УДК 004.056.5:004.75:004.41
DOI: 10.31673/2409-7292.2026.011651

Хвостенко В.С.

ЕВОЛЮЦІЯ СМАРТ-КОНТРАКТІВ У WEB3- ТА DEFI-СИСТЕМАХ: АРХІТЕКТУРНА ТРАНСФОРМАЦІЯ ЗАГРОЗ БЕЗПЕКИ ТА ПЕРСПЕКТИВИ КОМПЛЕКСНОГО ЗАХИСТУ

У статті здійснено дослідження еволюції смарт-контрактів як ключового функціонального компонента Web3-архітектури та децентралізованих фінансових середовищ. Встановлено, що смарт-контракти зазнали послідовної трансформації – від локалізованих програмних механізмів виконання транзакцій до складних мультиконтрактних протокольних структур, здатних реалізовувати фінансові, координаційні та управлінські функції в умовах відсутності централізованих посередників. У роботі проаналізовано архітектурні особливості виконання смарт-контрактів у різних Web3-платформах, зокрема в екосистемах Ethereum, Solana та Polkadot, а також розкрито роль композиційності та міжконтрактної взаємодії у формуванні сучасних DeFi-екосистем. Проведено аналіз еволюції наукових і технічних підходів до трактування поняття смарт-контракту. Запропоновано авторське визначення смарт-контракту. Проведено аналіз трансформації загроз безпеці смарт-контрактів, який охоплює протокольні й економічні механізми атак, зокрема front-running, маніпуляції з оракулами та практики максимального вилучення цінності. Узагальнено сучасні підходи до забезпечення безпеки смарт-контрактів, включно з методами формальної верифікації, символьного виконання, автоматизованого аналізу та інтеграції механізмів безпеки в життєвий цикл їх розроблення. Отримані результати обґрунтовують необхідність переходу від фрагментарних інструментів аудиту до комплексного, методологічно узгодженого підходу до забезпечення безпеки смарт-контрактів, який враховує еволюційну складність децентралізованих систем, багаторівневу архітектуру Web3-платформ і економічний контекст функціонування DeFi-протоколів. Запропоновані висновки створюють підґрунтя для подальшої розробки інтегрованих моделей і методологій забезпечення безпеки смарт-контрактів у децентралізованих середовищах.

Ключові слова: смарт-контракти, Web3-системи, DeFi-системи, трансформація загроз безпеки, комплексний захист.

Актуальність проблеми

Стрімкий розвиток технологій Web3 зумовив глибоку трансформацію архітектурних підходів до побудови розподілених інформаційних систем, перевівши їх від централізованих сервісно-орієнтованих моделей до децентралізованих протокольних екосистем. У межах цієї трансформації ключову роль відіграють смарт-контракти, які функціонують як автономні програмні об’єкти, здатні забезпечувати виконання транзакцій, координацію дій учасників та дотримання заданих правил без залучення довірених посередників. На ранніх етапах розвитку блокчейн-технологій смарт-контракти розглядалися переважно як інструменти автоматизації обмеженого кола операцій, однак із формуванням децентралізованих фінансових систем вони еволюціонували у складні протокольні механізми, що реалізують функції обміну активами, кредитування, управління ліквідністю та децентралізованого врядування, тощо.

Зростання функціональної насиченості та композиційності смарт-контрактів обумовило істотне розширення та ускладнення їхньої поверхні атак. Сучасні DeFi-протоколи являють собою багаторівневі мультиконтрактні системи, в яких окремі контракти взаємодіють між собою в межах динамічного, відкритого та конкурентного середовища. За таких умов традиційні припущення щодо ізольованої коректності та безпеки окремого смарт-контракту стають недоцільними. Таким чином, вразливості смарт-контрактів можуть призводити не лише до локальних технічних збоїв, а й до масштабних економічних втрат, порушення механізмів ринкової рівноваги та дестабілізації децентралізованих екосистем. Додатковим ризиком є властива блокчейн-системам незмінність розгорнутих контрактів, що суттєво ускладнює або унеможливлює оперативне усунення виявлених помилок після їх впровадження.

Паралельно з еволюцією архітектурної ролі смарт-контрактів зазнав трансформації й характер загроз їхній безпеці. Так на етапах їхнього становлення, наукові дослідження були присвячені переважно на технічних уразливостях програмного коду, таких як повторний вхід, переповнення цілочисельних змінних або помилки керування доступом. Натомість сучасні

DeFi-середовища характеризуються появою складних протокольних та економічних атак. До них належать маніпуляції порядком транзакцій, front-running, зловживання механізмами оракулів, атаки з використанням flash loan, а також стратегії максимального вилучення цінності. Такі загрози формуються на перетині програмної логіки смарт-контрактів, механізмів досягнення консенсусу та ринкової динаміки, що значно ускладнює їх формалізацію, виявлення та нейтралізацію традиційними засобами безпекового аналізу.

