УДК 004

М.Фадєєв, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ З ВИКОРИСТАННЯМ МУЛЬТИВАРІАНТНОГО ЦЕНТРУ РЕАЛІЗАЦІЇ КРИПТОАЛГОРИТМІВ

У статті розроблено програмне забезпечення, яке призначено для системи з використанням мультиваріантного центру реалізації криптоалгоритмів. Метою розробки є дослідження та програмна реалізація системи з використанням мультиваріантного центру реалізації криптоалгоритмів. Об’єктом дослідження є процес з використанням мультиваріантного центру реалізації криптоалгоритмів. Предметом дослідження є методи з використанням мультиваріантного центру реалізації криптоалгоритмів. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи з використанням мультиваріантного центру реалізації криптоалгоритмів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.
комп’ютерна інженерія, захист інформації

Постановка проблеми. Останнім часом досить широке поширення одержали різні програмно-апаратні системи захисту інформації, призначені для шифрування даних, що зберігаються на жорстких дисках. Як приклади можна привести відомі PGPdisk і BestCrypt, StrongDisk, Zdisk і Zserver від SecurIT, і т.д.

Крім цього, існують вартим особняком системи шифрування окремих файлів і каталогів, найбільш відома й розповсюджена з яких – EFS (Encrypted File System), що входить до складу MS Windows, починаючи з Windows 2000.

Всі ці системи відрізняються друг від друга способом шифрування, алгоритмами, можливостями й т.д. настільки, що потенційний користувач таких систем часом губиться, і не завжди може зрозуміти, які саме можливості надає та або інша система, і навіщо йому все це потрібно.

Незважаючи на масу розходжень, всі сучасні системи шифрування даних працюють за принципом «прозорого» шифрування. Суть цього принципу полягає в тому, що шифрування даних не є окремою операцією, що повинен виконувати користувач у процесі роботи, а здійснюється одночасно з роботою користувача, автоматично, при читанні й записі даних. Користувач тільки повинен включити шифрування, ввівши при цьому якийсь пароль або ключ шифрування.

У наших українських умовах легко уявити собі ситуацію, коли з комп'ютера, що зберігає конфіденційну інформацію, витягається жорсткий диск і підключається до іншого комп'ютера. А там бажаючий ознайомитися з інформацією знає свій пароль і має права адміністратора. З урахуванням такої можливості покладатися на один тільки пароль досить легковажно.

Разом з тим шифрування безсило проти різних програмних і апаратних закладок, «троянів», мережного злому й інших атак, яким може піддатися працюючий комп'ютер із завантаженими ключами шифрування, коли користувач або адміністратор може просто не знати, що на комп'ютер проникнув сторонній.

У цьому випадку зловмисник тим або іншим способом прикидається легальним користувачем, і одержує доступ до інформації також, як і легальний користувач. На жаль, шифрування не вміє перевіряти права доступу користувачів на доступ до інформації.

Тому, шифрування даних – це лише один з важливих елементів системи інформаційної безпеки, але зовсім не достатній.

Необхідна наявність грамотна настроєної системи розмежування доступу, контролю цілісності операційного середовища, засобів виявлення проникнень, антивірусного й антитроянського захисту й т.д.

У різних системах можуть використовуватися різні способи шифрування даних. Це може бути шифрування на рівні файлів, або шифрування на рівні секторів диска.

Аналізуючи дані з відомих джерел, можна рекомендувати використовувати файл-контейнер для захисту даних окремих користувачів на їхніх комп'ютерах; у цьому випадку навантаження не занадто високе, і падіння продуктивності не так помітно. Більше проста процедура установки й керування такою системою навіть якоюсь мірою компенсує ці недоліки.

Для захисту ж корпоративних серверів, до яких пред'являються більше високі вимоги по продуктивності й надійності, рекомендується використовувати блокове шифрування розділів диска.

У цьому випадку додаткові, до того ж, як правило, разові роботи з інсталяції й настроювання системи захисти цілком виправдуються більше високим ступенем надійності й меншим падінням продуктивності.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи з використанням мультиваріантного центру реалізації криптоалгоритмів.

Мета й завдання дослідження.

Метою роботи є дослідження та програмна реалізація системи з використанням мультиваріантного центру реалізації криптоалгоритмів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем з використанням мультиваріантного центру реалізації криптоалгоритмів.

– Дослідження системи з використанням мультиваріантного центру реалізації криптоалгоритмів.

– Програмна реалізація системи з використанням мультиваріантного центру реалізації криптоалгоритмів.

Об'єктом дослідження є процес з використанням мультиваріантного центру реалізації криптоалгоритмів.

Предметом дослідження є методи з використанням мультиваріантного центру реалізації криптоалгоритмів.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Опис технологій центру шифрування

Розроблене програмне забезпечення дозволяє виконувати наступні функції захисту інформації:

– проводити шифрування;

– будувати геш-функції масивів інформації;

– реалізовувати алгоритми генерації псевдовипадкових чисел;

– підраховувати контрольну суму файлів.

Розглянемо ці технології захисту інформації більш докладно.

Алгоритми шифрування реалізовані у програмному забезпеченні базуються на симетричних алгоритмах.

Криптографічні алгоритми відіграли вирішальну роль в історії та розвитку криптовалюти. Ці алгоритми постійно вдосконалювалися, щоб забезпечити безпечні та приватні транзакції в цифровій сфері.

