УДК 621.396.4
DOI https://doi.org/10.32782/2663-5941/2023.2.1/15

Сайко В.Г.
Київський національний університет імені Тараса Шевченка

Наритник Т.М.
Інститут електроніки та зв'язку Української академії наук

ЗАСТОСУВАННЯ БЛОКЧЕЙН СИСТЕМИ ДЛЯ БЕЗПЕЧНОГО ОБМІНУ ПОВІДОМЛЕНЬ В ГЕТЕРОГЕННИХ МОБІЛЬНИХ МЕРЕЖАХ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ

Наведено рекомендаційні аспекти щодо впровадження блокчейн рішення в одну з перспективних послуг мереж нового покоління, таку як забезпечення подолання ефектів блокування передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль. Представлене рішення дозволяє підвищити конфіденційність і надійність переданих даних, забезпечити появу нових можливостей щодо прийняття рішень і знизити затримки та підвищити енергоефективність. Запропоновано інноваційний тип блокчейн, який можна використовувати для ефективної перевірки надійності вузлів та повідомлень про події мікросервісу забезпечення подолання ефектів блокування передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль. Основними його особливостями є: нова інфраструктура блокчейна для зберігання достовірності вузлів та повідомлень у мобільній мережі 5G. У цій структурі достовірність вузла та повідомлення, які діють як транзакції, подібні до блокчейну Біткойн. Але при цьому маємо справу з повідомленнями про події як із транзакціями, а не з криптовалютою. Для зменшення затримки при генерації блоків, застосовуються граничні обчислення в блокчейн. Прикордонні обчислення зменшать затримку за рахунок перенесення складних обчислень на прикордонні пристрої. На основі нової структури блокчейну наведено розроблений загальний алгоритм адаптивного функціонування абонента при блокуванні передачі прямої видимості в гетерогенній мобільній мережі терагерцового діапазону. Застосування запропонованого рішення в децентралізованій мережі мобільного зв'язку 5G, основою якої є інфраструктура блокчейн, потенційно знижує складність мережі, значно зменшує експлуатаційні витрати оператора і відповідно підвищує надійність та оперативність управління механізмом адаптивного забезпечення абоненту зв'язком в режимі реального при блокуванні передачі прямої видимості.

Ключові слова: *блокчейн, мобільний зв'язок, терагерцового діапазону, блокування передачі.*

Постановка проблеми. У сучасних мобільних мережах під час передачі обслуговування (хендовера) користувацького обладнання об'єкт управління мобільністю повинен використовувати контекстну інформацію обладнання. Ця подія запускає послідовну взаємодію та передачу сигналів між кількома об'єктами керування мобільністю та сеансом. У гетерогенній мережі при використанні терагерцового діапазону хвиль цей спосіб є мало ефективний, особливо при частих подіях передачі обслуговування при блокуванні передачі в терагерцовому діапазоні. Тому автори запропонували для вирішення такої задачі використати технологію розподіленого реєстру для реалізації механізму попереджуючого хендоверу при блокуванні передачі в терагерцовому діапазоні [1, 2].

Але при реалізації даного рішення необхідно враховувати наступне.

Основними причинами проблем, пов'язаних з інформаційною безпекою гетерогенних мереж терагерцового діапазону, є:

- можливість прослуховування каналів та підміни повідомлень, яка обумовлена загальнодоступністю середовища передачі;
- необхідність використання складних алгоритмів маршрутизації, які враховують ймовірність отримання невірної інформації від скомпрометованих мобільних терміналів унаслідок змін топології мережі;
- неможливість реалізації традиційної безпекової політики обумовлена особливостями класичної архітектури терагерцової мережі, такими як відсутність фіксованої топології та центральних вузлів.

При спілкуванні у мережі з підтримкою реконфігурованих інтелектуальних поверхонь (РІП) з об'єктами мобільної інфраструктури передається

різна інформація, зокрема ідентифікаційні дані РІП, місцезнаходження, зміст запиту та інші. У разі порушення конфіденційності та цілісності таких даних можуть постраждати користувачі. Така інтелектуальна система включає величезну кількість динамічних критично важливих даних в реальному часі, тому її безпека є серйозною проблемою. Через гостру необхідність забезпечення незмінності та цілісності даних пропонується використовувати спеціальні механізми, які доступні у рішеннях блокчейн.

