ВСТУП

Умови сучасного цифрового суспільства характеризуються стрімким зростанням обсягів інформації та широким впровадженням інформаційно-комунікаційних технологій у всі сфери діяльності людини. За таких обставин питання надійного зберігання та захисту даних набувають особливої ваги, оскільки витоки, підміна або несанкціонований доступ до інформації можуть призводити до значних матеріальних і репутаційних втрат. Саме тому дослідження можливостей застосування блокчейн-технологій для підвищення рівня безпеки даних є надзвичайно актуальним і своєчасним.

Технологія блокчейн, що першочергово була створена як основа функціонування криптовалютних систем, зокрема Bitcoin, сьогодні розглядається як універсальний інструмент забезпечення цілісності, достовірності та захищеності інформації. Концепція блокчейну передбачає зберігання даних у вигляді послідовно пов’язаних блоків, достовірність яких підтверджується всіма учасниками розподіленої мережі. Такий підхід практично унеможливлює несанкціоновану зміну інформації та забезпечує високий рівень довіри до збережених даних. Важливою перевагою блокчейн-технології є її децентралізована архітектура, за якої відсутній єдиний центр зберігання інформації, що значно знижує ризики успішних атак на систему. Окрім цього, незмінність записів та публічність перевірки транзакцій сприяють підвищенню прозорості обміну даними та контролю їх достовірності.

Сфери застосування блокчейну для захисту інформації є надзвичайно різноманітними та охоплюють фінансовий сектор, медичні інформаційні системи, логістичні процеси, електронне голосування та інші критично важливі галузі. Водночас упровадження цієї технології супроводжується низкою викликів, серед яких проблеми масштабування, енергоспоживання та недостатня сформованість нормативно-правової бази. Незважаючи на це, блокчейн залишається перспективним напрямом розвитку систем інформаційної безпеки, здатним суттєво підвищити рівень захищеності даних у цифровому середовищі.

Протягом останніх років системи відеоспостереження та безпеки зазнали значних змін завдяки активному використанню мереж IP та концепції Інтернету речей (IoT). Сучасні IP-системи відеонагляду забезпечують передавання даних через мережу Інтернет і підтримують розширений функціонал, зокрема автоматичне виявлення руху, хмарне зберігання відео, інтелектуальний аналіз зображень та оперативне сповіщення користувачів. Завдяки цьому такі системи широко застосовуються для захисту промислових об’єктів, державних установ та інших критичних інфраструктурних елементів [1, 2].

Разом із тим використання відкритої мережевої інфраструктури робить IP-системи відеоспостереження вразливими до кіберзагроз. Різноманіття архітектурних рішень і протоколів взаємодії ускладнює забезпечення належного рівня безпеки та збільшує кількість потенційних точок атаки. У результаті користувачі можуть стикатися з такими загрозами, як DDoS-атаки, атаки типу «людина посередині» (MitM), порушення конфіденційності, інфікування шкідливим програмним забезпеченням та несанкціонований витік відеоданих [3].

З огляду на значні обсяги інформації, що накопичуються державними та приватними структурами, системи відеоспостереження часто стають об’єктом підвищеної уваги з боку зловмисників. Оскільки існуючі підходи не гарантують абсолютного рівня захисту, виникає необхідність розроблення нових методів і алгоритмів забезпечення безпеки даних у системах відеонагляду. У цьому контексті інтеграція блокчейн-технологій може стати ефективним інструментом мінімізації ризиків та підвищення надійності зберігання й передавання відеоінформації.

Метою кваліфікаційної роботи є обґрунтування доцільності та можливостей застосування блокчейн-технологій для забезпечення безпеки даних у системах відеоспостереження.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- узагальнити базові поняття інформаційної безпеки та захисту даних;
- дослідити етапи становлення та розвитку технології блокчейн;

- проаналізувати існуючі підходи до використання блокчейну для захисту інформації;
- виконати аналіз методів забезпечення безпеки даних у системах відеоспостереження;
- розглянути технології побудови сучасних систем відеонагляду;
- проаналізувати криптографічні примітиви, що застосовуються для шифрування зображень;
- розробити узагальнений алгоритм шифрування відеозображень;
- визначити ключові характеристики та особливості блокчейн-технології.

Об’єктом дослідження є процеси шифрування та передавання зображень у системах відеоспостереження з використанням блокчейн-технологій. **Предметом дослідження** є методи й алгоритми забезпечення конфіденційності, цілісності та доступності відеоданих.

Практична значущість отриманих результатів полягає у можливості їх використання під час проєктування та впровадження захищених систем відеонагляду на основі блокчейну. Наведені у роботі приклади практичного застосування технології дозволяють визначити реальні сценарії її використання та сформувати ефективні стратегії підвищення рівня безпеки відеоданих.

.

1 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙНУ

1.1 Основні поняття захисту інформації та забезпечення безпеки даних

У сучасному інформаційному суспільстві питання захисту даних набуває статусу однієї з ключових проблем. Практично кожна дія людини так чи інакше фіксується в електронних інформаційних системах, унаслідок чого обсяги персональних і службових даних постійно зростають, а рівень їх уразливості підвищується. В умовах розвитку кіберпростору організації змушені безперервно виявляти слабкі місця власних інформаційних систем і впроваджувати нові механізми захисту. Ефективні заходи безпеки мають бути спрямовані на забезпечення ключових властивостей інформації — конфіденційності, цілісності та доступності, що дозволяє протидіяти сучасним кіберзагрозам.

Поняття «інформація» походить від латинського слова *informatio*, що означає пояснення, повідомлення або виклад відомостей. У філософському аспекті інформація розглядається як форма відображення навколишньої дійсності за допомогою даних. У наукових та нормативних джерелах існує велика кількість визначень цього терміна [2]. У межах даної роботи інформація розуміється як документовані або публічно доступні відомості про події, явища та процеси, що відбуваються в суспільстві, державі та навколишньому середовищі.

У наукових дослідженнях поняття інформації трактується ширше та охоплює відомості про людей, об’єкти, технології, ресурси, події й процеси, що мають місце в різних сферах життєдіяльності. Залежно від способу подання, інформація може існувати у вигляді сигналів, зображень, символів або інших форм представлення [26].

Перші спроби формалізації поняття інформації у науковому середовищі пов’язані з роботами англійського вченого Р. Фішера, який у 1921 році використав цей термін у межах математичної статистики. Він трактував інформацію як будь-які відомості, що передаються різними способами, зокрема

усно або письмово. Такий підхід вважається класичним і належить до так званого докібернетичного етапу розвитку теорії інформації [15].

Сучасна наукова спільнота виділяє три основні підходи до трактування поняття інформації: філософський, кібернетичний та правовий. Кібернетичний підхід сформувався в середині XX століття завдяки працям К. Шеннона та Н. Вінера. У межах теорії інформації та теорії передачі даних інформація розглядається як сукупність повідомлень, що передаються каналами зв'язку, а для її кількісної оцінки застосовуються ймовірнісні методи. Також була запропонована узагальнена модель системи передачі інформації, яка включає джерело повідомлення, передавач, канал зв'язку, приймач, одержувача та джерела завад [2].

Особливістю кібернетичного підходу є його універсальність, оскільки інформацією вважаються не лише повідомлення, а й команди, сигнали управління або заборони. При цьому форма подання інформації не обмежується природною мовою та може реалізовуватися у вигляді різних кодів, зокрема електронних, біологічних або імпульсних. Такий підхід дозволяє розглядати носіями та джерелами інформації не тільки людину, а й технічні системи, живі організми та процеси неживої природи.

Аналіз законодавчих і нормативних документів дає змогу дійти висновку, що інформація є універсальним і багатогранним поняттям, яке охоплює будь-які відомості незалежно від форми їх подання, способу зберігання чи передавання. Вона може існувати у текстовому, графічному, звуковому, електронному або матеріальному вигляді. Така різноманітність підтверджує провідну роль інформації як стратегічного ресурсу розвитку суспільства, економіки та технологій.

До основних властивостей інформації відносять [2]:

цілісність — здатність інформації зберігати коректність і повноту та бути захищеною від несанкціонованих змін або знищення;

доступність — можливість отримання інформації уповноваженими користувачами за умови захисту від блокування;

об'єктивність — відповідність інформації реальним подіям і процесам.

Інформаційні процеси охоплюють сукупність взаємопов'язаних етапів, що формують життєвий цикл інформації [3]:

отримання інформації шляхом збирання та накопичення даних;

обробка інформації, яка включає введення, перетворення, зберігання, передавання та знищення даних із використанням технічних і програмних засобів;

використання інформації для задоволення потреб громадян, організацій і держави;

зберігання інформації та забезпечення належного стану її носіїв;

знищення або оновлення інформації в джерелах її походження.

Інформація пронизує всі сфери життєдіяльності людини, що зумовлює необхідність її захисту від різноманітних загроз. Потреба у стабільному та надійному захисті інформації постійно зростає, оскільки ефективне управління інформаційними ресурсами є важливим чинником забезпечення національних інтересів. Формування безпечного інформаційного середовища розглядається як одна з умов сталого розвитку суспільства та держави.

Водночас стрімкий розвиток інформаційних технологій спричинив зростання кількості загроз несанкціонованого втручання в інформаційні системи, а можливі наслідки таких інцидентів стають дедалі серйознішими. Це стимулює пошук нових підходів і технічних рішень у сфері інформаційної безпеки. Однією з визначальних ознак науково-технічного прогресу є активне впровадження цифрових технологій, що, водночас, підвищує вимоги до їх захищеності.

Згідно з законодавством України, інформаційна безпека спрямована на захист інформаційного простору людини, суспільства та держави з метою забезпечення їх сталого розвитку. Захист інформації передбачає запобігання її несанкціонованому розголошенню, спотворенню або знищенню, а також мінімізацію ризиків випадкового впливу. Створення та функціонування системи захисту інформації є одним із ключових завдань інформаційної безпеки підприємства [2].

Сучасний рівень автоматизації процесів у різних галузях зумовлює універсальний характер проблем інформаційної безпеки. Особливе місце серед методів захисту займає криптографія, яка забезпечує захист даних незалежно від фізичних характеристик середовища або апаратного забезпечення.

Криптографічні методи базуються на математичних властивостях інформації, що робить їх ефективним інструментом протидії несанкціонованому доступу [6].

Отже, захист інформації являє собою комплекс організаційних, технічних і програмних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних за умов існування потенційних загроз. Реалізація таких заходів дозволяє запобігти завданню шкоди власникам і користувачам інформації.

Поняття захисту інформації тісно пов’язане з інформаційною безпекою, оскільки порушення механізмів захисту може призвести до втрати достовірності, конфіденційності та цілісності даних. Забезпечення інформаційної безпеки передбачає також захист конституційних прав громадян на доступ до інформації та її використання [3].

Зростання обсягів даних, зокрема в умовах застосування технологій великих даних, потребує впровадження комплексних заходів захисту та контролю доступу. До таких заходів належать організаційно-правові, програмно-апаратні та технічні рішення, що формують загальний рівень захищеності інформації [3].

Захист даних у цифровому середовищі передбачає сукупність практик і технологій, спрямованих на запобігання несанкціонованому доступу, порушенню цілісності або втраті інформації. Він охоплює фізичний захист обладнання, механізми контролю доступу, програмні засоби безпеки та організаційні політики.

Ефективні системи безпеки дозволяють організаціям мінімізувати ризики, пов’язані з кіберзлочинністю, внутрішніми загрозами та людським фактором. Сучасні інструменти захисту забезпечують шифрування, маскування та контроль використання конфіденційної інформації, а також автоматизацію процесів звітності та відповідність нормативним вимогам [7].

У світовій практиці інвестиції в захист даних розглядаються як необхідна умова збереження ділової репутації, інтелектуальних ресурсів і довіри клієнтів. Недостатній рівень безпеки може призвести до серйозних фінансових втрат і зниження конкурентоспроможності організацій.

Таким чином, захист інформації та безпека даних є критично важливими складовими діяльності будь-якої організації. Ефективне забезпечення безпеки потребує комплексного підходу, що поєднує технічні, організаційні та правові

заходи. Лише системне планування, впровадження сучасних технологій і дотримання відповідних політик дозволяють досягти належного рівня захищеності інформаційних ресурсів.

1.3 Застосування технології блокчейн для безпеки даних

Основні переваги технології блокчейн полягають у сукупності характеристик, які забезпечують її ефективність і стійкість до загроз, зокрема децентралізованій архітектурі, прозорості процесів, високому рівні надійності, а також оптимізації швидкості та вартості операцій. Відсутність єдиного центру керування забезпечує розподілене зберігання інформації на багатьох вузлах мережі, що істотно ускладнює здійснення успішних атак на систему. Прозорість реалізується через можливість перевірки транзакцій усіма учасниками мережі в режимі реального часу, а надійність досягається завдяки використанню криптографічних хеш-функцій, які пов’язують кожен блок із попереднім, роблячи будь-які зміни легко виявними.

Використання блокчейн-технологій також дозволяє скоротити витрати на обробку транзакцій за рахунок усунення посередників. У традиційних фінансових системах значна частина витрат пов’язана з оплатою послуг банківських або клірингових установ, тоді як у блокчейн-мережах обмін даними та активами здійснюється безпосередньо між учасниками. Захищеність транзакцій забезпечується застосуванням криптографічних методів, зокрема цифрових підписів, які дозволяють підтвердити автентичність і цілісність переданих даних. Надійність цієї технології базується на строгих математичних алгоритмах і протоколах узгодження.

Ключовим елементом функціонування блокчейн-мереж є механізм консенсусу, відповідно до якого всі учасники повинні дійти згоди щодо коректності транзакцій. У разі спроби внесення недостовірних даних більшість вузлів мережі автоматично відхиляє таку транзакцію, не дозволяючи їй бути доданою до реєстру. Це підвищує рівень безпеки системи та водночас забезпечує

відкритість і псевдонімність обміну даними. Завдяки децентралізованій природі кожен користувач може долучитися до мережі без необхідності отримання дозволу від централізованого органу. На сьогодні блокчейн активно застосовується у фінансовій сфері, логістиці, медицині, управлінні нерухомістю та інших галузях, що підтверджує його значний потенціал для підвищення прозорості та ефективності процесів [4].

Механізми безпеки та довіри в блокчейні реалізуються через низку технічних рішень. Зокрема, блоки додаються до ланцюга послідовно та у хронологічному порядку, що унеможливлює їх редагування після підтвердження. Кожен блок містить власний хеш-код і хеш попереднього блоку, тому будь-яка зміна даних автоматично призводить до порушення цілісності всього ланцюга. Наприклад, спроба змінити окрему транзакцію вимагала б перерахунку всіх наступних блоків, що потребує надзвичайно великих обчислювальних ресурсів. Для перевірки вузлів, які бажають приєднатися до мережі, застосовуються спеціальні механізми, одним із яких у мережі Bitcoin є алгоритм «доказу роботи» (Proof of Work) [10].

У межах алгоритму доказу роботи вузли повинні розв’язати складну обчислювальну задачу, підтверджуючи виконання певного обсягу роботи. Лише після цього вони отримують право додати новий блок до ланцюга. Процес створення блоків, відомий як майнінг, є ресурсомістким і значно ускладнює реалізацію атак. Хоча цей механізм не забезпечує абсолютного захисту, потенційні витрати на здійснення атаки, як правило, значно перевищують можливу вигоду [10]. Основне призначення блокчейну полягає у фіксації та поширенні цифрових даних без можливості їх подальшого редагування.

Завдяки властивості незмінності блокчейн забезпечує високий рівень цілісності інформації, що дозволяє ефективно протидіяти загрозам, таким як підміна даних, імітація джерела, повторна передача повідомлень або заперечення факту передачі. Відповідно до вимог державних стандартів технічного захисту інформації ТЗІ 1.1-003-99 [3], системи на основі блокчейну можуть відповідати критеріям «ЦД-4. Абсолютна довірча цілісність» та «ЦЗ-3. Повна цілісність при обміні».

Блокчейн-мережі є розподіленими, оскільки всі учасники зберігають копії реєстру та мають можливість відстежувати транзакції в реальному часі. Некоректні операції можуть бути відхилені ще до їх фіксації у реєстрі, що значно спрощує аудит і знижує ризик шахрайства. Крім того, розвиток блокчейн-платформ сприяє створенню нових прикладних рішень для управління ланцюгами постачання та бізнес-процесами, відкриваючи додаткові можливості для формування нових продуктів і сервісів.