Протягом багатьох років було досягнуто значного прогресу, перейшовши від простих методів шифрування до більш складних і витончених алгоритмів. Не можна недооцінювати вплив цих досягнень на зростання криптовалют.

У цьому розділі ми досліджуємо історичний розвиток криптографічних алгоритмів у світі крипто, висвітлюючи ключові моменти, які сформували ландшафт цифрових транзакцій. Розуміючи роль криптографічних алгоритмів, читачі зможуть краще зрозуміти їх значення в поточному розвитку та впровадженні криптовалют.

Приєднуйтесь до нас, коли ми розгадаємо подорож криптографічних алгоритмів та їхній вплив на світ криптовалюти, що постійно розвивається.

Ранні криптографічні алгоритми

На ранніх етапах розвитку криптовалюти криптографічні алгоритми відігравали вирішальну роль у забезпеченні безпеки та цілісності транзакцій. Ці алгоритми лягли в основу криптографічної еволюції, яка сформувала історію криптовалют.

Найпоширенішим криптографічним алгоритмом у цей час був SHA-256 (Secure Hash Algorithm 256-bit), який використовувався при створенні Bitcoin. Алгоритм SHA-256 забезпечив безпечний метод для перевірки цілісності транзакції та запобігання втручанню.

Оскільки криптовалюти набули популярності, виникла потреба в більш досконалих криптографічних алгоритмах. Це призвело до розробки алгоритмів блокчейну, включаючи алгоритми Proof of Work (PoW) і Proof of Stake (PoS). Ці алгоритми запровадили нові механізми для захисту транзакцій і підтримки цілісності блокчейну.

Еволюція криптографічних алгоритмів у сфері криптовалют мала значний вплив на розвиток галузі. Забезпечуючи безпечну та децентралізовану систему для перевірки транзакцій, ці алгоритми вселили довіру до криптовалют. Крім того, вони проклали шлях для розробки нових програм і варіантів використання, таких як смарт-контракти та децентралізовані фінанси.

Введення геш-функцій

Впровадження геш-функцій стало важливою віхою в еволюції криптографічних алгоритмів у сфері криптовалют. Геш-функції, які є математичними алгоритмами, приймають вхідні дані (або повідомлення) і створюють рядок символів фіксованого розміру, відомий як геш-значення або геш-код. Ці функції створені для того, щоб бути швидкими та ефективними, генеруючи унікальний вихід для кожного унікального входу.

У контексті криптовалют використання геш-функцій має кілька важливих наслідків. По-перше, вони забезпечують цілісність транзакцій і даних шляхом створення унікального ідентифікатора для кожного блоку транзакцій. Це дозволяє учасникам мережі перевіряти автентичність даних, не покладаючись на центральний орган. По-друге, геш-функції забезпечують певний рівень конфіденційності та безпеки, унеможливлюючи зворотне проектування початкового введення з геш-значення.

Щоб краще зрозуміти вплив геш-функцій на криптовалюти, давайте розглянемо деякі ключові віхи в криптоіндустрії:

– 2008: Білий документ про біткойн – Сатоші Накамото представляє біткойн, децентралізовану криптовалюту, яка використовує геш-функції для захисту транзакцій. Ця революційна концепція усуває потребу в посередниках і забезпечує однорангові транзакції.

– 2013: Представлення Scrypt – Scrypt, функція отримання ключів, представлена, щоб зробити майнінг більш доступним і стійким до спеціалізованого обладнання. Це заохочує ширшу участь у майнінгу та допомагає підтримувати децентралізований характер криптовалют.

– 2015: Ethereum Blockchain – Ethereum представляє концепцію розумних контрактів, розширюючи використання геш-функцій за межі безпеки транзакцій. Це дозволяє розробляти децентралізовані програми (DApps) і полегшує створення нових токенів і проектів на основі блокчейну.

– 2021: Proof of Stake (PoS) – багато криптовалют переходять від Proof of Work (PoW) до консенсусних алгоритмів PoS, які покладаються на геш-функції для перевірки транзакцій.

Цей перехід зменшує споживання енергії та покращує масштабованість, роблячи криптовалюти більш стійкими та ефективними.

Впровадження геш-функцій мало глибокий вплив на розвиток криптографічних алгоритмів у криптовалютах. Це проклало шлях для створення децентралізованих систем, покращило безпеку та конфіденційність, а також уможливило зростання інноваційних програм. Оскільки криптоіндустрія продовжує розвиватися, геш-функції, безсумнівно, відіграватимуть вирішальну роль у формуванні її майбутнього.

Геш-функції у світі криптовалют служать багатьом важливим цілям, крім безпеки. Ці математичні алгоритми перетворюють дані в рядки фіксованого розміру, які називаються геш-значеннями, забезпечуючи цілісність і автентичність цифрових транзакцій.

Однак їхнє значення виходить за межі безпеки. Геш-функції відіграють важливу роль у майнінгу, який є основою багатьох криптовалют. Вони надають унікальні ідентифікатори для транзакцій і блокувань, уможливлюючи перевірку та перевірку, таким чином гарантуючи легітимність і захист від несанкціонованого доступу.

Крім того, геш-функції знаходять застосування для зберігання даних, цифрових підписів і алгоритмів підтвердження роботи.

Багатогранна природа геш-функцій у криптовалютному ландшафті досліджується в цій статті, проливаючи світло на їхню важливість за межі їх ролі в забезпеченні безпеки.