Критичними проблемами при впровадженні блокчейн технології в *мобільні мережі з підтримкою РІП при використанні терацерцового діапазону хвиль* є: низькі обчислювальні ресурси, обмежений обсяг пам'яті та енергії на мобільних засобах, часта зміна їх місцезнаходження у просторі та обмежені ресурси зв'язку.

Аналіз останніх досліджень і публікацій. В [3] автори використали базову концепцію блокчейна для спрощення управління розподіленими ключами у різноманітних корпоративних мережах. Автори в [4] об'єднали концепції додатків на основі блокчейну мережі VANET та Ethereum і створили прозору та децентралізовану систему. Вони використовували систему смарт-контрактів Ethereum для запуску всіх типів програм на блокчейні Ethereum. Навпаки, запропонована нами робота застосовує інший тип блокчейну для безпечного розповсюдження повідомлень в гетерогенних мережах при використані терагерцового діапазону. У [5] запропоновано технологію блокчейн для безпеки з використанням оверлейної мережі. Вузли оверлейної мережі згруповані у виді кластерів, і ці кластери відповідають за обробку блокчейна та виконання його основних функцій. Однак, введення додаткових вузлів оверлея приводить до високої затримки і може стати центральною точкою відмови, якщо головна частина кластера буде скомпрометована.

Постановка завдання. Розробка принципів технічної реалізації нової інноваційної послуги мереж 5-го та наступних поколінь – використання ресурсу локального кластеру мережевої інфраструктури терагерцового діапазону на базі РІП для забезпечення надійності зв'язку на основі розподіленого реєстру для механізму попереджуючого хендоверу при блокуванні каналу прямої видимості перешкодами при передачі на вкрай високих частотах.

Виклад основного матеріалу дослідження.

Загальні зауваження та пропозиції

Застосування блокчейна для надійної передачі інформації є важливим при передачі та уникненні втрат або спотворень, які можуть спричинити негативні наслідки. Завдяки конструкції системи довірчого керування в блокчейні її можна успішно застосовувати між вузлами (мобільними терміналами) з децентралізованими системами. При цьому «шкідливі» мобільні термінали можуть проникати в мережу та поширювати неправдиву інформацію, що призводить до збою в роботі гетерогенної мобільної мережі з підтримкою РІП. Але застосування блокчейну для оцінки рейтингу учасника мобільної мережі при використанні терагерцового діапазону хвиль також є ефективним рішенням для використання в такій інтелектуальній системі, оскільки рейтингова оцінка об'єкта дозволить застосовувати заходи до порушників та заохочувати порядних користувачів. Це дозволить забезпечити зниження кількості повідомлень неправильної поведінки, що створюють ризик або знижують ефективність роботи самої систем.

Використання алгоритмів з довірчого управління та поділу пріоритетів дозволяє учасникам мобільної мережі з підтримкою РІП при використанні терацерцового діапазону хвиль визначати з високою ймовірністю, чи отримане повідомлення є надійним. Так для об'єктів з високим рейтингом репутації інформація буде прийнята швидше, так як якість даних залежить від репутації об'єкта. Значення довіри до учасників мережі визначається на основі оцінок, отриманих в результаті минулої поведінки, які прикріплюються та зберігаються в системі за допомогою блокчейн технології. Даний метод дозволить об'єктивніше сприймати реальну обстановку, стимулювати користувачів на порядну поведінку та послідовно записувати події для подальшої обробки та використання.

