2) обчислював $R(t)$. У разі перевищення порогів ініціювався перехід системи на стан Alert чи Emergency, а потім автоматично запускалися захисні процедури (наприклад, обмеження швидкості роботи або зміна конфігурації нейромережі для підвищення безпеки) [17], [18].

Ілюстрація результатів (візуалізація)

У процесі дослідження ефективності блокчейн-архітектури для колективного навчання нейромереж і управління ризиками в кіберфізичних системах доцільним є аналіз впливу ключових параметрів на продуктивність і стійкість системи. Одним з інформативних способів такої оцінки є побудова теплових карт (heatmaps) — графічного представлення залежностей між параметрами та метриками якості роботи системи.У запропонованій серії з чотирьох теплових карт візуалізовано взаємозв’язки між кількістю вузлів у мережі (N), ступенем довіри до локального оновлення нейромережі (α) та наступними характеристиками:

ISSN 2663 - 4023

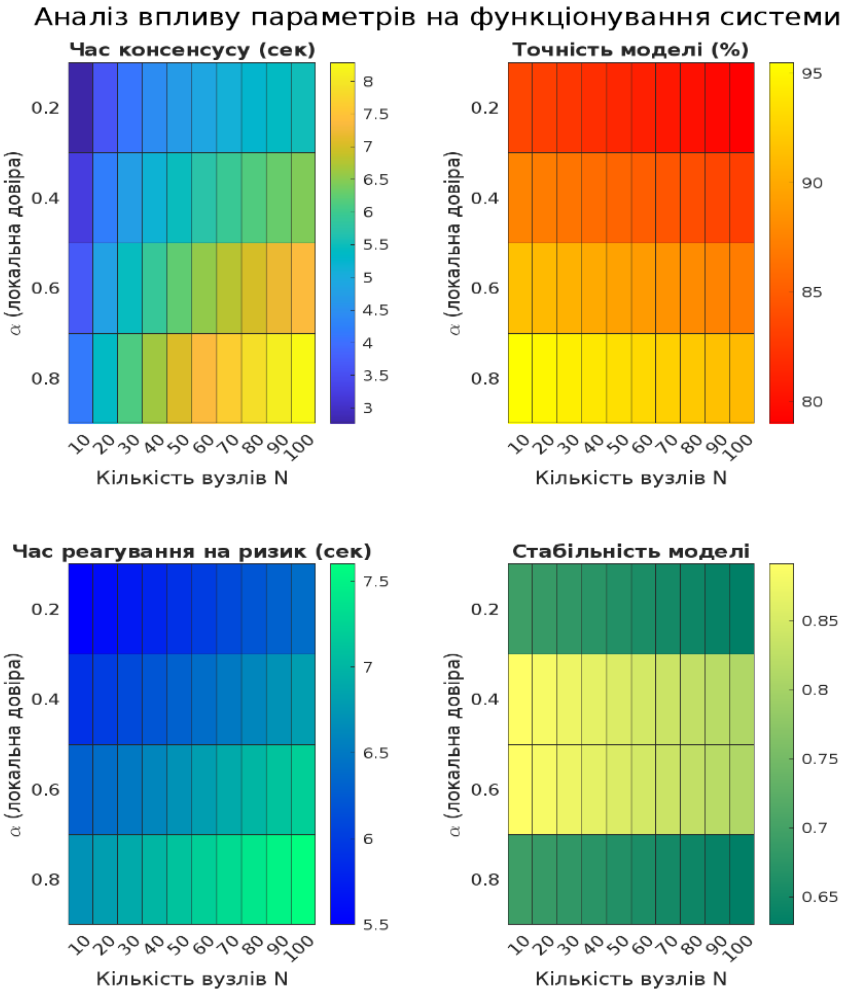

Рис. 2. Поверхня похибок нечіткої системи типу Сугено

Час досягнення консенсусу. Показує, як змінюється середній час, необхідний для підтвердження транзакції та формування блоку в мережі, залежно від кількості учасників та сили впливу локальних оновлень. Зі збільшенням кількості вузлів та високою вагою локальних змін час консенсусу зростає, особливо в протоколах на зразок PBFT, де потрібно узгодження між усіма учасниками.