Підвищення цілісності даних

Використання геш-функцій у криптовалюті відіграє вирішальну роль у підвищенні цілісності даних. Ці математичні алгоритми генерують рядок символів фіксованого розміру, відомий як геш-значення, унікальний для вхідних даних. Застосовуючи геш-функції до крипто-транзакцій, зберігається цілісність даних. Будь-яка зміна даних транзакції призведе до іншого геш-значення, попереджаючи систему про можливе втручання.

Геш-функції також відіграють значну роль у видобутку блокчейнів. Кожен блок у блокчейні містить геш-значення, отримане з геш-значення попереднього блоку, створюючи ланцюжок блоків. Це гарантує, що будь-яка зміна блоку призведе до зміни геш-значення, розриваючи ланцюжок і роблячи весь блокчейн недійсним. Таким чином, геш-функції використовуються для перевірки та захисту даних, що зберігаються в блоках.

Крім ролі в забезпеченні цілісності даних, геш-функції мають різні інші застосування в сфері криптовалют. Вони використовуються, зокрема, у цифрових підписах, зберіганні паролів і створенні адрес. Надійність і ефективність геш-функцій робить їх важливим інструментом у світі криптовалют.

Перевірка автентичності транзакції

Автентичність транзакцій у криптовалюті забезпечується за допомогою геш-функцій. Ці функції відіграють вирішальну роль у перевірці цілісності та дійсності транзакцій шляхом генерації унікальних вихідних даних фіксованої довжини, відомих як геш, коли вони застосовуються до даних транзакцій. Потім цей геш використовується для перевірки автентичності транзакції.

Одним із способів використання геш-функцій для перевірки автентичності транзакцій є використання цифрових підписів. У програмі цифрової валюти цифровий підпис створюється шляхом шифрування гешу транзакції за допомогою закритого ключа відправника. Потім одержувач може розшифрувати підпис за допомогою відкритого ключа відправника, тим самим перевіряючи автентичність транзакції. Цей процес гарантує, що транзакція не була підроблена під час передачі та походить від заявленого відправника.

Щоб додатково проілюструвати важливість геш-функцій для перевірки автентичності транзакцій, у наведеній нижче таблиці висвітлено деякі ключові переваги, які вони надають у додатках цифрових валют:

- Забезпечує цілісність даних.
- Запобігає фальсифікації транзакцій.
- Вмикає безпечні цифрові підписи.
- Сприяє ефективній перевірці транзакцій.

– Підтримує невідмову від транзакцій.

Запобігання подвійним витратам

Використання геш-функцій є вирішальним аспектом у запобіганні подвійним витратам у криптовалюті. Подвійне витрачання означає шахрайську діяльність під час спроби витратити ту саму криптовалюту кілька разів. Геш-функції відіграють важливу роль у забезпеченні цілісності та безпеки криптовалютних транзакцій.

Коли транзакція ініціюється, вона проходить процес, відомий як гешування, де геш-функція застосовується до даних транзакції. Цей процес генерує унікальний результат, який називається геш, який служить цифровим відбитком для транзакції. Потім геш зберігається в блокчейні. Будь-яка зміна даних транзакції, незалежно від того, наскільки мала, призведе до зовсім іншого гешу.

Щоб запобігти подвійним витратам, мережа блокчейну покладається на консенсусні алгоритми, такі як proof-of-work або proof-of-stake, які широко використовують геш-функції. Ці алгоритми перевіряють і підтверджують транзакції шляхом вирішення складних математичних головоломок або за допомогою механізмів на основі ставок. Використовуючи геш-функції в ці алгоритми, мережа гарантує, що кожна транзакція є унікальною, тим самим запобігаючи будь-яким спробам витратити ту саму криптовалюту більше одного разу.

Крім того, геш-функції також використовуються в майнінгу, процесі додавання нових транзакцій до блокчейну. Майнери змагаються, щоб знайти геш, який відповідає певним критеріям, що вимагає значної обчислювальної потужності. Цей процес не тільки захищає мережу, але й запобігає подвійним витратам, забезпечуючи додавання в блокчейн лише дійсних транзакцій.

Забезпечення ефективних процесів майнінгу

Геш-функції відіграють вирішальну роль в оптимізації процесів майнінгу в екосистемі криптовалюти. У контексті криптовалюти майнінг включає перевірку та додавання нових транзакцій до блокчейну, що вимагає значної обчислювальної потужності та має важливе значення для підтримки цілісності та безпеки мережі.

Ефективні процеси майнінгу значною мірою залежать від властивостей геш-функцій. Криптографічні геш-функції, як-от SHA-256, спеціально розроблені, щоб розв’язувати їх обчислювально, але їх легко перевірити. Така конструкція робить їх ідеальними для майнінгу, оскільки це гарантує, що процес не можна легко маніпулювати або підробити.

Майнери використовують геш-функції, щоб змагатися у вирішенні складних математичних головоломок, відомих як алгоритми підтвердження роботи. Перший майнер, який розгадає головоломку, отримує винагороду щойно відкарбованими монетами та комісією за транзакції. Це стимулює майнерів інвестувати в потужне обладнання та конкурувати за швидше вирішення цих головоломок, тим самим підвищуючи ефективність процесу видобутку.

Крім того, геш-функції полегшують створення майнінг-пулів, де кілька майнерів об’єднують свої обчислювальні потужності, щоб підвищити ймовірність вирішення головоломки та отримання винагороди. Таке об’єднання ресурсів забезпечує більш ефективний і послідовний процес видобутку, оскільки майнери колективно вирішують головоломки швидше.

