УДК 004.056.5
Козіна Г.Л.[1], Головко І.О. [2]
[1] канд. фіз.-мат. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. РТ-812м НУ «Запорізька політехніка»

АНАЛІЗ ВПЛИВУ МУТАБЕЛЬНОСТІ ДАНИХ В БЛОКЧЕЙНІ НА ЗАХИЩЕНІСТЬ

Звичайний спосіб зберігання даних не завжди гарантує їх безпеку та цілісність. У цьому контексті, технологія блокчейн визнана одним з найбільш перспективних інструментів для збереження даних і забезпечення їх захищеності. Блокчейн є розподіленою базою даних, яка зберігається на різних комп'ютерах, але відображається в єдиному блокчейні, що робить його надійним і стійким до кібератак.

Застосування блокчейну для збереження та передачі інформації вже знайшло своє застосування в багатьох галузях, включаючи фінансову сферу, логістику, медицину, громадську безпеку та багато інших. Однак, разом зі

зростанням застосування блокчейну, з'являються нові виклики щодо безпеки та цілісності даних.

Дані на будь-якому етапі обробки можуть бути спотворенні, навіть без втручання зловмисника. А дані, які зазвичай записують в блокчейн, мають особливу важливість, тобто їх спотворення є неприпустимими. Але, так як в будь-якій системі є непередбачувані фактори, стає нагальною можливість змінювати (мутувати) дані в ланцюжку.

Мутабельність даних є одним з факторів, що можуть вплинути на захищеність блокчейну. Мутабельність відноситься до можливості зміни даних, що вже зберігаються в блокчейні. Якщо дані можна змінювати, то це може призвести до порушення безпеки, підробки та втрати даних.

Спочатку розглянемо як саме досягається мутабельність даних в блокчейну. Адже сама концепція блокчейну заперечує можливість змінювати або видаляти дані, що зберігаються у блоках ланцюжка. Що призвело до виникнення семантичних прийомів що дозволили імітувати мутабельність даних в блокчейні.

Є два основні підходи, що дозволяють мутувати дані в блокчейні. Суть першого методу полягає в тому, що створюється друга підмережа блокчейну в якій зберігаються дані про зміни що мають відбутися над батьківськими даними перед видачею.

Другий метод полягає у додаванні в протокол для вузлів блокчейну нової директиви, що при запиті на зміну даних, створює новий блок з посиланням на вже існуючий (батьківський) блок. Новостворений блок буде містити дані, що вказують на зміни, які повинні відбутися з батьківським блоком перед видачею його користувачеві, або він може містити вже перетворені дані. Слід зазначити, що даний метод може організовуватися не лише на рівні блокчейну, такий підхід можна організувати на рівні застосунку.

Обидва методи мають свої переваги та недоліки. Хоч вони по суті є лише семантичним доповненням блокчейну, але ці методи надають інструмент видозміни даних в блокчейні. Незважаючи на те що насправді дані в блоках не мутують, це все одно створює проблему, бо ми вже не можемо гарантувати цілісність даних, адже тепер при викриттю секретного ключу не можна гарантувати що останні перетворення були внесені не зловмисником (вразливість 1).

Хоч вразливість 1 притаманна і звичайному блокчейну, так як ця вразливість відноситься більше до людського фактору. Але у випадку звичайного блокчейну момент викриття секретного ключа можна відслідкувати краще.

При застосуванні обох методів збільшує навантаження на мережу блокчейну, адже окрім запитів на створення та видачу даних з'являються також запити на оновлення даних. При збільшенні кількості запитів виникає

збільшення небезпека атаки на подвійне витрачання. Адже через великий потік запитів вірогідність неузгодження між декількома вузлами збільшується, відповідно можливе дублювання даних.

В блокчейні який використовує перший метод також збільшується вірогідність атаки більшості (або атака 51%). Тому що зловмиснику або групі зловмисників тепер немає необхідності складати більшість всієї системи, їм достатньо стати більшою частиною підмережі. Слід зазначити що другий метод хоч і вирізняється більшим навантаженням на мережу ніж перший, але з точки зору атаки більшості є більш захищений навіть за звичайну мережу блокчейну.

Слід також зазначити головну перевагу додавання функціоналу що реалізує мутацію даних, яка в свою чергу походить від недоліку збільшення навантаження на блокчейн, це зменшення вірогідності того що у зловмисника буде можливість рахувати швидше за блокчейн. Несанкціонована зміна даних в блокчейні можлива лише за умови, що потужності зловмисника більші за потужність системи блокчейну. А у випадку великих навантажень та наявності пропорційно великої кількості вузлів дана умова фізично неможлива.

Аналізуючи загрози описані в тезах вище, можна зробити висновок, що хоч мутабельність є корисним та необхідним інструментом він також приносить з собою ряд загроз. В залежності від методу, який був реалізований для функціоналу мутації даних, загрози можуть різнитися, і навіть з'являтися переваги над класичною реалізацією.