Для організації цього процесу пропонується застосовувати блокчейн з удосконалений алгоритмом консенсусу Practical Byzantine Fault Tolerance [6-8], який відповідає за ефективну роботу в асинхронних мережах, дозволяє досягти консенсусу, навіть якщо деякі вузли мережі не відповідають або дають неправильну інформацію. Даний алгоритм передбачає вибір 2 видів вузлів – лідера та резервних вузлів. Кожен вузол у мережі підтримує свій власний внутрішній стан, і коли він отримує повідомлення, він виконує обчислення та готує рішення про нове отримане повідомлення. Індивідуальне рішення кожного вузла надсилається лідеру вузлів, який підтверджує довіру до нового повідомлення на основі рішень усіх вузлів. Лідером пропонується використовувати технології граничних обчислень, тоді як резервні вузли – учасників мобільної мережі з підтримкою РІП при

використанні терацерцового діапазону хвиль, підключені до інтелектуальної системи управління.

При передачі інформації пристрій мережі формує повідомлення у вигляді транзакції, записуючи в нього значення рейтингу репутації і пріоритет ситуації. Транзакції записуються до блоку та передаються всім учасникам мережі. Чим вище репутація та пріоритет повідомлення, тим швидше приймається рішення про його прийняття. Блок фіксується, коли більше 2/3 валідаторів попередньо фіксують один і той же блок в тому самому раунді для транзакцій. Якщо повідомлення є компрометуючим або невірним, поведінка відправника повідомлення потім передається в блокчейн і повідомляється довірчому органу. Таким чином репутація відправника повідомлення погіршується.

Більшість сучасних блокчейн-систем є архітектурою єдиного ланцюжка. Таким чином, кожен вузол повинен виконувати безліч дубльованих обчислювальних завдань, що призводить до втрати енергії. Крім того, зниження його продуктивності стає очевиднішим, якщо виникають піки трафіку [6].

У випадку запропонованого рішення немає необхідності ділитися блоками за межі зони обслуговування окремого РІП. Для вирішення проблеми масштабованості пропонована архітектура використовує підхід сегментування. Сегментування – це поділ робочого навантаження блокчейн-мережі по одноранговій мережі, щоб кожен вузол не відповідав за транзакційне навантаження всієї мережі [7,8]. Це дозволяє різним сегментам паралельно обробляти транзакції для збільшення пропускної спроможності, що прискорює процеси валідації, а також перевірки блоків у ситуаціях, що залежать від часу, зберігаючи при цьому сумісність. Відповідно до високої мобільності вузлів незалежних підмереж, різні підмережі можуть мати різну кількість вузлів та час генерації блоків.

Удосконалена модель блокчейна для безпечного обміну повідомлень

Для реалізації запропонованого принципу функціонування мережі пропонується удосконалений тип блокчейна для вирішення проблем, пов'язаних із довірчим розповсюдженням повідомлень гетерогенної мобільної мережі при використанні терагерцового діапазону частот. Цей підхід є новим, оскільки використовується концепція незмінної розподіленої загальнодоступної бази даних для безпечного розповсюдження повідомлень у бездротовій мережі, де будь-який вузол може отримати доступ до інформації. Це стало можливим завдяки впровадженню блокчейну Біткойн. Проте наша проблематика відрізняється від Біткойна, оскільки маємо справу з повідомленнями про події, а не з криптовалютними транзакціями.

Компонентами запропонованої інфраструктури блокчейна є наступні:

– базові станції, які використовуються для зв'язку в зоні обслуговування, та відповідають за автентифікацію та надання сертифіката місцезнаходження мобільних терміналів у межах локального кластера.

– Fog-термінали є основними елементами системи блокчейна у зоні обслуговування локального кластера. Вони генерують повідомлення про події, добувають нові блоки та зберігають повідомлення про події у блокчейні після перевірки. Існує два типи Fog-терміналів, тобто повний вузол та нормальний вузол. Повний вузол має високий рівень довіри та потужну обчислювальну потужність, яка відповідає за видобуток блоків. А інші вузли є звичайними вузлами, які допомагають у генерації повідомлень під час блокування передачі в мобільних системах, а також у пересиланні та перевірці отриманих повідомлень.