Зберігання даних у блокчейні здійснюється у зашифрованих блоках, а рівень довіри між учасниками визначається алгоритмами консенсусу. Для додавання нового блоку необхідне підтвердження більшості вузлів мережі, зазвичай не менше 51 %, після чого інформація стає незмінною. Відсутність центрального вузла або посередника є принциповою відмінністю блокчейн-архітектури від традиційних централізованих систем. Завдяки зв’язку блоків через хеші будь-які спроби несанкціонованого втручання легко виявляються.

Аналіз практичного досвіду свідчить, що блокчейн є ефективним засобом захисту від фальсифікації та крадіжки даних, оскільки підробка блоків потребує значних ресурсів. Водночас не виключається можливість зловживань окремими реалізаціями цієї технології. Очікується, що блокчейн залишатиметься стійким навіть у постквантовий період, однак реалізація таких атак вимагатиме витрат, які перевищують вартість атак на традиційні інформаційні системи.

На практиці найбільш уразливими елементами залишаються централізовані криптовалютні біржі, які через свою архітектуру стають мішенями для кібератак. Саме ця обставина стимулює розвиток децентралізованих рішень і зростання інтересу до блокчейн-технологій з боку організацій різного профілю.

Отже, використання блокчейн-технології для забезпечення безпеки даних демонструє значний потенціал. Завдяки децентралізації, криптографічному захисту та незмінності записів блокчейн дозволяє створювати надійні системи зберігання й обміну інформацією, мінімізуючи ризики маніпуляцій і підробок. Водночас впровадження цієї технології потребує зваженого підходу та врахування

специфіки конкретної галузі застосування. У цілому блокчейн відкриває нові перспективи для побудови ефективних і захищених інформаційних систем.

1.4 Ключові характеристики технології блокчейн

Блокчейн є різновидом розподіленого реєстру, який безперервно поповнюється новими записами, об’єднаними у послідовні блоки, що мають вбудований захист від несанкціонованих змін і підробки. Кожен окремий блок містить часову позначку та криптографічний зв’язок із попереднім елементом ланцюга у вигляді хеш-значення. Зазначена технологія була запропонована особою або групою осіб, відомих під псевдонімом Сатоші Накамото, і з моменту формалізації принципів її функціонування набула широкого поширення та зазнала суттєвого розвитку у світовому масштабі [6].

Блокчейн розглядається як інноваційний та надійний підхід до зберігання даних, здатний докорінно змінити традиційні методи побудови баз даних. Його особливістю є можливість поширення інформації між учасниками мережі без необхідності створення та передачі численних копій. У результаті формується нова інфраструктура для розвитку глобальних інформаційних систем. Хоча початкове призначення блокчейну було пов’язане з функціонуванням криптовалют, зокрема Bitcoin та Ethereum, подальші дослідження дозволили адаптувати цю технологію для інших сфер, зокрема для організації захищених систем електронного документообігу.

Ключовою рисою блокчейну є децентралізований характер управління, за якого жоден окремий комп’ютер або установа не контролює всю мережу. Дані зберігаються на множині незалежних вузлів, які географічно розподілені та не мають єдиного центру керування. Такий підхід суттєво знижує ймовірність фальсифікації інформації, оскільки зловмиснику необхідно одночасно змінити дані на всіх учасниках мережі. Будь-які зміни у блокчейні стають доступними для перевірки всіма користувачами та потребують підтвердження більшістю, що значно ускладнює реалізацію атак [9].

Основним призначенням технології блокчейн є забезпечення безпечної передачі та підтвердження прав власності на цифрові активи у середовищі без довіри та без залучення посередників. Розподілене зберігання дозволяє одночасно зберігати критично важливу інформацію на великій кількості серверів, що підвищує відкритість і стійкість системи. До таких даних можуть належати фінансові транзакції, результати електронного голосування, офіційні документи або медичні записи. Завдяки механізмам колективного підтвердження та властивості незмінності записів, ці дані стають практично недосяжними для підробки чи несанкціонованого видалення.

Отже, концепція блокчейну ґрунтується на можливості обміну цінною інформацією між сторонами, які не мають взаємної довіри, із забезпеченням високого рівня захищеності та цілісності даних. Незмінність інформації досягається шляхом застосування криптографічних методів, а не через централізований контроль. Основними криптографічними інструментами, що використовуються в блокчейн-системах, є хеш-функції та механізми електронного підпису, які забезпечують перевірку автентичності та цілісності транзакцій.

– Функціонування блокчейн-мережі відбувається за наступною послідовністю дій (рисунок 1.1):

– нові транзакції передаються до всіх вузлів мережі;

– кожен вузол формує блок із набору транзакцій та здійснює пошук відповідного хеш-значення;

– після знаходження коректного хешу блок поширюється серед інших учасників;

–

– вузли приймають блок лише за умови підтвердження коректності всіх транзакцій у ньому;

– після погодження даних учасники переходять до формування наступного блоку, використовуючи хеш попереднього як початкове значення.

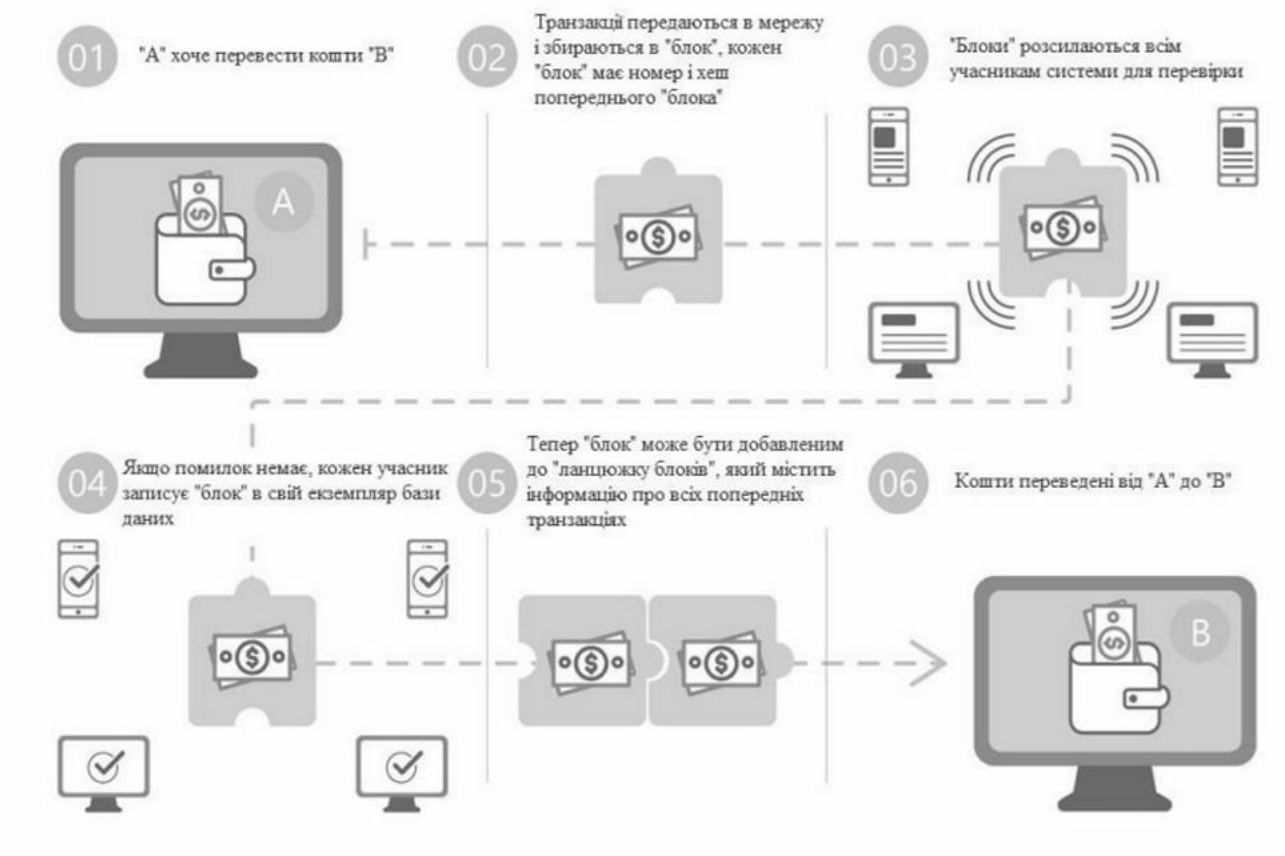


Рис. 1.1 Схема роботи системи блокчейн

Одним із найбільш перспективних напрямів використання блокчейн-технологій є побудова систем захищеного електронного документообігу. Їх надійність істотно зростає завдяки застосуванню децентралізованого реєстру документів, у якому внесені записи неможливо приховано змінити або скоригувати. За таких умов користувачі отримують можливість працювати з цифровими документами, маючи обґрунтовану впевненість у їхній цілісності, справжності та походженні.

Функціонування блокчейн-систем ґрунтується на сукупності сучасних методів обробки та захисту інформації [4], серед яких ключову роль відіграють:

асиметричні криптографічні алгоритми;

криптографічні хеш-функції (зокрема сімейства MD та SHA);

хеш-таблиці, що використовуються для збереження результатів хешування у блоках транзакцій;

смарт-контракти, які реалізують автоматизований механізм передавання цифрових активів між сторонами;

токени та застосування підходу Proof of Concept (PoC), що використовується як спосіб підтвердження подій або фактів виконання угод у системі.

Під час класифікації блокчейн-мереж доцільно використовувати підхід, запропонований засновником платформи Ethereum В. Бутеріним, відповідно до якого розрізняють три основні типи блокчейнів: публічні, консорціумні та приватні, що відрізняються рівнем доступу та ступенем децентралізації.

Публічний блокчейн з відкритим доступом являє собою мережу, в якій будь-який користувач може переглядати дані та ініціювати транзакції. Захист операцій у таких системах забезпечується криптографічними методами підтвердження, зокрема цифровими підписами. На сьогодні цей тип блокчейну є найбільш поширеним і застосовується в криптовалютах Bitcoin, Ethereum, Ripple та інших. Його використання є доцільним для систем документообігу, де критично важливими є незалежність від третіх сторін, прозорість операцій та висока довіра до результатів обробки даних. Важливою особливістю є також обмеження впливу розробників на систему, оскільки вони не мають можливості одноосібно змінювати програмний код або збережені дані. Основні характеристики публічного блокчейну наведено нижче [4]:

повна відкритість блоків для всіх учасників;

відсутність потреби у взаємній довірі між користувачами;

максимальна децентралізація та незалежність від посередників;

забезпечення безпеки за рахунок криптографічних алгоритмів і значних обчислювальних ресурсів мережі.

Приватний блокчейн з відкритим доступом характеризується тим, що повноваження щодо підтвердження транзакцій, проведення аудиту безпеки та внесення змін до програмного забезпечення мають лише визначені привілейовані учасники. Інші користувачі, як правило, отримують доступ лише до перегляду інформації. Така архітектура вже не є повністю децентралізованою та залежить

від обмеженого кола керуючих суб’єктів, однак може бути ефективною для використання в державних і корпоративних структурах. Основні властивості цього типу блокчейну включають [9]:

наявність перевірених та авторизованих валідаторів;

скорочений час підтвердження транзакцій;

неможливість реалізації атаки типу 51%;

можливість коригування або видалення записів у реєстрі;

зменшення вартості транзакцій завдяки відсутності потреби у значних обчислювальних потужностях.

Приватний блокчейн із закритим доступом зберігає перелічені властивості, однак передбачає ще жорсткіші обмеження: звичайні користувачі не можуть приєднатися до мережі без схвалення валідаторів і, у деяких випадках, не мають доступу навіть до перегляду даних. Така система фактично втрачає ознаки відкритості та функціонує під повним контролем однієї організації, яка визначає порядок створення блоків і правила здійснення транзакцій. Користувачі можуть виконувати лише функції контролю, тоді як управління базами даних і програмними компонентами залишається за довіреними вузлами. Основні характеристики цього типу блокчейну є такими:

обмежений доступ до даних для непривілейованих учасників;

повна закритість мережі для неавторизованих користувачів;

відсутність загрози атаки 51%;

повна залежність від групи привілейованих валідаторів;

висока надійність і стабільність за умови довіри до керуючої сторони.

Додатковою перевагою приватних блокчейн-систем є підвищений рівень адміністративного контролю. На відміну від публічних мереж, вони дозволяють оперативно вносити зміни до функціональності та адаптувати систему до потреб організації. Саме тому такі рішення є привабливими для установ, що працюють із фінансовими, бухгалтерськими та управлінськими документами, оскільки забезпечують передбачуване та контрольоване середовище. Порівняльні характеристики розглянутих типів блокчейнів доцільно узагальнити

Таким чином, у практиці застосування розрізняють два базові різновиди блокчейн-мереж: публічні та приватні. У публічному блокчейні будь-який користувач має можливість переглядати інформацію та ініціювати операції без обмежень. Натомість у приватному блокчейні процес формування блоків здійснюється централізовано, а повний обсяг повноважень щодо виконання транзакцій належить одній організації або визначеному колу довірених учасників. У такій архітектурі широке коло користувачів зазвичай має лише доступ до перегляду даних, тоді як керування базами даних, смарт-контрактами та іншими програмними компонентами здійснюється виключно авторизованими вузлами.

За своєю логікою приватний блокчейн наближається до класичних централізованих мереж, проте відрізняється можливістю ведення незмінного ланцюга блоків. Саме ця властивість робить його доцільним для використання у внутрішніх корпоративних мережах, системах захищеного документообігу підприємств або державних установ, де ключовим є збереження та контроль конфіденційної інформації. Враховуючи зазначене, у межах даного дослідження найбільш обґрунтованим є застосування приватного блокчейну.

Блок транзакцій можна розглядати як спеціалізовану електронну структуру керування записами, призначену для фіксації сукупності транзакцій. Перед тим як транзакція буде визнана коректною, виконується перевірка її формату та криптографічних підписів, після чого група перевірених транзакцій об’єднується та зберігається у відповідному блоці. Завдяки наявності в кожному блоці посилання на попередній блок, інформація легко піддається перевірці на цілісність. Усі блоки формують єдиний ланцюг, який акумулює відомості про всі операції, виконані в системі з моменту її створення. Початковий елемент цього ланцюга — первинний блок (Genesis block) — розглядається окремо, оскільки він не містить посилання на попередній блок [4].

Типова структура блоку включає заголовок, блок даних та перелік транзакцій. Заголовок блоку містить службові метадані, необхідні для його ідентифікації та зв’язку з іншими блоками, зокрема хеш-значення поточного

блоку, хеш попереднього блоку, хеші транзакцій, а також додаткову технічну інформацію.

Інформація, що зберігається в блоці, поділяється на дві категорії: прикладну, яка безпосередньо описує транзакції або виконання смарт-контрактів, та внутрішню, що відповідає за захист блоку й забезпечує його криптографічний зв’язок з іншими елементами ланцюга. Після формування блоки автоматично поширюються мережею, проходять перевірку та пов’язуються між собою за допомогою хеш-значень.

– Заголовок блоку, структура якого наведена на рисунку 1.2 [9], включає такі основні елементи:

– номер або висоту блоку в загальному ланцюзі;

– хеш-значення попереднього блоку;

– хеш-представлення даних поточного блоку (яке може формуватися, наприклад, у вигляді кореневого хешу дерева транзакцій або як результат хешування всіх об’єднаних даних блоку);

– часову мітку створення блоку;

– розмір блоку;

– параметр nonce, який генерується під час створення блоку та використовується для отримання криптографічного хешу заголовка. Саме цей параметр відіграє ключову роль у процесі формування першого ланцюга блоків.

– До складу блоку даних входять такі компоненти [9]:

– перелік транзакцій і подій журналу, включених до блоку;

– інші додаткові дані, необхідні для коректного функціонування системи.