Незважаючи на значну кількість наукових праць, присвячених безпеці смарт-контрактів, більшість існуючих підходів має фрагментарний характер і орієнтована на окремі класи уразливостей або інструментальні методи аналізу. При цьому недостатньо враховується еволюційна природа смарт-контрактів, особливості їхнього життєвого циклу та системна роль у межах Web3-архітектури й DeFi-протоколів. Відсутність узгодженої концептуальної та методологічної основи призводить до розриву між зростаючою складністю децентралізованих систем і можливостями наявних механізмів забезпечення їхньої безпеки.

Отже, актуальність даного дослідження зумовлена необхідністю комплексного аналізу еволюції смарт-контрактів у Web3- та DeFi-середовищах із урахуванням трансформації їхніх архітектурних, функціональних і загрозових характеристик. Такий підхід є необхідною передумовою для формування інтегрованих, еволюційно орієнтованих методів забезпечення безпеки смарт-контрактів, здатних адекватно реагувати на сучасні технічні, протокольні та економічні виклики децентралізованих систем.

Метою статті є виявлення та обґрунтування закономірностей еволюції смарт-контрактів у процесі переходу від Web2 до Web3-архітектури як якісно нового архітектурно-економічного типу децентралізованих систем, а також визначення впливу цієї еволюції на трансформацію функціонального призначення смарт-контрактів і появу нових типів загроз безпеці, що обґрунтовує необхідність комплексного, еволюційно орієнтованого підходу до забезпечення їх безпеки.

Для досягнення поставленої мети в статті вирішуються такі **завдання**:

- проаналізувати еволюцію підходів до трактування смарт-контрактів у наукових дослідженнях, нормативно-технічних джерелах і практичних реалізаціях у контексті розвитку Web3-архітектури та запропонувати авторське визначення, що відповідає сучасним вимогам кібербезпеки децентралізованих систем;
- систематизувати етапи розвитку смарт-контрактів з урахуванням змін їх архітектурної ролі, рівня композиційності та функціонального призначення, а також показати формування архітектурно-економічних децентралізованих систем нового типу;
- ідентифікувати характерні та нові типи безпекових загроз і обмежень, притаманні кожному етапу еволюції смарт-контрактів, з урахуванням технічних, протокольних, економічних і управлінських факторів;
- встановити причинно-наслідковий зв’язок між ускладненням архітектури децентралізованих систем і трансформацією загроз безпеці смарт-контрактів, включаючи перехід від локальних уразливостей до системно-екосистемних ризиків;
- обґрунтувати доцільність переходу від ізольованого аналізу окремих смарт-контрактів до комплексних, еволюційно орієнтованих моделей забезпечення безпеки, які враховують архітектурний, протокольний та економічний контексти функціонування Web3- та DeFi-систем.

Виклад основного матеріалу

В роботі Ніка Сабо «Формалізація та забезпечення безпеки відносин у публічних мережах» смарт-контракти визначаються як поєднання протоколів та інтерфейсів, що формалізують і формують відносини між учасниками через комп’ютерні мережі. Ці механізми застосовують криптографічні та інші засоби безпеки для того, щоб алгоритмічно специфіковані відносини були захищені від порушень і щоб весь цикл «узгодження – виконання» міг бути автоматизований і захищений [1].

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651

У технічних стандартах, зокрема в глосарії NIST [2], смарт-контракт трактують як сукупність коду та пов'язаних даних, що розгортається на блокчейн-мережі за допомогою криптографічно підписаних транзакцій і виконується її вузлами з детермінованими результатами, які фіксуються в розподіленому реєстрі. Це визначення підкреслює комп'ютерну природу контракту як автономної програми, інтегрованої з інфраструктурою блокчейну.

У фундаментальному документі блокчейн-спільноти – Ethereum White Paper [3], смарт-контракти визначено як криптографічні «контейнери», які зберігають значення та автоматично розблоковують його, коли певні умови виконані. Така інтерпретація розширює попередні концепції, дозволяючи задавати довільні правила функціонування децентралізованих програмних об'єктів, котрі працюють у рамках Web3-інфраструктури і забезпечують автономне виконання логіки, заданої в коді.

Подальший підхід до визначення поняття смарт-контракту ідентифікує його як автоматизовану та забезпечувану до виконання угоду, виконання якої може гарантуватися як правовими механізмами, так і незмінним виконанням програмного коду. Такий підхід поєднує юридичне розуміння контракту з технічною реалізацією в розподілених системах і створює концептуальну основу для сучасних Web3- та DeFi-протоколів, у яких забезпечення виконання дедалі більше зміщується від правового поля до криптографічно захищеного виконання коду [4].

В інженерно-орієнтованих оглядових дослідженнях смарт-контракти визначаються передусім як комп'ютерні програми, що автоматично виконують задані дії у блокчейн-середовищі відповідно до наперед визначених правил. Зокрема, смарт-контракт розглядається як детермінований програмний об'єкт, який взаємодіє зі станом розподіленого реєстру та виконується без можливості зовнішнього втручання [5]. Таке трактування формує підґрунтя для застосування формальних методів специфікації, верифікації та аналізу безпеки смарт-контрактів.