– Повідомлення у зоні локального кластера. У зоні обслуговування локального кластера є два типи повідомлень. Це повідомлення маяка та повідомлення про події, які пов'язані з сервісом для забезпечення подолання ефектів блокування передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль. Повідомлення маяка періодично передаються для інформування сусідніх Fog-терміналів про стан робочого напрямку зв'язку та положення Fog-терміналів для забезпечення спільної поінформованості інших Fog-терміналів у локальному кластері для управління процесом обслуговування. Повідомлення про події блокування передачі в мобільних системах надсилаються, коли в локальному кластері відбуваються критичні події. Залежно від серйозності надзвичайної ситуації повідомлення про події поділяються на різні рівні залежно від пріоритету, наприклад, рівень 1, рівень 2 та рівень 3, де рівень 1 вказує на повідомлення про вкрай важливі події з найвищим пріоритетом тощо. Ми розглядаємо повідомлення безпеки лише як транзакції у блокчейні, тому що вони відіграють важливу роль у забезпеченні надійності зв'язку. Оскільки повідомлення маяка часто передаються у широкомовному режимі, вони несуть накладні витрати, і такі повідомлення маяка підписується та автентифікується.

– Блоки. Блок складається із заголовка блоку та тіла блоку. Заголовок блоку складається з хеша

попереднього блоку, одноразового номера, мітки часу та кореня Меркла. Тіло блоку складається зі списку повідомлень про події безпеки, які поводяться як транзакції у тілі блоку.

– Сертифікат місцезнаходження, заснований на методі визначення місцезнаходження (Proof of Location, PoL) [9] та використовується для підтвердження розташування Fog-терміналів в локальному кластері. Кожен Fog-термінал вимагає, щоб алгоритм PoL упевнився, що Fog-термінал знаходиться поряд з активним Fog-терміналом. Крім того, дані алгоритму PoL використовується як підтвердження місцезнаходження в повідомленні про подію для блокчейна. БС виступає як валідатор для надання сертифіката місцезнаходження Fog-терміналам в межах зони локального кластера. При цьому всі Fog-термінали та БС мають свої власні пари відкритих та закритих ключів. Запитуючий Fog-термінал відправляє ініціююче повідомлення зі своїм відкритим ключем в БС, а потім БС відправляє випадковий ідентифікатор сеансу Fog-терміналу. БС перевіряє справжність підпису з відкритим ключем Fog-терміналу і перевіряє час для обміну ідентифікатором сеансу. Якщо різниця в часі між відправкою та отриманням ідентифікатора сеансу менше кількох мілісекунд, БС публікує сертифікат розташування, який включає місце місцезнаходження, час і відкритий ключ Fog-терміналу, який підписаний закритим ключем БС. Дані системи GPS не можна використовувати, тому що їх легко підробити. Алгоритм PoL є безпечним, оскільки Fog-термінали не можуть створити підроблений сертифікат місцезнаходження без дійсного підпису БС. Однак використання тільки даних алгоритму PoL не гарантує достовірності повідомлень, тому нам потрібен механізм блокчейну, щоб зробити повідомлення більш надійним.

Сертифікат на використання послуги мікросервісу для забезпечення подолання ефектів блокування передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль, який формується заздалегідь блокчейному і передається абоненту після завершення процедур оформлення запиту на встановлення сеансу зв'язку.

Запропонована структура блокчейна для безпечного розповсюдження повідомлень працює наступним чином.

Всі Fog-термінали локального кластера в мережі завантажують та оновлюють блокчейн. Інфраструктура блокчейн діє як розподілена загальнодоступна книга, в якій зберігається повна історія рівнів довіри Fog-терміналів у блокчейні разом із повідомленнями про події. Fog-термінали, що стикається з «критичною» подією, такою як блокування передачі, будуть передавати повідомлення про подію з кількома параметрами сусіднім Fog-терміналам локального кластера мережі блокчейна. Ці термінали функціонують в режимі моніторингу робочого стану лінії зв'язку абонента, який знаходиться в режимі ведення зв’язку. Коли інші Fog-термінали отримують нове повідомлення про подію, вони спочатку його перевіряють на предмет відповідності зазначеної області знаходження. Потім сусідні Fog-термінали перевіряють інші параметри повідомлення про подію. Кожен Fog-термінал незалежно перевіряє кожне повідомлення про подію, перш ніж поширювати її далі, щоб запобігти розсилці спаму, відмову в обслуговуванні та інші неприємні атаки на систему.