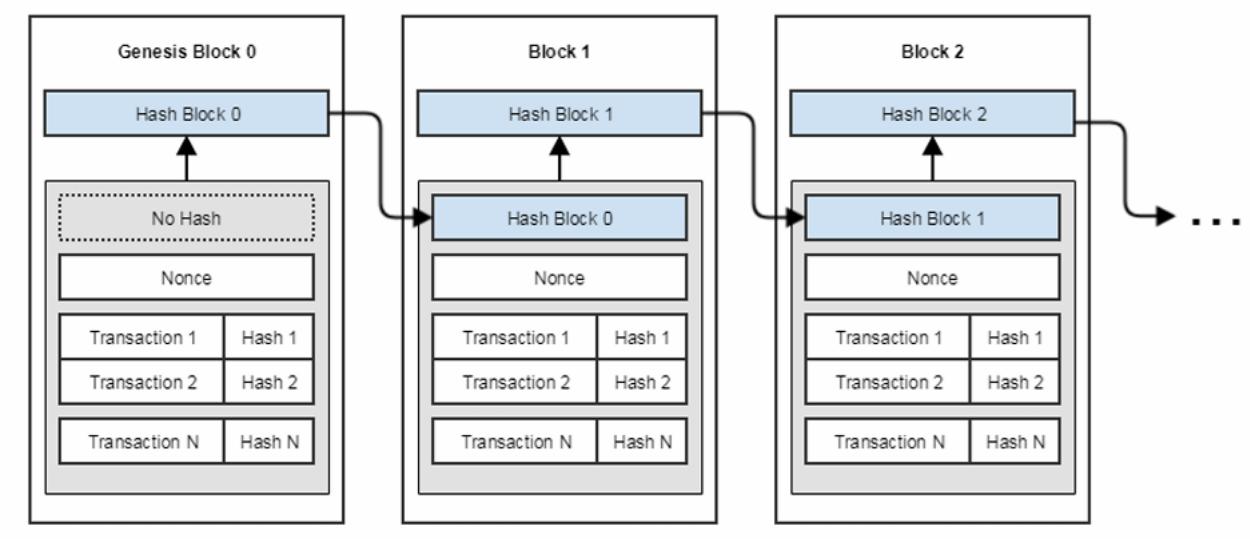


Рис. 1.2 Структура блокчейну

Блокчейн починається з первинного блоку, відомого як Genesis block, до якого поступово додаються нові блоки. Кожен блок містить записи про проведені транзакції. Вузли мережі взаємодіють для об’єднання цих блоків у єдиний ланцюг та формування незмінної книги записів, де зміна даних можлива лише шляхом повторного виконання підтвердження Proof of Work (PoW). Кожен вузол зберігає власну копію блокчейну, а синхронізація та оновлення ланцюга забезпечуються алгоритмічно та прозоро, що дозволяє відстежувати та перевіряти всі дії в мережі. Кожна транзакція отримує унікальний буквено-цифровий ідентифікатор, що забезпечує її однозначну ідентифікацію.

У блоках зберігаються останні транзакції, які ще не включені в попередні блоки. Для їх організації застосовується хеш-дерево (Merkle tree), що дозволяє ефективно перевіряти цілісність даних. Під час створення блоку його заголовок хешується, і якщо отримане хеш-значення відповідає певній складності (порогу), блок вважається прийнятим іншими учасниками мережі. У разі невідповідності параметр nonce змінюється, і хеш обчислюється повторно, що зазвичай потребує великої кількості ітерацій. Після знаходження правильного хешу блок розсилається всім підключеним вузлам, і, якщо помилок не виявлено, він додається до ланцюга, а наступний блок використовує його хеш як посилання [4].

Блоки можуть створюватися одночасно кількома майнерами, що інколи призводить до розгалуження ланцюга. У таких випадках обирається основний

ланцюг за критеріями довжини та складності хешу, а транзакції у відхиленій гілці втрачають статус підтверджених. База даних блокчейну постійно зростає і синхронізується на всіх вузлах, включаючи незашифровані дані транзакцій, підписані асиметричним шифруванням. Для запобігання подвійним витратам використовуються мітки часу та послідовні посилання на попередні блоки, що унеможливлює зміну вже доданих записів без перерахунку всіх наступних блоків. Це робить атаки на подвійне витрачання практично неможливими [4].

Отже, механізм функціонування блокчейну базується на унікальному цифровому підписі кожного блоку, який формується як хеш-суму з унікальним ідентифікатором. Це дозволяє зберігати блоки у суворо визначеному порядку — власне, у вигляді ланцюга блоків. Будь-яка спроба змінити порядок або дані блоку автоматично виявляється системою через невідповідність хеш-значень. Для захисту від несанкціонованих змін використовуються криптографічні механізми Proof of Work (PoW) та Proof of Stake (PoS).

Хешування у блокчейн

Хешування є фундаментальним елементом блокчейн-технології, який гарантує безпеку, цілісність та прозорість даних. Хеш-функція перетворює довільні вхідні дані у рядок фіксованої довжини, створюючи унікальний цифровий "відбиток" інформації. Цей процес є детермінованим, тобто один і той самий вхід завжди дає однаковий результат, і одностороннім, що унеможливлює відновлення вихідних даних з хеш-значення (рис. 1.3).

Хешування використовується як для підтвердження транзакцій через PoW, так і для формування дерева Меркла, що дозволяє ефективно перевіряти цілісність всіх транзакцій у блоці. Саме завдяки цим механізмам блокчейн забезпечує незмінність, верифікованість та надійність розподіленого реєстру даних [9].

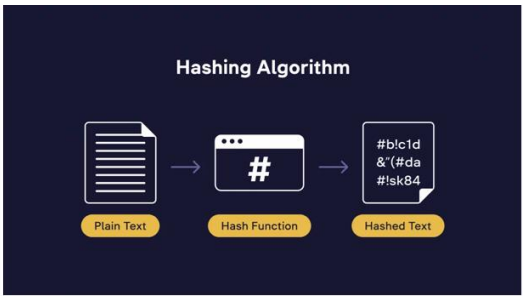


Рис. 1.3 Алгоритм хешування

Блокчейн починається з первинного блоку, відомого як Genesis block, до якого поступово додаються нові блоки. Кожен блок містить записи про проведені транзакції. Вузли мережі взаємодіють для об’єднання цих блоків у єдиний ланцюг та формування незмінної книги записів, де зміна даних можлива лише шляхом повторного виконання підтвердження Proof of Work (PoW). Кожен вузол зберігає власну копію блокчейну, а синхронізація та оновлення ланцюга забезпечуються алгоритмічно та прозоро, що дозволяє відстежувати та перевіряти всі дії в мережі. Кожна транзакція отримує унікальний буквено-цифровий ідентифікатор, що забезпечує її однозначну ідентифікацію.

У блоках зберігаються останні транзакції, які ще не включені в попередні блоки. Для їх організації застосовується хеш-дерево (Merkle tree), що дозволяє ефективно перевіряти цілісність даних. Під час створення блоку його заголовок хешується, і якщо отримане хеш-значення відповідає певній складності (порогу), блок вважається прийнятим іншими учасниками мережі. У разі невідповідності параметр nonce змінюється, і хеш обчислюється повторно, що зазвичай потребує великої кількості ітерацій. Після знаходження правильного хешу блок розсилається всім підключеним вузлам, і, якщо помилок не виявлено, він додається до ланцюга, а наступний блок використовує його хеш як посилання [4].

Блоки можуть створюватися одночасно кількома майнерами, що інколи призводить до розгалуження ланцюга. У таких випадках обирається основний ланцюг за критеріями довжини та складності хешу, а транзакції у відхиленій гілці втрачають статус підтверджених. База даних блокчейну постійно зростає і синхронізується на всіх вузлах, включаючи незашифровані дані транзакцій,

підписані асиметричним шифруванням. Для запобігання подвійним витратам використовуються мітки часу та послідовні посилання на попередні блоки, що унеможливлює зміну вже доданих записів без перерахунку всіх наступних блоків. Це робить атаки на подвійне витрачання практично неможливими [4].

Отже, механізм функціонування блокчейну базується на унікальному цифровому підписі кожного блоку, який формується як хеш-суму з унікальним ідентифікатором. Це дозволяє зберігати блоки у суворо визначеному порядку — власне, у вигляді ланцюга блоків. Будь-яка спроба змінити порядок або дані блоку автоматично виявляється системою через невідповідність хеш-значень. Для захисту від несанкціонованих змін використовуються криптографічні механізми Proof of Work (PoW) та Proof of Stake (PoS).

Хешування у блокчейн

Хешування є фундаментальним елементом блокчейн-технології, який гарантує безпеку, цілісність та прозорість даних. Хеш-функція перетворює довільні вхідні дані у рядок фіксованої довжини, створюючи унікальний цифровий "відбиток" інформації. Цей процес є детермінованим, тобто один і той самий вхід завжди дає однаковий результат, і одностороннім, що унеможливлює відновлення вихідних даних з хеш-значення (рис. 1.3).

Хешування використовується як для підтвердження транзакцій через PoW, так і для формування дерева Меркла, що дозволяє ефективно перевіряти цілісність всіх транзакцій у блоці. Саме завдяки цим механізмам блокчейн забезпечує незмінність, верифікованість та надійність розподіленого реєстру даних [9].

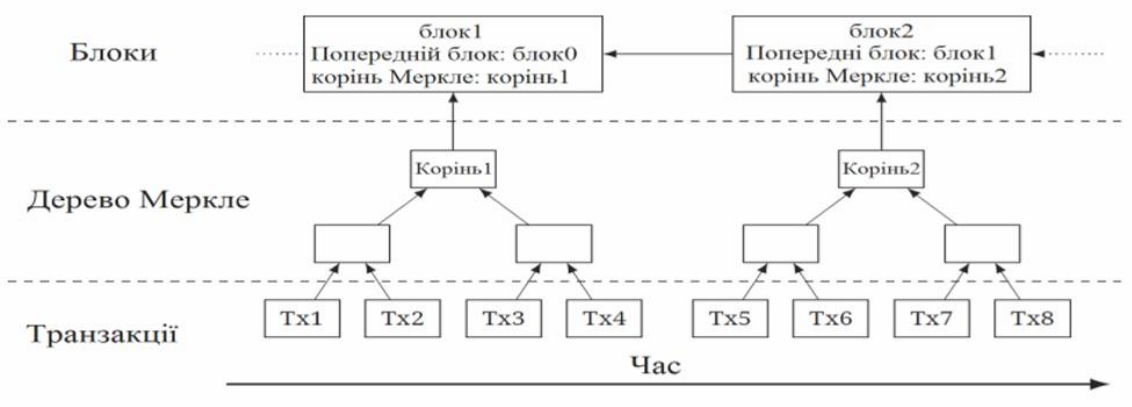


Рис. 1.4 Графічне представлення хешування блоків транзакцій

Отже, хешування в блокчейн-технології забезпечує недоторканність даних і безпеку транзакцій, одночасно підвищуючи надійність та стабільність мережі. Завдяки хеш-функціям кожен блок у ланцюзі має унікальне хеш-значення, яке включає посилання на хеш попереднього блоку. Це створює послідовний і захищений ланцюг транзакцій, де будь-яка зміна даних одного блоку одразу виявляється системою.

Для підвищення ефективності обробки даних усі транзакції в блоці об’єднуються в одне хеш-значення за допомогою дерева Меркле (Merkle tree). Кожен лист цього дерева відповідає окремій транзакції, а внутрішні вузли формуються шляхом хешування пар дочірніх вузлів. Таким чином, дерево Меркле забезпечує швидку перевірку цілісності всіх транзакцій у блоці, зменшуючи обчислювальні витрати та підвищуючи загальну безпеку блокчейну.

1.5 Класифікація блокчейн-мереж

У публічних блокчейнах нові вузли можуть підключатися без дозволу, а користувачі визначають рівень участі залежно від своїх ресурсів. Такі мережі тісно пов’язані з криптовалютами та фінансовими інструментами, які сприяють розвитку технології, але одночасно стають об’єктом атак на цифрові активи. Кожна транзакція підписується приватним ключем користувача, а перевірка

відбувається за допомогою публічного ключа. Це забезпечує криптографічний захист, незважаючи на анонімність учасників [18].

Приватні блокчейн-мережі працюють на основі контролю доступу: транзакції перевіряють лише довірені вузли, а нові користувачі підключаються за дозволом адміністратора. Це дозволяє організаціям забезпечувати вищий рівень конфіденційності, безпеку та контроль над інфраструктурою, використовуючи оптимізовані алгоритми консенсусу (BFT, Raft, Proof-of-Authority тощо) та обмежуючи доступ до записів у реєстрі [9].

Гібридні блокчейн-мережі поєднують елементи публічних і приватних ланцюгів. Учасники можуть обирати, які транзакції будуть публічними, а які приватними, зберігаючи при цьому незмінність даних. Основні переваги гібридних мереж:

робота у закритій екосистемі, що захищає від витоку інформації;

захист від атак типу 51%;

конфіденційність користувачів при збереженні взаємодії з зовнішнім світом;

низька вартість транзакцій завдяки перевірці лише кількома авторитетними вузлами [8].

Отже, публічні мережі забезпечують відкритість і прозорість, приватні — контроль і конфіденційність, а гібридні — поєднують переваги обох підходів, забезпечуючи ефективність і безпеку. Незалежно від типу блокчейну, безпека залишається ключовим аспектом, і методи її забезпечення повинні ретельно плануватися при проектуванні системи.

1.6 Смарт-контракти

Смарт-контракт — це інструмент, що поєднує протоколи блокчейн-мереж з користувацьким інтерфейсом, дозволяючи сторонам брати на себе зобов’язання без потреби у взаємній довірі. Виконання умов контракту контролюється автоматично: у разі порушення — контракт анулюється. Найбільш поширеною платформою для смарт-контрактів є Ethereum [16].

Кожен контракт може містити кілька умов, що дозволяє контролювати виконання завдань. Для створення контракту необхідно: визначити структуру транзакцій, встановити правила їх виконання, передбачити можливі винятки та розробити механізм вирішення спорів. Сучасні бізнес-організації часто надають шаблони та онлайн-інструменти, спрощуючи процес створення смарт-контрактів.

Переваги смарт-контрактів:

Швидкість та ефективність: негайне виконання умов без ручної обробки документів;

Довіра та прозорість: зашифровані записи транзакцій доступні учасникам мережі;

Безпека: зміна транзакцій ускладнена через структуру блокчейну;

Економія: відсутність посередників знижує комісії та час на обробку [16].

Недоліки та вразливості смарт-контрактів:

Цілочисельне переповнення (integer underflow/overflow) може призвести до багатомільйонних шахрайських транзакцій;

Неналежний контроль доступу дозволяє стороннім особам знімати кошти;

Незахищене самознищення контракту дає змогу зловмисникам «вбити» контракт і переказати кошти на будь-яку адресу [2].

Смарт-контракти, розроблені для гібридних блокчейн-мереж, можуть значно зменшити ризики та стати надійним інструментом безпечної передачі інформації.

Висновки до другого розділу

Проведено аналіз технології блокчейн, її архітектури та унікальних особливостей. Основні переваги: незмінність, децентралізація, прозорість та конфіденційність.

Здійснено порівняння протоколів консенсусу та типів блокчейн-мереж (публічні, приватні, гібридні), виявлено переваги та недоліки кожного типу. Гібридний блокчейн визнано найбільш доцільним для захисту інформації, оскільки він поєднує переваги обох підходів та мінімізує їхні недоліки.

Розглянуто смарт-контракти: публічні контракти мають певні ризики безпеки, тоді як контракти на базі гібридних мереж можуть ефективно їх усунути.

Використання блокчейн для цифрової ідентифікації

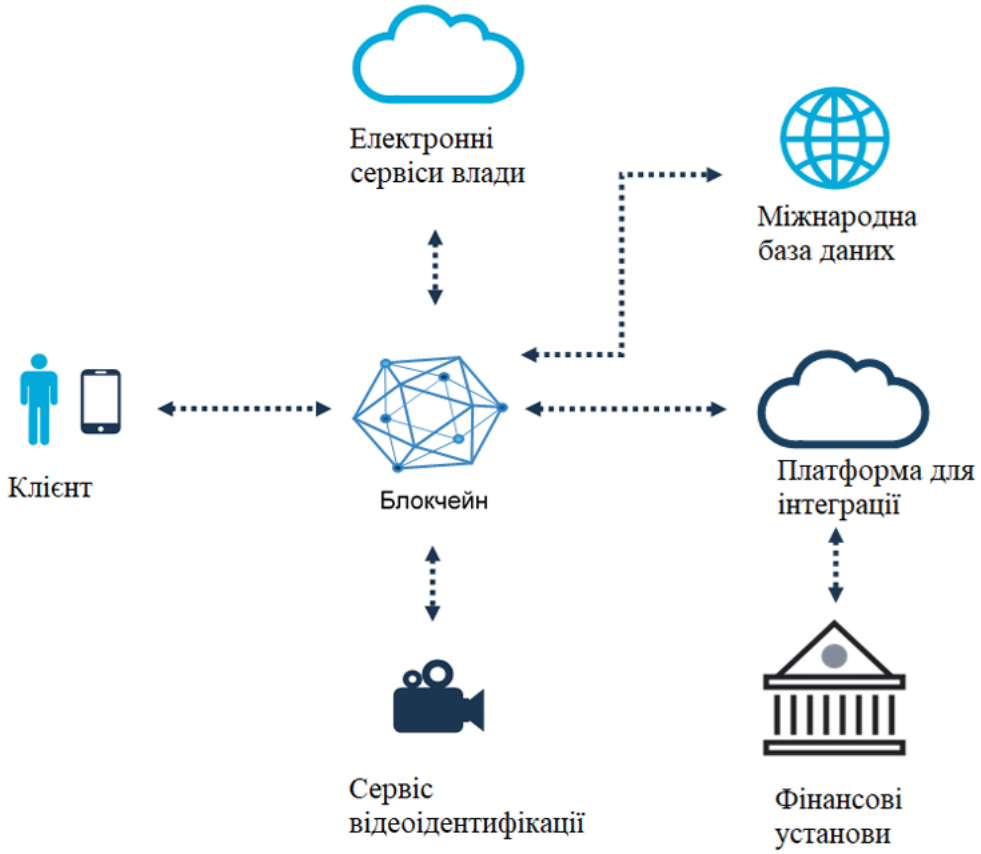
Блокчейн дозволяє створити безпечну та ефективну систему цифрової ідентифікації, завдяки децентралізованому зберіганню даних, що забезпечує перевірку автентичності без участі посередників. Це знижує вартість транзакцій і підвищує безпеку персональних даних.