Забезпечення механізмів консенсусу

Включення механізмів консенсусу є важливим аспектом геш-функцій у індустрії криптовалют. Ці механізми відіграють вирішальну роль у перевірці транзакцій і підтримці цілісності мережі.

Роль у перевірці транзакцій

Механізми консенсусу в криптовалюті значною мірою покладаються на геш-функції для підтвердження транзакцій. Геш-функції відіграють вирішальну роль у забезпеченні цілісності та безпеки мережі криптовалют.

Нижче наведено три ключові способи, за допомогою яких геш-функції забезпечують перевірку транзакцій:

1. Цілісність даних: геш-функції генерують унікальні вихідні дані фіксованого розміру для заданого вхідного даних. Застосовуючи геш-функції до даних транзакцій, будь-яка зміна даних призведе до іншого геш-значення. Це дозволяє учасникам мережі перевірити, чи дані транзакції не були підроблені.

2. Перевірка транзакцій: геш-функції використовуються для створення цифрових підписів, які перевіряють автентичність і цілісність транзакцій. Порівнюючи геш-значення транзакції з цифровим підписом, учасники можуть переконатися, що транзакція не була підроблена.

3. Ефективний консенсус: геш-функції використовуються в механізмах консенсусу, таких як підтвердження роботи (PoW) і підтвердження частки (PoS), щоб забезпечити згоду щодо дійсності транзакції. Виконуючи складні обчислення за допомогою геш-функцій, учасники можуть досягти консенсусу щодо порядку та дійсності транзакцій, уможливлюючи децентралізований і недовірливий консенсус.

Вплив на масштабованість мережі

Вплив геш-функцій на масштабованість мережі та ефективну роботу механізмів консенсусу є ключовим аспектом, який слід враховувати в контексті криптовалюти. Геш-функції відіграють важливу роль у створенні консенсусних механізмів, таких як Proof of Work (PoW) і Proof of Stake (PoS), які необхідні для підтримки цілісності та безпеки криптовалютної мережі.

Ці механізми покладаються на геш-функції для підтвердження та перевірки транзакцій, гарантуючи додавання в блокчейн лише дійсних транзакцій. Однак обчислювальна складність геш-функцій може мати наслідки для масштабованості мережі. Зі збільшенням кількості транзакцій та учасників криптовалютної мережі зростають і обчислювальні ресурси, необхідні для механізмів консенсусу. Це потенційно може призвести до вузьких місць і сповільнення часу обробки транзакцій.

Тому оптимізація ефективності геш-функцій має вирішальне значення для забезпечення масштабованості та безперебійної роботи мереж криптовалюти.

Увімкнення функції смарт-контракту

Реалізація функції смарт-контракту в криптовалютах передбачає інтеграцію геш-функцій, які забезпечують цілісність і безпеку процесу виконання контракту. Геш-функції відіграють вирішальну роль у забезпеченні безперебійного виконання смарт-контрактів, надаючи механізми перевірки та підтвердження.

Нижче наведено три ключові способи, за допомогою яких геш-функції забезпечують роботу смарт-контракту:

– Цілісність даних: геш-функції використовуються для перевірки цілісності даних, що зберігаються в розумному контракті. Згенерувавши унікальне геш-значення для даних контракту, можна легко виявити будь-яке підроблення або модифікацію. Це гарантує, що виконання контракту базується на точній і незмінній інформації.

– Умовне виконання: розумні контракти часто вимагають виконання певних умов, перш ніж їх можна буде виконати. Геш-функції дають змогу створити умовне виконання шляхом включення конкретних умов у контракт. Ці умови можуть бути закодовані як геш-значення, і контракт буде виконано, лише якщо геш-значення відповідає попередньо визначеній умові.

– Незмінний код: геш-функції використовуються для створення унікальних ідентифікаторів для смарт-контрактів, відомих як адреси контрактів. Ці адреси походять від коду контракту, що забезпечує незмінність коду. Ця незмінність має вирішальне значення для гарантії того, що логіка та функціональність контракту не можуть бути змінені після розгортання.

Підтримка технології незмінного блокчейну

Геш-функції відіграють вирішальну роль у підтримці незмінності технології блокчейн у криптовалютах. Ці функції забезпечують цілісність даних, генеруючи унікальні геш-коди

для кожного блоку в блокчейні. Цей процес надзвичайно ускладнює зміну минулих транзакцій без виявлення.

Запобігаючи втручанню та шахрайству, геш-функції дозволяють здійснювати ненадійні транзакції, усуваючи потребу в посередниках.

Як наслідок, використання геш-функцій підвищує безпеку та прозорість мережі блокчейн.

Забезпечення цілісності даних

Цілісність даних є фундаментальним аспектом технології блокчейн, оскільки вона забезпечує точність і незмінність інформації, що зберігається децентралізованим способом. Геш-функції відіграють вирішальну роль у підтримці цілісності даних у мережі блокчейн.

Наступні три ключові способи демонструють, як геш-функції забезпечують цілісність даних:

1. Перевірка: геш-функції генерують унікальні геш-значення для кожного блоку даних, діючи як цифровий відбиток. Порівнюючи ці геш-значення, користувачі можуть перевірити цілісність даних і переконатися, що вони не були підроблені.