Подальший етап еволюції поняття смарт-контракту пов'язаний із формуванням децентралізованих фінансових середовищ. У роботі [6], смарт-контракти розглядаються як самовиконуваний програмний код, що виконує функцію базового протокольного елемента фінансової інфраструктури, забезпечуючи автоматичне визначення та виконання правил кредитування, обміну активів і управління без участі посередників. Таке трактування підкреслює перехід від ізольованого програмного об'єкта до системного компонента децентралізованих фінансових ринків і обумовлює принципово нові вимоги до їх безпеки.

У сучасних інституційних і безпекових дослідженнях смарт-контракти розглядаються вже не лише як програмні або протокольні об'єкти, а як критичні компоненти цифрової інфраструктури, здатні породжувати системні кібернетичні та економічні ризики. Зокрема, у звітах ENISA смарт-контракти визначаються як програмні компоненти, розгорнуті на платформах розподіленого реєстру, що автоматично виконують задані дії та забезпечують управління цифровими активами, при цьому їх уразливості можуть мати масштабні наслідки для стабільності децентралізованих екосистем. Таке трактування акцентує необхідність комплексного та багаторівневого підходу до забезпечення безпеки смарт-контрактів [7].

Проведений аналіз еволюції трактувань смарт-контрактів у наукових, технічних та інституційних джерелах свідчить про послідовну зміну їх ролі та функціонального призначення в архітектурі цифрових систем. Первинно смарт-контракти розглядалися як механізми формалізації та автоматизації відносин у комп'ютерних мережах, зосереджені на забезпеченні виконання домовленостей між сторонами. З розвитком блокчейн-технологій це поняття було уточнено в технічному вимірі як програмний код із власним станом, що детерміновано виконується у розподіленому середовищі.

Подальший перехід до Web3-архітектури та формування децентралізованих фінансових середовищ призвів до якісної трансформації смарт-контрактів. У сучасних DeFi-екосистемах

вони виконують роль протокольних елементів цифрової фінансової інфраструктури, які визначають правила обігу цифрових активів, взаємодії учасників і механізми децентралізованого управління. Таким чином, смарт-контракти перестали бути ізольованими програмними об'єктами й набули системного значення, а їх коректність і надійність безпосередньо впливають на стійкість та безпеку всієї децентралізованої екосистеми.

Узагальнення існуючих підходів дозволяє дійти висновку, що жодне з наявних визначень не відображає повною мірою сучасну природу смарт-контрактів з позицій кібербезпеки цифрових активів і інфраструктури. Більшість трактувань акцентують увагу або на програмній реалізації, або на правовій чи економічній складовій, залишаючи поза увагою їхню комплексну роль як джерела потенційних технічних, протокольних і економічних ризиків. За таких умов постає необхідність формування узагальненого визначення, здатного слугувати концептуальною основою для подальшої розробки стандартів і методологій забезпечення безпеки смарт-контрактів.

З урахуванням наведеного у роботі пропонується таке авторське визначення: смарт-контракт – це автономний програмно-протокольний об'єкт децентралізованої цифрової інфраструктури, що функціонує в середовищі розподіленого реєстру, формально визначає, автоматично виконує та забезпечує дотримання правил управління цифровими активами і процесами, має власний стан і детерміновану логіку виконання, а також виступає об'єктом кібербезпеки, уразливості якого можуть призводити до технічних, протокольних та економічних ризиків у межах Web3- та DeFi-екосистем.

Запропоноване визначення поняття смарт-контракту як автономного програмно-протокольного об'єкта цифрової інфраструктури зумовлює необхідність аналізу архітектурних середовищ, у яких такі об'єкти функціонують. Саме архітектура децентралізованих систем визначає модель виконання смарт-контрактів, характер їх взаємодії та передумови виникнення безпекових ризиків. У зв'язку з цим доцільним є розгляд еволюції архітектурних підходів до виконання смарт-контрактів у Web3- та DeFi-середовищах.

У роботі [8] здійснено комплексний огляд уразливостей смарт-контрактів, у якому вони розглядаються як програмні об'єкти, що функціонують у децентралізованій Web3-архітектурі та виконуються у середовищі блокчейн-віртуальної машини.

Автори систематизують загрози безпеці на рівні програмного коду, віртуальної машини та блокчейн-інфраструктури, що дозволяє продемонструвати багаторівневу природу ризиків, притаманних сучасним децентралізованим системам. Значну увагу приділено класичним уразливостям, таким як повторний вхід, некоректна ініціалізація змінних стану, залежність від часових міток та особливості виконання байткоду, які можуть призводити до істотних фінансових втрат. Водночас дослідження зосереджене переважно на технічних аспектах безпеки окремих смарт-контрактів і лише опосередковано відображає їх еволюцію як складових DeFi-протоколів, у межах яких загрози формуються також на протокольному та економічному рівнях. Це обґрунтовує необхідність подальших досліджень еволюції смарт-контрактів.