Щоразу, коли відбуваються події, прилеглі Fog-термінали транслюватимуть повідомлення про подію. Сусідні Fog-термінали будуть збирати інформацію від транслюючих Fog-терміналів. Повідомлення про подію містить всю пов'язану інформацію, таку як тип події, псевдоідентифікатор, ідентифікатор події, рівень довіри, величина потужності сигналу захоплення в довільній точці радіуса дії локального кластера, позначку часу, дані алгоритму PoL тощо. Fog-термінали, які отримують повідомлення про подію, спочатку перевіряють рівень довіри Fog-терміналу – відправника у блокчейні, а потім перевіряють повідомлення про подію. Вони перевіряють кожне повідомлення про подію на основі доказів, що стосуються рівня довіри відправляючого Fog-терміналу, місця розташування події, ідентифікатора події, дані алгоритму PoL, позначки часу і т. д., і зберігають повідомлення в локальному пулі пам'яті, якщо повідомлення вважається заслуговує на довіру. В іншому випадку, повідомлення відкидається. Повідомлення про подію транслюється в локальній мережі блокчейну, і кожен Fog-термінал у мережі підтверджує повідомлення про подію. Fog-пристрої для майнінгу збирають різні повідомлення про події з пула непідтверджених повідомлень про події та перевіряють правильність параметрів прийнятих повідомлень. Пристрій майнінгу використовує політики перевірки повідомлень, щоб дізнатися достовірність повідомлення. Якщо отримане повідомлення про подію є дійсним і заслуговує на довіру на основі політики перевірки, то її рівень довіри буде оновлений. Рівень довіри окреслюється як частка справжніх повідомлень про події m, відправлених Fog-терміналом, до загальної кількості повідо-

млень про події m+n, де n – кількість хибних повідомлень про події. Рівень довіри змінюється згодом, залежно від дійсних чи хибних повідомлень. Рівень довіри до Fog-терміналу збільшується зі збільшенням кількості правдивих повідомлень. Пристрої для майнінгу обчислять оновлений рівень довіри пристрою-відправника і відправлять цей рівень довіри до блокчейну після додавання нового блоку до локального ланцюжка наступним.

Пристрій-майнер на основі рішення задачі візантійських генералів виконає умови механізму консенсуса Practical Byzantine Fault Tolerance (PBFT), коли вирішить головоломку складності, знаходячи значення одноразового номера. Знайшовши одноразовий номер, його транслює мережі блокчейн. Інші Fog-термінали отримують новий блок і відповідно до політик перевірки самостійно перевіряють правильність повідомлення про подію. Це гарантує, що у мережі транслюються лише законні блоки. Незалежна перевірка також гарантує, що пристрої для майнінгу, які поводяться чесно, інтегрують свої блоки в блокчейн і таким чином отримують винагороду. Fog-пристрої для майнінгу, які поводяться нечесно, отримують відмову у своїх блоках. В результаті вони не тільки втрачають винагороду, а й витрачають марну енергію, що використовується для обчислення рішення механізму консенсуса PBFT. Якщо інформація про новий блок вірна, то Fog-пристрої для майнінгу приймають її і починають видобувати нові блоки поверх неї. Існування повідомлення про подію в блокчейні є свого роду підтвердженням того, що повідомлення про подію заслуговує на довіру.