2. Консенсус: геш-функції використовуються в механізмах консенсусу блокчейн-мереж, таких як підтвердження роботи (PoW) або підтвердження частки (PoS). Завдяки перевірці транзакцій і блоків за допомогою гешування досягається консенсус щодо правильної версії блокчейну, додатково гарантуючи цілісність даних.

3. Ланцюжок блоків: геш-функція, яка використовується в технології блокчейн, створює ланцюжок блоків, причому кожен блок містить геш-значення попереднього блоку. Це гарантує, що будь-яка модифікація блоку вимагатиме перерахунку гешу всіх наступних блоків, що робить фактично неможливим зміну даних без виявлення.

Запобігання втручанню та шахрайству

Геш-функції відіграють вирішальну роль у запобіганні підробці та шахрайству в технології блокчейн. Ці функції приймають вхідні дані, такі як транзакція або блок даних, і генерують вихідні дані фіксованого розміру, відомі як геш-значення. Це геш-значення є унікальним для вхідних даних, тобто навіть незначна зміна вхідних даних призведе до зовсім іншого геш-значення.

Зберігання цих геш-значень у блокчейні гарантує, що будь-яка спроба підробити дані буде негайно виявлена.

Крім того, геш-функції використовуються в процесі майнінгу для забезпечення цілісності блокчейну. Майнери змагаються, щоб знайти конкретне геш-значення, яке відповідає певним умовам. Цей процес робить практично неможливим втручання в минулі транзакції без повторного виконання всіх наступних блоків.

У результаті геш-функції підтримують незмінність і надійність технології блокчейн, роблячи її високостійкою до шахрайства та маніпуляцій.

Увімкнення безнадійних транзакцій

Геш-функції відіграють вирішальну роль у підвищенні безпеки та надійності технології блокчейн. Вони забезпечують безнадійні транзакції, усуваючи потребу в посередниках або перевірених третіх сторонах. Це досягається шляхом надання унікального цифрового відбитка, або геш-значення, для кожної транзакції, забезпечуючи її цілісність і автентичність.

Існує три ключові способи, за допомогою яких геш-функції забезпечують безнадійні транзакції та підтримують незмінність блокчейну:

1. Перевірка: учасники можуть перевірити цілісність транзакцій, порівнюючи геш-значення, згенероване з даних транзакцій, із геш-значенням, що зберігається в блокчейні.

2. Консенсус: геш-функції використовуються в алгоритмах консенсусу, таких як Proof of Work, щоб гарантувати, що всі вузли в мережі погоджуються щодо дійсності транзакцій.

3. Цілісність блокчейну: геш-функції створюють ланцюжок блоків, пов’язуючи геш-значення кожного блоку з геш-значенням попереднього блоку. Це надзвичайно ускладнює зміну минулих транзакцій без виявлення.

Геш-функції відіграють вирішальну роль у підвищенні ефективності процесів майнінгу криптовалюти. Забезпечуючи цілісність даних і запобігаючи подвійним витратам, вони сприяють безперебійній роботі системи. Геш-функції забезпечують швидкий і безпечний спосіб перевірки транзакцій, дозволяючи майнерам перевіряти блоки та конкурувати за винагороду в децентралізованій мережі. Їх впровадження забезпечує надійність і надійність системи криптовалют, роблячи її більш ефективною та безпечною для всіх учасників.

Геш-функції в криптовалюті служать різним цілям, крім забезпечення цілісності даних і запобігання подвійним витратам. Вони мають різноманітні додатки, включаючи створення унікальних ідентифікаторів, створення цифрових підписів і сприяння безпечному спілкуванню між сторонами в децентралізованій мережі.

Геш-функції відіграють вирішальну роль у забезпеченні функції смарт-контрактів у технології блокчейн. Вони забезпечують цілісність і незмінність даних, надають унікальний ідентифікатор для кожного контракту та забезпечують безпечну та ефективну перевірку виконання контракту. Використовуючи геш-функції, мережа блокчейну може перевірити справжність транзакцій і запобігти будь-яким підробкам або несанкціонованим змінам контракту. Крім того, геш-функції допомагають оптимізувати зберігання та пошук даних контракту шляхом створення компактного представлення вмісту контракту. Це дозволяє швидше та ефективніше обробляти смарт-контракти в блокчейні. Загалом геш-функції є важливим компонентом технології блокчейн, що забезпечує надійність і безпеку функціональності смарт-контракту.

Геш-функції відіграють вирішальну роль у підтримці механізмів консенсусу, які використовуються в криптовалютах. Вони надають засоби перевірки цілісності даних транзакцій, гарантуючи, що кожен блок у ланцюжку блоків залишається унікальним, незмінним і стійким до втручання. Застосування геш-функцій посилює безпеку та надійність усієї системи.

Геш-функції мають відомі вразливості та обмеження, які потенційно можуть вплинути на безпеку криптовалют. Ці вразливості включають атаки на зіткнення, атаки на попередні зображення та ймовірність того, що майбутні квантові комп’ютери порушать поточні геш-функції.

Геш-функції в криптовалюті відіграють вирішальну роль, а не просто забезпечення безпеки. Вони пропонують кілька переваг, які підвищують загальну функціональність і надійність екосистеми цифрової валюти. Ці переваги включають:

1. Підвищення цілісності даних: геш-функції гарантують, що дані залишаються недоторканими та незмінними. Вони генерують унікальні ідентифікатори (геш-значення) для кожного фрагмента інформації, що дозволяє легко виявити будь-які зміни чи підробку.