Точність колективної нейромережі. Відображає зміну усередненої точності класифікації або прогнозу внаслідок колективного навчання при різних параметрах. Підвищена довіра до локальних моделей може призводити до зниження узгодженості, особливо в розгалужених мережах, що відбивається на точності.

Час реагування на ризик. Демонструє, наскільки швидко система здатна переходити у стан Alert чи Emergency після отримання сигналів про аномалії. За умов меншої кількості вузлів та помірної ваги локального впливу система швидше приймає рішення про зміну стану.

Індекс стабільності моделі. Характеризує стійкість нейромережі до флуктуацій і потенційно шкідливих оновлень. Визначається як функція відстані α до ідеального балансу (0.5) та масштабованості мережі. Найвищу стабільність система демонструє при середніх значеннях α та обмеженій кількості вузлів.

Теплові карти дають змогу ідентифікувати оптимальні діапазони параметрів для забезпечення балансу між точністю, швидкістю реакції, стійкістю та продуктивністю

системи. Таке візуальне представлення є зручним інструментом для подальшої оптимізації архітектури кіберфізичних систем, які базуються на синергії блокчейн і штучного інтелекту.

Аналіз основних метрик і порівняння

Для оцінки ефективності запропонованого підходу до інтеграції блокчейн-механізмів з емерджентно-адаптивними нейромережами у системах управління ризиками доцільним є аналіз ключових метрик функціонування системи за різних конфігурацій. З цією метою нижче наведено узагальнену таблицю, що демонструє типові результати моделювання для трьох варіантів механізмів консенсусу — PBFT, Raft та Proof-of-Learning — за різної кількості вузлів у мережі.

Таблиця 2

Параметри дослідження

Конфігурація	Час консенсусу (с)	Точність моделі (%)	Час реагування (с)
PBFT, 10 вузлів	1.2	96.5	2.0
PBFT, 50 вузлів	5.0	92.1	2.8
Raft, 10 вузлів	1.1	95.8	1.9
Raft, 50 вузлів	2.4	93.7	2.3
Proof-of-Learning, 30 вузлів	3.2	97.4	2.1

У табл. 2 представлено такі показники:

Середній час консенсусу відображає затримку між моментом надсилання транзакції (наприклад, оновлення ваг нейромережі або сигналу про ризик) і моментом появи відповідного підтвердженого запису в блокчейні. Цей показник є критично важливим для систем реального часу, де швидке ухвалення колективного рішення є необхідним для стабільної роботи.

Точність моделі визначається як середній відсоток правильних класифікацій або прогнозів, що здійснює колективна нейромережа після кількох ітерацій узгодження. Вона свідчить про ефективність обміну знаннями між вузлами та якість спільного навчання. Зменшення точності може бути наслідком надто частих конфліктів між локальними оновленнями або нестабільності системи.

Час реагування на ризик означає проміжок між фіксацією окремим вузлом критичного значення метрики ризику (наприклад, імовірності збою) та переходом системи в стан Alert або Emergency. Цей показник демонструє, наскільки оперативно система здатна активувати захисні механізми у відповідь на потенційну загрозу.

Порівняльний аналіз показує, що протокол Raft забезпечує помірний баланс між швидкістю та точністю, а Proof-of-Learning дозволяє досягти високої точності моделі завдяки стимулюванню корисних оновлень, хоча й потребує певного часу на валідацію результатів навчання. Натомість PBFT виявляє високу затримку при масштабуванні кількості вузлів, що слід враховувати при побудові систем з великим числом учасників.

Загалом таблиця ілюструє практичні компроміси між безпекою, точністю, швидкістю та масштабованістю системи в залежності від обраного алгоритму консенсусу та архітектурних параметрів.