Традиційні методи ідентифікації ризикують витоком даних, тоді як блокчейн зберігає інформацію в розподіленому реєстрі, який неможливо змінити без погодження всіх учасників.

Система цифрової ідентифікації на блокчейні дозволяє аутентифікувати дані без прямого обміну інформацією, застосовуючи криптографічні методи: хеш-функції та цифрові підписи. Кожен документ перетворюється у хеш, який виконує роль цифрового відбитка. Довірені органи можуть надавати цифрові підписи, надаючи документам юридичну силу.

Кожний запис у блокчейн підтверджується вузлами мережі, що гарантує достовірність і надійність інформації. Вузли можуть виконувати роль державних органів або організацій, затверджуючи дані та забезпечуючи їх вищу юридичну та інформаційну цінність [22].

Таким чином, блокчейн є перспективним інструментом для управління цифровою ідентифікацією та перевірки документів, підвищуючи безпеку зберігання та передачі особистої інформації.


Електронні
сервіси влади
Міжнародна
база даних
Клієнт
Блокчейн
Платформа для
інтеграції
Сервіс
відеоідентифікації
Фінансові
установи

2 АНАЛІЗ ЗАХИСТУ ДАНИХ В СИСТЕМАХ ВІДЕОНАГЛЯДУ

2.1 Аналіз підходів до захисту даних в системах відеонагляду

Основою безпечного проєктування систем відеоспостереження з функцією потокової передачі відеоданих є використання інтегрованої платформи, яка гарантує захист інформації, конфіденційність та реалізацію наскрізного шифрування. Дану проблематику можна аналізувати з різних позицій. Частина спеціалістів вважає, що застосування платформ із механізмами автентифікації, зокрема захистом доступу паролем, є обов'язковою умовою безпеки відеоконтенту, оскільки це дозволяє мінімізувати ризик несанкціонованого перегляду. Інші дослідники надають перевагу комплексному підходу, який передбачає використання спеціалізованих програмних рішень для потокового відео та вдосконалення інфраструктури шляхом впровадження алгоритмів шифрування AES і додаткових засобів захисту інформації. Для організації безпечної відеотрансляції та конфіденційного обміну відеоданими застосовується низка методів, описаних у роботах [1, 4].

Передавання даних із використанням протоколу HTTPS є ефективним засобом захисту від атак типу «людина посередині». Подібні загрози досить часто виникають у сфері розроблення програмних рішень для онлайн-трансляції відео, зокрема у випадках підключення користувачів через публічні мережі доступу, такі як кав'ярні, бібліотеки або навчальні заклади. Дані, що передаються через відкриті мережі, мають підвищений рівень уразливості та можуть бути перехоплені зловмисниками без належних механізмів захисту.

Процес підключення користувача до вебресурсу приховується завдяки застосуванню шифрування під час доставки HLS-контенту через HTTPS з використанням цифрових сертифікатів і криптографічних ключів, що практично унеможливлює несанкціоноване втручання з боку зловмисників. У ході перегляду відеоматеріалів уся взаємодія між серверною частиною та клієнтом відбувається в зашифрованому вигляді відповідно до протоколу HTTPS. Застосування HTTPS

для передавання відеоданих є ефективним механізмом забезпечення захисту контенту під час онлайн-перегляду, оскільки воно формує додатковий рівень інформаційної безпеки для всіх переданих ресурсів.

Захист відеоконтенту за допомогою пароля є одним із базових, проте ефективних методів обмеження доступу до потокових відеоматеріалів. Незважаючи на простоту реалізації, такі програмні рішення дозволяють запобігти несанкціонованому перегляду та забезпечують контроль над колом користувачів, які мають право доступу до відповідного контенту.

Як і передбачалося, відеоконтент, захищений паролем, зберігає повну функціональність системи. На початковому етапі користувач визначає перелік відеоматеріалів, доступ до яких необхідно обмежити. Надалі для їх перегляду потрібне введення відповідного пароля, без якого відтворення стає неможливим. Такий механізм доцільно застосовувати для попереднього перегляду матеріалів, внутрішнього корпоративного використання, збору відгуків клієнтів та інших сценаріїв, де потрібен контроль доступу. Парольний захист, попри простоту реалізації, залишається ефективним інструментом забезпечення інформаційної безпеки.

Водночас слід враховувати, що парольний захист не може розглядатися як остаточний рівень безпеки. Існує ризик розповсюдження паролів у відкритих джерелах або на публічних платформах, особливо у випадку відомих або масштабних брендів. Саме тому багато мовників практикують регулярну зміну облікових даних з метою збереження конфіденційності зон з обмеженим доступом. У поєднанні з додатковими механізмами захисту парольна автентифікація потокового відео здатна забезпечити належний рівень безпеки відеоконтенту.

Захищені центри обробки відеоданих та мережі доставки контенту (CDN) відіграють ключову роль у функціонуванні онлайн-платформ потокового відео. Під час використання відеохостингових сервісів файли відеоконтенту зберігаються та обробляються в дата-центрах, що є складовою інфраструктури CDN і забезпечують їх подальше ефективне розповсюдження користувачам.

Мережа доставки контенту (CDN) являє собою розподілену комп’ютерну систему, що застосовує спеціалізовані програмні засоби балансування навантаження для оперативного поширення мультимедійних даних у глобальному масштабі. Використання CDN під час розроблення додатків для потокового відео забезпечує стабільне відтворення відеоматеріалів із мінімальними затримками та підвищує якість сервісу для кінцевих користувачів.

Інтеграція мережі доставки контенту (CDN) з платформами розроблення додатків для онлайн-трансляції відео сприяє підвищенню рівня безпеки та захисту від різноманітних кіберзагроз.

Зокрема, CDN ефективно протидіють розподіленим атакам типу відмови в обслуговуванні (DDoS), метою яких є перевантаження цільових вебресурсів надмірним обсягом трафіку, значно знижуючи їхній вплив на працездатність системи. Окрім цього, використання CDN забезпечує стійкість до апаратних відмов завдяки механізмам резервування та надлишковості, що гарантує збереження відеоконтенту та стабільне, швидке завантаження вебсторінок для користувачів.

Використання шифрування AES значно ускладнює несанкціонований доступ до відеоконтенту, оскільки навіть у разі перехоплення потоків зловмисники не зможуть відтворити захищений вміст. Цей метод відзначається простотою впровадження та непомітністю для кінцевих користувачів. Більшість сучасних програм для потокового відео підтримують активацію AES-шифрування без додаткового навчання персоналу або користувачів.

Використання шифрування AES надає корпоративним платформам відеохостингу суттєву перевагу в забезпеченні захисту контенту. Створення комплексної системи безпеки відеоматеріалів можливе шляхом інтеграції цієї технології з іншими засобами захищеного потокового передавання.

Для забезпечення безпечної передачі даних усі відеопотоки, а також інформація про користувачів, включно з іменами та паролями, повинні бути зашифровані, особливо під час передачі через Інтернет. Існує широкий спектр методів шифрування, серед яких найпоширенішими є SSL/TLS для захисту даних

користувачів та IPsec або MACsec для передачі пакетів даних. Використання належних криптографічних механізмів запобігає перехопленню та модифікації інформації, що може статися під час атак типу «людина посередині» (MitM).

1. Підтвердження походження даних і застосування цифрових водяних знаків дозволяють забезпечити цілісність відеоконтенту та знизити ризик його фальсифікації. Додатково для захисту можна використовувати проактивні методи виявлення та запобігання перехопленню даних, наприклад, технологію Active Fiber Monitoring від компанії Allied Telesis.

Використання стійких паролів та багаторівневих механізмів доступу. Надійні паролі є ключовим компонентом системи інформаційної безпеки. Їхня довжина, складність та регулярна зміна визначають ефективність захисту. Особливу увагу слід приділяти цьому аспекту у випадках, коли пристрій доступний через перенаправлення портів, оскільки це підвищує ризик несанкціонованого доступу.

Для підвищення рівня безпеки облікових записів адміністраторів доцільно впроваджувати багатофакторну автентифікацію. Надійність пароля значно зростає, оскільки користувач має надати додаткову унікальну інформацію, наприклад код із SMS, а також отримує сповіщення про будь-які спроби входу. Якщо кілька користувачів мають доступ до відеопотоків, система повинна підтримувати багаторівневу авторизацію, захищену паролями. Деякі користувачі можуть отримувати обмежений доступ лише до перегляду зображень на певних пристроях, інші — на рівні оператора з базовими функціями керування. Повний доступ адміністратора передбачає можливість створення нових облікових записів, зміни орієнтації камер, додавання нових пристроїв до мережі та управління всіма налаштуваннями системи.

Використання систем виявлення та запобігання вторгненням є важливою складовою комплексної стратегії кіберзахисту. На терміналах користувачів та цифрових відеореєстраторах (DVR) слід встановлювати антивірусне програмне забезпечення для своєчасного виявлення та блокування шкідливих програм. У нерозподілених топологіях з відкритим фізичним каналом (POC), де мережеві пристрої, такі як камери та DVR, мають публічні IP-адреси, система мережевого

виявлення вторгнень (NIDS) здатна ідентифікувати шкідливі або аномальні шаблони трафіку, які можуть сигналізувати про спроби несанкціонованого доступу. Для реалізації NIDS та забезпечення захисту мережевого трафіку можна використовувати брандмауери VPN, зокрема брандмауери наступного покоління UTM від Allied Telesis, які дозволяють одночасно блокувати загрози та шифрувати критично важливі дані.

Оновлення програмного забезпечення. Системи IP-відеоспостереження потребують регулярного оновлення програмного забезпечення для підтримки належного рівня безпеки. Мікропрограми можуть виходити як у вигляді планових оновлень, так і у формі виправлень для усунення конкретних вразливостей. Для своєчасного отримання повідомлень про доступні оновлення важливо зареєструвати пристрій на вебсайті виробника та своєчасно завантажувати й встановлювати всі нові версії. Процес оновлення мікропрограми може тимчасово впливати на роботу мережі, оскільки перезавантаження пристрою перериває відеопотік, а оновлення великої кількості пристроїв може займати значний час і створювати додаткові ризики у масштабних системах. Тому важливо використовувати функції, які дозволяють мінімізувати перебої та автоматизувати процес оновлення для забезпечення безперервної роботи мережі.

Компанія Allied Telesis розробила технологію Continuous PoE, яка забезпечує безперервне живлення підключених пристроїв, таких як камери, навіть під час перезавантаження комутатора. Це дозволяє мінімізувати час простою та відновити відеопотік без очікування повного перезапуску камер. Autonomous Management Framework (AMF) від Allied Telesis — це рішення для автоматизації, яке спрощує налаштування та управління великими мережами. Однією з ключових його функцій є автоматичне оновлення мікропрограми, що дозволяє впроваджувати нові версії програмного забезпечення з мінімальними перебоями та без потреби ручного втручання адміністратора.

Навчання користувачів основам кібербезпеки. У будь-якій мережі або системі пристроїв люди часто є найбільш вразливим елементом у ланцюзі безпеки. Тому надзвичайно важливо розробити та задокументувати політики й рекомендації з

кібербезпеки та провести навчання для всіх користувачів, які мають доступ до системи відеоспостереження. Користувачів необхідно ознайомити з потенційними шляхами атак та пояснити, як реагувати на підозрілі запити зловмисників, що надходять під фальшивими приводами. Крім того, вони повинні усвідомлювати ризики доступу до системи через мобільні додатки або використання незашифрованих публічних Wi-Fi мереж.

Важливо постійно відстежувати актуальні стандарти кібербезпеки та впроваджувати найкращі практики на рівні організації, забезпечуючи їх дотримання на всіх рівнях управління. У співпраці з NUARI організації можуть отримати сучасні навчальні програми з кіберзахисту, адаптовані до специфічних потреб їхньої діяльності.
Завдяки низьким витратам на експлуатацію, простоті розгортання та широкому спектру розширених функцій багато підприємств та державних установ переходять від аналогових систем відеоспостереження до IP-рішень, що забезпечує підвищений рівень безпеки та спокій. Водночас, у міру зростання складності кіберзагроз і активності зловмисників, організації повинні усвідомлювати ризики, пов’язані з використанням IP-систем, особливо коли вони інтегровані в мережі з критично важливими для бізнесу даними та додатками. Ігнорування цих загроз може мати серйозні наслідки, тому закриття циклу безпеки мережі має залишатися пріоритетним завданням.

2.2 Шифрування в системах відеонагляду

Спеціалісти з кібербезпеки застосовують різноманітні методи шифрування для захисту інформації від різних загроз. Використання шифрування дозволяє забезпечити конфіденційність даних, їхню цілісність та автентифікацію користувачів. Зазвичай шифрування поділяють на дві основні категорії: симетричне та асиметричне, кожна з яких включає різні алгоритми та призначена для вирішення специфічних завдань у сфері безпеки [5, 6].

Зазвичай симетричне шифрування застосовується у випадках, коли продуктивність є критичною, оскільки процеси шифрування та дешифрування повинні виконуватися швидко. Основним недоліком симетричних алгоритмів є необхідність обміну спільним секретним ключем між сторонами, що взаємодіють [7]. Найпоширенішим алгоритмом у цій категорії є Advanced Encryption Standard (AES).

Асиметричне шифрування використовується там, де швидкість обробки не є головним фактором. Воно не потребує наявності спільного секретного ключа у сторін, що обмінюються повідомленнями. Кожен учасник має пару ключів: один секретний, а інший — відкритий. Ці ключі математично пов’язані, що дозволяє шифрувати дані одним ключем та розшифровувати іншим. Для забезпечення конфіденційності повідомлення шифрується відкритим ключем одержувача, що гарантує можливість розшифрування лише для нього. Для автентифікації відправник шифрує повідомлення власним закритим ключем, після чого одержувач може перевірити його за допомогою відкритого ключа відправника.

Найпоширенішим асиметричним алгоритмом є RSA. Його безпека ґрунтується на високій обчислювальній складності зламу, яка забезпечується проблемою факторизації великих простих чисел. Для створення ключів обираються два дуже великі прості числа ppp і qqq та обчислюється їх добуток n=p·qn = p \cdot qn=p·q. Вважається, що знайти ppp і qqq, знаючи nnn, практично неможливо. Алгоритм RSA широко описаний у науковій літературі та застосовується у багатьох системах, зокрема для цифрових сертифікатів і захисту даних у різних програмних продуктах.

Хоча ключі довжиною 1024 біти можуть вважатися достатньо надійними, сучасні рекомендації радять використовувати ключі довжиною щонайменше 2048 біт [8].

Комбінування симетричного та асиметричного шифрування дозволяє усунути проблему обміну ключами, характерну для симетричних методів. Асиметричне шифрування забезпечує безпечний обмін ключами, після чого симетричні алгоритми можна застосовувати для тривалого та швидкого шифрування даних.

Алгоритм AES (Advanced Encryption Standard) затверджений для захисту надсекретних документів уряду США та використовується у багатьох додатках, зокрема для захисту WPA2 Wi-Fi. У AES можна застосовувати ключі довжиною 128, 192 або 256 біт, при цьому 128-бітний ключ вважається достатнім для більшості завдань.

Щоб гарантувати цілісність повідомлень та захист від їх підробки під час передачі, використовуються хеш-значення (дайджест повідомлення), що додаються до даних як ознака оригінальності. Крім того, для підтвердження автентичності повідомлень застосовуються алгоритми хеш-коду автентифікації повідомлень (HMAC). Серед найбільш поширених методів — HMAC-MD5, який генерує 128-бітні хеші з використанням спільного ключа, та SHA-1, що формує 160-бітні хеші [9–11].