2. Перевірка автентичності транзакцій: геш-функції використовуються для перевірки автентичності транзакцій. Порівнюючи геш-значення транзакції з її відповідним відкритим ключем, користувачі можуть переконатися, що транзакція не була змінена чи підроблена.

3. Запобігання подвійним витратам: геш-функції допомагають запобігти проблемі подвійних витрат, коли користувач намагається витратити ту саму криптовалюту двічі. Генеруючи унікальні геш-значення для кожної транзакції, блокчейн може ідентифікувати та відхиляти будь-які повторювані транзакції.

4. Забезпечення ефективних процесів майнінгу: геш-функції є невід’ємною частиною процесу майнінгу криптовалют, таких як біткойн. Майнери використовують обчислювальну потужність для вирішення складних математичних головоломок, а геш-функції допомагають забезпечити справедливість і безпеку цього процесу.

5. Підтримка механізмів консенсусу: механізми консенсусу, такі як Proof of Work або Proof of Stake, покладаються на геш-функції для досягнення згоди щодо дійсності транзакцій і створення нових блоків. Геш-функції відіграють вирішальну роль у підтримці цілісності та безпеки цих механізмів консенсусу.

6. Увімкнення функцій смарт-контракту: смарт-контракти — це самовиконувані контракти з попередньо визначеними правилами та умовами. Геш-функції використовуються для забезпечення цілісності та безпеки цих контрактів, що робить їх надійними та захищеними від підробки.

7. Полегшення використання незмінної технології блокчейну: геш-функції необхідні для створення незмінності технології блокчейну. Кожен блок у блокчейні містить унікальне геш-значення, яке залежить від даних у блоці. Будь-яка зміна в даних призведе до іншого геш-значення, роблячи очевидним, що блок було змінено.

Пропонуючи ці переваги, геш-функції сприяють довірі, надійності та безпеці всієї екосистеми криптовалюти. Вони є важливими компонентами для забезпечення цілісності транзакцій, блоків і загального функціонування цифрових валют у світі, що постійно розвивається.

Симетричні ключові алгоритми набувають популярності

Алгоритми із симетричним ключем набули значного значення в еволюції криптографічних алгоритмів у сфері криптовалют. Ці алгоритми використовують той самий ключ як для шифрування, так і для дешифрування, що робить їх високоефективними та придатними для різноманітних криптографічних програм.

Зростання популярності алгоритмів із симетричним ключем можна пояснити їх здатністю забезпечувати безпечні та швидкі процеси шифрування та дешифрування. У світі криптовалют, де транзакції потрібно проводити швидко та безпечно, це надзвичайно важливо. Алгоритми симетричного ключа, такі як Advanced Encryption Standard (AES) і Data Encryption Standard (DES), стали кращими виборами для шифрування конфіденційних даних, забезпечуючи конфіденційність і цілісність транзакцій.

Крім того, симетричні ключові алгоритми пропонують масштабованість, забезпечуючи ефективне шифрування та дешифрування великих обсягів даних. Ця масштабованість особливо важлива в контексті криптовалют, де обсяг транзакцій і даних може бути значним. Використовуючи симетричні ключові алгоритми, криптовалютні платформи можуть забезпечити безперебійну роботу своїх систем без шкоди для безпеки.

Криптографія з відкритим ключем революціонізує криптовалюту

Криптографія з відкритим ключем зробила революцію у світі криптовалют, змінивши спосіб проведення та захисту транзакцій у цифрових валютах. Цей криптографічний алгоритм запровадив революційний підхід, який усуває обмеження алгоритмів із симетричним ключем.

На відміну від алгоритмів із симетричним ключем, які покладаються на один ключ як для шифрування, так і для дешифрування, у криптографії з відкритим ключем використовується пара різних ключів: відкритий ключ і закритий ключ. Відкритий ключ широко поширений і використовується для шифрування, тоді як закритий ключ, відомий лише власнику, використовується для дешифрування та цифрових підписів.

Однією з ключових переваг криптографії з відкритим ключем є її здатність забезпечувати безпечний зв’язок і цифрові підписи без необхідності довіреної третьої сторони. Ця система дозволяє здійснювати безпечні транзакції, які можна перевірити, оскільки закритий ключ можна використовувати для підтвердження права власності без розкриття конфіденційної інформації.

Завдяки запровадженню криптографії з відкритим ключем криптовалюти стали більш безпечними, прозорими та стійкими до шахрайства. Він усунув необхідність безпечного обміну ключами та забезпечив безпечний метод для цифрових підписів. Цей прогрес значно підвищив безпеку та функціональність криптовалют, проклавши шлях для подальших інновацій у цій галузі.

Крім того, криптографія з відкритим ключем відкрила нові можливості для конфіденційності та анонімності в транзакціях з криптовалютою. Тепер користувачі можуть використовувати унікальні пари ключів для кожної транзакції, гарантуючи, що їх

ідентифікаційні дані залишаються прихованими, зберігаючи при цьому цілісність процесу транзакції.

Поточний стан і майбутнє криптографічних алгоритмів у криптовалюті

Поточний стан і майбутні перспективи криптографічних алгоритмів у криптовалюті зазнали значної еволюції. Важливість безпечних і ефективних криптографічних алгоритмів неможливо переоцінити, оскільки криптоіндустрія продовжує розвиватися. Щоб забезпечити безпечні транзакції та цифрові підписи, більшість криптовалют наразі покладаються на асиметричні криптографічні алгоритми, такі як криптографія з еліптичною кривою (ECC) і RSA (Rivest-Shamir-Adleman).