У whitepaper платформи Solana запропоновано нову архітектуру блокчейна, орієнтовану на високопродуктивне виконання смарт-контрактів у Web3-середовищі, що ґрунтується на механізмі Proof of History як криптографічно перевірюваному джерелі часу. Запропонований підхід усуває залежність від зовнішньої синхронізації та дозволяє забезпечити детермінований порядок транзакцій, що є критично важливим для масштабованих DeFi-систем. Автором також описано механізм виконання смарт-контрактів на основі eBPF-байткоду з підтримкою паралельної обробки та GPU-прискорення, що відображає еволюцію смарт-контрактів від послідовних моделей виконання до архітектур, здатних підтримувати складні багатокомпонентні фінансові протоколи [9]. Водночас питання безпеки смарт-контрактів розглядаються опосередковано, без формалізації моделей загроз, що вказує на необхідність подальших досліджень у цьому напрямі.

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651

У роботі [10] смарт-контракти розглядаються не лише як програмні об’єкти, що виконуються у блокчейн-віртуальній машині, а як ключові економічні компоненти децентралізованих фінансових протоколів. На прикладі Compound показано, що безпека смарт-контрактів у DeFi-середовищах визначається не тільки коректністю коду, а й динамікою взаємодії учасників, параметрами ліквідації, волатильністю ринку та глибиною ліквідності. Застосування агент-орієнтованого моделювання дозволяє оцінювати економічну стійкість протоколу під дією екзогенних шоків, що відображає еволюцію смарт-контрактів від ізольованих Web3-компонентів до складних фінансових механізмів з багаторівневою моделлю ризиків.

У роботі [11], смарт-контракти розглядаються як еволюціонуючий елемент Web3-архітектури, що пройшов шлях від простих програмних сценаріїв до складних логічних компонентів децентралізованих застосунків і фінансових протоколів. Авторами встановлено, що зростання функціональної складності смарт-контрактів, їх взаємодія у межах децентралізованих екосистем та інтеграція у DeFi-середовища зумовили появу нових класів уразливостей і ризиків, які не можуть бути повністю охоплені традиційними підходами до безпеки. У дослідженні наголошується на необхідності розгляду смарт-контрактів як архітектурних компонентів Web3-платформ, безпека яких має оцінюватися з урахуванням їх еволюції, міжконтрактних залежностей та протокольного контексту виконання.

Таблиця 1

Етапи еволюції смарт-контрактів у Web3- та DeFi-середовищах: архітектурний контекст і трансформація безпекових ризиків

Етап еволюції	**Хронологічні межі**	**Архітектурна модель виконання**	**Архітектурна роль смарт-контрактів у системі**	**Характерні безпекові ризики**
Концептуальний	1990-ті роки	Теоретичні моделі без реалізованого середовища виконання	Формалізація ідеї автоматизованого виконання договірних умов	Ризики нефомалізованості, відсутність перевірюваних моделей коректності та безпеки
Ранні блокчейн-реалізації	2015-2017	Послідовна модель виконання у блокчейн-віртуальній машині	Автономні програмні компоненти для виконання транзакцій	Програмні уразливості логіки виконання (reentrancy, переповнення), помилки контролю доступу
Web3-додатки	2017-2019	Віртуальні машини з глобальним станом (EVM, WASM)	Логічні компоненти децентралізованих застосунків	Залежність від стану, некоректна ініціалізація, атаки типу DoS
Ранні DeFi-протоколи	2019-2020	Мультиконтрактні архітектури з міжконтрактною взаємодією	Фінансові протокольні компоненти кредитування, обміну та стейкінгу	Маніпуляції станом, flash-loan-атаки, порушення логіки міжконтрактної взаємодії
Масштабовані DeFi-екосистеми	2020-2022	Протокольні архітектури з оракулами та механізмами ліквідності	Економічні та протокольні компоненти ринкових механізмів	Протокольні та економічні атаки (front-running, oracle manipulation, MEV)
Сучасні Web3/DeFi-системи	2022 - дотепер	Паралельні та композиційні моделі виконання смарт-контрактів	Базові елементи децентралізованої цифрової інфраструктури та управління	Системно-економічні та екосистемні ризики, каскадні відмови, governance-атаки

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651

Для систематизації результатів аналізу літературних джерел та виявлення закономірностей розвитку смарт-контрактів доцільно розглянути їх еволюцію в хронологічному та архітектурно-функціональному вимірах. Такий підхід дозволяє простежити зміну ролі смарт-контрактів у децентралізованих системах – від ізольованих програмних механізмів автоматизації транзакцій до ключових компонентів протокольних і економічних екосистем Web3 та DeFi. Узагальнені характеристики основних етапів еволюції смарт-контрактів наведено в таблиці.