На сьогодні існує ряд методів скремблювання зображень, які можуть застосовуватися для обробки відеокадрів. Проте їх необхідно оптимізувати для роботи в умовах обмежених ресурсів, наприклад, на Edge-камерах. Крім того, такі методи повинні забезпечувати збалансоване поєднання конфіденційності, чіткості, оборотності, безпеки та надійності.

Серед методів захисту відеоконтенту шифрування є найбільш надійним підходом. Воно дозволяє захистити особисту інформацію та конфіденційні дані від несанкціонованого доступу, а також підвищує безпеку обміну даними між двома сторонами. Проте, через особливості обробки відео в реальному часі, традиційні симетричні криптографічні механізми, такі як AES, не здатні забезпечити повний захист від атак, спрямованих на цілісність відео та підміну зображень [12].

Механізми хаотичного шифрування розглядаються як перспективніші рішення, оскільки характеризуються підвищеною продуктивністю, високою чутливістю до мінімальних змін початкових умов, значним рівнем випадковості, великим простором ключів, аперіодичністю та загалом високим рівнем безпеки. Водночас нещодавно запропоновані методи хаотичного шифрування зображень, хоча й вважаються надійними, демонструють нижчу ефективність при використанні в Edge-мережах.

Крім того, такі схеми захисту конфіденційності не забезпечують повного захисту та анонімізації чутливих атрибутів під час передачі даних, окрім окремих областей зображення. Застосований підхід маскування орієнтований переважно на розмиття визначених фрагментів кадру і не придатний для обробки всього зображення. По-перше, він є ефективним для обчислень у межах локальних ділянок, однак його використання для повнокадрового маскування супроводжується значним зниженням швидкодії. Це зумовлено застосуванням обмеженої кількості параметрів керування з великими числовими значеннями, що негативно впливає на обчислювальну складність. По-друге, простір ключів такого методу є обмеженим і становить лише 128 біт [13].

2.3 Протокол передачі потокового відео

Протокол реального часу (RTP) широко застосовується для потокової передачі медіаданих і визначений у RFC 3550 робочою групою IETF [14]. Потоки RTP можуть піддаватися різноманітним атакам, включно з перехопленням і модифікацією даних. Хоча RTP можна захистити за допомогою IPSec, його обмеження роблять необхідним більш універсальне та масштабоване рішення, яке зменшило б потребу у динамічному розподілі сеансів, інфраструктурі відкритих ключів (PKI) та вирішило проблему проходження через NAT.

Внаслідок цього було розроблено протокол захищеного реального часу (SRTP) [6]. Для його роботи потрібен механізм обміну криптографічними ключами перед початком передачі відео, тому використовуються протоколи керування ключами, такі як SDescriptions і Multimedia Internet KEYing (MIKEY). SRTP, визначений у RFC 3711 і опублікований у 2004 році, забезпечує конфіденційність, цілісність і автентифікацію потоків відео.

SRTP призначено для захисту додатків реального часу, включаючи голосові та відеопередачі, і підтримує як дротові, так і бездротові мережі з обмеженою пропускною здатністю. Його ефективність у різнорідних мережевих середовищах

робить його зручним і надійним засобом забезпечення безпеки мультимедійних потоків.

SRTP забезпечує мінімальне збільшення розміру пакетів та високу пропускну здатність. Він застосовується для захисту потоків RTP і RTCP, надаючи пакетам механізми шифрування та автентифікації. Для автентифікації повідомлень у зашифрований потік додається функція на основі хешу ключа (SHA-1) [15].

Протокол SRTP відзначається низькими обчислювальними витратами та невисокою пропускною здатністю, необхідною для криптографічних операцій, що робить його придатним для використання у додатках із невеликим обсягом коду. SRTP є незалежним від фізичного, мережевого та транспортного рівнів, проте він залишається вразливим до втрати пакетів і зміни їх порядку. Ці властивості спрощують впровадження протоколу у вбудованих системах з обмеженими ресурсами процесора та пам’яті.

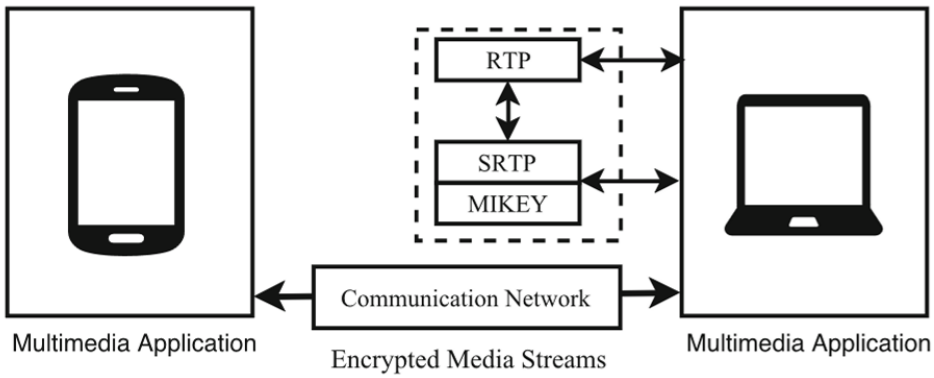


Рис. 2.1 Кодування в SRTP

Перед передачею пакетів RTP через мережу їх необхідно спершу перетворити на пакети SRTP, а на кінцевому вузлі ці пакети розшифровуються для відновлення оригінальних RTP-потоків, як показано на рисунку 2.1. Вхідні дані, наприклад відеопотік з камер, надходять до програми, де сигнал кодується за допомогою систем кодування, таких як Motion-JPEG (MJPEG) або H.264. Після кодування програма формує корисне навантаження для RTP.

Корисне навантаження RTP шифрується з використанням алгоритму Advanced Encryption Standard (AES) у режимі лічильника (CTR) із довжиною ключа 128 біт.

Оскільки AES у режимі лічильника не потребує додаткового розширення пакетів при шифруванні, він застосовується за замовчуванням у протоколі SRTP. Алгоритм AES розбиває дані на блоки, які обробляються непослідовно, що дозволяє виконувати паралельну обробку. Навіть якщо зашифровані пакети надходять не в порядку, кожен блок обробляється окремо, не впливаючи на процес дешифрування. Таким чином, програма SRTP перетворює RTP-пакети на SRTP перед передачею, а на кінцевому вузлі пакети SRTP розшифровуються для відновлення оригінальних RTP-потоків.

SRTP застосовує додатковий тег, відомий як MKI (Master Key Identifier). Цей тег призначений для ідентифікації головного ключа, за допомогою якого генеруються ключі сеансу, що використовуються для шифрування та/або автентифікації поточних пакетів. Зазвичай довжина MKI становить 4 байти.

2.4 Конфіденційність у системах відеонагляду

На сьогодні уряди, компанії та приватні особи широко використовують камери відеоспостереження у міських просторах, основною метою яких є забезпечення фізичної безпеки. Наприклад, підраховано, що середньостатистичний мешканець Лондона потрапляє у поле зору камер приблизно 300 разів на день під час пересування містом [5]. Внаслідок цього відеоспостереження фіксує значну кількість персональної інформації про людей без їхньої свідомої згоди. Тому, у зв’язку з розширенням кількості стаціонарних камер і використанням безпілотних літальних апаратів, оптимальним підходом до захисту приватності є впровадження вимог для виробників відеокамер щодо розробки пристроїв із вбудованими механізмами конфіденційності [16–18].

Ретельні дослідження та спостереження показують, що порушення конфіденційності у системах відеоспостереження зумовлені, насамперед, двома чинниками: перехопленням відеопотоків під час їх передачі та зловживанням відеоданими з боку операторів камер, а також проблемами у балансі між приватністю та зручністю користування. Більшість сучасних систем

відеоспостереження реалізується на базі хмарних технологій. Це створює ризик перехоплення відеопотоків під час транзиту через мережу через наявні вразливості, що може призвести до витоку приватної інформації.

Додатково, оператори або особи, відповідальні за управління камерами, можуть неправомірно збирати персональні дані. За даними Американського союзу громадянських свобод (ACLU), такі зловживання включають кримінальні та інституційні порушення, використання камер для особистої вигоди, а також дискримінаційне спрямування на окремі групи. Проте на сьогодні жоден із цих документів не пропонує універсального рішення; вони лише ідентифікують основні вразливі місця щодо конфіденційності у системах відеоспостереження [19].

Атрибути конфіденційності особи. Інформація, яку люди прагнуть захищати, відома як особисті або конфіденційні атрибути. До неї належить інформація, зафіксована на відеокадрах і зображеннях систем відеоспостереження, яка може розкривати значну кількість даних про особу, її поведінку та щоденні дії [8]. Наприклад, риси обличчя дозволяють ідентифікувати конкретних людей, а кадри, що відображають приватні дії або ситуації, у разі перехоплення можуть спричинити соціальне збентеження. Люди також відчувають дискомфорт через спостереження в приватних просторах, таких як медичні заклади або власні домівки, наприклад, через вікна.

Існуючі роботи намагаються виявляти та класифікувати конфіденційні об’єкти, однак вони часто не забезпечують механізмів захисту приватності. Наприклад, система рекомендацій щодо конфіденційності на основі машинного навчання для обміну зображеннями в соціальних мережах, запропонована в [8], не розкриває, як конфіденційність даних користувачів зберігається під час передачі зображень на хмарний сервер для обробки.

У цій роботі основна увага приділяється захисту конфіденційної інформації від перехоплення та поширення під час передачі зображень, отриманих камерами відеоспостереження, з метою запобігання їх візуальному розкриттю та забезпечення анонімності осіб. На сьогоднішній день відсутні надійно розроблені

методи або схеми, які б ефективно протидіяли зловживанню камерами спостереження, що залишається актуальною проблемою у сфері конфіденційності.

2.5 Технології побудови систем відеонагляду

Архітектура системи відеоспостереження відіграє ключову роль у створенні рішень, здатних забезпечувати конфіденційність даних. У цьому контексті активно досліджуються та розробляються системи з архітектурою на основі краю (Edge), туману (Fog) та хмари (Cloud). У хмарних середовищах практично відсутні механізми захисту приватності, оскільки периферійні камери переважно займаються зйомкою відео та його передачею через глобальну мережу Інтернет до віддалених центрів обробки та зберігання даних [20, 21]. Усі відеокадри, незалежно від їх значущості для працівників служби безпеки, передаються на хмарні сервери, що створює додаткове навантаження на мережу. Порівняно з іншими архітектурами, хмарна модель має найбільший вплив на пропускну здатність мережі та потребує великого обсягу сховища через масову передачу потоків з численних камер.

Архітектура туману зазвичай використовується у межах приватних мереж кампусів (CAN), що забезпечує доступ лише внутрішнім користувачам. Туманова архітектура пропонує вищий рівень конфіденційності порівняно з хмарною моделлю, оскільки трафік ізольований всередині корпоративної мережі, а відстань передачі скорочується. Це, у свою чергу, зменшує вплив на пропускну здатність, затримку відповіді та обсяг пам’яті, необхідний для обробки відеопотоків.

Архітектура відеоспостереження на основі периферії (Edge) відрізняється від хмарної та туманової тим, що відеопотоки не передаються на центральні або віддалені сервери. У цій моделі вся відеоаналітика виконується безпосередньо на пристроях на краю мережі, а інформація про події передається лише у вигляді сигналів попередження, наприклад електронною поштою або SMS через модеми GSM, уповноваженим користувачам. Такий підхід дозволяє повністю зберегти

конфіденційність, оскільки жодне відео не надсилається та не переглядається персоналом. Крім того, використання Edge-архітектури мінімально впливає на пропускну здатність мережі та потребує обмеженого обсягу пам’яті.

Разом із тим, периферійні підходи мають обмеження продуктивності. Наприклад, сучасні методи класифікації та виявлення легких об’єктів на основі глибоких нейронних мереж (DNN) здатні обробляти лише до 4 кадрів на секунду на пристроях з обчислювальними можливостями, порівнянними з останніми моделями Raspberry Pi. Крім того, певні відеозаписи можуть знадобитися як доказ у судових процесах, але така архітектура не передбачає їх збереження для подальшого використання [22].

2.6 Атаки на системи відеонагляду

Система відеоспостереження може стикатися з різними загрозами безпеці даних, тому під час організації потокового відео необхідно впроваджувати низку заходів захисту. Основні загрози включають [20]:

1. **Конфіденційність.** Відеопотоки повинні бути доступні лише авторизованим компонентам системи. Не допускається, щоб сторонні особи переглядали контрольоване відео або надсилали неавтентичні потоки.
2. **Цілісність.** Щоб гарантувати достовірність даних, до відеопотоку можна додавати метадані. Для контролю цілісності використовуються контрольні суми, CRC-коди, коди автентифікації повідомлень (MAC), водяні знаки або цифрові підписи, які підтверджують справжність та незмінність відео.

Доступність. Важливо забезпечити безперервну роботу системи відеоспостереження. Якщо контрольовану зону можуть зловмисно перехоплювати інші камери або шкідливі пристрої блокують передачу відеопотоку, необхідно впроваджувати надійний контроль периметра та механізми запобігання сторонньому втручанню, щоб гарантувати безперебійне функціонування системи.

3 БЛОКЧЕЙН В СИСТЕМАХ ВІДЕОНАГЛЯДУ З ЗАСОБАМИ ШИФРУВАННЯ ЗОБРАЖЕНЬ

3.1 Криптографічні хеш-функції

Криптографічні хеш-функції є ключовим інструментом у сучасній криптографії і використовуються для таких завдань, як створення цифрових відбитків повідомлень, автентифікація повідомлень та генерація криптографічних ключів. Протягом останніх років було запропоновано кілька високошвидкісних програмних хеш-функцій, більшість із яких ґрунтуються на принципах алгоритму MD4, розробленого Роном Рівестом. Одним із таких рішень став алгоритм RIPEMD, створений у рамках європейського проєкту RIPE (Race Integrity Primitives Evaluation). Існують три основні причини розглянути RIPEMD як можливу альтернативу [17].

128-бітні хеш-значення вже не забезпечують належного рівня безпеки. Атака на пошук колізій методом грубої сили для 128-бітного хешу потребує приблизно 2642^{64}264 або $2{,}10\times10^{19}$ оцінок функції. У 1994 році Пол ван Оорсхот та Майк Вінер продемонстрували, що таку атаку можна виконати менше ніж за місяць при інвестиціях близько 10 мільйонів доларів США, причому очікувалося, що витрати на подібні атаки з часом зменшуватимуться вдвічі приблизно кожні 18 місяців.

У першій половині 1995 року Ганс Доббертін виявив колізії для версії RIPEMD, що мала лише два з трьох раундів. Використовуючи аналогічні методи, восени того ж року він знайшов колізії для повного трьохраундового MD4. Атака на MD4 виконується за кілька секунд на сучасному комп’ютері та дозволяє певну свободу у виборі повідомлення, що робить MD4 непридатною для застосувань, які вимагають стійкості до колізій. Навесні 1996 року Доббертін також виявив колізії для функції стиснення MD5. Хоча ці колізії ще не були поширені на всю MD5, вони серйозно ставлять під сумнів її надійність як хеш-функції, стійкої до колізій. У зв’язку з цим RSA Data Security, для якої Рон Рівест розробив MD4 та MD5,

рекомендує припинити використання MD4 і уникати застосування MD5 у програмах, де необхідна стійкість хеш-функції до колізій.

Під час основної сесії конференції Crypto 2004 було повідомлено, що дослідники Сяоюнь Ван, Денгго Фенг, Сюецзя Лай та Хунбо Ю виявили колізії для MD4, MD5, RIPEMD та 128-бітної версії HAVAL.

Код автентифікації повідомлення на основі хешу (HMAC). HMAC дозволяє використовувати секретний ключ для хешування даних. Цей ключ залишається відомим лише сторонам, що спілкуються (наприклад, Бобу та Алісі), і забезпечує автентифікацію не лише самих даних, а й підтверджує, що відправник знає секретний ключ [15].

HMAC використовується для перевірки цілісності повідомлення та його автентичності. Його робота ґрунтується на хешуванні повідомлення із застосуванням секретного ключа, що відрізняє його від звичайних односторонніх хеш-функцій. Як і будь-який MAC (код автентифікації повідомлення), HMAC може працювати зі стандартними хеш-функціями, такими як MD5 або SHA-1, утворюючи варіанти на кшталт HMAC-MD5 або HMAC-SHA-1. Надійність HMAC визначається якістю обраної хеш-функції та довжиною отриманого хеш-коду. Крім того, на безпеку алгоритму впливає довжина секретного ключа.