ECC набув популярності завдяки своїй здатності забезпечувати той самий рівень безпеки, що й RSA, але з меншими розмірами ключів, що робить його ефективнішим з точки зору обчислень. Ця ефективність особливо важлива в контексті технології блокчейн, де підтримка децентралізованої мережі залежить від ефективності.

Крім ECC і RSA, інші криптографічні алгоритми, такі як SHA-256 (Secure Hash Algorithm 256-bit) і HMAC (Keyed-Hash Message Authentication Code), використовуються для цілісності даних і автентифікації. Ці алгоритми гарантують, що дані залишаються незмінними, і дозволяють сторонам, залученим у транзакцію, перевірити автентичність даних.

Дивлячись у майбутнє, розробка квантових комп’ютерів становить потенційну загрозу для традиційних криптографічних алгоритмів. Квантові комп’ютери мають здатність зламати типові алгоритми шифрування, роблячи їх неефективними. Щоб вирішити цю проблему, дослідники вивчають використання квантово-стійких криптографічних алгоритмів, таких як криптографія на основі решітки та багатоваріантна криптографія, для захисту криптовалют у постквантову еру.

в криптовалютах, були менш безпечними та простішими порівняно з передовими методами шифрування, які використовуються сьогодні. Еволюція криптографічних алгоритмів призвела до розробки більш складних методів, які забезпечують безпеку та цілісність криптовалют. Ці досягнення посилили захист конфіденційних даних і транзакцій в екосистемі криптовалют. Сучасні криптографічні алгоритми, які використовуються в криптовалютах, включають сильніші алгоритми шифрування, геш-функції та схеми цифрового підпису, що робить їх більш стійкими до атак і підробки. Ці посилені заходи безпеки забезпечують вищий рівень довіри та надійності в системі криптовалюти, захищаючи цілісність і конфіденційність цифрових активів.

Впровадження геш-функцій у криптографічних алгоритмах у криптовалюті мало значний вплив як на безпеку, так і на ефективність цих алгоритмів. Геш-функції відіграють вирішальну роль у перевірці цілісності даних і захисту від підробки. Крім того, вони сприяють прискоренню обчислень, підвищуючи загальну ефективність криптографічних алгоритмів, які використовуються в криптовалюті.

Алгоритми з симетричним ключем отримали провідне місце в еволюції криптографічних алгоритмів у криптовалюті завдяки своїй ефективності та простоті. Ці алгоритми дозволяють виконувати швидкі процеси шифрування та дешифрування, що робить їх придатними для захисту великих обсягів даних у децентралізованій мережі. Нижче наведено переваги алгоритмів симетричних ключів у криптовалюті:

1. Ефективність: алгоритми симетричного ключа можуть швидко шифрувати та дешифрувати дані, забезпечуючи ефективні транзакції та безпечний зв’язок у мережі криптовалюти.

2. Простота: ці алгоритми відносно легко реалізувати та зрозуміти, що зменшує складність криптографічних операцій у системах криптовалюти.

3. Масштабованість: симетричні ключові алгоритми можуть обробляти великі обсяги даних, завдяки чому вони добре підходять для захисту транзакцій і підтримки цілісності блокчейну.

4. Надійність: ці алгоритми забезпечують надійний захист від несанкціонованого доступу та втручання, забезпечуючи безпеку та цілісність транзакцій криптовалюти.

5. Сумісність. Алгоритми симетричного ключа широко підтримуються та сумісні з різними платформами та пристроями, що дозволяє бездоганно інтегрувати в системи криптовалюти.

Криптографія з відкритим ключем зробила революцію в безпеці та транзакційних можливостях криптовалют, запровадивши систему асиметричних ключів. Цей інноваційний підхід забезпечив більш безпечний спосіб шифрування та дешифрування даних, забезпечуючи конфіденційність, цілісність і автентичність цифрових транзакцій. Замість того, щоб покладатися на один ключ як для шифрування, так і для дешифрування, криптографія з відкритим ключем використовує пару математично пов’язаних ключів: відкритий та закритий ключ. Відкритий ключ вільно розповсюджується та використовується для шифрування, тоді як закритий ключ зберігається в таємниці та використовується для дешифрування. Ця система забезпечує безпечний зв’язок і перевірку між сторонами без необхідності довіреної третьої сторони. Завдяки криптографії з відкритим ключем можна надійно зберігати криптовалюти, впевнено проводити транзакції, а загальна безпека цифрової економіки значно підвищується.

Масштабованість, квантова стійкість і пошук правильного балансу між безпекою та зручністю використання є одними з поточних проблем у розробці криптографічних алгоритмів для криптовалют. У майбутньому галузь може досліджувати нові алгоритми, вдосконалювати функції конфіденційності та вирішувати проблеми з регулюванням для подальшого прогресу в цій галузі.

Еволюція криптографічних алгоритмів мала значний вплив на розвиток і впровадження криптовалют. Спочатку використовувалися базові методи шифрування, але з часом були представлені більш складні та безпечні алгоритми.

Ці криптографічні алгоритми постійно покращують безпеку та конфіденційність цифрових транзакцій. Оскільки криптовалюти продовжують розвиватися, майбутнє криптографічних алгоритмів містить величезний потенціал для подальшого прогресу в забезпеченні цілісності та конфіденційності цих цифрових валют.