Застосування у розробленій інфраструктурі граничних обчислень для блокчейну можуть скоротити затримку генерації блоків за рахунок розвантаження потужного механізму консенсуса PBFT на прикордонні сервери для майнінгу блоків Fog-майнерами. Крім того, затримку розповсюдження блоків можна зменшити за допомогою граничних хмарних обчислень. Mobile Edge Computing (MEC) може надавати граничні хмарні послуги на периферії для вузлів локального кластера Fog-терміналів та переносити ресурсомістку роботу з термінальних вузлів на прикордонні сервери. MEC можна використовувати для розповсюдження блокових повідомлень між вузлами майнера, що може зменшити затримку розповсюдження. На додаток до цього термінальні вузли розвантажують процес майнінгу на сервери MEC, щоб прискорити процес майнінгу. Оскільки ми маємо справу з повідомленнями про надзвичайні ситуації, своєчасність розповсюдження повідомлень має першочергове значення. Прикордонні обчислення можна використовувати для швидшого майнінгу блоків у пропонованій нами інфраструктурі блокчейну.

Загальний алгоритм адаптивного функціонування абонента при блокуванні прямої видимості в гетерогенній мобільній мережі терагерцового діапазону здійснюють наступним чином.

Крок 1. Абонент спочатку встановлює з'єднання з довільною базовою станцією, і надсилає власні вимоги.

Крок 2. Базова станція надсилає запит сервісу абонента разом з його публічним ключем у блокчейн для перевірки смарт-контрактом.

Крок 3. Якщо інформація про абонента підтверджена у розподіленому реєстрі, смарт-контракт визначає локальний кластер Fog-пристроїв на базі алгоритма K-середніх для визначення центру скупчення користувачів, а також бджолиного алгоритму для визначення пристрою туману, який виконує необхідні вимоги до міграції на нього відповідного мікросервісу для забезпечення подолання ефектів блокування передачі в мобільних системах.

Крок 4. Базова станція направляє абоненту сертифікат на використання послуги мікросервісу для забезпечення подолання ефектів блокування передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль, який формується заздалегідь блокчейном і передається абоненту після завершення процедур оформлення запиту на встановлення сеансу зв'язку.

Крок 5. Абонент надсилає запит на реєстрацію у мережі обраного оператора вибраного кластера Fog-пристроїв.

Крок 6. Оператор підтверджують реєстрацію абонента в мережах обраного оператором вибраного кластера Fog-пристроїв.

Крок 7. Процедура установлення адресного з'єднання оператором і переведення Fog-пристроїв вибраного кластера у режим моніторингу робочого стану зв'язку лінії абонента, який знаходиться в режимі ведення зв'язку.

Крок 8. Fog-пристрої вибраного кластера оновлюють реєстр угоди про рівень обслуговування (SLA) в мережі блокчейн для запуску процесу тарифікації зв'язку для абонента.

Крок 9. Процес перевибору Fog-пристроїв у локальному кластері базової станції при блокуванні передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль.

Fog-термінали, які отримують повідомлення про подію, спочатку перевіряють рівень довіри Fog-терміналу – відправника у блокчейні, а потім перевіряють повідомлення про подію. Вони перевіряють кожне повідомлення про подію на основі доказів, що стосуються рівня довіри відправляючого Fog-терміналу, розташування події, ідентифікатора події, дані алгоритму PoL, позначки часу і т. д., і зберігають повідомлення в локальному пулі пам'яті, якщо повідомлення вважається заслуговує на довіру. В іншому випадку, повідомлення відкидається. Повідомлення про подію транслюється в локальній мережі блокчейну, і кожен Fog-термінал у мережі підтверджує повідомлення про подію.

Крок 10. Запускається механізм виконання процедур смарт-контракту сертифікату на використання послуги мікросервісу для забезпечення подолання ефектів блокування передачі в мобільних системах.

Висновки. Запропоновано удосконалений тип блокчейн, який можна використовувати для ефективної перевірки надійності вузлів та повідомлень про події мікросервісу для забезпечення подолання ефектів блокування передачі в мобільних системах при застосуванні терагерцового діапазону довжин хвиль. Наведено загальний алгоритм адаптивного функціонування абонента при блокуванні передачі прямої видимості при застосуванні терагерцового діапазону довжин хвиль.