Під час передачі повідомлення воно перетворюється на код HMAC за допомогою секретного ключа та обраної функції хешування. Цей код надсилається разом із повідомленням. Отримувач, використовуючи той самий секретний ключ, обчислює власний HMAC для отриманого повідомлення і порівнює його з надісланим кодом. Якщо значення збігаються, це підтверджує автентичність відправника та цілісність повідомлення (рис. 3.1).

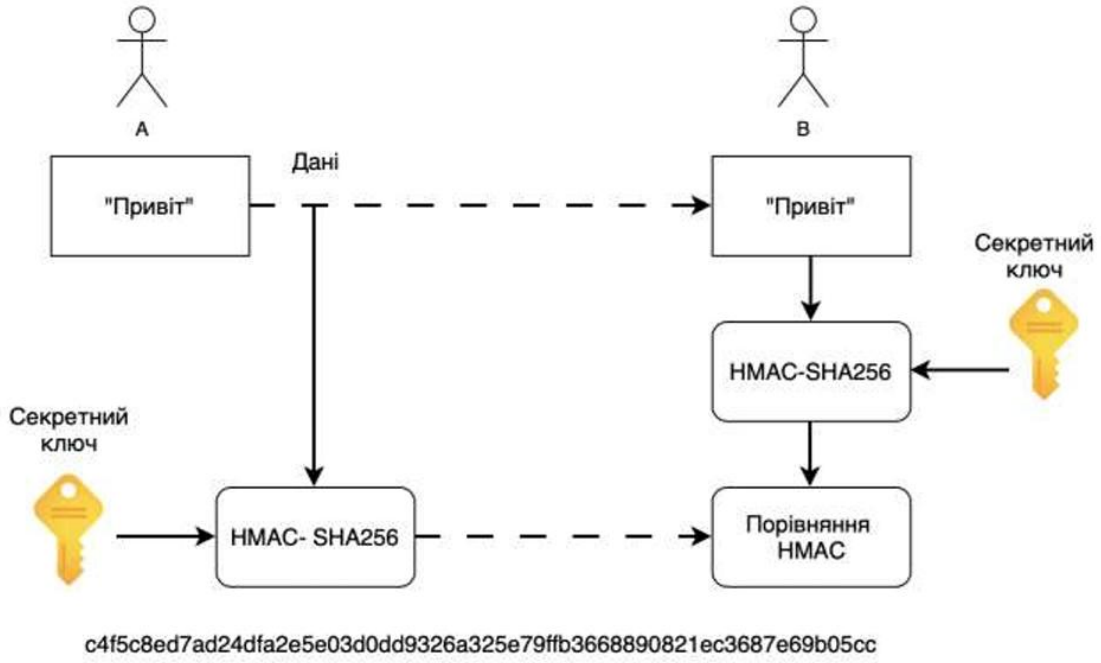


Рис. 3.1 Схема роботи коду автентифікації повідомлення на основі хешу

Алгоритм HMAC. На першому етапі обирається алгоритм хешування. Залежно від обраного алгоритму, дані обробляються блоками певного розміру BBB, а результат хешування має довжину LLL. Важливо відзначити, що HMAC використовує хеш-функції, які працюють як блокові шифри, тобто обробляють інформацію блоками фіксованого розміру. Наприклад, якщо вхідний потік містить 160 біт, блочний шифр може обробляти його блоками по 8 біт. На відміну від цього, потокові шифри виконують обробку даних побітово.

Формування внутрішнього та зовнішнього ключів. Далі з основного криптографічного ключа формуються два допоміжні ключі – внутрішній та зовнішній. Внутрішній ключ отримується шляхом доповнення основного ключа нулями до довжини BBB, після чого він обробляється операцією XOR з ipad, що складається з байтів 0x36, повторених BBB разів. Така процедура підготовки внутрішнього ключа дозволяє правильно інтегрувати його в обчислення HMAC для забезпечення надійності автентифікації та цілісності повідомлень.

Наприклад, якщо розмір блоку BBB становить 64 байти (512 біт), а довжина ключа LLL – 20 байт (160 біт), то для формування внутрішнього ключа до ключа

додаються нулі до довжини BBB, після чого виконується операція XOR з ipad, що складається з байтів 0x36, повторених BBB разів. Результатом є внутрішній ключ, готовий до використання в обчисленні HMAC.

Зовнішній ключ формується аналогічно: до оригінального ключа додаються нулі до розміру BBB, після чого виконується операція XOR із opad, який складається з байтів 0x5C, повторених BBB разів.

Отримувач, маючи власну копію секретного ключа та отримані дані, може виконати алгоритм HMAC і порівняти обчислений хеш із надісланим. Якщо обидва значення збігаються, це підтверджує два важливі моменти:

1. Вхідні дані та ключ співпадають, оскільки обчислений хеш ідентичний надісланому.
2. Ключ є секретним між відправником і одержувачем, що засвідчує автентичність відправника.

Алгоритм HMAC реалізується наступним чином [18]:

HMAC=H(KXOR opad, H(KXOR ipad || дані)),\text{HMAC} = H\big(K_{\text{XOR opad}},\, H(K_{\text{XOR ipad}} \,||\, \text{дані})\big),HMAC=H(KXOR opad ,H(KXOR ipad||дані)),

де KKK – криптографічний ключ, за потреби доповнений нулями до розміру блоку.

Принцип роботи HMAC полягає у двоетапному хешуванні: спочатку виконується хешування конкатенації внутрішнього ключа k1k_1k1 та вхідного повідомлення, після чого вихід цього хешу з’єднується з зовнішнім ключем k2k_2k2 і знову хешується. Ключі k1k_1k1 та k2k_2k2 детерміновані на основі секретного ключа kkk. Схематичне зображення процесу обчислення HMAC представлено на рисунку 3.2.

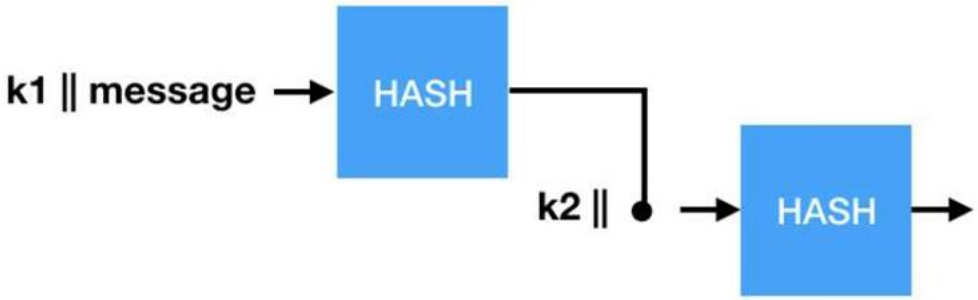


Рис. 3.2 Обчислення HMAC

Процес обчислення HMAC включає такі основні етапи:

1. З основного секретного ключа формуються два похідні ключі: k1=k⊕ipadk_1 = k \oplus \text{ipad}k1=k⊕ipad та k2=k⊕opadk_2 = k \oplus \text{opad}k2=k⊕opad, де ipad і opad – це константні значення, які використовуються в операції XOR.
2. Ключ k1k_1k1 об’єднується з повідомленням, після чого результат проходить через хеш-функцію.
3. Вихід цього першого хешу з’єднується з ключем k2k_2k2 і хешується вдруге.
4. На виході формується остаточний тег автентифікації.

Розмір тегу автентифікації визначається обраною хеш-функцією: наприклад, HMAC-SHA256 генерує тег довжиною 256 біт, а HMAC-SHA512 – 512 біт. Хоча технічно можливе скорочення довжини тегу для економії ресурсів, рекомендовано, щоб його довжина становила щонайменше 128 біт. У деяких обмежених випадках, наприклад для систем з низьким числом запитів, допускається використання тегів довжиною 64 біти, але це знижує рівень безпеки.

HMAC спроектований таким чином, щоб полегшити формальне доведення його безпеки. Дослідження показують, що цей алгоритм стійкий до підробок, якщо хеш-функція, на якій він базується, володіє властивостями, притаманними криптографічно стійким хеш-функціям.

Саме тому HMAC може працювати з різними хеш-функціями. На сьогодні найбільш поширеним є використання HMAC у поєднанні з SHA-2, що забезпечує високий рівень надійності та захисту даних.

3.2 Режими шифрування алгоритму AES

Об’єднання систем відеоспостереження з технологією блокчейн дозволяє створювати безпечніші та прозоріші платформи, де відеодані зберігаються у розподіленому реєстрі. Це гарантує захист від підробки, злому та несанкціонованого доступу, що особливо важливо для IoT-пристроїв, розумних будинків та логістичних ланцюгів, де критична цілісність відео-доказів. Блокчейн забезпечує довіру та незмінність записів завдяки децентралізації та криптографічним методам.

Принцип роботи:

1. **Фіксація та хешування:** Камери записують відеопотік, після чого система генерує криптографічний хеш для кожного блоку відео та заносить його в блокчейн. Самі відеофайли можуть зберігатися у децентралізованих сховищах, таких як IPFS або Filecoin.
2. **Незмінне зберігання:** Кожен новий блок з хешем відеоданих додається до ланцюга. Завдяки розподіленому характеру блокчейну будь-які спроби змінити або видалити старі записи виявляються одразу, оскільки потребують корекції всіх наступних блоків, що практично неможливо.

Децентралізація: Замість зберігання даних на одному центральному сервері, інформація розподіляється між багатьма вузлами мережі, що підвищує стійкість системи до атак, збоїв та несанкціонованого доступу.

Режими шифрування AES: Для правильної та безпечної роботи алгоритму AES необхідно використовувати відповідний режим шифрування. Некоректна реалізація або неправильне застосування режимів може значно знизити рівень безпеки. Серед найбільш поширених режимів AES виділяють [12]:

- **ECB (Electronic Codebook) – режим електронної кодової книги:** найпростіший режим, де кожен блок даних шифрується окремо.

Режими шифрування AES:

- **CBC (Cipher Block Chaining) – режим ланцюжка блоків шифру:** забезпечує, щоб однакові блоки відкритого тексту шифрувалися по-різному за рахунок використання вектора ініціалізації (IV).
- **CFB (Cipher Feedback) – режим зворотного зв'язку шифру:** перетворює блочний шифр у потоковий, дозволяючи обробляти дані по частинах.
- **OFB (Output Feedback) – режим вихідного зворотного зв'язку:** також створює потоковий шифр, де ключові потоки генеруються незалежно від відкритого тексту.
- **CTR (Counter – режим лічильника):** генерує ключовий потік на основі лічильника, що дозволяє паралельну обробку блоків і високу продуктивність.
- **GCM (Galois/Counter Mode – режим Галуа/лічильник):** поєднує шифрування в режимі лічильника з аутентифікацією даних, забезпечуючи одночасно конфіденційність і цілісність.

Порівняльний аналіз CBC і GCM:

- **AES-CBC:** кожен блок відкритого тексту перед шифруванням об'єднується з попереднім за допомогою операції XOR із вектором ініціалізації (IV). Це гарантує, що однакові блоки тексту шифруються по-різному. Потім результат шифрується ключем AES, після чого вихідний блок впливає на обробку наступного блоку відкритого тексту. Принцип роботи показаний на рисунку 3.3. CBC забезпечує конфіденційність, але не має вбудованого механізму автентифікації.
- **AES-GCM:** дозволяє паралельне шифрування та одночасно надає тег автентифікації для перевірки цілісності даних. Завдяки цьому режиму дані можна перевіряти на наявність змін або підробки, що особливо важливо для відеопотоків і критично чутливих записів.

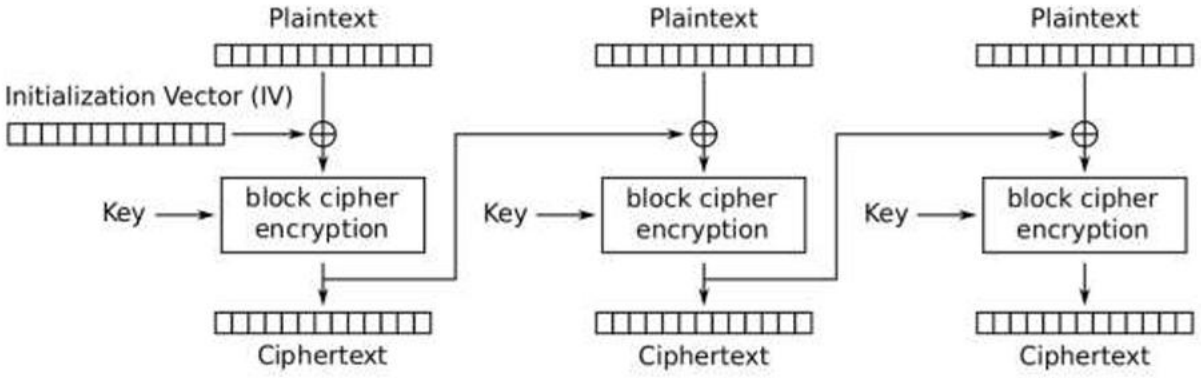


Рис. 3.3 Принцип шифрування AES-CBC

Проблеми режиму AES-CBC:

Однією з ключових вразливостей режиму CBC є ефект лавини: помилка в одному блоці відкритого тексту впливає на всі наступні блоки. Крім того, CBC вразливий до декількох видів криптографічних атак:

- **Атака з вибраним відкритим текстом (CPA, Chosen Plaintext Attack):** зловмисник має можливість обирати відкритий текст і отримувати відповідні зашифровані блоки, що потенційно дозволяє витягувати інформацію про ключ або інші дані.
- **Атака з вибраним зашифрованим текстом (CCA, Chosen Ciphertext Attack):** зловмисник отримує зашифровані блоки за своїм вибором і на основі них намагається відновити відкритий текст або ключ.

Хоча як AES-CBC, так і AES-GCM можуть забезпечувати конфіденційність за правильної реалізації, для протидії складнішим атакам, таким як CPA і CCA, потрібне **автентифіковане шифрування**.

Переваги AES-GCM:

- Забезпечує одночасно **конфіденційність та автентифікацію** даних, запобігаючи атакам на цілісність.
- Паралельна обробка блоків дозволяє значно збільшити пропускну здатність у порівнянні з CBC.
- Знижує накладні витрати на шифрування, що особливо важливо для потокових відеоданих у реальному часі.

Схематичне порівняння процесів AES-CBC та AES-GCM наведено на рисунку 3.4.

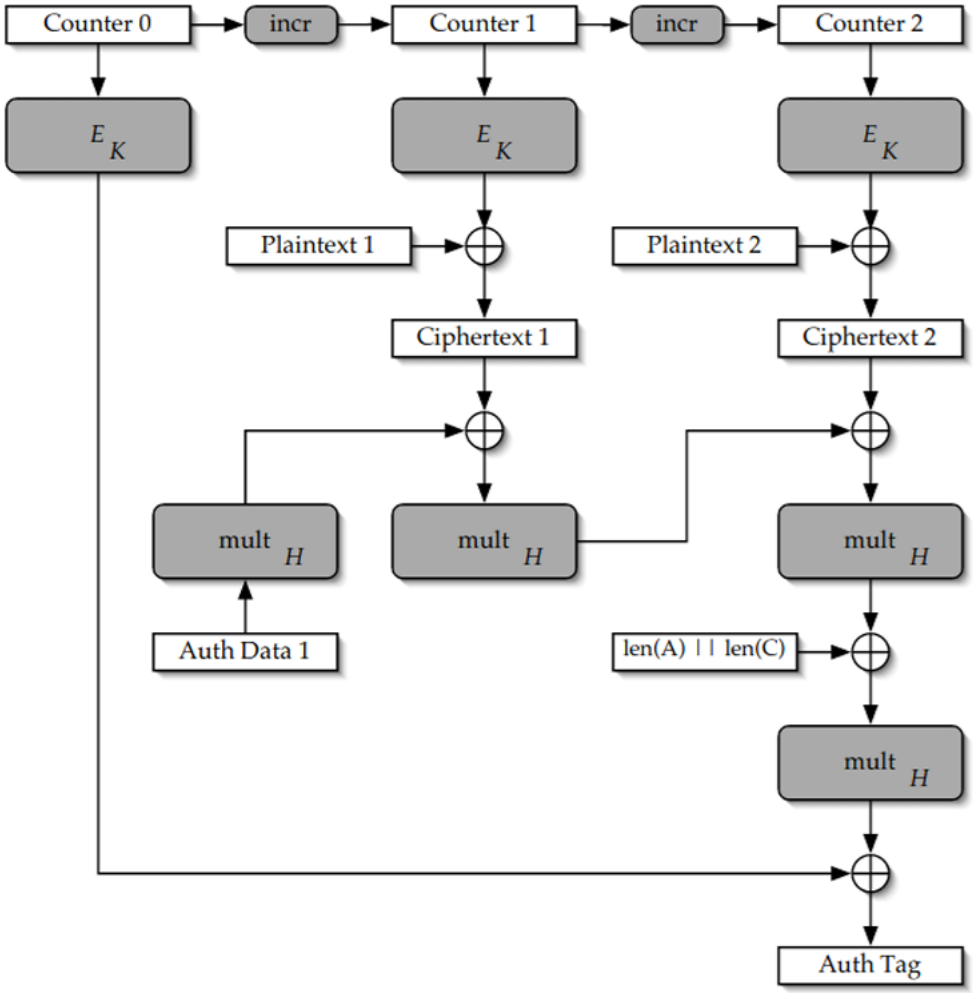


Рис. 3.4 Принцип шифрування AES- GCM

Особливості режиму AES-GCM та порівняння з ECB

Режим GCM підтримує конвеєрну та паралельну обробку даних, що забезпечує мінімальні обчислювальні затримки. Завдяки цьому він є ефективним рішенням для систем з високою швидкістю передавання інформації, зокрема для потокового відео.