Розробка структурної схеми

На рисунку 1 зображено структурну схему розробленого програмного забезпечення.

Програмне забезпечення структурно складається з наступних блоків:

– Головний модуль програми.
– База даних алгоритмів шифрування.
– База даних геш-функцій.
– База даних алгоритмів генерації псевдовипадкових чисел (ГПВЧ).
– База даних алгоритмів підрахунку контрольних сум (CRC).
– Шифрування файлів та папок.
– Шифрування даних на змінних носіях інформації.
– Шифрування даних, які передаються по мережі.
– Шифрування листів e-mail.
– Створення зашифрованих архівів, що саморозпаковуються.
– Генератор псевдовипадкових чисел.
– Перевірка цілісності та автентичності файлів.
– Створення віртуального зашифрованого диску.
– Створення паролю.

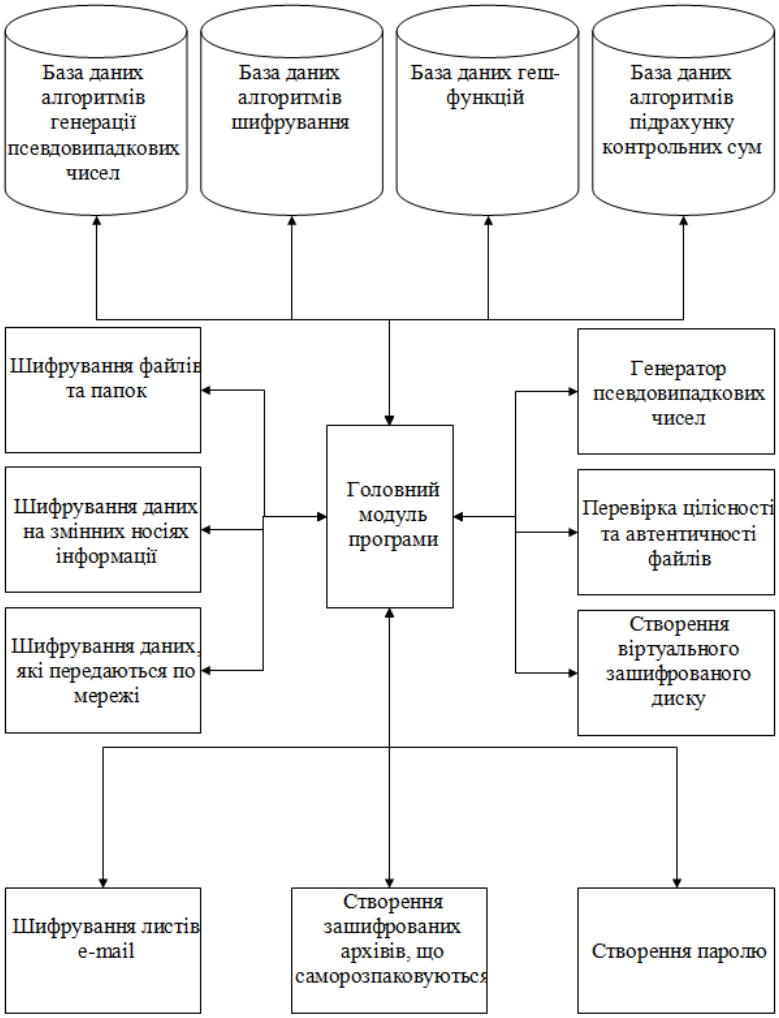

Рисунок 1 – Структурна схема розробленого програмного забезпечення

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів з використанням мультиваріантного центру реалізації криптоалгоритмів.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем з використанням мультиваріантного центру реалізації криптоалгоритмів.

– Досліджена система з використанням мультиваріантного центру реалізації криптоалгоритмів.

– На основі отриманих результатів досліджень створена програмна реалізація системи з використанням мультиваріантного центру реалізації криптоалгоритмів.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання з використанням мультиваріантного центру реалізації криптоалгоритмів.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143.

2. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207..
3. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58..
4. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256..
5. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114..
6. Smirnov O.A., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346..
7. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131..
8. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14..
9. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84..
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587..
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136..
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379..
13. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43..
14. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645..
15. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.,.
16. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407..
17. Смирнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А.Смирнов, В.В.Босько, Е.В.Мелешко // Системи обробки інформації. – Х.: ХУ ПС, 2008. – Вип.7(74). – С.120-123.
18. Смирнов А.А. Усовершенствование метода управления очередями в многопротокольных узлах телекоммуникационной сети / А.А.Смирнов, Е.В.Мелешко // Збірник тез та доповідей другої всеукраїнської науково-практичної конференції «Системний аналіз. Інформатика. Управління». Запоріжжя. Тези доповідей. Запоріжжя: КПУ, 2011.
19. Смирнов С.А. Метод безопасной маршрутизации метаданных в облачные антивирусные системы / А.К. Дидык, С.А. Смирнов // Информационные технологии в управлении, образовании, науке и промышленности: монография / Под редакцией профессора В.С. Пономаренко. – Х.: Видавець Рожко С.Г., 2016. – 566 с.
20. Смирнов С. А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А. А. Смирнов, А. В. Коваленко, С. А. Смирнов // Системи обробки інформації: зб. наук. праць. – Х.: ХУПС, 2014. – Вип. 9(125). – 105-110.