

УДК 004.056.5

Ксенія Олександрівна КРАТАСЮК,

*курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;*

Віталій Анатолійович СВІТЛИЧНИЙ,

кандидат технічних наук,

*доцент кафедри кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;*

ORCID: <https://orcid.org/0000-0003-3381-3350>

ЗАХИСТ ОСОБИСТИХ ДАНИХ З ТЕХНОЛОГІЄЮ БЛОКЧЕЙН

Вступ і постановка проблеми.

Сучасні технології завдали відчутного удару по захисту нашої конфіденційної інформації. Велика частина того, чим займаються окремі особи або організації, стало надбанням громадськості. Сторонні особи беруть під контроль, зберігають і використовують особисті та корпоративні дані, шаблони, переваги і заняття. Багато нових бізнес-моделей ґрунтуються на зборі, організації та перепродажу наших особистих даних. Технології також спрощують пошук конкретної особи за його даними, навіть якщо цей користувач відмовився від

соціальних мереж. Наприклад, зрушення в технології розпізнавання осіб знайшли широке застосування в сфері торгівлі і забезпечення безпеки.

Технологія блокчейн може обмежити вплив цієї ерозії конфіденційності, надаючи при цьому особисту інформацію, якщо та необхідна для справи. Наприклад, користувач може зберігати особисту інформацію в блокчейні і тимчасово оприлюднити частину її для отримання тієї чи іншої послуги.

Розкриття особистих даних

Facebook, Twitter та інші соціальні мережі змінили очікування щодо конфіденційності в Інтернеті. Люди, які використовують ці платформи, добровільно надають особисту інформацію та погоджуються поділитися нею з обмеженою аудиторією або з усіма. Проте, навіть люди, які не хочуть ділитися своєю особистою інформацією (наприклад, ті, у кого немає аккаунта Facebook або Twitter), можуть відчувати необхідність зробити це заради кар'єри або в рамках маркетингу. Роботодавці часто шукають відомості на своїх кандидатів в Google. І оскільки відсутність результату краще, ніж поганий результат, сьогоднішні кандидати на роботу зазвичай використовують Інтернет для власного просування, або створюючи обліковий запис LinkedIn, або демонструючи досягнення через персональний сайт, блог або статті. Те ж саме відноситься і до малих підприємств: у більшості з них або є присутність в Інтернеті, або, за відсутності такого, вони втрачають бізнес [1].

Особисті дані, які ми надаємо в соціальних мережах і сервісах послуг за запитом, можуть служити комусь непоганою підмогою для розподілу людей по таким категоріям, як місце розташування, вік, стать, споживчі переваги, соціальні переваги і по іншим аналогічним ознаками. Особиста інформація дає власнику певну владу, тому люди повинні чітко встановлювати комфортний для себе в тих чи інших обставинах рівень особистої недоторканності.

Захист клієнтської інформації

Для організацій, які обслуговують інші організації (наприклад, компанії по веденню бухгалтерського обліку або надання юридичних послуг), захист інформації про клієнта також має вирішальне значення для підтримки відносин з клієнтами. Зловмисники орієнтуються на професійні сервісні компанії, щоб отримати дані їх клієнтів, намагаючись обійти складні заходи захисту даних клієнтів. Розуміючи цей ризик, великі компанії докладають значних зусиль для захисту інформації клієнтів.

Blockchain – це спосіб цифрової реєстрації операцій у загальнодоступній мережі Інтернет як основної частини світової інфраструктури [1].

В основі системи є побудований блок криптовалют, який є незмінним хронологічним переліком всіх транзакцій у системі. Отже, теоретично, розслідується відмивання грошей або придбання

незаконних товарів криптовалютами, ніж, скажімо, готівкою. Кримінальним особам не потрібно використовувати криптографічні курси, оскільки вони мають грошові кошти та свою банківську систему. Злочинці на такому підпільному ринку будуть зрештою знищені шляхом відстеження платежів у загальнодоступній блокчейн книжці.