На відміну від цього, у режимі ECB (Electronic Code Book) для алгоритму AES однаковий відкритий текст, зашифрований з використанням одного й того самого ключа, завжди дає ідентичний зашифрований результат. Оскільки AES є блоковим шифром, доповнення (padding) може змінювати лише кінцеві байти

повідомлення, однак за умови фіксованого розміру блоку (16 байтів) перший блок шифротексту залишатиметься незмінним. Це створює серйозну загрозу безпеці, оскільки дозволяє виявляти шаблони у зашифрованих даних.

Розглянемо режим потокового шифрування GCM та проаналізуємо ситуацію, коли використовується той самий ключ і той самий вектор ініціалізації (IV). У цьому випадку пароль спочатку перетворюється на ключ шифрування, після чого вектор ініціалізації встановлюється у фіксоване значення (наприклад, усі нулі), разом із тією ж самою «сіллю», що застосовується під час генерації ключа.

Для прикладу, якщо повідомленням є **«Taras 123»**, а паролем — **«password321»**, отримаємо такі результати:

- Повідомлення: Taras 123
- Зашифрований текст: 80fc096b6f98d14f540d7212bffa94ff59f9b3697792d83595
- Ключ: 2f7ffec39904ee5b61a73d881f6d2f36c27d2a60a42d828b52b6409dc13d1318
- Nonce (IV): 000000000000000000000000
- Результат дешифрування: Taras 123

Цей приклад демонструє важливість правильного вибору та унікальності вектора ініціалізації в режимі GCM. Повторне використання одного й того самого ключа та IV може призвести до серйозних криптографічних вразливостей, незважаючи на загальну стійкість алгоритму.

Висновок щодо вибору режиму шифрування

Для забезпечення надійного захисту даних у стані спокою рекомендується використовувати режим шифрування Galois/Counter Mode (GCM). Цей режим поєднує ефективне шифрування та автентифікацію, забезпечуючи високу стійкість до атак та мінімальні обчислювальні затримки.

Для наочності розглянемо приклад шифрування зображення. Для порівняння зашифруємо його за допомогою алгоритму AES у режимах ECB та CBC. Оригінальне зображення наведено на рисунку 3.5.

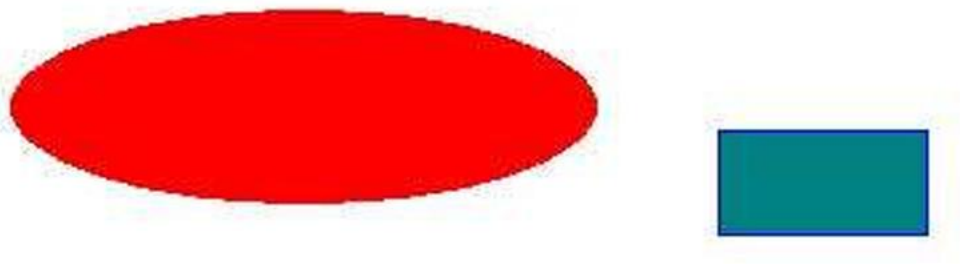


Рис. 3.5 Оригінальне зображення

Для практичної демонстрації шифрування файлу зображення **test.bmp** використано бібліотеку **OpenSSL**. Зашифрування виконано за допомогою алгоритму **AES-128** у режимі **ECB** із командою:

openssl enc -aes-128-ecb -e -in test.bmp -out ECBpic.bmp -K 1011011 -iv 1011001

Отримане зашифроване зображення у режимі **AES-ECB** наведено на рисунку 3.6.

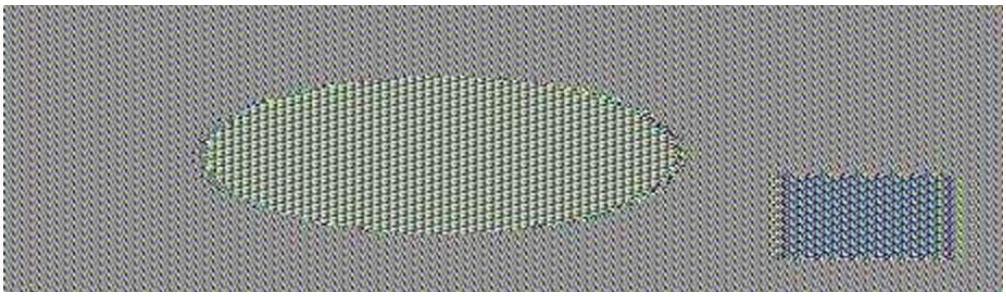


Рис. 3.6 Зашифроване зображення алгоритмом AES-ECB

Для шифрування файлу зображення **test.bmp** у режимі **AES-CBC** використовується команда OpenSSL:

openssl enc -aes-128-cbc -e -in pic_original.bmp -out CBCpic.bmp -K 1011011 -iv 1011001

Результатом шифрування є зашифроване зображення, яке представлено на рисунку 3.7.



Рис. 3.7 Зашифроване зображення алгоритмом AES- CBC

Як видно з рисунок 3.7 алгоритм AES- CBC надійно шифрує зображення.

3.3 Загальний алгоритм шифрування зображення

Під час шифрування зображення перетворюється на послідовність байтів, які обробляються за допомогою криптографічних алгоритмів. Після цього зашифровані дані передаються через відкриті канали до іншої системи, де вони розшифровуються для відновлення оригінального зображення за допомогою відповідного алгоритму розшифрування. Як для шифрування, так і для розшифрування використовується криптографічний ключ, на основі якого виконуються всі операції. Запропонована методика спрямована на забезпечення автентифікації, конфіденційності та цілісності даних у системі відеоспостереження. До захищеної мережі входять камери, периферійні обчислювальні пристрої (МПО) та хмарні сервери.

Перед передачею відеоданих усі пристрої повинні пройти взаємну автентифікацію, що встановлює довірчі відносини й дозволяє використовувати алгоритми шифрування для збереження конфіденційності інформації. Для забезпечення конфіденційності та оптимальної продуктивності в цій архітектурі застосовується алгоритм AES для шифрування відеопотоків, які надсилаються камерами до хмарного середовища. Оскільки AES передбачає використання спільного ключа на обох кінцях каналу, для його безпечного обміну пропонується протокол на основі асиметричного шифрування. Цей протокол також виконує

функцію автентифікації камер у системі. Основні етапи роботи запропонованого алгоритму наведені на рисунку 3.8.



Рис. 3.8 Протокол автентифікації та керування сеансом

1. **Генерація ключів камерами та хмарним сервером.** Кожна камера та хмарний сервер створюють власну пару відкритого та приватного ключів. Це необхідно для автентифікації сервера перед камерами. Камери можуть встановлювати з'єднання лише з сервером, чий відкритий ключ відомий заздалегідь. Відповідно, на всіх камерах повинен бути налаштований відкритий ключ хмарного сервісу.
2. **Автентифікація камер та створення ключа сеансу (чотиристоронній протокол «рукостискання»):**

- **Крок 1:** Камера (DC) надсилає хмарному серверу (CL) повідомлення M1 для автентифікації. M1 містить відкритий ключ DC і шифрується відкритим ключем CL:

  E(CL's KPUB,M1)E(\text{CL's K}_{\text{PUB}}, M1)E(CL's KPUB,M1)

  де E() – функція асиметричного шифрування (наприклад, RSA).
- **Крок 2:** Сервер CL розшифровує M1 і відправляє камері відповідь M2, що містить випадково згенероване число (Rnd). M2 шифрується подвійно: спочатку закритим ключем CL, а потім відкритим ключем DC:

  E(DC's KPUB,E(CL's KPRIV,M2))E(\text{DC's K}_{\text{PUB}}, E(\text{CL's K}_{\text{PRIV}}, M2))E(DC's KPUB,E(CL's KPRIV,M2))

Це гарантує, що лише DC може розшифрувати Rnd, а повідомлення дійсно походить від CL. Крім того, використання випадкових чисел забезпечує свіжість даних та захист від атак повтору.

- **Крок 3:** Камера (DC) розшифровує повідомлення M2, спочатку використовуючи власний приватний ключ, а потім відкритий ключ сервера CL (двошарове шифрування). Після цього DC збільшує значення Rnd на 1 для формування повідомлення M3 і шифрує його аналогічним двошаровим способом: спочатку приватним ключем DC, а потім відкритим ключем CL:
  E(CL’s KPUB,E(DC’s KPRIV,M3))E(\text{CL’s K}_{\text{PUB}}, E(\text{DC’s K}_{\text{PRIV}}, M3))E(CL’s KPUB,E(DC’s KPRIV,M3))
- **Крок 4:** Сервер CL розшифровує M3 і перевіряє, що Rnd збільшено на 1. Це підтверджує автентичність камери та правильність протоколу. Після цього сервер надсилає повідомлення про прийняття M4, яке містить підтвердження автентифікації, ключ сеансу для симетричного шифрування (наприклад, AES) та час дії сеансу. Після отримання M4 сесія вважається встановленою та готовою до обміну даними.

1. **Генерація ключів сеансу:**
   Після завершення автентифікації DC та CL можуть безпечно згенерувати ключі сеансу для подальшого захищеного обміну даними. Ключі сеансу можуть бути передані та використані пристроями МПО. Після встановлення ключів сеансу AES застосовується для довгострокового шифрування відеопотоків.
2. **Режим шифрування та цілісність даних:**
   Для забезпечення додаткової безпеки використовується режим CBC (Cipher Block Chaining). Він гарантує, що навіть при повторній відправці того самого повідомлення шифртекст буде іншим, оскільки кожен блок відкритого тексту об’єднується з попереднім зашифрованим блоком перед шифруванням. Шифрування може виконуватися:

- для всього відеокадру у форматі MJPEG,
- для всього GOP у форматах MPEG4 або H.264,
- або для кожного пакета окремо.

Для забезпечення цілісності відеопотоків застосовується HMAC-SHA256 з використанням узгодженого ключа сеансу.

Як і у випадку зі шифруванням, HMAC-SHA256 може обчислюватися для кожного окремого пакета або для цілого відеокадру. Отримане хеш-значення додається до відеопотоку перед його шифруванням та передачею до хмарного сервера, що дозволяє забезпечити автентичність та цілісність переданих даних.

4 ВПРОВАДЖЕННЯ БЛОКЧЕЙНУ ДЛЯ СИСТЕМИ ВІДЕОНАГЛЯДУ В АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБАХ

4.1 Інтеграція MEC та блокчейну для відеонагляду в автономних транспортних засобах

Системи аудіовізуальної передачі на основі блокчейну були створені для створення розподіленої та гнучкої системи розумного транспорту (STS). Ця система дозволяє клієнтам, творцям відео та постачальникам послуг безпосередньо спілкуватися між собою. Пристрої STS на основі блокчейну потребують великої комп'ютерної потужності для зміни якості та форм відеопотоку у різні версії та структури, які відповідають потребам різних користувачів. З іншого боку, існуючі блокчейни не можуть підтримувати пряму трансляцію, оскільки обробляються надто довго і не мають достатньої комп'ютерної потужності. Великі обсяги відеоданих, які надсилаються та аналізуються, створюють надмірне навантаження на мережі для транспортних засобів.

У цому розділі запропонується метод відеоспостереження для покращення продуктивності даних блокчейн-системи та зниження затримки у системі з краєм доступу (MEC). Було запропоновано інтеграцію MEC та блокчейну для відеоспостереження в автономних транспортних засобах (IMEC-BVS).

Результати симуляції показують, що запропонований метод швидко сходиться і покращує продуктивність MEC і блокчейну при спільному використанні для відеоспостереження в безпілотних автомобілях порівняно з іншими методами.

Завдяки потоковим медіа на основі блокчейну відеопровайдери (VP), слухачі та оператори мережі (NO) можуть обмінюватися відео без участі третьої сторони. Процедури потокового відео можуть бути самоорганізовані як бонус за допомогою консенсусного протоколу.

Відеосистеми на основі блокчейну не можуть транскодувати відео через обмежені обчислювальні вимоги. MEC, який забезпечує обчислювальну продуктивність на периферії системи STS, є потенційним рішенням для забезпечення можливості доставки контенту споживачам.

Сервери з MEC забезпечують споживачам послуги зі зменшеною затримкою, звільняючи мережеву пропускну здатність і витрати на зберігання. Архітектура на основі MEC дозволяє MEC-серверу транслювати бітрейт аудіовізуальних даних відповідно до умов зв'язку та вимог оператора. Інтеграція блокчейнів і MEC може мати значні переваги і бути чудовою ідеєю для цієї захопливої сфери. Досягнуто прогресу у сфері MEC та розподіленого реєстру, щоб максимально використати сильні та слабкі сторони обох технологій.

Останніми роками глибоке підкріплене навчання (DRL) стало потужною технікою для розв'язання проблем розподілу ресурсів у бездротовому зв'язку та мережах за допомогою штучного інтелекту (ШІ). Методи на основі DRL мають нижчу обчислювальну складність, ніж стандартні методи оптимізації, і можуть максимізувати ресурси з низькою складністю в комунікаційних системах.

Використовуючи платформу MEC для відеоспостереження, можна підвищити пропускну здатність і зменшити затримку в автономних автомобілях з підтримкою блокчейну.

Було впроваджено фреймворк відеоспостереження, що використовує MEC для STS. Далі описується смарт-контракт для відеоаналітики. Поєднання Ethereum з периферійними пристроями може захистити критично важливі інформаційні системи STS та захистити приватну інформацію в інфраструктурі та сервісах. Загальна модель представлена для критеріїв розвантаження відео в обставинах STS, які включають системи STS, що створюють взаємодії, схему MEC, що підтримує відеоспостереження, та блокчейн-схему, що взаємодіє з подією.

Архітектура відеонагляду.

На рисунок 4.1 показує рамки для інтеграції MEC і блокчейну для відеоспостереження в автономних транспортних засобах. MEC використовується для розвантаження завдань відеоспостереження з STS, який має два аспекти:

вузол транспортного засобу з камерою та вузол Road Segments (RS) з MEC. Камери, встановлені на вузлах транспортних засобів, можуть ініціювати аудіовізуальні доручення, обгортати їх у відеоблоки та передавати до вузлів RS через транспортні системи. MEC з вузлом RS дозволяє виконувати складну відеоаналітику. Він також забезпечує збереження відео на RS та обробку інформації між сусідніми транспортними засобами. Для сприйняття та прийняття рішень STS камери є привабливим сенсорним вибором. Багато сучасних професійних систем підтримки водіння, наприклад, використовують камери для ідентифікації руху та пішоходів. У режимі реального часу відеоаналітика в STS може виконуватися за допомогою edge computing через великий обсяг даних, потреби у обчисленнях і обмеження затримки.