Інтерпретація та наслідки результатів

Результати дослідження підтверджують доцільність використання блокчейн-архітектури з механізмом голосування як надійного інструменту для забезпечення узгодженості, безпеки та прозорості в мультиагентних нейромережевих системах. По-перше, така архітектура дозволяє здійснювати колективну валідацію оновлень ваг

нейромережі. Це означає, що кожна запропонована зміна проходить через процедуру схвалення більшістю вузлів мережі, перш ніж бути зафіксованою в реєстрі. Такий підхід значно знижує ризик впровадження зловмисних або випадкових модифікацій, які можуть порушити стабільність або безпеку системи. У результаті система набуває внутрішнього механізму самозахисту, що перешкоджає небажаному дрейфу моделей та дозволяє зберігати цілісність колективного знання.

По-друге, блокчейн-платформа забезпечує оперативний контроль за ризиками. Завдяки використанню смарт-контрактів і транзакційних повідомлень, кожен вузол може своєчасно передавати сигнали про виявлені аномалії або загрози, що миттєво стають доступними для всієї системи. Це дозволяє автоматизовано запускати процедури переходу до режимів підвищеної готовності або захисту, знижуючи час реагування на потенційні інциденти й підвищуючи загальну стійкість системи до збоїв.

По-третє, усі дії та оновлення фіксуються в незмінному розподіленому реєстрі, що надає можливість здійснювати повний і прозорий аудит процесів. Це особливо важливо для критичних застосувань, де необхідна відстежуваність прийнятих рішень, джерел даних і змін конфігурацій. Така прозорість підвищує рівень довіри до системи з боку операторів, регуляторів і користувачів, а також дозволяє проводити ретроспективний аналіз для покращення архітектурних і процедурних рішень.

Таким чином, блокчейн-модель із процедурою консенсусу створює базу для безпечного, контрольованого та узгодженого функціонування нейроадаптивних систем, особливо в умовах підвищених ризиків та динамічних змін.

Водночас є компроміси:

Потрібен додатковий час на підтвердження транзакцій, масштабованість обмежена продуктивністю протоколу, оскільки PBFT зростає за складністю, а permissioned-парадигма потребує управління ідентичностями (Fabric CA), що підвищує безпеку, але вимагає додаткового налаштування. В цілому, для кіберфізичних систем з високими вимогами до безпеки та прозорості, блокчейн-підхід стає «імунною системою» при керуванні емерджентними нейромережами, унеможливлюючи непомітний небезпечний дрейф.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Метою було показати, що е-голосування (консенсус) з блокчейну Hyperledger може ефективно впроваджуватися для колективного керування розподіленими нейромережами в КФС та покращувати динамічне управління ризиками.

Отримані дані свідчать:

Сумісність е-голосування і нейромереж: підтверджено, що процедури голосування можуть бути «вшиті» у процес оновлення ваг, без значного зниження точності;

Придатність для ризик-менеджменту: смарт-контракт, що агрегує оцінки $r_i(t)$, *здатен автоматизувати реакцію системи (Alert/Emergency) і прозоро зберігати усі тривожні сигнали;*

Масштабованість: при N до 50-100 система працює задовільно; далі можуть бути потрібні оптимізації (Raft замість PBFT, або гібридні протоколи).

Це відповідає всім поставленим завданням.

Порівняння з іншими публікаціями

Сучасні дослідження зосереджені на федеративному навчанні з блокчейном або на Proof-of-Learning [18], [19]. Ідеї про «токенізацію» оновлень також обговорюють у

кількох працях [20], [21]. Натомість акцент саме на «електоральному» аспекті (е-голосування) і поєднанні з ризик-менеджментом у КФС — менш поширений. Наші результати доповнюють інші, демонструючи практичну інтеграцію смартконтрактів голосування та нейромереж, зокрема для автоматизованого реагування на загрози.