За результатами аналізу встановлено, що розвиток смарт-контрактів у Web3- та DeFi-середовищах має системний і закономірний характер та супроводжується послідовною трансформацією їх архітектурної ролі, контексту виконання і домінуючих безпекових ризиків. Якщо на ранніх етапах смарт-контракти виконували обмежені функції автоматизації окремих транзакцій і розглядалися переважно як ізольовані програмні компоненти, то в сучасних децентралізованих фінансових екосистемах вони еволюціонували до статусу ключових елементів протокольної, економічної та управлінської інфраструктури.

Ускладнення архітектури децентралізованих систем, зростання рівня композиційності та міжконтрактної взаємодії, а також інтеграція смарт-контрактів у багатокомпонентні фінансові протоколи зумовили якісну зміну характеру безпекових загроз. Домінування локальних технічних уразливостей на початкових етапах поступилося системним, протокольним та економічним ризикам, що формуються на рівні взаємодії контрактів, консенсусних механізмів і ринкових стимулів учасників.

Виявлені закономірності свідчать про методологічну обмеженість підходів до забезпечення безпеки, орієнтованих виключно на аналіз програмного коду окремих смарт-контрактів. У сучасних Web3- та DeFi-системах безпека смарт-контрактів має розглядатися в ширшому архітектурному та економічному контексті їх функціонування, що обґрунтовує необхідність переходу до комплексних, еволюційно орієнтованих моделей забезпечення безпеки децентралізованих систем.

Отримані результати свідчать, що загрози безпеці смарт-контрактів не є ізольованими або випадковими, а формуються як похідні від архітектурної еволюції децентралізованих систем та зміни функціональної ролі смарт-контрактів у Web3- і DeFi-середовищах. У міру ускладнення моделей виконання, зростання рівня міжконтрактної взаємодії та інтеграції економічних механізмів характер безпекових ризиків зазнає системної трансформації.

З огляду на це, адекватний аналіз сучасних і перспективних загроз безпеці смарт-контрактів потребує розгляду архітектурних моделей їх виконання, протокольних механізмів та динаміки взаємодії учасників децентралізованих екосистем. Для наочного відображення встановлених причинно-наслідкових зв’язків між архітектурними рішеннями, роллю смарт-контрактів і домінуючими класами загроз у роботі запропоновано узагальнювальну схему еволюції архітектури виконання смарт-контрактів у Web3- та DeFi-середовищах (рис.1).

На рис. 1 подано формалізовану схему, що відображає причинно-наслідковий зв’язок між ускладненням архітектури децентралізованих систем та трансформацією загроз безпеці смарт-контрактів. Схема демонструє, що зі зміною типу децентралізованої системи змінюється архітектурна роль смарт-контрактів, рівень реалізації бізнес-логіки та характер їх взаємодії з іншими компонентами екосистеми, що безпосередньо впливає на домінуючі класи безпекових ризиків.

Запропоноване узагальнення дозволяє інтерпретувати еволюцію загроз безпеці смарт-контрактів не як набір ізольованих уразливостей, а як результат послідовних архітектурних зрушень – від транзакційних моделей виконання до мультиконтрактних протокольних і економічних структур. У міру зростання автономності, композиційності та економічної інтеграції смарт-контрактів відбувається зміщення фокусу загроз із локального програмного рівня на протокольний та системно-економічний рівні. Таким чином, схема наочно підтверджує, що сучасні загрози безпеці смарт-контрактів у Web3- та DeFi-середовищах не

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651

можуть бути адекватно описані моделями, орієнтованими виключно на аналіз вихідного коду окремих контрактів. Значна частина ризиків формується на рівні архітектури виконання, механізмів взаємодії між контрактами та економічних стимулів учасників децентралізованих систем.