Список літератури:

1. Сайко В.Г., Наритник Т.М. Модель підвищення показників якості обслуговування гетерогенної мережної інфраструктури терагерцового діапазону. *Вчені записки Таврійського національного університету імені В.І. Вернадського: серія технічні науки.* 2023. Т. 34(73). № 1.

2. Saiko Volodymyr, Narytnyk Teodor. High-reliability 5G / IoT mobile communication method when using the terahertz wavelength range. *Theoretical and scientific foundations in research in Engineering:* collective monograph / Saiko V., Narytnyk T. – etc. – International Science Group. – Boston : Primedia eLaunch, 2022. pp..477-497. Available at : DOI – 10.46299/ISG.2022.MONO.TECH.1 URL: https://isg-konf.com/theoretical-and-scientific-foundations-in-research-in-engineering/

3. A. Lei, C. Ogah, E. Al. A Secure Key Management Scheme for Heterogeneous Secure Vehicular Communication Systems. *ZTE Communication Magazine.* 2016. vol. 111.

4. B. Leiding, P. Memarmoshrefi, D. Hogrefe Self-managed and blockchain-based vehicular ad-hoc networks *Proc. 2016 ACM Int. Jt. Conf. Pervasive Ubiquitous Comput. Adjun*. – UbiComp, 2016. vol. 16 , p. 137140 January

5. A. Dorri, M. Steger, S. Kanhere, R. Jurdak. BlockChain: a distributed solution to automotive security and privacy. *IEEE Commun. Mag. Mag.,* 2017. vol. 55 (12), Article 119125

6. Табернакулов, А. Блокчейн на практике. Москва: Альпина Паблишер, 2019. 260 с.

7. Igor M. Coelho; Vitor N. Coelho; Rodolfo P. Araujo; Wang Yong Qiang; Brett D. Rhodes. (2020). Challenges of PBFT-Inspired Consensus for Blockchain and Enhancements over Neo dBFT. *Future Internet*. 2020. vol. 12 (8).

8. Бардин, А.П. Обработка ошибочных ситуаций в больших блокчейн – сетях алгоритмом достижения консенсуса, основанном на решении задачи византийских генералов. *Вестник МГТУ имени М.Э.Баумана*. 2021. № 4. С. 28-37.

9. Фокин Г.А. Технологии сетевого позиционирования 5G. М.: Горячая линия – Телеком, 2021. 456 с.

Saiko V.G., Narytnyk T.M. APPLICATION OF BLOCKCHAIN SYSTEM FOR SECURE MESSAGING IN GETEROGENNIC MOBILE NETWORKS OF TERAHERTZ RANGE

Recommendations are made on the implementation of blockchain solution in one of the promising services of the new generation networks, such as the provision of mitigation of the effects of blocking of transmission in mobile systems at the application of terahertz range of wavelengths. The presented solution allows to increase confidentiality and reliability of the transmitted data, to provide new opportunities for decision making and to reduce delays and increase energy efficiency. An innovative type of blockchain is offered, which can be used for effective verification of reliability of nodes and messages about events of microservice providing mitigation of effects of blocking of transmission in mobile systems at application of terahertz range of wavelengths. Its main features are: a new block infrastructure for storing node and message authenticity in a 5G mobile network. In this structure, the host's authenticity and the messages that act as transactions similar to blockchain Bitcoin. However, we deal with reporting events as transactions, not cryptocurrencies. To reduce the delay at generation of blocks, the boundary calculation in blockchain is applied. Border calculations will reduce delays by transferring complex calculations to border devices. On the basis of the new blockchain structure the general algorithm of adaptive functioning of the subscriber at blocking of the transmission of direct visibility in the heterogeneous mobile network of terahertz range has been developed. Application of the proposed solution in the decentralized network of mobile communications 5G, the basis of which is the infrastructure of blockchain, potentially reduces the complexity of the network, significantly reduces the operator's operating expenses and accordingly increases the reliability and efficiency of the mechanism of adaptive provision of the subscriber with real mode in blocking the transmission of direct visibility.

Key words: *blockchain, mobile communication, terahertz range, transmission blocking.*