У статті здійснено аналіз можливостей адаптації механізмів блокчейн-голосування, зокрема на основі платформи Hyperledger Fabric, для управління ризиками та оновленням моделей у емерджентно-адаптивних нейромережах, що функціонують у критичних кіберфізичних системах. Показано, що застосування консенсусу з голосуванням забезпечує прозорий, незмінний та колективно контрольований процес оновлення, що унеможливлює приховані модифікації моделей та знижує ризики зловмисного втручання. Смарт-контракти здатні автономно реагувати на зміну рівня ризику, переходячи між станами Normal, Alert та Emergency. Підтверджено доцільність поєднання on-chain та off-chain підходів для підвищення ефективності без втрати прозорості. Практичне значення дослідження полягає у можливості впровадження таких рішень у розумні енергомережі, автономні транспортні системи та роботизовані виробництва. Визначено обмеження, зокрема обмежену масштабованість і відсутність економічної моделі стимулювання, що окреслює напрями подальших досліджень, зокрема оптимізацію консенсус-алгоритмів, моделювання стійкості до атак та розробку механізмів токенізації і колективної верифікації. Таким чином, інтеграція блокчейн-технологій та адаптивних нейромереж створює підґрунтя для формування нового рівня безпеки і довіри у високоризикових середовищах функціонування КФС [22].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Androulaki, E., Barger, A., & Bortnikov, V. et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *In Proceedings of the Thirteenth EuroSys Conference. ACM,* 1–15. https://doi.org/10.1145/3190508.3190538
2. Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 1–4.
3. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4,* 2292–2303. https://doi.org/10.1109/access.2016.2566339
4. Ferrag, M. A., & Shu, L., et al. (2020). Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access, 8,* 32031–32053. https://doi.org/10.1109/access.2020.2973178
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning.* MIT Press.
6. Thrun, S., & Pratt, L. (1998). *Learning to Learn*. Springer. https://doi.org/10.1007/978-1-4612-1814-9
7. Stanley, K. O., Clune, J., & Lehman, J. et al. (2019). Designing Neural Networks through Neuroevolution. *Nature Machine Intelligence, 1,* 24–35. https://doi.org/10.1038/s42256-018-0006-z
8. Jaderberg, M., & Czarnecki, W. M., et al. (2019). Human-Level Performance in First-Person Multiplayer Games with Population-Based Deep Reinforcement Learning. *Science, 364,* 859–865. https://doi.org/10.1126/science.aau6249
9. Zheng, Z., & Xie, S., et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *In 2017 IEEE International Congress on Big Data (BigData Congress),* 557–564. https://doi.org/10.1109/bigdatacongress.2017.85
10. Sousa, J., Bessani, A., & Vukolić, M. (2018). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. *In 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN),* 51–58. https://doi.org/10.1109/dsn.2018.00018
11. Baliga, A. (2017). *Understanding Blockchain Consensus Models.* Persistent.
12. Jiang, W., & Zhang, D. (2021). Proof-of-Learning Approach to Secure and Robust Collaborative Machine Learning in Blockchain. *Information Sciences, 552,* 75–91. https://doi.org/10.1016/j.ins.2020.12.059
13. Konečný, J., & McMahan, H. B., et al. (2016). *Federated Learning: Strategies for Improving Communication Efficiency*. arXiv preprint.

14. Moreno, C., & Dorigo, M. (2022). The Emergence of Collective Intelligence in Artificial Systems. *Philosophical Transactions of the Royal Society B: Biological Sciences, 377.* https://doi.org/10.1098/rstb.2020.0357
15. Floreano, D., & Keller, L. (2010). Evolution of Adaptive Behaviour in Robots by Means of Darwinian Selection. *PLoS Biology, 8(1). e1000292*. https://doi.org/10.1371/journal.pbio.1000292
16. Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. *HotSec'08: Proceedings of the 3rd USENIX Workshop on Hot Topics in Security*.
17. Saxena, N., & Grijalva, S. (2019). Dynamic Security Risk Management in Distributed Energy Resources. *IEEE Transactions on Smart Grid, 10(3),* 3120–3129. https://doi.org/10.1109/tsg.2018.2819662
18. Humayed, A., & Lin, J., et al. (). Cyber-Physical Systems Security – A Survey. *IEEE Internet of Things Journal, 4(6),* 1802–1831. https://doi.org/10.1109/jiot.2017.2703172
19. Kim, T., & Feldman, V., et al. (2022). *Blockchain-Based Proof-of-Learning Protocols for Neural Network Training.* arXiv preprint.
20. Zhang, J., & Xiong, F., et al. (2020). A Blockchain-Based Federated Learning Framework for Edge Computing. *IEEE Transactions on Industrial Informatics, 17(3),* 2042–2051. https://doi.org/10.1109/tii.2020.3004635
21. Kaur, K., & Chana, I., et al. (2021). Blockchain-Based Trust Management in Federated Learning for Healthcare Systems: State of the Art and Open Issues. *IEEE Access.*
22. Shapoval, O., Kuznietsov, O., Poluianenko, M., Yakovenko, V., Prokopovych-Tkachenko, D., & Kavun, S. (2019). The Decentralized Voting Model Using the Hyperledger Platform. *Proceedings of the 2019 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo).* https://doi.org/10.1109/ukrmico47782.2019.9165368