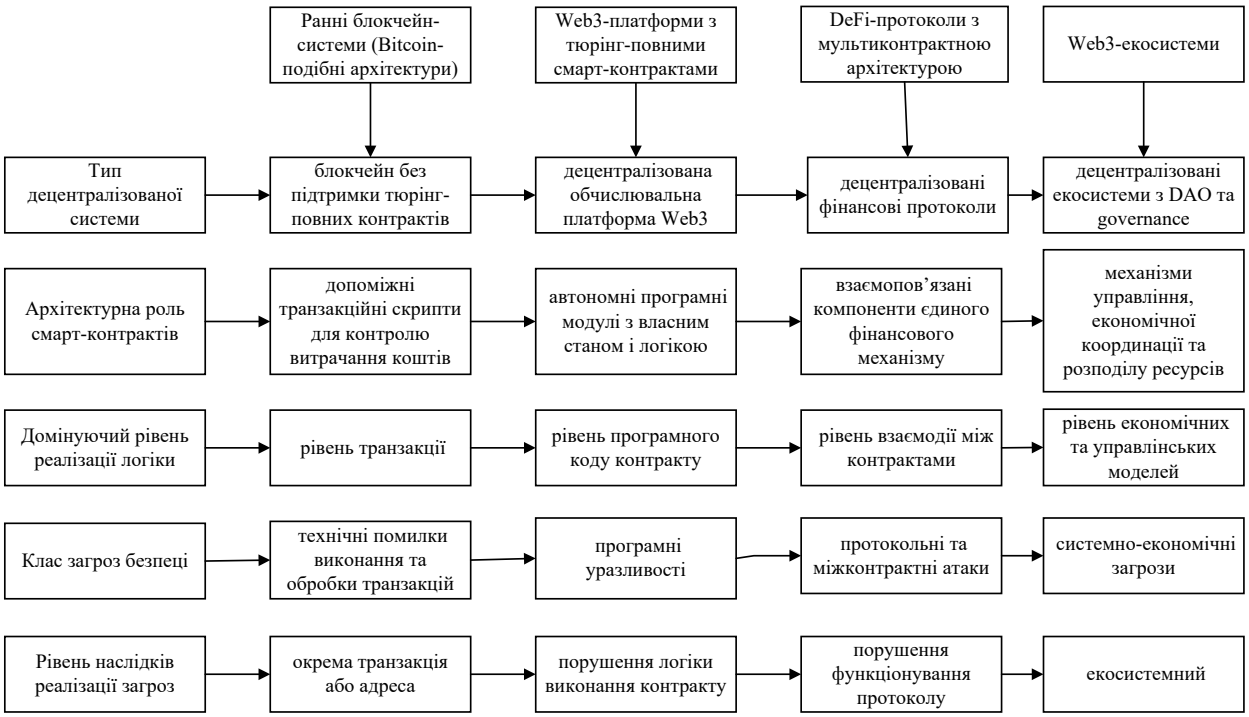

Рис. 1. Еволюція архітектурної ролі смарт-контрактів та трансформація загроз безпеки у Web3- та DeFi-системах

Отримані результати обґрунтовують необхідність переходу до комплексних, еволюційно орієнтованих підходів до забезпечення безпеки смарт-контрактів, у межах яких аналіз архітектурних моделей виконання розглядається як ключовий чинник виявлення сучасних і перспективних класів загроз.

Згідно з установленим у роботі положенням про те, що загрози безпеці смарт-контрактів формуються як похідні від архітектурної еволюції децентралізованих систем, подальший розвиток Web3-екосистем створює передумови для формування нового класу децентралізованих систем, орієнтованих не стільки на виконання заздалегідь визначеної програмної логіки, скільки на адаптивну координацію поведінки учасників, ресурсів і економічних процесів.

Якщо на ранніх етапах еволюції смарт-контракти виконували допоміжну роль транзакційних скриптів, а згодом трансформувалися в автономні програмні модулі та ключові компоненти фінансових протоколів, то на наступному етапі вони можуть розглядатися як виконавчі механізми рішень, сформованих на надпротокольному рівні децентралізованого управління. У межах таких адаптивних координаційних систем смарт-контракти забезпечують формальне, детерміноване та незмінне виконання результатів колективних рішень, тоді як ключові управлінські функції реалізуються через механізми децентралізованого governance, економічної координації, репутаційних моделей та алгоритмів адаптації.

На відміну від класичних DeFi-протоколів, у яких безпека значною мірою визначається коректністю міжконтрактної взаємодії, у таких системах визначальним чинником стає стійкість механізмів координації автономних агентів і стабільність процедур прийняття рішень у динамічному середовищі. Це зумовлює трансформацію домінуючих загроз безпеці – від програмних і протокольних уразливостей до координаційно-адаптивних загроз, пов'язаних

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651

із маніпуляцією правилами управління, спотворенням економічних стимулів, впливом на механізми зворотного зв'язку та виникненням небажаної емерджентної поведінки системи.

Таблиця 2

Формалізована відповідність класів загроз безпеці смарт-контрактів, методів протидії та рівнів реалізації в еволюціонуючих Web3- та DeFi-системах