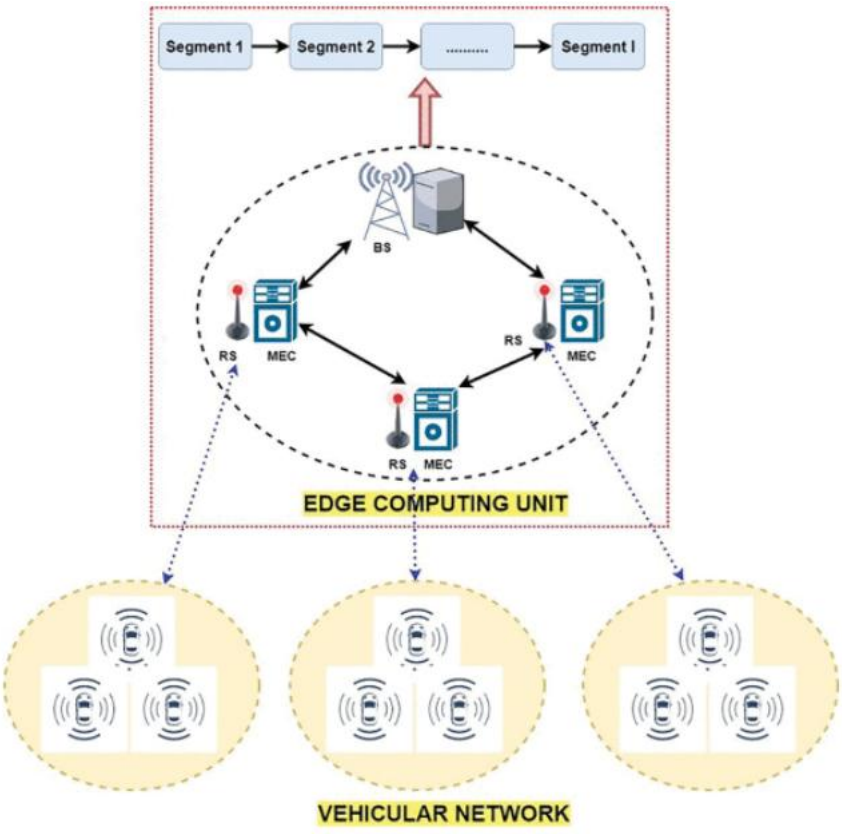


Рис. 4.1 Фреймворк для інтеграції MEC та блокчейну для відеоспостереження в автономних транспортних засобах

4.2 Модель системи для STS

Було досліджено мережу STS, активовану блокчейном із використанням блокчейну. Ядро зони покриття розташоване в мережах STS з однією макро-комірковою базовою станцією (BS). Різні RS розподілені по всьому BS, а дротові з'єднання з'єднують усі RS. Припустимо, що система без перерв, де користувачі використовують узгоджену пропускну здатність для передачі інформації. Нехай множина RS позначена як N = {1, 2, ..., N}. Отже, P = {1, 2, ..., P} позначається для набору транспортних засобів, де *n* транспортних засобів мають відповідний RS *n*. Периферійне буферизування також є важливим для потокового відео на вимогу у стільниковій мережі. Запити на відеоспостереження в автомобільному кіберпросторі були розглянуті, а ключовими обов'язками є розшифрування відео, попередня обробка та розпізнавання об'єктів. Тому було досліджено можливості підключення та обробки для максимізації транзакцій блокчейн-платформи та зменшення затримки платформи MEC. RS на основі MEC використовуються у завданнях для відеоаналізу.

Досліджено можливості підключення та обробки для максимізації транзакцій блокчейн-платформи та зменшення затримки платформи MEC. RS на основі MEC використовуються у завданнях для відеоаналізу.

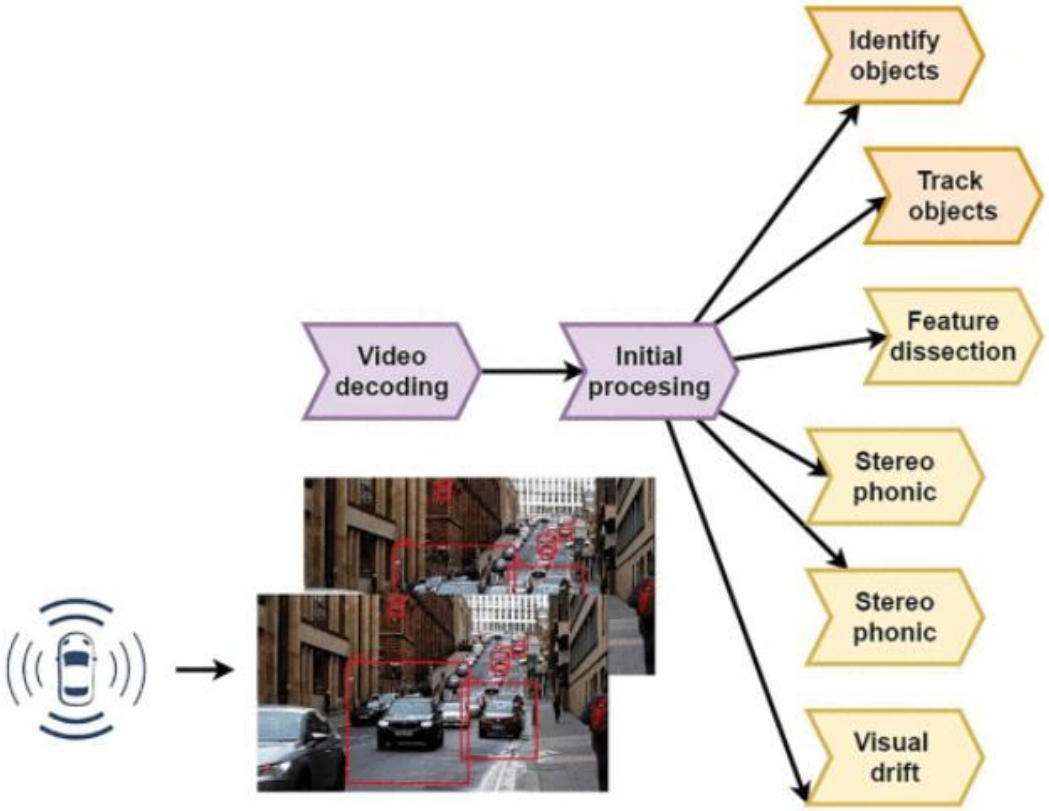


Рис.4.2 Відеоспостереження в STS

Рисунок 4.2 показує методологію відеоспостереження в STS, багато модулів дозволяють розглядати та пояснювати процес відеоаналізу.

Розшифрування відео: це процедура декодування або миттєве розшифрування закодованого відео. Кодек може витягувати та розгортати мультимедійне мовлення у послідовній послідовності, побудованій на протоколі реального часу (RTSP) або протоколі обміну повідомленнями в реальному часі (RTMP). Внаслідок цього AVS, H.264/AVC та H.265/HEVC є одними з найпоширеніших стандартів кодування відео.

Початкова обробка: процедура корекції — це неоднорідна модифікація яскравості кольорів і амплітуди. Через низький контраст і розмиття зображення корекція об'єктива та покращене зображення мають покращити якість відеопослідовностей.

Розпізнавання об'єктів: Потрібно виявляти екземпляри семантичних сутностей певного класу, що є необхідним для досягнення незалежної навігації. Важливими об'єктами STS є автомобілі, футбол, велосипед і дорожні знаки.

Відповідно, було використано однофазний метод, що складається з методологій розпізнавання об'єктів на основі глибокого навчання (DL). Класи включають регіональну інтеграцію, мережу об'єднання просторових пірамід (SPP-Net) та регіональні мережі пропозицій (RPN). Модель одиночної техніки складається з одного екранного детектора (SSD).

Об'єкти відстеження: Стан одного або кількох об'єктів потрібно оцінювати за час виконання за допомогою датчиків. Спостереження за іншими водіями є необхідним для автономних транспортних засобів. Виявлення об'єктів складається з чотирьох етапів: пошук функцій, навігаційна модель, фреймворк пошуку та онлайн-оновлення. Підходи до виявлення та відстеження об'єктів включають генерацію, дискримінацію та глибоке навчання.

Розбір ознак: Кожному пікселю зображення потрібно присвоїти тег, що складається з набору класів. Поділ зображень на семантичні області дозволяє автомобілям усвідомлювати їхню атмосферу, щоб автономні транспортні засоби могли безпечно бути включені до наших сучасних доріг.

Stereo Phonic: Метод отримання знань з неактивних 2D-зображень, зроблених лазерним сканером, — це стереопрогноз.

Візуальний дрейф: Він може надавати важливу інформацію про сцену та слугувати інтерфейсом для конкретних дій, включно з оцінкою руху та спостереженням.

4.3 Процес блокчейну

Блокчейни можуть мати три характеристики закону трилеми масштабованості:

- універсальність;
- безпека;
- децентралізація.

Три ключові особливості блокчейну зображені на рисунку 4.3. Кожна з цих особливостей була детально пояснена наступним чином.

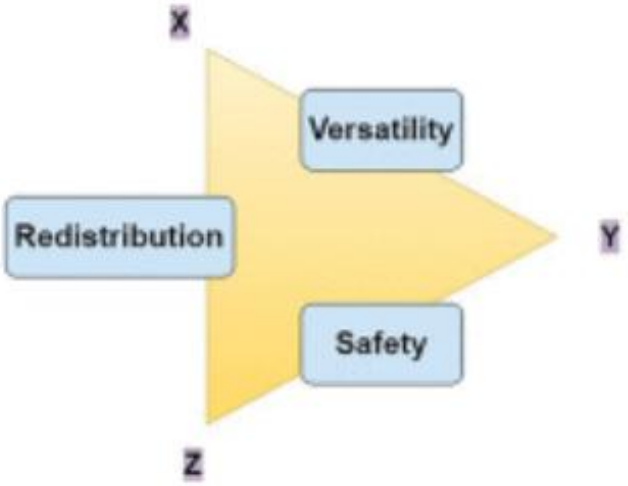


Рис. 4.3 Особливості блокчейну

Універсальність

Вона визначає мережеву інфраструктуру, включаючи кількість вузлів, які мережа може обробляти, кількість транзакцій, які мережа може здійснити тощо. Операції з блокчейн-мережею були зафіксовані. На основі запропонованого підходу за розкладом обирається виробник блоків, а потім генерується виробник блоків шляхом операцій збору, верифікації та пакування.

Безпека

Безпека означає ступінь захисту блокчейну від зовнішніх атак і стійкість платформи до маніпуляцій. Блокчейн-система містить різні вектори атак, включно з атаками з подвійними витратами, атаками через червоточину, DDoS (розподіленою відмовою в обслуговуванні) атаками та атаками з 51 відсотком. Тому слід обмежувати такі обмеження для гарантування безпеки смарт-контрактів.

Перерозподіл

Перерозподіл означає ступінь авторитету, домінування та різноманіття цінностей блокчейну. Усі дії та блоки розповсюджуються, перевіряються, фіксуються та децентралізовані серед усіх зацікавлених сторін у приватному блокчейні, забезпечуючи незмінність, надійність і довговічність усієї структури. Водночас понад половина комп'ютерних ресурсів залишається справедливою.

Коли блокчейн використовується в налаштуваннях STS, масштабування стає великою проблемою. По-перше, збільшуючи розмір сегмента або зменшуючи інтервали блоків, можна збільшити вихід транзакцій. По-друге, зменшення розриву блоку забезпечує більш суттєве обмеження затримки. Розмір сегмента та періодичні зміни або вибір виробників блоків і методи консенсусу слід ретельно виконувати, щоб вивести сталість блокчейну до стандартного рівня.

4.4 Потік процесів контракту в блокчейні для STS

Потік процесів контрактів у блокчейні показано на рисунку 4.4. Було створено централізований репозиторій із сумісністю та безпекою блокчейн-експертизи, яка володіє аудіовізуальним спостереженням у недорогих STS-ситуаціях. Рисунок 4.4 показує топологію блокчейну STS, з записами про запаси даних і спільне використання, включені до даних транзакцій. Взаємодії, створені як середовища STS, представлені з інтелектуальними контрактами на зберігання та процедури обміну даними.

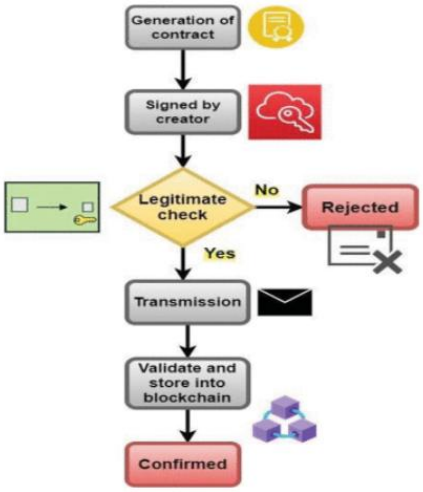


Рис. 4.4 Потік процесів контракту в блокчейні для STS

Блокчейн-мережа має пройти два етапи:

– об'єднання транзакцій і генерація сегментів;
– реєстрація сегментів за *угодою q*.

Також є певні обмеження та недоліки.

Обмеження: Запропонований метод може зіткнутися з труднощами при масштабуванні до великої кількості автономних транспортних засобів. Хоча алгоритм демонструє ефективність для різних вхідних даних, продуктивність може погіршуватися зі значним збільшенням розміру мережі, особливо в середовищах з високою щільністю автономних транспортних засобів. Ще одним обмеженням є оптимізація обчислювальних ресурсів, яка може бути неповністю застосовною в реальних умовах, де ресурси, такі як обчислювальна потужність і пам'ять, обмежені.

Недоліки: Поточна робота згадує пропускну здатність і стимулювання як ключові показники ефективності, але інші важливі показники, такі як енергоефективність, безпека (окрім пропускної здатності) та відмовостійкість, не розглядаються детально. Ці фактори мають вирішальне значення для систем автономного водіння і можуть обмежити практичність системи, яку буде досліджувати в майбутньому.

ВИСНОВКИ

В кваліфікаційній роботі розв’язано актуальну задачу впровадження блокчейну та підвищення ефективності захисту в системах відеонагляду.

Розглянута та проаналізована технологія блокчейн, її структура та особливості. На підставі отриманих даних зроблено висновок про ряд переваг технології блокчейн, зокрема: незмінність, децентралізація, прозорість та конфіденційність. Було проведено порівняльний аналіз трьох типів протоколів досягнення консенсусу, а також публічних, приватних та гібридних мереж блокчейн. Крім цього, визначено основні переваги, проблеми та недоліки різних типів блокчейну. Досліджено, що найбільш доцільним типом для забезпечення безпеки інформації є гібридний блокчейн, який поєднує переваги обох типів технології, намагаючись при цьому обмежити їх недоліки і таким чином забезпечує всі аспекти інформаційної безпеки. З урахуванням цієї інформації, гібридний блокчейн є безпечним та надійним засобом для захисту інформації. Детально розглянуто смарт-контракти, написані на базі публічних мереж блокчейн, та виявлено ряд недоліків у сфері забезпечення інформаційної безпеки. Блокчейн може створити безпечну, ефективну та децентралізовану інфраструктуру для фінансових операцій, забезпечуючи високий рівень захисту від шахрайства та забезпечуючи швидкість та доступність для всіх користувачів. Зараз, коли індустрія фінансових послуг активно адаптується до цифрової ери, впровадження технології блокчейн стане ключовим фактором у формуванні майбутнього ландшафту.

При цьому отримано наступні результати.

1. Проведено аналіз підходів до захисту даних в системах відеоспостереження. Серед який виділено: доставка контенту через HTTPS, програми потокового відео, захищені паролем, захищені центри відеоданих, алгоритми симетричного шифрування, шифрування даних при передачі.

2. Досліджено технології побудови систем відеоспостереження, зокрема: граничні обчислення та технологія FPGA. Проектування систем

відеоспостереження на основі вказаних технологій дозволить значно підвищити їх ефективність.

3. Проаналізовано основні криптографічні примітиви для шифрування зображень. Вказано їх переваги та можливість застосування при проектуванні захищених систем відеоспостереження.

4. Розглянуто структуру системи відеоспостереження на основі технології мобільних периферійних обчислень та хмарного сервісу, яка забезпечує надійне зберігання відеоданих на центральному хмарному сервері з оптимальною якістю. Для забезпечити цілісності відеопотоків використано аутентифікація повідомлень на основі хешування HMAC-SHA256.

5. Представлено алгоритм шифрування зображення на основі AES з режимом ланцюжка блоків, що забезпечує створення нового шифру при надсиланні тих самих зображень.

6. Було запропоновано інтеграцію MEC та блокчейну для відеоспостереження в автономних транспортних засобах (IMEC-BVS). Результати симуляції показують, що запропонований метод швидко сходиться і покращує продуктивність MEC і блокчейну при спільному використанні для відеоспостереження в безпілотних автомобілях порівняно з іншими методами.

Застосування блокчейн-технологій в сфері забезпечення безпеки даних має великий потенціал. Вони надають можливості для створення безпечних, незмінних та децентралізованих систем збереження та передачі інформації. Отже, використання блокчейн технологій може стати ефективним рішенням для забезпечення безпеки даних у майбутньому.