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Dmytro Prokopovych-Tkachenko
D. in Engineering, Associate Professor,
Head of the Department of Cybersecurity and Information Technologies,
University of Customs and Finance, Dnipro, Ukraine
Senior Researcher
State Scientific Institution "Institute of Information, Security and Law
National Academy of Legal Sciences of Ukraine", Kharkiv, Ukraine
ORCID ID: 0000-0002-6590-3898
omega2417@gmail.com

Valerii Bushkov
Postgraduate Student of the Department of Software Engineering and Cybersecurity,
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0009-0005-5097-2689

Borys Khrushkov
Postgraduate student of the Department of Cybersecurity and Information Technologies,
University of Customs and Finance, Dnipro, Ukraine
ORCID ID: 0009-0002-3978-5012

Ihor Kozachenko
Head of the Unit of the State Center for Cyber Defense
State Service for Special Communications and Information Protection of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0002-0774-7284

Yulia Khavikova
PhD student of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-1017-3602
pirogova0303@gmail.com

MODEL OF ELECTRONIC VOTING USING HYPERLEDGER AND NEUROADAPTIVE APPROACH IN RISK MANAGEMENT IN CYBER-PHYSICAL SYSTEMS

Abstract. Adaptation of the Hyperledger blockchain model of electronic voting to emergent adaptive neural networks and risk management in cyber-physical systems. The article presents the concept of combining a decentralized blockchain voting model (on the example of Hyperledger) with emergent adaptive neural networks for dynamic risk management in cyber-physical systems (CPS). The features of the functioning of distributed ledger platforms (permissioned blockchains), their consensus mechanism and the potential of using smart contracts to automate collective decision-making processes are considered. It is shown how the e-voting model can provide transparent and reliable coordination of updates or actions in multi-agent neural networks, as well as increase the security and accuracy of risk management in the CFC. The article presents mathematical approaches to formalizing the integration of neural networks with the blockchain level, describes consensus algorithms based on Proof-of-Learning and voting. The mechanisms of decentralized storage and validation of model weight updates, inclusion of risk assessment logic in smart contracts, and the possibility of using tokens to stimulate correct updates and prevent data poisoning are considered in detail. The methods that allow combining the emergent capabilities of collective self-learning of neural networks and the advantages of blockchain technologies (data immutability, automated security policies, audit) are analyzed. Using the example of managing autonomous robotic platforms in production systems, the paper demonstrates how such a synergistic system can increase resilience to internal and external threats and reduce emergency response times. It is proved that the distributed registry acts as an "immune system" during the evolution of neural networks and prevents the

legitimization of dangerous changes in model parameters. Promising directions for future research are outlined, including the creation of prototypes of high-loaded CFCs with emergent II modules and the formation of formal reliability criteria for such hybrid solutions. In general, the presented adaptation of the blockchain voting model for the tasks of dynamic risk management and distributed learning is promising for building more flexible, transparent, and secure cyber-physical systems.