Клас загроз безпеці	**Формалізований опис загроз**	**Методологічний підхід до захисту**	**Рівень реалізації захисту в системі**
1	2	3	4
Транзакційно-технічні загрози	Порушення коректності виконання транзакцій, недетермінованість обробки даних, залежність від порядку включення транзакцій у блок, обмеження консенсусних механізмів	Формальна специфікація транзакційних правил, верифікація детермінізму виконання, обмеження недетермінованих операцій	Рівень базової блокчейн-інфраструктури
Програмно-логічні загрози	Уразливості логіки смарт-контрактів, некоректна робота зі станом, помилки управління викликами, повторний вхід, неконтрольовані винятки	Формальна верифікація смарт-контрактів, аналіз інваріантів стану, доказ коректності виконання	Рівень окремого смарт-контракту
Міжконтрактні (протокольні) загрози	Небезпечні сценарії взаємодії між контрактами, каскадні виклики, некоректна композиція логіки, порушення протокольних інваріантів	Архітектурне моделювання протоколів, аналіз сценаріїв взаємодії, формалізація та перевірка протокольних інваріантів	Рівень децентралізованого протоколу
Інтеграційні (оракульні) загрози	Спотворення або маніпуляція зовнішніми даними, асиметрія інформації між компонентами системи, залежність від ненадійних джерел	Криптографічно захищені механізми отримання даних, багатоджерельна валідація, консенсус щодо зовнішніх подій	Рівень інтеграції із зовнішнім середовищем
Економіко-стимульні загрози	Атаки, що використовують допустимі механізми протоколу (арбітраж, flash loan, викривлення стимулів), порушення економічної рівноваги	Формалізація економічних моделей, аналіз рівноваги, обмеження небажаних стратегій учасників	Рівень економічної логіки протоколу
Управлінсько-координаційні загрози	Маніпуляції механізмами децентралізованого управління, захоплення governance, концентрація впливу, викривлення колективного прийняття рішень	Формалізація правил governance, аналіз моделей колективного вибору, обмеження концентрації влади	Рівень децентралізованого управління
Адаптивно-поведінкові загрози	Небажана еволюція поведінки децентралізованої системи внаслідок адаптивних механізмів, зворотних зв'язків та колективного навчання агентів	Поведінкове та агент-орієнтоване моделювання, контроль глобальних інваріантів, динамічний моніторинг	Надпротокольний (системний) рівень координації
Системно-архітектурні загрози	Емерджентні ефекти, ланцюгові відмови, втрата керованості та стабільності децентралізованої екосистеми	Комплексні еволюційно орієнтовані моделі безпеки, міжрівневий аналіз архітектури	Архітектура децентралізованої екосистеми

Реалізація таких загроз може відбуватися без порушення формальної коректності смарт-контрактів, однак призводити до системних збоїв, економічної нестабільності або втрати керованості децентралізованої екосистеми в цілому. Це підтверджує, що ізольований аналіз

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651

смарт-контрактів є недостатнім для перспективних архітектур Web3, а забезпечення безпеки потребує еволюційно орієнтованих моделей, здатних враховувати архітектурний контекст, механізми координації та динаміку розвитку децентралізованих систем.

З урахуванням прогнозованого переходу до децентралізованих адаптивних координаційних систем, традиційні підходи до кібербезпеки, орієнтовані на статичний аналіз програмного коду смарт-контрактів, виявляються методологічно недостатніми. У таких архітектурах домінуючі загрози формуються не на рівні синтаксичної або семантичної коректності коду, а на рівні механізмів координації, адаптації та колективного прийняття рішень, що обумовлює необхідність принципового розширення спектра методів захисту.

По-перше, перспективним напрямом є перехід від контрактно-орієнтованої до архітектурно-орієнтованої моделі безпеки, у межах якої об'єктом аналізу та захисту виступає не окремий смарт-контракт, а сукупність взаємодіючих компонентів децентралізованої системи. Такий підхід передбачає розроблення моделей безпеки, здатних аналізувати поведінку системи на рівні сценаріїв взаємодії, потоків управлінських рішень та економічних стимулів, а також виявляти небезпечні конфігурації, що виникають унаслідок формально допустимих, але системно небажаних комбінацій дій.

По-друге, необхідним є розвиток поведінкових та інваріантно-орієнтованих методів захисту, спрямованих на збереження глобальних властивостей стійкості та безпеки децентралізованих систем. На відміну від традиційних підходів, зосереджених на перевірці коректності окремих функцій, доцільним є формулювання та контроль інваріантів безпеки, порушення яких свідчить про небезпечну еволюцію системи навіть за відсутності формальних помилок у коді смарт-контрактів. Такий підхід дозволяє виявляти загрози, пов'язані з емерджентною поведінкою та маніпуляціями механізмами адаптації.

По-третє, важливим напрямом є інтеграція методів моніторингу та динамічного контролю, що забезпечують безпеку не лише на етапі проєктування та розгортання, а й у процесі експлуатації децентралізованих систем. У контексті адаптивних Web3-екосистем це передбачає спостереження за змінами параметрів управління, економічних стимулів і результатів колективних рішень з метою своєчасного виявлення відхилень, здатних призвести до системних збоїв або втрати керованості.

Крім того, перспективним є розвиток економіко-орієнтованих механізмів кібербезпеки, спрямованих на зниження привабливості атак шляхом коректного проєктування стимулів, обмеження можливостей маніпуляцій та формування механізмів відповідальності в децентралізованих середовищах. У межах таких підходів безпека розглядається не лише як технічна властивість системи, а як результат збалансованої взаємодії економічних, протокольних і управлінських механізмів.

Узагальнюючи, забезпечення безпеки децентралізованих систем наступного покоління потребує розвитку комплексних, еволюційно орієнтованих підходів до кібербезпеки, що поєднують архітектурний аналіз, поведінкове моделювання, динамічний моніторинг та економічні механізми захисту. Саме ці напрями формують методологічну основу для створення стійких і керованих Web3-екосистем в умовах зростаючої архітектурної та економічної складності.