Спеціальне програмне забезпечення вимагає фільтрацію інформації в загальних реєстрах блокчейнів та роз'яснення того, які транзакції виглядають підозрілими, і це ускладнюється тим, що шахраї переходять у все більш і більш анонімні валюти. Такі криптовалюти, як Monero, Ethereum і Zcash набувають популярності в цифровому підпіллі. Пропонуючи додаткові функції конфіденційності, Monero та Zcash приховують відправника, одержувача та вартість усіх транзакцій, що майже неможливо відслідковувати всередині системи. Група Zcash наполягає на тому, що лише тому, що збільшується конфіденційність, не означає, що існують ознаки злочинного використання.

Що стосується злочинної діяльності проти самих мереж, то фішинг – це головна тенденція, Прикладом цього існують вигадливі посилення на електронну пошту, що представляють собою ваш банк, криптофішинг зазвичай передбачає залучення інвесторів у надсилання грошей на неправильну адресу для передбачуваного перепродажу монет в ICO, а часто використовується для розповсюдження дезінформації.

Незважаючи на сертифікати безпеки блоків, технологія не обов'язково є *абсолютно* безпечною. В такому разі наслідки можуть бути руйнівними. З огляду на величину, в декількох основних блокчейнах (насамперед, Bitcoin та Ethereum).

Так як автори монет займаються різноманітними тіньовими практиками, секретний перепродаж знаків, для існуючих інвесторів за більш низькою ціною, що і стає фактом злочину.

Технологія блокчейн зі спеціальними протоколами, що допускають різну ступінь анонімності та конфіденційності, може забезпечити захист персональних даних, допускаючи при цьому використання цих даних в додатках з штучним інтелектом. Наприклад, користувач може використовувати блокчейн з особистою інформацією про здоров'я і розкривати певні елементи цієї інформації виключно для певних цілей постачальникам товарів або послуг.

Блокчейн, по суті, є публічним реєстром, що зберігаються в кількох місцях, і тим не менш він може забезпечити анонімність і довіру, про що свідчать численні додатки на основі блокчейна і вже існуючі криптовалюти з високим ступенем захисту особистої інформації.

В даний час особисті дані, які збирають сторонні особи, зазвичай зберігаються в централізованих базах даних з єдиною точкою відмови. Виток цих даних часто залишається непоміченим і не

фіксується. Якщо наші дані потрапляють в чужі руки, ми фактично не можемо контролювати їх використання.

Сфери застосування блокчейна. Сутність «ланцюга блоків» як загальнодоступною, розподіленою і 100% достовірною бази даних робить застосування блокчейн дуже привабливим для компаній, що працюють в різних областях. В даний час вже існує ряд розширень для розробки бізнес-додатків на блокчейн, що забезпечують: безпечне адміністрування мереж, що виключає хакерські атаки MIM (Man-in-the-Middle, що означає «людина посередині») і знімає проблему централізованого адміністрування; зберігання цифрових сертифікатів, що робить повністю захищеним доступ користувачів до сайтів (зокрема, виключаючи перехоплення паролів); безпечні двосторонні угоди; фіксацію часу розміщення документів, що дозволяє вирішувати питання патентування, авторського права; систему DNS (Domain Name System), невразливу для DDOS-атак (Distributed Denial of Service – attacks), та інше.

Висновок. Наша особиста інформація в даний час зосереджена в Інтернеті і в базах даних компаній, тобто по суті контролюється кількома гравцями. Можна очікувати, що такі темпи зростання обсягів створюваних і зібраних даних і далі будуть послаблювати захист нашої особистої інформації. Рішення із застосуванням технології блокчейн або засновані на принципах цієї технології можуть допомогти знизити загрозу конфіденційності, дозволяючи нам при цьому прискорити вчинення транзакцій, поліпшити сервіс і використовувати найбільш ефективні алгоритми штучного інтелекту.

Список бібліографічних посилань

1. Ray S. How Blockchains Will Enable Privacy // Towards Data Science. Mar 3, 2018. URL: <https://towardsdatascience.com/how-blockchains-will-enable-privacy-1522a846bf65> (дата звернення: 28.10.2018).

Одержано 30.10.2018