Keywords: blockchain; Hyperledger; e-voting; smart contracts; cyber-physical systems; neural networks; emergence; risk management; Proof-of-Learning; decentralized learning.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Androulaki, E., Barger, A., & Bortnikov, V. et al. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *In Proceedings of the Thirteenth EuroSys Conference. ACM*, 1–15. https://doi.org/10.1145/3190508.3190538
2. Cachin, C. (2016). Architecture of the Hyperledger Blockchain Fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 1–4.
3. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/access.2016.2566339
4. Ferrag, M. A., & Shu, L., et al. (2020). Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access, 8*, 32031–32053. https://doi.org/10.1109/access.2020.2973178
5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning.* MIT Press.
6. Thrun, S., & Pratt, L. (1998). *Learning to Learn*. Springer. https://doi.org/10.1007/978-1-4612-1814-9
7. Stanley, K. O., Clune, J., & Lehman, J. et al. (2019). Designing Neural Networks through Neuroevolution. *Nature Machine Intelligence*, *1*, 24–35. https://doi.org/10.1038/s42256-018-0006-z
8. Jaderberg, M., & Czarnecki, W. M., et al. (2019). Human-Level Performance in First-Person Multiplayer Games with Population-Based Deep Reinforcement Learning. *Science*, *364*, 859–865. https://doi.org/10.1126/science.aau6249
9. Zheng, Z., & Xie, S., et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *In 2017 IEEE International Congress on Big Data (BigData Congress),* 557–564. https://doi.org/10.1109/bigdatacongress.2017.85
10. Sousa, J., Bessani, A., & Vukolić, M. (2018). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. *In 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 51–58. https://doi.org/10.1109/dsn.2018.00018
11. Baliga, A. (2017). *Understanding Blockchain Consensus Models*. Persistent.
12. Jiang, W., & Zhang, D. (2021). Proof-of-Learning Approach to Secure and Robust Collaborative Machine Learning in Blockchain. *Information Sciences, 552*, 75–91. https://doi.org/10.1016/j.ins.2020.12.059
13. Konečný, J., & McMahan, H. B., et al. (2016). *Federated Learning: Strategies for Improving Communication Efficiency*. arXiv preprint.
14. Moreno, C., & Dorigo, M. (2022). The Emergence of Collective Intelligence in Artificial Systems. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *377*. https://doi.org/10.1098/rstb.2020.0357
15. Floreano, D., & Keller, L. (2010). Evolution of Adaptive Behaviour in Robots by Means of Darwinian Selection. *PLoS Biology, 8(1). e1000292*. https://doi.org/10.1371/journal.pbio.1000292
16. Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. *HotSec'08: Proceedings of the 3rd USENIX Workshop on Hot Topics in Security.*
17. Saxena, N., & Grijalva, S. (2019). Dynamic Security Risk Management in Distributed Energy Resources. *IEEE Transactions on Smart Grid, 10(3)*, 3120–3129. https://doi.org/10.1109/tsg.2018.2819662
18. Humayed, A., & Lin, J., et al. (). Cyber-Physical Systems Security – A Survey. *IEEE Internet of Things Journal, 4(6)*, 1802–1831. https://doi.org/10.1109/jiot.2017.2703172
19. Kim, T., & Feldman, V., et al. (2022). *Blockchain-Based Proof-of-Learning Protocols for Neural Network Training.* arXiv preprint.

20. Zhang, J., & Xiong, F., et al. (2020). A Blockchain-Based Federated Learning Framework for Edge Computing. *IEEE Transactions on Industrial Informatics, 17(3),* 2042–2051. https://doi.org/10.1109/tii.2020.3004635
21. Kaur, K., & Chana, I., et al. (2021). Blockchain-Based Trust Management in Federated Learning for Healthcare Systems: State of the Art and Open Issues. *IEEE Access.*
22. Shapoval, O., Kuznietsov, O., Poluianenko, M., Yakovenko, V., Prokopovych-Tkachenko, D., & Kavun, S. (2019). The Decentralized Voting Model Using the Hyperledger Platform. *Proceedings of the 2019 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo).* https://doi.org/10.1109/ukrmico47782.2019.9165368