Висновки

У статті здійснено комплексний аналіз еволюції смарт-контрактів у контексті розвитку Web3-архітектури та децентралізованих фінансових систем, що дало змогу встановити стійкий причинно-наслідковий зв'язок між ускладненням архітектурних рішень децентралізованих систем і трансформацією загроз їх безпеці. Показано, що зі зміною функціональної ролі смарт-контрактів – від ізольованих транзакційних механізмів до базових елементів економічної координації, управління та прийняття рішень – відбувається закономірний перехід від локальних технічних уразливостей до багаторівневих протокольних, економічних і системно-екосистемних загроз.

Отримані результати засвідчують методологічну обмеженість традиційних підходів до забезпечення безпеки смарт-контрактів, орієнтованих переважно на ізольований аналіз програмного коду. У сучасних Web3- та DeFi-середовищах істотна частина безпекових ризиків формується поза межами окремого контракту – на рівні міжконтрактної взаємодії, протокольних механізмів, економічних стимулів і систем децентралізованого управління, що зумовлює необхідність відмови від вузькокодових моделей безпеки на користь комплексних, багаторівневих підходів до захисту. У межах дослідження ідентифіковано нові типи загроз безпеці смарт-контрактів, характерні для сучасних і перспективних архітектур Web3-екосистем, зокрема архітектурно-емергентні, економіко-стимульні, governance-орієнтовані та системно-екосистемні загрози. Встановлено, що реалізація таких загроз можлива за формально коректного програмного коду та без порушення базових протокольних правил, що істотно ускладнює їх виявлення та нейтралізацію традиційними засобами аудиту.

Обґрунтовано доцільність застосування еволюційно орієнтованого підходу до забезпечення безпеки смарт-контрактів, який враховує архітектурний контекст функціонування децентралізованих систем, зміну домінуючих класів загроз на різних етапах їх розвитку та взаємозв'язок між технічними, протокольними й економічними аспектами безпеки. Запропонована в роботі класифікація загроз і відповідних методів протидії формує концептуальну основу для побудови формалізованих моделей захисту децентралізованих систем наступного покоління. Перспективи подальших досліджень пов'язані з розробленням інструментів архітектурного, економічного та поведінкового аналізу безпеки смарт-контрактів, формалізацією інваріантів стійкості мультиконтрактних і мультипротокольних систем, а також інтеграцією моделей стимулів, управління та ризиків у комплексні фреймворки кібербезпеки Web3- та DeFi-екосистем.

Перелік посилань

1. Szabo N. Formalizing and securing relationships on public networks // First Monday. 1997. Vol. 2, no. 9. URL: https://firstmonday.org/ojs/index.php/fm/article/view/548.

2. Smart contract // Glossary / National Institute of Standards and Technology (NIST). URL: https://csrc.nist.gov/glossary/term/smart_contract.

3. Buterin V. Ethereum: a next-generation smart contract and decentralized application platform: white paper. 2014. URL: https://ethereum.org/whitepaper.

4. Clack C. D., Bakshi V. A., Braine L. Smart contract templates: foundations, design landscape and research directions // arXiv. 2016. arXiv:1608.00771. URL: https://arxiv.org/abs/1608.00771.

5. Tolmach P., Li Y., Lin S.-W., Liu Y., Li Z. A survey of smart contract formal specification and verification // ACM Computing Surveys. 2020. Vol. 54, no. 7. Art. 148. DOI: 10.1145/3399438.

6. Schär F. Decentralized finance: on blockchain- and smart contract-based financial markets // Federal Reserve Bank of St. Louis Review. 2021. Vol. 103, no. 2. P. 153–174. DOI: 10.20955/r.103.153-174.

7. Smart contracts security: threat landscape and risk assessment / European Union Agency for Cybersecurity (ENISA). 2021. URL: https://www.enisa.europa.eu/publications.

8. Chu H., Zhang Z., Chen J., Wang X., Li Z. A survey on smart contract vulnerabilities // Information and Software Technology. 2023. Vol. 155. Art. 107097. DOI: 10.1016/j.infsof.2022.107097.

9. Yakovenko A. Solana: a new architecture for a high performance blockchain: white paper. Version 0.8.13. Solana Labs, 2020. 32 p. URL: https://solana.com/solana-whitepaper.pdf.

10. Kao H.-T., Chitra T., Chiang R., Morrow J. An analysis of the market risk to participants in the Compound protocol // Proceedings of the Third International Symposium on Foundations and Applications of Blockchain (FAB'20). Santa Cruz, CA, USA, 2020. P. 1–10. DOI: 10.1145/3380745.3405124.

11. Smart contracts in blockchain systems: architecture, applications and security challenges // Computers. 2025. Vol. 14, no. 2. Art. 226. URL: https://www.mdpi.com/2073-431X/14/2/226.

Надійшла до редакції (Received): 18.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

© Хвостенко В.С. Еволюція смарт-контрактів у Web3- та DeFi-системах: архітектурна трансформація загроз безпеки та перспективи комплексного захисту. Сучасний захист інформації, 1(65), 132–141. https://doi.org/10.31673/2409-7292.2026.011651